TARIF 1971

PERIODIQUES SCIENTIFIQUES

ABONNEMENTS ET ANNEES ANTERIEURES

Tous nos abonnements sont payables d'avance et partent de janvier

Titre et périodicité des revues	Tarif France	Etranger F.F.	
Annales d'Histochimie (4 N^{os})	90	110	
Annales de l'Ecole Normale Supérieure (4 N^{os})	150	200	
Annales de Physique Biologique et Médicale (4 N^{os})	80	96	
Annales de l'Institut Henri Poincaré (2 séries)	174	195	
Série A (Physique théorique) (2 tomes de 4 N^{os})	116	130	
Série B (Calcul des Probab. et Statistiq.) (1 tome de 4 N^{os}).	58	65	
Bulletin de la Société Mathématique de France (4 N^{os} + 4 suppléments)	150	150	
Bulletin des Sciences Mathématiques (4 N^{os})	120	145	
Comptes rendus de l'Académie des Sciences : Hebdomadaire de 2 tomes par an			
1er **Fascicule.** Séries AB : Sciences Math. et Phys.	470	765	
2^{e} **Fascicule.** Série C : Sciences Chimiques	405	675	
3^{e} **Fascicule.** Série D : Sciences Naturelles	450	755	
Les trois Fascicules	980	1 655	
Journal de Mathématiques pures et appliquées (4 N^{os})	165	185	
Journal de Mécanique (4 N^{os})	110	130	
Mathématiques et Sciences Humaines (4 N^{os})	35	45	
Œcologia Plantarum (4 N^{os})	80	96	
Physiologie Végétale (4 N^{os})	95	110	
Revue d'Ecologie et de Biologie du Sol (4 N^{os})	80	96	
Revue de Chimie Minérale (6 N^{os})	175	200	

BULLETIN D'ABONNEMENT 1971

à retourner aux Editions GAUTHIER-VILLARS — 55, quai des Grands-Augustins, Paris 6^{e}

Veuillez m'inscrire pour un abonnement d'un an à ______________________

Je vous adresse le montant de cette commande soit

France ______________________ Etranger ______________

Par chèque : ☐ bancaire ou ☐ postal (C C.P. Paris 29 323) — Par mandat*

* *Rayer la mention inutile.*

NOM · ______________________ Adresse ______________

ATTENTION !

Cet abonnement peut être pris en charge par le Laboratoire, l'Organisme ou la Société dont vous dépendez. Ceux-ci peuvent imputer la dépense à leur budget "Documentation scientifique". Dans ce cas, c'est bien volontiers que nous ferons parvenir la facture en plusieurs exemplaires.

ACTES
DU
CONGRÈS INTERNATIONAL DES MATHÉMATICIENS
1970

ACTES

DU

CONGRÈS INTERNATIONAL DES MATHÉMATICIENS

1970

publiés sous la direction du
Comité d'Organisation du Congrès

1

Documents - Médailles Fields
Conférences générales (G)
Logique (A) - Algèbre (B)

GAUTHIER-VILLARS ÉDITEUR
55, quai des Grands-Augustins, Paris 6^{e}
1971

PRÉPARATION DU CONGRÈS

Un *Comité consultatif international* de neuf membres, désigné par l'Union mathématique internationale, et présidé par M. Adrian ALBERT, a constitué 33 Commissions spécialisées ; les compositions de ce Comité, de ces Commissions et les recommandations faites par eux au Comité d'organisation, sont confidentielles.

Le Comité national français de mathématiciens a constitué le *Comité d'organisation* dont les membres sont : MM. F. BRUHAT, H. CABANNES, J. CERF, G. CHOQUET, J. DIEUDONNÉ, J.-P. KAHANE, P. LELONG, J. LERAY, président, A. LICHNEROWICZ, J.-L. LIONS, J. NEVEU, L. SCHWARTZ, J.-P. SERRE.

Ce Comité d'organisation a constitué un *Comité local* dont les membres sont : MM. J. DIEUDONNÉ, président, P. KRÉE, E. MÉNAGER et un *Comité financier*, dont les membres sont : MM. P. BELGODÈRE, R. CHÉRADAME, J. DIEUDONNÉ, R. FORTET, P. LELONG, président, Y. MARTIN, E. MÉNAGER, L. MOTCHANE, M. d'OLIER.

Le Congrès a bénéficié de l'aide d'un *Comité de soutien pour la diffusion des travaux du Congrès*, composé comme suit : Président : M. Georges DESBRIÈRE, Vice-Président de Péchiney, Président de l'Association pour le Développement de l'Enseignement et des Recherches auprès des Facultés des Sciences de l'Université de Paris (A.D.E.R.P.).

Membres : MM. BAUMGARTNER, Président de Rhône-Poulenc, CHASSAGNY, Président de l'Union syndicale des industries aéronautiques et spatiales, DELOUVRIER, Président de l'Électricité de France, DONTOT, Président de la Fédération nationale des industries électroniques, FERRY, Président de la Chambre syndicale de la sidérurgie, GALICHON, Président d'Air France, GLASSER, Président du Syndicat général de la Construction électrique, GRANDPIERRE, Président de l'Institut des hautes études scientifiques, HAAS-PICARD, Président de l'Union des Chambres syndicales de l'industrie du pétrole, HOTTINGUER, Président de l'Association professionnelle des Banques, HUVELIN, Président du Conseil National du Patronat Français, LESOURNE, Président de la S. E. M. A. (METRA International), d'ORNHJELM, Président de la Chambre syndicale des Constructeurs d'Automobiles, Ambroise ROUX, Président de la Compagnie générale d'Électricité.

M. Étienne WOLFF, Administrateur du Collège de France, a eu l'obligeance d'y accueillir le Secrétariat du Comité d'organisation.

Ce Secrétariat a été assuré par Mme M. GOYVAERTS.

*
* *

La publication des Actes du Congrès a été assumée par MM. M. BERGER, J. DIEUDONNÉ, J. LERAY, J.-L. LIONS, P. MALLIAVIN, J.-P. SERRE.

Monsieur Georges POMPIDOU,

Président de la République Française,
a accordé son haut patronage au Congrès.

Monsieur Jacques CHABAN-DELMAS,

Premier Ministre,
a accordé son patronage au Congrès.

Le Congrès a bénéficié des dons suivants :

Subvention du Gouvernement de la République Française	328.000 F
Don du Comité de soutien pour la diffusion des travaux du Congrès	162.000 F
Subvention du Conseil général des Alpes-Maritimes.	50.000 F
Prêt gracieux du Palais des Expositions par la Ville de Nice.	
Prêt gracieux et subvention de l'Université . . .	15.000 F
Le total des cotisations des Congressistes fut de .	576.000 F

Les Donateurs qui ont répondu à l'appel du Comité de soutien pour la diffusion des travaux du Congrès sont :

Organisations professionnelles

Association professionnelle des Banques
Chambre syndicale des Constructeurs d'Automobiles
Chambre syndicale de la Sidérurgie française
Comité des Salines de France
Fédération nationale du Bâtiment
Fédération nationale des Travaux Publics
Syndicat général de la Construction électrique
Union des Chambres syndicales de l'Industrie du Pétrole
Union des industries textiles
Conseil national du Patronat français

Entreprises

Air France
L'Air Liquide
Alcatel
Banque française du Commerce extérieur
Banque de France
Banque de l'Indochine
Banque Nationale de Paris
Banque de Paris et des Pays-Bas
Banque de l'Union parisienne C. F. C. B.
Bertin et Cie
Boussois-Souchon-Neuvesel
Chantiers de l'Atlantique
Ciments Lafarge
Compagnie Électro-Mécanique
Compagnie financière de Suez et de l'Union parisienne
Compagnie française de Crédit et de Banque
Compagnie Générale d'Électricité
Compagnie I. B. M. France
Compagnie industrielle des Télécommunications
Compagnie de Saint-Gobain-Pont-à-Mousson
Comptoir des Entrepreneurs
Comptoir Lyon-Alemand

Crédit foncier de France
Crédit industriel et commercial
Crédit Lyonnais
Dunlop
Électricité de France
Engins Matra
Esso-Chimie
Générale sucrière
Gervais-Danone
Groupe des Assurances nationales
Groupe de Paris
Imprimerie Georges Lang
Kodak-Pathé
Laboratoire Central de Télécommunications
La Foncière-Capitalisation
L'Oréal
Penarroya
Péchiney
La Radiotechnique
Régie autonome des Transports parisiens
Rhône-Poulenc
Roussel-Uclaf
SIC-SAFCO (Condensateurs)
Société anonyme de Télécommunications
Société d'Applications générales d'Électricité et de Mécanique (SAGEM)
Société Audax
Société d'Études et de Mathématiques appliquées
Société Générale
Société marseillaise de Crédit
Société nationale des Chemins de fer français
Société nationale d'Étude et de Construction de Moteurs d'Aviation
Solvay et Cie
Sopad
Thomson-C. S. F.
Ugine-Kuhlmann
Caisse des Dépôts et Consignations

Don adressé directement au Congrès

Springer-Verlag

SÉANCE INAUGURALE

Monsieur Olivier GUICHARD, Ministre de l'Éducation nationale, déclare ouvert le Congrès international des mathématiciens de Nice, le mardi 1[er] septembre 1970, à 9 h 30.

Il donne la parole à Monsieur Henri CARTAN, Président de l'Union mathématique internationale, qui propose aux Congressistes d'élire Président du Congrès Monsieur Jean LERAY, Président du Comité d'organisation ; cette élection a lieu ainsi que celle d'un Président d'honneur, Monsieur Paul MONTEL.

Monsieur Paul MONTEL et Monsieur Jean LERAY accueillent les Congressistes et remercient les personnalités qui ont collaboré à l'organisation du Congrès.

Monsieur Jacques MÉDECIN, Député-Maire, souhaite la bienvenue aux Congressistes dans le Palais des expositions de la Ville de Nice.

Monsieur Henri CARTAN fait le rapport suivant :

C'est au Professeur J.-C. FIELDS *que revient l'initiative d'une fondation qui permettrait, à l'occasion de chaque Congrès International des Mathématiciens, d'honorer par deux médailles d'or des travaux mathématiques d'un intérêt exceptionnel. Sa proposition fut acceptée, après sa mort, par le Congrès International de Zürich en 1932. Les fonds nécessaires provenaient d'un excédent de recettes du Congrès International de 1924, tenu à Toronto (Canada), sous la présidence du* Professeur FIELDS. *Les deux premières médailles Fields furent attribuées en 1936 au Congrès d'Oslo ; puis, après une longue interruption due à la guerre, deux médailles furent décernées lors de chacun des Congrès Internationaux des Mathématiciens : à Harvard en 1950, à Amsterdam en 1954, à Edinburgh en 1958, à Stockholm en 1962. Au Congrès de Moscou, en 1966, quatre médailles Fields furent attribuées. Chaque médaille est accompagnée d'un chèque de 1.500 dollars canadiens ; le nom de Fields ne figure pas sur la médaille.*

Se conformant à une procédure maintenant bien établie, le Comité Exécutif de l'Union Mathématique Internationale a nommé, il y a quelque temps, un Comité International de huit membres, chargé de choisir les lauréats pour le présent Congrès. Ce Comité Fields 1970 se composait des Professeurs J. L. DOOB, F. HIRZEBRUCH, L. HÖRMANDER, S. IYANAGA, J.-W. MILNOR, I. R. SHAFAREVITCH, P. TURÁN, *et moi-même comme président. J'ai hautement apprécié la collaboration de chacun de mes collègues, et je suis heureux de leur exprimer mes chaleureux remerciements. Je suis aussi reconnaissant aux mathématiciens qui, consultés en privé, ont préparé des rapports qui ont grandement aidé notre Comité dans sa tâche.*

Le Comité a décidé, non sans quelque hésitation, de se conformer à la tradition qui veut que seuls soient pris en considération les titres de mathématiciens âgés de moins de quarante ans. Les candidats proposés par les différents membres du Comité composaient initialement une liste d'une vingtaine de noms. Après une discussion au cours de laquelle, conformément au vœu du Professeur FIELDS, *nous n'avons pris en considération que le point de vue scientifique en laissant de côté toute question de nationalité, nous sommes progressivement arrivés à établir une liste de quatre noms. Ce fut un choix* *difficile ; nous sommes parfaitement conscients que d'autres mathématiciens très brillants auraient aussi pu être choisis pour une médaille Fields ; nous savons également que d'autres, plus jeunes encore, et dont les titres n'ont même pas été discutés cette fois-ci, pourront avoir des chances sérieuses dans quatre ans. Quoi qu'il en soit, nous sommes convaincus que ceux que nous avons finalement choisis sont des mathématiciens d'un mérite exceptionnel, et que chacun d'eux a contribué à donner un nouveau visage à une branche importante des mathématiques. Ce sont, dans l'ordre alphabétique :*

Alan BAKER,
Heisuke HIRONAKA,
Sergei NOVIKOV,
John G. THOMPSON.

Malheureusement, Sergei NOVIKOV *a été dans l'impossibilité de venir à ce Congrès. Je prie* Messieurs BAKER, HIRONAKA et THOMPSON *de venir recevoir leur médaille des mains de Monsieur le Ministre de l'Éducation nationale,* M. Olivier GUICHARD.

Monsieur Olivier GUICHARD, Ministre de l'Éducation nationale, remet les médailles Fields aux quatre lauréats, qu'il félicite.

Il prononce un discours, qui décrit l'essor mathématique actuel et la gravité des problèmes d'enseignement et d'éducation en résultant. Ce discours est publié et analysé le jour-même par la presse.

Monsieur Jean LERAY rappelle le fonctionnement du Congrès :

— chaque matin, deux conférences générales consécutives, d'une heure, s'adressent à tous les Congressistes ;

— chaque après-midi, un choix d'exposés spécialisés, de cinquante minutes, chacun des Congressistes ayant la possibilité d'en écouter trois ;

— chaque Congressiste a reçu, imprimées, les 265 Communications individuelles ; elles ne peuvent pas être exposées oralement ;

— des groupes de Congressistes peuvent obtenir des salles pour des réunions mathématiques non prévues au programme officiel.

Les travaux des quatre nouveaux titulaires de médailles Fields sont alors exposés par les rapports ci-après (p. 1-16).

SÉANCE DE CLÔTURE

Monsieur Jean DIEUDONNÉ, au nom du Comité d'organisation, déclare notamment :

The Acts of the Congress will be printed as soon as possible, and distributed to every mathematician regularly registered at the Congress. The cost of the printing will be borne partly by the fees of the participants, partly by a subsidy from the French government, and partly by a subsidy granted by the « Comité de soutien pour la diffusion des travaux du Congrès » sponsored by associations of french companies and chaired by Mr. G. DESBRIÈRE, *Vice-Chairman of Péchiney.*

Puis il pose la question suivante, en français et en anglais :

As you know, this Congress is the first one in which there are no 10 minutes talks, although printed communications have been accepted. The decision to allow only 50 minutes lectures given by invitation was taken unanimously by the international advisory Committee and the organizing Committee. Of course the corresponding Committees for the 1974 Congress are not bound by this decision and may adopt a different policy. But the Organizing Committee thinks that it might be useful to the organizers of the 1974 Congress to have the opinion of this Congress regarding the new organization of the lectures. I will therefore ask those who are in favor of the continuation of the policy adopted in the 1970 Congress, namely to have only 1 hour and 50 minutes invited talks, plus written communications, but no 10 minutes talks, to raise their hands.

Against this continuation, and for a return to the previous tradition?

Abstentions?

Le résultat de ce sondage d'opinion est le suivant : *deux fois plus de voix pour la suppression des Communications individuelles orales* que pour leur rétablissement ; pas d'abstention.

Monsieur M. F. ATIYAH, au nom du Comité exécutif de l'Union Mathématique Internationale, remercie tous ceux qui ont subventionné et organisé le Congrès.

Monsieur Henri CARTAN fait la communication suivante :

Comme Président sortant de l'Union Mathématique Internationale, j'ai l'agréable devoir d'annoncer que la Sixième Assemblée Générale de l'Union, tenue à Menton les 28 et 29 août 1970, a élu pour une période de quatre ans, commençant le 1er janvier 1971, le nouveau Comité Exécutif que voici :

Président	Professeur K. CHANDRASEKHARAN,
Vice-Présidents	Dean Adrian A. ALBERT, Académicien M. PONTRYAGIN,

Secrétaire		Professeur Otto FROSTMAN,
Membres	{	Professeur M. F. ATIYAH, Professeur Y. KAWADA, Professeur N. H. KUIPER, Académicien M. NICOLESCU, Professeur G. VESENTINI.

Vous voudrez certainement, comme moi-même, souhaiter au nouveau Comité Exécutif un plein succès dans les tâches qui l'attendent. L'Union Mathématique Internationale s'efforcera, comme par le passé, j'en suis sûr, de prendre toutes les initiatives pouvant favoriser la coopération active et amicale entre les mathématiciens du monde entier, ou contribuer au développement des mathématiques dans les pays moins favorisés.

Je me réjouis que ce Congrès ait permis de réunir à Nice de nombreuses délégations de presque tous les pays où l'on cultive les mathématiques. La participation de certains d'entre eux aurait été souhaitée plus complète encore ; j'exprime le vœu qu'elle le soit lors du prochain Congrès de 1974.

Au nom du Comité qui a été désigné pour étudier le lieu du Congrès de 1974, je prie le Président LERAY *de bien vouloir donner la parole au* Professeur H. A. HEILBRONN, *qui va parler au nom de la Société Mathématique du Canada.*

Monsieur H. A. HEILBRONN, au nom de la Société Mathématique du Canada et au nom de l'Université de la Colombie Britannique, offre au Congrès International des Mathématiciens de se réunir en 1974 à Vancouver (Canada).

Cette offre est chaleureusement acceptée par le Congrès, dont le Président remercie Monsieur H. A. HEILBRONN et l'Université de la Colombie Britannique.

Aucun Congressiste ne demandant la parole, le Président remercie tous ceux qui ont apporté leur patronage et qui ont généreusement contribué à la diffusion des travaux du Congrès, notamment Monsieur le Président de la République, Monsieur le Premier Ministre, Monsieur le Ministre de l'Éducation nationale et le Comité de soutien pour la diffusion des travaux du Congrès. Il adresse ses remerciements à tous les Congressistes et spécialement aux Conférenciers. Il déclare le Congrès International des Mathématiciens de 1970 clos, le jeudi 10 septembre, à 15 h 30.

LISTE DES CONGRESSISTES

Les noms des *Membres de Délégations* sont en italique.
(G) désigne les Auteurs d'une conférence générale (T. I. de ces Actes),
(A), ..., (F2) désigne les Auteurs d'un exposé publié dans la Section (A), ..., (F2) de ces Actes,
* désigne les auteurs de l'une des

« 265 Communications Individuelles, Congrès International des Mathématiciens, Nice, 1970, Gauthier-Villars, éditeur ».

A

AARNES Johan F. (Norvège)
ABELLANAS Pedro (Espagne)
ABHYANKAR S. (U. S. A.)
ABRAHAM Samuel (Israël)
ABUBAKAR Iya (Nigéria)
ACKERMANS Stan T. (Pays-Bas)
ACKLER Lynn (U. S. A.)
ACZÉL Janos (Canada)
ADAMS Frank (Grande-Bretagne) *
ADAMSON Iain Th. (Grande-Bretagne)
ADJAN S. I. (U. R. S. S.) (B1)
ADOMIAN G. (U. S. A.)
AGINS B. R. (U. S. A.)
AGMON Shmuel (Israël) (D10)
AGOSTINELLI Cataldo (Italie)
AGOSTON Max (U. S. A.)
AHLUWALIA Daljit (U. S. A.)
AHMAD Salah (Syrie)
AIGNER Alexander (Autriche)
AIRAULT Hélène (France)
AKBAR-ZADEH Hassan (France)
AKIZUKI Yasuo (Japon)
AKKAR Marie-Thérèse (France)
AKKAR Mohamed (France)
AKUTOWICZ Edwin J. (France)
ALAS Ofelia (Brésil)
ALBASINY Ernest L. (Grande-Bretagne)
AL-BASSAM Mohammed (Irak)
ALBERT Adrian (U. S. A.)
ALBRECHT Ernst (All. de l'Ouest)
ALBRIGHT Hugh (U. S. A.)
ALDER Henry (U. S. A.)
ALDERSON POPOVA Helen (Grande-Bretagne)
AL DHAHIR Nawar (Grande-Bretagne)
ALEKSANDRIAN R. A. (U. R. S. S.)
ALEXEYEV V. M. (U. R. S. S.) (D12)
ALIC' Mladen (Yougoslavie)
ALJANČIČ Slobodan (Yougoslavie)
ALLEN Rory J. (Grande-Bretagne)
ALLING Norman (U. S. A.)
ALMGREN Frederick (U. S. A.) (D11)
ALPERIN Jonathan (U. S. A.)
ALTERMAN Zipora S. (Israël) *
ALTMAN Allen (U. S. A.)
AMANN Herbert (All. de l'Ouest)
AMARA Mohamed (Tunisie)
AMATO Francesco
AMATO Vittoria
AMAYO Ralph (Grande-Bretagne)
AMBROSE Thomas (Irlande)
AMICE Yvette (France)
AMIR Dan (Israël)
AMIR-MOÉZ Ali (U. S. A.) *
AMITSUR Shimshon (U. S. A.) (B1)
AMMANN André (Suisse)
ANANDAM Victor (France)
ANCOCHEA German (Espagne)
ANCONA Vincenzo
ANDERSEN Erik (Danemark)
ANDERSON Donald W. (U. S. A.) (C1)
ANDERSON Karl (Suède)
ANDERSON Richard D. (U. S. A.) (C1)
ANDERSON Robert V. (U. S. A.)
ANDRÉ Bernard (France)
ANDRÉ Michel (Suisse) (B2)
ANDREIAN CAZACU Cabiria (Roumanie) *
ANDREOTTI Aldo (Italie) (D8)
ANDREW Merle (U. S. A.)
ANDRIANOV A. N. (U. R. S. S.) (C5)
ANDRUNAKIEVITSH V. A. (U. R. S. S.)
ANDRUSHKIW Joseph (U. S. A.) *
ANTCHEV-ATANASOV Atanas (Bulgarie)
ANTIBI André (France)
ANTILLE André (Suisse)
ANVARI Morteza (Iran) *
APERY Roger (France)
APPLEBY Peter G. (Grande-Bretagne)
AQUARO Giovanni (Italie)
ARAKELIAN N. U. (U. R. S. S.) (D7)
ARAKI Fujihiro (Japon) (D2)
ARAKI Shoro (Japon)
ARATÓ Mátyas (Hongrie)
ARBAULT Jean (France)
ARCHINARD Gabriel (France)
ARHANGELSKIJ A. (U. R. S. S.) (C1)
ARIS Henri (France)
ARKOWITZ Martin (U. S. A.)
ARLT Dietmar (All. de l'Ouest)
ARMBRUST H. K.
ARMENTROUT Steve (U. S. A.)
AROCA HERNANDEZ José M. (Espagne)
AROIAN Leo A. (U. S. A.)
ARONSSON D. G. (Suède)
ARREGUI FERNANDEZ Joaquin (Espagne)
ARTIN Michael (U. S. A.) (B5)
ARTZNER Philippe (France)

ARVESON William B. (U. S. A.)
ASCHER Marcia (U. S. A.)
ASH Marshall (U. S. A.)
ASTESIANO Egidio (Italie)
ATIYAH Michael (U. S. A.) (C4)
ATTEIA Marc (France)
AUBERT Karl E. (U. S. A.)
AUBIN Thierry (France)
AUBINEAU Jean P.
AUCHMUTY Giles (U. S. A.)
AUGE Juan (Espagne)
AULT John C. (Grande-Bretagne)
AUPETIT Bernard (Canada)
AURORA Silvio (France)
AUSFELD Christoph (Suisse)
AVANISSIAN Vazgain (France)
AX James (U. S. A.) (B6)
AXELSSON Owe (Suède)
AYEL Marc (France)
AYKAN Faruk (Turquie)
AYOUB Raymond (U. S. A.)
AZRA Jean-P. (France)

B

BA Boubakar (France)
BAAS Nils (Danemark)
BABENKO K. I. (U. R. S. S.)
BACHMAKOV M.
BACOPOULOS Alex (Grèce)
BADE William (U. S. A.)
BADJJ Cherif (France)
BAGGETT Lawrence (U. S. A.)
BAHLOUL (France)
BAHVALOV N. S. (U. R. S. S.) (E8)
BAILEY G. H. (Grande-Bretagne)
BAILLETTE Aimée (France)
BAILLOT Geneviève (France)
BAIOCCHI C. (Italie)
BAJPAI A. C. (Grande-Bretagne)
BAKER Alan (Grande-Bretagne) (G)
BAKER Irvine (Grande-Bretagne)
BAKER John A. (Canada)
BAKTAVATSALOU (Côte-d'Ivoire)
BALABAN T. (Pologne)
BALAKRISHNAN A. V. (U. S. A.) (E4)
BALÁZS János (Hongrie)
BALCERZYK Stanislaw (Pologne)
BALCONI Giorgio (Italie)
BALLET Bernard
BALLIEU Robert F. (Belgique)
BALSLEV Erik (U. S. A.)
BANCHOFF Thomas (U. S. A.)
BANG Thoger (Danemark)
BANTEGNIE Robert (France)
BAOUENDI Mohamed (Tunisie)
BARBANCE Christiane (France)
BARBIERI Francesco (Italie)

BARCILLON Victor (U. S. A.)
BARDOS Claude (France)
BAREISS Erwin (U. S. A.) *
BARKER Charles (Grande-Bretagne)
BARLOTTI Adriano (Italie)
BARLOW Richard (U. S. A.)*
BARNARD Anthony (Grande-Bretagne)
BARNEV Petar (Bulgarie)
BARR Michael (Canada) (B2)
DE BARRA Gearoid (Grande-Bretagne)
BARRETT John (Grande-Bretagne)
DE BARROS Constantino (Brésil) *
BARRUCAND Pierre (France)
BARSKY Daniel (France)
BARTH Karl (U. S. A.)
BARTH Theodore (U. S. A.)
BARTLETT Maurice S. (Grande-Bretagne) *
BARWISE Jon (U. S. A.)
BASKIOTIS Chrysostome (France)
BASS Hyman (U. S. A.)
BASS Jean (France)
BASSOTTI-RIZZA Lucilla (Italie)
BATEMAN Paul Tr. (U. S. A.)
BATHO Edward (U. S. A.)
BAUER Gunther (All. de l'Ouest)
BAUM Leonard (U. S. A.)
BAUR Walter (Suisse)
BAUSCH Helmut (All. de l'Est)
BAUSSET Max (France)
BAXENDALE Peter (Grande-Bretagne)
BAZLEY Norman (Suisse)
BEALS Richard (U. S. A.)
BEARDON Alan F. (Grande-Bretagne)
BECKENBACH E. F. (U. S. A.)
BECKER Ronald (Le Cap)
BECKMANN Martin (All. de l'Ouest)
BEETHAM Michael (Grande-Bretagne)
BEGUERI Lucile (France)
BEHBOODIAN Javad (Iran)
BEHNKE Heinrich (All. de l'Ouest)
BEHNCKE Horst (All. de l'Ouest)
BEHR Helmut (All. de l'Ouest)
BEITER Marion (France)
BELAGE Abel (France)
BELLAICHE André (France)
BENABOU J. (France)
BENEDICTY Mario (U. S. A.)
BENENTI Sergio (Italie)
BENES Vaclav (U. S. A.)
BENGEL Gunter (All. de l'Ouest)
BENIAMINO J.-Claude (France)
BENNETT Mary (U. S. A.)
BENOS Anastase (France)

BENZAGHOU Benali (Algérie) *
BERAN Ladislav (Tchécoslovaquie)
BERARD BERGERY Lionel (France)
BERG Christian (Danemark)
BERGAU Peter (All. de l'Ouest)
BERGER Marcel (France)
BERGER Neil Ev. (U. S. A.)
BERGLUND-FINDLEY John (Grande-Bretagne)
BERGMAN Stefan (U. S. A.)
BERGSTROM Harald (Suède)
BERLEKAMP E. (U. S. A.)
BERMAN Joël (U. S. A.)
BERNARD Alain
BERNARD Daniel (France)
BERNARDI Marco (Italie)
BERNARDI Marco (Italie)
BERNAT Pierre (France)
BERNEZ Madeleine Jeanne (Maroc)
BERRICK Jon (Grande-Bretagne)
BERRIEN MOORE 3 Berrien (U. S. A.)
BERROIR André (France)
BERTHELOT Pierre R. (France)
BERTHIAUME Gilles (Grande-Bretagne)
BERTIN Émile M. (Pays-Bas)
BERTIN Jean (France)
BERTIN Marie-José (France)
BERTOLINI Fernando (Italie)
BERTOLINO Milorad (Yougoslavie) *
BERTRANDIAS Jean-Paul (France)
BESCHLER Edwin (U. S. A.)
BESOV O. V. (U. R. S. S.) (D4)
BESUDEN Heinrich (All. de l'Ouest)
BEYER William (U. S. A.) *
BEZUSZKA Stanley (U. S. A.)
BEZZI Franco (Italie)
BHATNAGAR P. L. (Indes)
BIALYNICKI Andrzej (Pologne)
BICHOT Jacques
BIEBINGEN
BIERLEIN Dietrich (All. de l'Ouest)
BIERSTEDT Klaus (All. de l'Ouest)
BILINSKI Stanko (Yougoslavie)
BILLIGHEIMER Claude E. (Canada) *
BILLOTTI Joseph (U. S. A.)
BING R. H. (U. S. A.)
BINGEN Franz (Belgique)
BINGHAM Nicholas (Grande-Bretagne)
BIRCH Bryan (Grande-Bretagne)
BIRKELAND Bent (Norvège)
BIRMAN Joan (France)
BIROLI Marco (Italie)
BITSADZE A. V. (U. R. S. S.) (D10)
BJORCK Coran (Suède)

BKOUCHE Rudolphe (France)
BLACKSTOCK May C. (U. S. A.)
BLAIR David (U. S. A.)
BLANC Brice (France)
BLANCHARD André (France)
BLANCHARD Philippe (Suisse)
BLANCHETON Éliane (France)
BLANTON John D. (U. S. A.)
BLANUŠA Danilo (Yougoslavie)
BLATTER Christian (Suisse)
BLATTNER Robert (U. S. A.)
BLICKENDOERFER Arndt (All. de l'Ouest)
BLOCK Richard (U. S. A.)
BLONDEL J.-Marie (France)
BLOOM Thomas (Canada)
BLUM Lenore (U. S. A.)
BLUMAN George (Canada)
BLYTH Thomas S. (Grande-Bretagne)
BOCHNAK J. (France)
BODEKER Werner (All. de l'Ouest)
BODFISH Edward (U. S. A.)
BODIOU Georges (France)
DE BOER Jan (Pays-Bas)
BOGDAN M. Baishanski (U. S. A.)
BOHNKE Georges (France)
BOHUN-CHUDYNIV Boris (U. S. A.)
BOHUN-CHUDYNIV Volodymyr (U. S. A.)
BOJOROFF (Bulgarie)
BOLDER Harm (Pays-Bas)
BOLLE Erik (Pays-Bas)
BOLSHEV L. N. (U. R. S. S.) (E6)
BOMAN Jan (Suède)
BONDESEN Aage (Danemark)
BONDY Adrian (Canada)
BONGAARTS Peter (Pays-Bas)
BONIC Robert (U. S. A.)
BONNAN Raymond (Grande-Bretagne)
BONNARD Michel (France)
BONNET Robert (France)
BONY J.-M. (France) (D10)
BONZINI Celestina (Italie)
BOONE William (U. S. A.)
BOOTHBY Ruth R. (U. S. A.)
BOOTHBY William M. (U. S. A.)
BORCHERS Hans-Juergen (All. de l'Ouest)
BOREL Armand (U. S. A.)
BORGHI Osvaldo (Argentine)
BORJA Manuel (Suisse)
BOROVKOV A. A. (U. R. S. S.)
BOROWCZYK Jacques (France)
BOROZDIN K. V. (U. R. S. S.)
BÖRSCH-SUPAN Wolfgang (All. de l'Ouest)
BORSUK Karol (Pologne)
BOS Werner (All. de l'Ouest)
BOSÁK Juraj (Tchécoslovaquie)
BOSE Raj. C. (U. S. A.)
BOSSARD Yvon (France)
BOTT Raoul (U. S. A.) (G)
BOUCHE Liane (France)
BOUCHON Hélène (France)
BOUIX Maurice (France)
BOURGIN David G. (U. S. A.)
BOURGIN Richard (U. S. A.)
BOURGUIGNON J.-P. (France)
BOUTET DE MONVEL Louis (France) (D10)
DE BOUVERE Karel (U. S. A.)
BOUVIER Alain (France)
BRADISTILOV Georgi (Bulgarie)
BRADSTEDT Walsh J. (U. S. A.)
BRAM Leila (U. S. A.)
BRANNAN David A. (Grande-Bretagne)
BRAUER Richard (U. S. A.) (B3)
BRAUMANN Pedro B. (Portugal)
BRAUN Hel (All. de l'Ouest)
BRAUN Martin (U. S. A.) *
BRAUN Robert (All. de l'Ouest)
BRAUNER Claude (France)
BRAWN Frederick (Grande-Bretagne)
BREGER Manfred (All. de l'Ouest)
BRELOT Marcel (France)
BRENNER Philip (Suède)
BREZIS Haim (France)
BRIESKORN Egbert (All. de l'Ouest) (C5)
BRILLA Josef (Tchécoslovaquie)
BRINKMANN Hans (All. de l'Ouest)
BRISCHLE Till (All. de l'Ouest)
BRITTON John L. (Grande-Bretagne)
BRONDSTED Arne (Danemark)
BROUÉ Michel (France)
BROUSSE Pierre (France)
BROWDER Felix (U. S. A.) (D11)
BROWDER William (U. S. A.) (G)
BROWN Edgar (U. S. A.)
BROWN Michael (U. S. A.)
BRUHAT François (France) (C5)
DE BRUIJN Nicolaas (Pays-Bas) (E5)
BRUMER Armand (U. S. A.)
BRUMFIEL Gregory (U. S. A.)
BRUNGS H.-H. (Canada)
BRUTER Claude P. (France) *
BUCUR Lionell (Roumanie)
BUEKENHOUT Francis (Belgique)
BUI DOAN Khanh (France)
BUI TRONG LIEU (France)
BUKOVSKY (Tchécoslovaquie)
BUNDSCHUH Peter (All. de l'Ouest)
BUNGE Marta C. (Canada)
BUNKE Olaf (All. de l'Ouest)
BURACZEWSKI Adam (Ghana)
BURDE Gerhard (All. de l'Ouest)
BURDE Klaus (All. de l'Ouest)
BUREAU Florent (Belgique)
BURGESS David (Grande-Bretagne)
BURGESS Derek Ch. (Irlande)
BURGHELEA Dan (Roumanie)
BURILLO LOPEZ Pedro (Espagne)
BURKHOLDER Donald L. (U. S. A.) (D6)
BURKILL John (Grande-Bretagne)
BURLEY David (Grande-Bretagne)
BURNS Robert (Canada)
BURR Stefan (U. S. A.)
BUSH Kenneth (U. S. A.)
BUSHNELL C. J. (Grande-Bretagne)
BUSK Thoger (Danemark)
BUTTIN Claudette (France)
BUTTON Lilian G. (Grande-Bretagne)
BUTZER Paul (All. de l'Ouest) *
BUZANO Piero (Italie)
BYERS William (Canada)

C

CABANNES Henri (France)
CABY Dominique (France)
CADE Roger (U. S. A.)
CAGNON
CAHEN Michel (Belgique)
CAILLEAU Annie (France)
CAILLIEZ Jean (France)
CALABI Eugenio (U. S. A.) (C4)
CALAIS Josette (France)
CALICA Arnold (U. S. A.)
CALIS J. N S. (Pays-Bas)
CAMINA Alan (Grande-Bretagne)
CAMPBELL Colin M. (Grande-Bretagne)
CAMPOS FERREIRA Jaime (Portugal)
CAMUS Jacques L. (Tunisie)
CANNONITO Franck B. (U. S. A.)
CANTINAT J.-Claude (France)
CAPOBIANCO Michael (U. S. A.)
CAPPELL Sylvain (U. S. A.)
CAPRIZ G.-Franco (Italie)
CARADUS Selwyn R. (Canada)
CARDON Albert (Belgique)
CARICATO Gaetano (Italie)
CARLSON James (U. S. A.)
CARLSTEDT Linda (U. S. A.)
CARMONA Jacques (France)
CARMONA René (France)

CARNAL Henri (Suisse)
CARR Peter (Grande-Bretagne)
CARRAL Michel (France)
CARRIER George (Grande-Bretagne) (E3)
CARRINGTON David C. (Grande-Bretagne)
CARRUCCIO Ettore (Italie)
CARTAN Henri (France)
CARTER Roger W. (Grande-Bretagne)
CARTIER Pierre (France) (C5)
CARTON Edmond (Belgique)
CARTWRIGHT Mary (Grande-Bretagne)
CASLAV V. Stannojevic (U. S. A.)
CASSELS John W. S. (Grande-Bretagne) (B4)
CASSOUNOGUES Philippe (France)
CASSOUNOGUES Pierrette (France)
CASTELEET Manuel
DE CASTRO Antonio (Espagne)
CATHELINEAU Jean-Louis (France)
CATHERINE Françoise (France)
CATTABRIGA Lamberto (Italie)
CATTANEO Carlo (Italie)
CATTANEO Ida (Italie)
CAUBET Jean-P. (France)
CAYFORD S.
CECCHERINI Pier U. (Italie)
CERF Jean (France)
ČERNAVSKII A. V. (U. R. S. S.) (C2)
CESARI Lamberto (U. S. A.) (E4)
CHABERT Jean-Luc (France)
CHACON Rafael V. (U. S. A.) (D6)
CHACRON Maurice (Canada)
CHADEMAN Arsalan (France)
CHADEYRAS Marcel (France)
CHALK John H. H. (Canada) *
CHAMBERS Barbara (U. S. A.)
CHAMBERS Llewelyn (Grande-Bretagne)
CHAN LAI K. (Canada)
CHAN Sui-Wah (U. S. A.)
CHANDRASEKHARAN Komaravol (Suisse)
CHANG Kok Wah (Canada) *
CHAPKAREV Ilija
CHAPMAN Thomas (U. S. A.)
CHAPTAL Nicole (France)
CHARLES Bernard (France)
CHARNES A. (U. S. A.) *
CHARPENTIER Rémy (France)
CHASTENET DE GERY Jérome (France)
CHATELET François (France)
CHATTERJI Srishti (Suisse)
CHATTERJI Subodh (Indes)
CHAVES Manuel L. (Portugal)
CHAZARAIN Jacques (France)
CHEIN Michel (France)
CHEN Kuo Tsai (U. S. A.)
CHEN Tung Liu (U. S. A.)
CHEN Yuh-Ching (U. S. A.)
CHEN Yung-Ming (Hong-kong) *
CHEN Yu-Why (U. S. A.)
CHENEY E. W. (U. S. A.)
CHENON René (France)
CHERKAS Barry (U. S. A.)
CHERN S. S. (U. S. A.) (G)
CHERUBINI Alessandra (Italie)
CHEVALIER Michel (France)
CHEVALLIER Dominique (France)
CHEVRIER Jean (France)
CHILLINGWORTH David R. (Grande-Bretagne)
CHING Wai-Mee (U. S. A.)
CHITCHONG THINGE Jean (Grande-Bretagne)
CHOQUET-BRUHAT Yvonne (France) (E2)
CHOW Pak S. (Grande-Bretagne)
CHRISTENSEN Carlton (Australie)
CHRISTENSEN Jens Peter (Danemark).
CHRISTIANSEN Bent (Danemark)
CHRYSSAGIS Vassilios (Grèce)
CHUNG Kai-Lai (U. S. A.) (D5)
CHURCH Alonzo (U. S. A.)
CHURCHHOUSE Robert F. (Grande-Bretagne)
CIARLET Philippe (France)
CIESIELSKI Zbigniew (Pologne)
CILIBERTO Carlo (Italie)
CIMMINO Gianfranco (Italie)
CINQUINI Silvio (Italie)
CITRON Richard (U. S. A.)
CLAESSON Tomas (Suède)
CLARK Allan (U. S. A.)
CLARK John (Grande-Bretagne)
CLAY J. R. (U. S. A.)
CLEMENS Charles (U. S. A.)
CLÉMENT F. M. (France)
CLÉMENT Philippe (Suisse)
CLIFFORD Alfred (U. S. A.)
CNOP Ivan (Belgique)
COATMELEC Christian (France)
CODDINGTON Earl A. (U. S. A.)
COEN Salvatore (Italie)
COEURE Gérard (France)
COFFI-NKETSIA B. J. (France)
COGHLAN Francis (Grande-Bretagne)
COHEN Hirsh G. (U. S. A.)
COHEN Joel M. (U. S. A.)
COHEN Maurice (France)
COHEN Simone (France)
COHN Harvey (U. S. A.) *
COHN John H. E. (Gde-Bretagne)
COHN Paul M. (Grande-Bretagne) (B1)
COHN Richard (U. S. A.)
COIFMAN Ronald R. (U. S. A.)
COLE Nancy (U. S. A.)
COLLATZ Lothar (All. de l'Ouest)
COLLINGWOOD Edward (Grande-Bretagne)
COLLINS Donald J. (Grande-Bretagne)
COLLINS Peter J. (Grande-Bretagne) *
COLLOP Michael (Grande-Bretagne)
COLOMBEAU Jean-F. (France)
COLOMBO Serge (France)
COLTON David (U. S. A.)
COMBES François (France)
COMBESCURE Jacques (France)
COMBET Edmond (France)
COMINCIOLI Valeriano (Italie)
COMPOINT Philippe (France)
COMTET Louis (France)
DI CONCILIO Anna (Italie)
CONLAN James (Canada)
CONLEY Charles (U. S. A.) (D12)
CONLON Lawrence (U. S. A.)
CONNETT William (U. S. A.)
CONWAY John H. (Grande-Bretagne) (B3)
COOPER Graeme (Grande-Bretagne)
CORAL Max (U. S. A.) *
CORREL Ellen (U. S. A.)
CORWIN Lawrence (U. S. A.)
COSTE Alain (France)
COUDRAIS Jacques (France)
COULOMB Geneviève (France)
COUOT Jacques (France)
COURTILLOT Marcel (France)
COUTRIS Nicole (France)
COUTY Raymond (France)
COVACI-MUNTEANU Marie-Janne (Belgique)
COX Maurice (Grande-Bretagne)
CRAW Ian G. (Grande-Bretagne)
CREE George (Canada)
CROFT Hallard (Australie)
CRUMEYROLLE Albert (France)
CRYER Colin (U. S. A.)
CSASZAR Akos (Hongrie)
CUADRA FERNANDEZ José-Luis (Espagne)
ČUDAKOV N. G. (U. R. S. S.) (B6)
CUDIA Dennis F. (U. S. A.)
CUMMINGS Larry (Canada)
ČUPONA Georgi (Yougoslavie)
CUPPENS Roger (France)
CURRY Haskell (Pays-Bas)

CURTIS Alan Rob (Grande-Bretagne)
CURTISS J. H. (U. S. A.)
CUSIK Thomas (U. S. A.) *

D

DACIC Ljubisa (France)
DACIC Rade (Yougoslavie)
DADE Everett (France)
DAGUENET M. (France)
DALLA VOLTA Vittorio (Italie)
D'AMBROSIO Ubiratan (U. S. A.) *
DAMERELL Robert M. (Grande-Bretagne)
DAMKOHLER Wilhelm (Argentine) *
DANCIS Jérôme (U. S. A.) *
DANCS Stephen (Hongrie)
DANG NGOC Nghiem (France)
DANICA Nikolic (Yougoslavie)
DANICIC Ivan (Grande-Bretagne)
DANIEL James W. (U. S. A.)
DANILYUK I. I. (U. R. S. S.) * (D10)
DANKERT Gabriele (Canada)
DARK Rex S. (Grande-Bretagne)
DAVIES Hilda M. (Grande-Bretagne)
DAVIDSON Luis (France)
DAVIS
DAVIS Chandler (Canada)
DAX Jean-P. (France)
DAYANITHY Kandiah (Grande-Bretagne)
DAYKIN David E (Grande-Bretagne)
DAZORD Jean (France)
DAZORD Pierre (France)
DEBRUNNER Hans (Suisse)
DECUYPER Marcel (France)
DEGRANDE-DEKIMPE Nicole (Belgique)
DEHEN Danièle (France)
DEHEN Michèle (France)
DEKKER Jacob (U. S. A.)
DELANGHE Richard (Belgique) *
DELAROCHE Claire (France)
DEL FRANCO Georgia (U. S. A.)
DELIGNE Pierre (France) (B5)
DELMER Francine (France)
DELMEZ Claude M. (Belgique)
DELPORTE Jean (France)
DEMBOWSKI Peter (All. de l'Ouest)
DEMENGEL G. (France)
DEMETRIUS L.
DENES Jozsef (Hongrie) *
DENJOY Arnaud (France)
DENK Franz (All. de l'Ouest)
DENNEBERG Dieter (All. de l'Ouest)
DENNETT John Roy (Grande-Bretagne)
DENTONI Paolo (Italie)
DEPAIX Michel (France)
DESCHASEAUX J.-Pierre (Maroc)
DESCLOUX Jean (Suisse)
DESFORGE Julien L. (France)
DESHOUILLERS Jean-Marc (France)
DESPLAND J.-Claude (France)
DESQ Roger (France)
DESTOUCHES Jean-Louis (France)
DEUTSCH Nimet (France)
DEVIDÉ Vladimir (Yougoslavie)
DHAHIR M. W. (Irak)
DHALIWAL Ranjit S. (Canada) *
DHOMBRES Jean (France)
DIAS AGUDO Fernando (Portugal)
DIAZ Joaquin (U. S. A.)
DICKINS John (Grande-Bretagne)
DIENER Karl (All. de l'Ouest)
DIEUDONNÉ Jean (France)
DIMITROV Georgiev (Bulgarie)
DIMOVSKI Ivan (Bulgarie)
DIONNE Philippe (Nouvelle-Zélande)
DITZIAN Zeev (Canada)
DIXMIER Jacques (France)
DIXMIER Suzanne (France)
DIXON John (Canada)
DIXON Peter Gr. (Gde-Bretagne)
DJAJA (Yougoslavie)
DJOKOVIC Dragomir (Canada)
DJORDJEVIC Radoslav (Yougoslavie)
DJRBASHIAN M. M. (U. R. S. S.) *
DJURIC Milan (Yougoslavie)
DLAB Vlastimil (Canada) *
DO Claude (France)
DOBBER Eelkje (Pays-Bas)
DOBRAKOV Ivan (Tchécoslovaquie)
DODSON Michael (Grande-Bretagne)
DOITCHINOV Doitchin (Bulgarie) *
DOLAPTSCHIEW Blagowest (Bulgarie)
DOLBEAULT Pierre (France)
DOLBEAULT-LEMOINE Simone (France)
DOLINSKY Rostislaw (All. de l'Ouest)
DOMINYAK Imre (Hongrie)
DONEDDU Alfred (France)
DONNELLY John (Gde-Bretagne)
DONOGHUE William (U. S. A.)
DORING Boro (All. de l'Ouest) *
DOSS Raoul (U. S. A.)
DOSTAL Milos (France)
DOTCHEV Guetchev (Bulgarie)
DOU Alberto (Espagne)
DOUGLAS Jim. Jr. (U. S. A.) (E3)
DOUGLAS Ronald (U. S. A.)
DOUIN Françoise (France)
DOWLING Thomas A. (U. S. A.)
DOWSON Henry (Grande-Bretagne)
DOXIADIS Apostolos (U. S. A.)
DOYEN Jean (Belgique)
DRASCIC Rajko (Yougoslavie)
DRESHER Melvin (U. S. A.)
DRESS François (France) *
DUBIN Daniel A. (Grande-Bretagne)
DUBINS Lester E. (U. S. A.)
DUBINSKY Ed. (Canada)
DUBOIS Donald (U. S. A.)
DUBREIL Paul (France)
DUDA Edwin (U. S. A.)
DUDLEY Richard M. (U. S. A.)
DUGDALE Jack (Grande-Bretagne)
DUHOUX,Michel (Belgique)
DUISTERMAAT Johannes (Pays-Bas)
DULMAGE Andrew (Canada)
DUNN Kenneth (Canada)
DUNWOODY Martin J. (Grande-Bretagne)
DU PLESSIS Johanners (Afrique du Sud)
DU PLESSIS Nicolaas (Grande-Bretagne)
DUPUY Maryvonne (France)
DUREN Peter (U. S. A.)
DUSSAUD R. (France)
DUVAL Victor (France)
DUVAUT Georges (Francc) (E3)
DWIVEDI T. O. (Canada)
DVORETZKY A. (Israël) (D6)
DYER-BENNET John (U. S. A.)
DYNKIN E. B. (U. R. S. S.) (D5)
DZYADYK V. Kirillovitch (U. R. S. S.) (D7)

E

EARLE Clifford (U. S. A.)
EASTRATIOS Galunis
EBERHARD Walter (All. de l'Ouest)
EBERSOLDT Franz (All. de l'Ouest)
EBIN D. G. (U. S. A.) (C4)
ECHIVARD Michel (France)
ECKERT John
ECKMANN Beno (Suisse)
EDER Otmar (All. de l'Ouest)
EDMONDS Sheila M. (Grande-Bretagne)
EDWARDS D. A. (Grande-Bretagne) (D1)

EELLS James (Grande-Bretagne) (C4)
EFFROS Edward (U. S. A.)
EFIMOV A. V. (U. R. S. S.)
EGOROV Iu. V. (U. R. S. S.) (D10)
EGUCHI K.
EHLERS Jürgen (U. S. A.) (E2)
EHRENPREIS Leon (U. S. A.)
EILENBERG Samuel (U. S. A.) (E7)
EINARSSON B. O. (Suède)
EINSELE Carl (Suisse)
EISELE Carolyn (U. S. A.) *
EISENBUD David (U. S. A.)
EISNER BILLO Silvia (Suisse)
EKE B. G. (Irlande)
EKELAND Ivar (France)
ELIAŠ Josef (Tchécoslovaquie)
ELIASSON Halldor (Islande)
ELJOSEPH Nathan (Israël)
ELKINGTON Gordon (Grande-Bretagne)
ELLIS Alan (Grande-Bretagne)
ELLMER Horst (All. de l'Est)
ELMABSOUT Badaoui (France)
ELWORTHY Kenneth (Grande-Bretagne)
ENFLO Perhenrik
ENGUEHARD Michel (France)
EPSTEIN Mordechai (Israël)
ERDELYI Ivan (U. S. A.) *
ERDOS John Al. (Grande-Bretagne)
ERDÖS Paul (Hongrie) (E5)
ERIKSSON S. Folke (Suède)
ERLANDER Sven (Suède)
ERŠOV Iu. L. (U. R. S. S.) (A)
ERVYNCK (Belgique)
ESCASSUT Alain (France)
ETHERINGTON Ivor (Grande-Bretagne)
EVANS Edward (U. S. A.)
EVANS W. Buell (U. S. A.)
EVIATAR Asriel (Israël)*
EWEN Alex Jam (Grande-Bretagne)
EWING John (U. S. A.)
EXBRAYAT Jean-Marie (France)
EXNER Robert (Australie)
EYMARD Pierre (France)
EYMERY Bernard (France)
EZAWA Hiroshi (Japon)
EZRA Jacques (France)

F

FADDEEV L. D. (U. R. S. S.) (E2)
FADELL Albert (U. S. A.)
FAGUE M. K. (U. R. S. S.)
FAISANT Alain (France)
FALK Sigurd (All. de l'Ouest)
FALL Souleyman (Sénégal)
FARAUT Jacques (Tunisie)
FARKAS Hershel (U. S. A.)
FARKAS Miklos (Hongrie) *
FARKOVA' Jana (Tchécoslovaquie)
FARRELLF Thomas (U. S. A.) (C2)
FAST Henryk (U. S. A.)
FAURE Robert (Sénégal)
FAVE
FEDIDA Edmond (Congo)
FEENEY Walter (U. S. A.)
FEFERMAN S. (U. S. A.) (A)
FEFFERMAN Charles (U. S. A.)
FEIT Walter (U. S. A.) (G)
FELD Joseph (U. S. A.)
FELDMAN Jacob (U. S. A.)
FÉLIX Lucienne (France)
FELL James (U. S. A.) (D2)
FENSTAD Jens. E. (Norvège)
FERNANDES DE CARVALHO José Alb. (Portugal)
FÉRON Robert (France)
FERRARI Mario
FERRIER Jean-P. (France)
FERRO Ruggero
FICHERA Gaetano (Italie) (E3)
FIDELIS Eugeniusz,(Pologne)
FIELDS Jerry (Canada)
FINKELSTEIN Mark (U. S. A.)
FINLEY
FINN Robert (U. S. A.) (E3)
FINZI Bruno (Italie)
FISCHER Pal. (France)
FISCHER Walther (All. de l'Ouest)
FISCHER Wolfgang (All. de l'Ouest)
FLEMING Wendell (U. S. A.) (E4)
FLETCHER Colin R. (Grande-Bretagne)
FLETCHER Trevor (Grande-Bretagne)
FLETT Thomas (Grande-Bretagne)
FLORES ESPINOZA Ruben (Mexique)
FLORIDES Petross (Irlande)
FLOYD R. W. (U. S. A.) (E7)
FOATA Dominique (France)
FODOR Gesa. (Hongrie)
FOIAS Ciprian (Roumanie) (D3)
FONG Paul (U. S. A.)
FORD James W. (Grande-Bretagne)
FORELLI Frank (U. S. A.) (D4)
FORSTER Otto (All. de l'Ouest) (D8)
FORT Jacques (France)
FOUNTAIN John (Grande-Bretagne)
FOUNTAIN Leonard (U. S. A.)
FOURES Léonce (France)
FOURNIER J.-Claude (France)
FOWLER David (Grande-Bretagne)
FOX Charles (Canada)
FOX Leslie (Grande-Bretagne)
FRAENKEL Aviezri (U. S. A.)
FRAGOZO ROBLES Arturo (Mexique)
FRANK (U. S. A.)
FRANK Evelyn (U. S. A.)
FRASNAY Claude (France)
FREDRIKSON Einar (Pays-Bas)
FREEDMAN Haya (Grande-Bretagne)
FREEDMAN Herbert (Canada)
FREESE Ralph (U. S. A.)
FREI Gunther (Canada)
FREMLIN David H. (Grande-Bretagne)
FRÉMOND Michel (France)
FRESNEL Jean (France) *
FREUD Geza (Hongrie) *
FREUDENTHAL Hans (Pays-Bas)
FRIED Jean (France)
FRIEDMAN Nathaniel (U. S. A.)
FRIESEN Donald (U. S. A.)
FRISCH Jacques (France) (D8)
FRITSCH Rudolf (All. de l'Ouest)
FRÖBERG Carl Erik (Suède)
FROSTMAN Otto (Suède)
FUAD Milla (Koweit)
FUCHS Laszlo (U. S. A.)
FUCHS Wolfgang (U. S. A.)
FUCHSSTEINER Benno (All. de l'Ouest)
FUGLEDE Bent (Danemark) (D5)
FUKAWA Masami (Japon)
FURSTENBERG Harry (Israël) (C5)
FUSTIVIA (Italie)

G

GAAL Steven A. (U. S. A.)
GAEDE Karl (All. de l'Ouest)
GAFFNEY Matthew (U. S. A.)
GAGLIARDO (U. S. A.)
GAIR Frank (Nouvelle-Zélande)
GALAMBOS Janos (Grande-Bretagne) *
GALBRAITH Alan St. (U. S. A.)
GALOFRE Modesto (U. S. A.)
GAMKRELIDZE R. V. (U. R. S. S.) (E4)
GAMST (All. de l'Ouest)
GANDHI Jeetmal (U. S. A.)
GANELIUS Tord H. (Suède)
GANI Naoum (France)
GARABEDIAN Paul (U. S. A.) (E3)
GARCIA ALVAREZ Miguel
GARCIA PEREZ Pedro (Espagne)
GARDINER Anthony (Grande-Bretagne)
GÅRDING Lars (Suède) (D10)
GAREL Emmanuelle (France)
GARG Krishna (Canada)

GARLING David (Grande-Bretagne)
GARNER Robert (U. S. A.)
GARNIER Henri G. (Belgique)
GARREAU Gabriel (Suisse)
GARRETT James R. (U. S. A.)
GARRISON Betty (U. S. A.) *
GASIMOV M. G. (U. R. S. S.) *
GAUDEFROY Alain L. (France)
GAVRILOV Mihail (Bulgarie)
GEBA K. (Pologne)
GEFFEN Nima (Israël)
GELBART Abe (U. S. A.)
GELBART Stephen (U. S. A.)
GELFAND I. M. (U. R. S. S.) (G)
GENTCHEV Todor G. (Bulgarie)
GEORGE Gwyneth (Canada)
GÉRARD Raymond (France)
GERGELY Tanas (Hongrie)
GERHARDTS Max D. (All. de l'Ouest)
GERLACH Eberhard (Canada)
GERMAIN Paul (France)
GERMAY Noël (Belgique)
GEROCH Robert (U. S. A.) (E2)
GERVOIS Mlle (France)
GETOOR Ronald (U. S. A.) (D5)
GEYMONAT Giuseppe (Italie)
GHAFFARI Abolghassem (U.S.A.) *
GHIRCOIASIU Nicolas (Roumanie)
GIELEN Wimpie (Pays-Bas)
GIFFEN Charles (U. S. A.)
GIGNETTI Alberto (Italie)
GIKHMAN I. I. (U. R. S. S.) *
GILBARG David (U. S. A.)
GILBERT William (Canada)
GILLAM B. E. (U. S. A.)
GILLIGAN Brucc (Canada)
GILLIS Joseph (U. S. A.)
GILLIS Paul P. (Belgique)
GILLMAN Leonard (U. S. A.)
GILMORE Lynnette (Grande-Bretagne)
GILORMINI Claude (France)
GINZBURG Abraham (Israël)
GIRARDEAU J.-Pierre (France)
GIRAUD Georges (France)
GIRAUD Jean (France) (B2)
GIUSTI Enrico
GIVENS Monique (France)
GIVENS Wallace (U. S. A.)
GLAESER Georges (France)
GLASNER Moses (U. S. A.)
GLAUBERMAN George I. (U.S.A.) (B3)
GLAUS Christian (Suisse)
GLEASON Andrew (U. S. A.) (E5)
GLICKSBERG Irving Leonard (U. S. A.)
GLIMM James (U. S. A.) (E1)
GLODEN Raoul (Luxembourg)
GOBLOT Rémy
GODEAUX Lucien (Belgique)
GODET-THOBIE Christiane (France)
GODUNOV S. K. (U. R. S. S.) (E3)
GOLAY Eric (Suisse)
GOLDIE Alfred (Grande-Bretagne)
GOLDIE Charles (Grande-Bretagne)
GOLDSCHMIDT Hubert (France)
GOLDSTEIN Jérôme A. (U. S. A.)
GOLOMB Michael (U. S. A.)
GONTSHAR A. A. (U. R. S. S.)
GONZALEZ Hilda (U. S. A.)
GONZALES VALLES Carlos (Espagne)
GOODINSON Patricia (Grande-Bretagne)
GOODMAN Gerald (Italie)
GOPALA KRISHNA Jonnalag (Indes)
GORDON Cameron (Grande-Bretagne)
GORDON Gerald (U. S. A.)
GORDON Samuel (U. S. A.)
GORENSTEIN Daniel (U. S. A.) (B3)
GÖRLICH Ernst (All. de l'Ouest) *
GOSSEZ Jean-Pierre (Belgique) *
GOULAOUIC Charles (France)
GOULD Gerald G. (Grande-Bretagne)
GOULD Sydney (All. de l'Ouest)
GOULLET DE RUGY Alain (France)
GOURSAUD Jean-Marie (France)
GOUT Gérard (France)
GOUYON Luce (France)
GRAD Harold (U. S. A.) (E3)
GRAFFI Dario (Italie)
GRAHAM Victor W. (Irlande)
GRAMSCH Bernhard (All. de l'Ouest)
GRANAS Andrzej (Canada)
GRANDALL Michael (U. S. A.)
GRANDET Marthe (France)
GRASSIN Jacques (France)
GRAVELEAU Jean (France)
GRAY Alfred (U. S. A.)
GRAY Jeremy (Grande-Bretagne)
GRAY Joan W. (Suisse)
GRAY Mary (U. S. A.)
DE GRAY Ronald W. (U. S. A.)
GRECO Antonio (Italie)
GREECHIE Richard (U. S. A.)
GREEN Mark L. (U. S. A.)
GREGUŠ Michel (Tchécoslovaquie)
GREVILLE Thomas (U. S. A.)
GRIFFITH J. Gareth (Canada)
GRIFFITH Philipp (U. S. A.)
GRIFFITHS H. Brian (Grande-Bretagne) (F2)
GRIFFITHS Phillip (U. S. A.) (G)
GRIGUELIONIS B. I. (U. R. S. S.)
GRISVARD Pierre (France) (D10)
GROH Hans J. (Canada)
GROMOLL Detlef (U. S. A.) (C3)
GROMOV M. L. (U. R. S. S.) (C4)
DE GROOTE Hans (All. de l'Ouest)
GROSSWALD Emil (U. S. A.)
GROTHENDIECK Alexandre (France) (B5)
GROWE Maledar (Grande-Bretagne)
GRUBB Gerd (Danemark)
GRUENBERG Karl (Grande-Bretagne)
GRUSHIN V. V. (U. R. S. S.) (D10)
GUARALDO
GUCKENHEIMER John (Grande-Bretagne)
GUEHO M.-France (France)
GUENHAN Asaf V. (Turquie)
GUENZLER Hans F. (All. de l'Ouest)
GUÉRARD DES LAURIERS Michel (France)
GUERASIMOV I. S. (U. R. S. S.)
GUERINDON Jean (France)
GUEVARA VASQUEZ Francisco (France)
GUGGENBUHL Laura (U. S. A.)
GUICHARDET Alain (France)
GUILLAUME Marcel (France)
GUILLEMIN Victor (U. S. A.) (C4)
GUILLERAULT-ASTIER Michel (France)
GUILLERNVO Fleitas (Espagne)
GUILLOT Christophe
GUILLOT J.-Claude (France)
GUINAND Andrew P. (Canada)
GUIRAUD Jean-Pierre (France) (E3)
GULDEN Samuel L. (U. S. A.)
GULONOV Alexander (Bulgarie)
GUNNING Robert (U. S. A.) (D8)
GUPTA Narain (Canada)
GUPTA Shiv-K. (U. S. A.)
GUREL Okan (U. S. A.) *
GUSEINOV A. I. (U. R. S. S.)
GUSTAFSON Sven-Ake (Suède)
GUY Roland (Canada)
GUZMAN Miguel (Espagne)
GYÒRY Kalman (Hongrie)

H

HADDAD Labib (France)
HAEFLIGER André (Suisse)
HAIGHT Frank (France)
HAIMO Deborah (U. S. A.) *
HAIMOVICI Mendel (Roumanie)

HAINZL Josef (All. de l'Ouest)
HAJNAL Andras (Hongrie)
HALBERSTADT Emmanuel (France)
HALE Jack K. (U. S. A.)
HALE Victor (Grande-Bretagne)
HALES Richard (Grande-Bretagne)
HALL Marshall (U. S. A.) (E5)
HALL Thomas (Grande-Bretagne)
HALPERIN Israël (Canada)
HAMITI Ejup (Yougoslavie)
HAMMER Peter (Canada)
HAMMOND SMITH David (Grande-Bretagne)
HAMOUI Adnan (Syrie)
HANANI Haim (Israël)
HANATANI Yoshito (Japon)
HANIOTIS Zeppos (Suisse)
HANN Alexander (Suisse)
HANN Robert
HANNER Olof (U. S. A.)
HARARI Roger (France)
HARBORTH Heiko (All. de l'Ouest) *
HARDER Günter (All. de l'Ouest) (C5)
HARDY F. Lane (U. S. A.)
HARMEGNIES René Victor
HARPER John R. (U. S. A.)
HARROLD Orville (U. S. A.) *
HART Neal (Kenya)
HARTIG Klaus (All. de l'Est)
HARTLEY Elizabeth (Ghana)
HARVEY Reese (U. S. A.)
HARZALLAH Khelifa (Tunisie)
HARZHEIM Egbert (All. de l'Ouest)
HATCHER William (Canada)
HATORI Tsukasa (Japon)
HATTON Michael (Grande-Bretagne)
HATZIANASTASSION Despina (France)
HAUDIDIER
HAUGAZEAU
HAUSSMANN Werner (All. de l'Ouest)
HAYEK CALIL Nacere (Espagne)
HAYMAN Walter (Grande-Bretagne) (D7)
HAZEWINKEL Michiel (Pays-Bas)
HECQUET Gérard (France)
HEDBERG Lars (Suède)
HEDBERG Torbjorn (Suède)
HEDRLIN Z. (Tchécoslovaquie)(B2)
HEIDEMA Johannes (Afrique du Sud)
HEILBRONN H. A. (Canada)
HEINIG Hans Paul (Canada)
HEINRICH Jurgen (All. de l'Ouest)
HEINS Maurice (U. S. A.)
HEINS
HEINTZE Ernst (All. de l'Ouest)
HEJNÝ Milan (Tchécoslovaquie)
HELFRICH Hans Peter (All. de l'Ouest)
HELGASON Sigurdur (U.S.A.) (C5)
HELSON Henry (U. S. A.) (D4)
HELTON J. William (U. S. A.)
HELVERSEN Anna (France)
HENDERSON David W. (U. S. A.)
HENNEQUIN
HENRARD Paul (Belgique)
HERRLICH Horst (All. de l'Ouest)
HERSZBERG Jerry (Grande-Bretagne)
HERZ Jean-Claude (France)
HERZOG F. (U. S. A.)
HERZOG Marcel (Israël)
HEUZE Guy (France)
HIGGINS Philip J. (Grande-Bretagne)
HIGGINSON John Alb (Canada)
HIGMAN D. G. (U. S. A.) (B3)
HIJAB Wasfi (Liban)
HILL C. Denson (Italie)
HILL Raymond (Grande-Bretagne)
HILL Walter (U. S. A.)
HILLE Einar (U. S. A.)
HILTON Peter (U. S. A.) (B2)
HINDLEY Roger (Grande-Bretagne)
HIRONAKA Heisuke (U. S. A.) (D8)
HIROSHI Umemura (Japon)
HIRSCH Gérard (France)
HIRSCH Kurt A. (Grande-Bretagne)
HIRSCHFELD James W. (Grande-Bretagne)
HITCHCOCK Anthony (Grande-Bretagne)
HITCHIN Nigel (Grande-Bretagne)
HOCQUENGHEM Alexis (France)
HOCQUENGHEM Serge (France)
HODGES Wilfrid (Grande-Bretagne)
HODGSON Jonathan (U. S. A.)
HOEDE Cornelis (Pays-Bas)
HOEHLE Ulrich (All. de l'Ouest)
HOFBAUER Johann (Autriche)
HOFFMAN Peter (Canada)
HOGBE-NLEND Henri (France)
HOLLADAY John (U. S. A.)
HOLLAND Samuel (U. S. A.)
HOLM Per (Norvège)
HOLMANN Harald (Suisse)
HOLME Audun (Norvège)
HOLVOET Roger (Belgique)
HOO C. (Canada)
HÖRMANDER Lars (Suède) (G)
HORNIX Elisabeth (Pays-Bas)
HORVATH John (U. S. A.)
HORVATIC Kreso (Yougoslavie)
HOSLI Hansueli (Suisse)
HOSSRU Miklos (Hongrie)
HOUDEBINE Jean (France)
HOUGHTON Charles (All. de l'Ouest)
HOUILLOT-ROYER Josette (France)
HOUSEHOLDER Alston (U. S. A.)
HOWES Norman R. (U. S. A.) *
HOWIE John M. (Grande-Bretagne)
HSIANG Fu-Cheng (République de Chine) *
HSIANG Wu-Chung (U. S. A.) (C2)
HSIUNG Chuan C. (U. S. A.)
HUARD Pierre (France)
HUBBUCK John R. (Grande-Bretagne)
HUBERT Jacqueline (France)
HUBERT Michel (France)
HUDSON John F. P. (Grande-Bretagne) (C2)
HUDSON Robin (Grande-Bretagne)
HUET Denise (France)
HUET Patrick (France)
HUGHES Kenneth (Grande-Bretagne)
HULANICKI Andrzej (Pologne)
HULSE John (Grande-Bretagne)
HUMBLOT Lionel (France)
Von der HUMBOLDT (All. de l'Est)
HUMPHREYS James E. (U. S. A.)
HUMPHREYS John (Grande-Bretagne)
HUNT John H. V. (Canada)
HUNT Richard (U. S. A.) (D9)
HUPPERTZ Hermann (All. de l'Ouest)
HUSAIN Taqdir (Canada)
HUTSON Vivian (Grande-Bretagne)

I

IBISCH Horst (France)
IBRAGUIMOV I. I. (U. R. S. S.) *
IHARA Yasutaka (Japon) (B4)
ILIEFF Ljubomir (Bulgarie)
ILJIN V. A. (U. R. S. S.) (D10)
ILLUSIE Luc (France)
IMAI Masataha (Japon)
IMANISHI Hideki (Japon)
IMHOF Jean-P. (Suisse)
IMRICH Wilfried (Autriche)
INFANTOZZI Carlos (Uruguay) *
INGELSTAM Lars Erik (Suède)

INSELBERG Alfred (U. S. A.)
INVERARITY William M. (Grande-Bretagne)
ION Patrick (Grande-Bretagne)
IONESCU Dumitru (Roumanie) *
IONESCU TULCEA Alexandra (U. S. A.)
De IONGH Johan J. (Pays-Bas)
IRWIN Michael (Grande-Bretagne)
ISBELL John (U. S. A.)
ISHAQ M. (Canada) *
ISHIHARA Shigeru (Japon)
ISHIHARA Tadashige (Japon)
ISLA Emilio (Pérou)
IVAN Jan (Tchécoslovaquie)
IVANOFF Vladimir (U. S. A.)
IWASAWA Kenkichi (U. S. A.) (B4)
IYAHEN Sunday (Nigéria)
IYANAGA Shokichi (Japon)
IZANS Chantal (France)
IZBICKI Herbert (Autriche)
IZUMI Maseko (Australie)
IZUMI Shin Ichi (Australie)

J

JACKSON Howard L. (Canada)
JACOBINSKI Heinz (Suède)
JACOBS Konrad (All. de l'Ouest)
JACOBSON David (Canada)
JACOBSON Florence (U. S. A.)
JACOBSON Nathan (U. S. A.)
JAEGER Arno (All. de l'Ouest)
JAFFARD Paul L. (France)
JAGERS Albertus (Pays-Bas)
JAGERS Peter (Suède)
JAKUBIK Jan (Tchécoslovaquie)
JAMBOIS W.
JAMES Donald (U. S. A.)
JAMES Ioan (Grande-Bretagne)
JAMES Ralph D. (Canada)
JAMES Robert (U. S. A.)
JANEKOSKI Viktor (Yougoslavie)
JANET Maurice (France)
JANICH Klaus (All. de l'Ouest)
JANIN Monique (France)
JANIN Pierre (France)
JANKO Zvonimir (U. S. A.) (B3)
JANKOVIĆ Zlatko (Yougoslavie)
JANSEN Karl (All. de l'Ouest)
JANSSEN Gerhard (All. de l'Ouest)
JANSSEN Jacques (Belgique)
JANSSENS Paul (Belgique)
JAYNE John E. (U. S. A.)
JEAN Michel (Canada)
JEANCLAUDE André (France)
JEANQUARTIER Pierre (Suisse)
JEFFERY R. L. (Canada)
JEFFRIES Clark D. (Canada)
JENSEN Christian (Danemark)
JENSEN Ronald, Björn (U. S. A.) (A)
JERISON Meyer (U. S. A.)
JIMENEZ POZO Miguel (France)
JOHN John (Grande-Bretagne)
JOHNSEN V. Ben (Norvège)
JOHNSON Guy (U. S. A.)
JONAC M.-Louise (France)
JONES Burton W. (U. S. A.)
JONES F. Burton (U. S. A.) *
JONES Harold T. (U. S. A.)
JONKER Peter (Pays-Bas)
JORDAN Dominic (Grande-Bretagne)
JORIS Henri (Suisse)
JOUBERT Gérard (France)
JOURLIN Michel (France)
JOUSSEN Jakob (All. de l'Ouest)
JUHASZ Istvan (Hongrie)
JULIA Gaston (France)
JUN Tomiyama (Japon)
JUN-ICHI Igusa (U. S. A.)
JUPP Peter (Grande-Bretagne)

K

KADISON Richard (U. S. A.) (D2)
KAHANE Jean-Pierre (France)
KAHRAMANER Suzan F. (Turquie)
KAIJSER Thomas (Suède)
KAJDAN D. (U. R. S. S.) (C5)
KAKA Léo
KAKUTANI Shizuo (U. S. A.)
KALISCH Gerhard K. (U. S. A.) *
KALLINA Carl (U. S. A.)
KALMAN John A. (Nouvelle-Zélande)
KALMÁR László (Hongrie)
KALVANI Raghuraja (Indes)
KAMBER Franz (U. S. A.)
KAMENAROVIC Ivan (Yougoslavie)
KAMPE DE FERIET Joseph (France)
KANEYUKI Soji (U. S. A.)
KAPADIA Ranesk (Grande-Bretagne)
KAPLAN Samuel (U. S. A.)
KAPLAN Wilfred (Suisse)
KAPPOS Demetrios (Grèce)
KARANIKOLOV Christo (Bulgarie)
KARATOPRAKLIEV Gueorgui (Bulgarie) *
KAREMAN Herman (U. S. A.)
KARGAPOLOV M. I. (U. R. S. S.)
KAROUBI Max (France) (C1)
KARTSAKLIS A. (France)
KASSAB Jani (Grande-Bretagne)
KATO Mitsuyo (France)
KATO Tosio (U. S. A.) (G)
KATONA Gyula (Hongrie)
KATSURADA Yoshie (Suisse) *
KATTSOFF Louis (U. S. A.)
KATZ Leo (U. S. A.)
KATZ Moshe (Israël)
KATZ Nicholas (U. S. A.) (B5)
KATZNELSON Yitzhak (Israël) (D9)
KATZOUPAKHS Iayan
KAUFMANN-BUHLER Walter (All de l'Ouest)
KAUP Burchard (Suisse)
KAWAGUCHI Akitsugu (Japon)
KAWAKAMI Hiroshi (France)
KAZCKES
KAZDAN Jerry L. (U. S. A.)
KEARTON Cherry (Grande-Bretagne)
KEATES Michael (Grande-Bretagne)
KEEDWELL Anthony (Grande-Bretagne)
KEGEL Otto (Grande-Bretagne)
KEIMEL Klaus (France)
KEISLER Jérôme (U. S. A.) (G)
KELENSON Philip (Israël)
KELLER Hans (Suisse)
KELLEY Al (U. S. A.)
KELLY Gregory (Australie)
KENNEDY Hubert (U. S. A.)
KENNEY Margaret (U. S. A.)
KEOWN E. Ray (U. S. A.)
KERKYACHARIAN Gérard (France)
KERR-LAWSON Angus (Canada)
KERVAIRE Michel (U. S. A.)
KESTEN Harry (U. S. A.) (D5)
KEUNE Frans (Pays-Bas)
KHALIL Idriss (France)
KHARATISHVILI G. L. (U. R. S. S.) (E4)
KIBBEY Donald (U. S. A.)
KIEFER Jack (U. S. A.) (E6)
KIEFFER Lucien (Luxembourg)
KIEHL Reinhardt (All. de l'Ouest) (D8)
KIELY John (Grande-Bretagne)
KIRBY David (Grande-Bretagne)
KIRBY Robion (U. S. A.) (C2)
KISELMAN C. O. (Suède)
KITBALIAN A. A. (U. R. S. S.)
KJELDSEN Kjell (Norvège)
KLAMKIN Murray S. (U. S. A.)
KLASSEN John (Canada)
KLEIMAN Steven (U. S. A.) (B5)
KLEIN (France)
KLEIN Abraham (Israël)
KLEIN Samuel (U. S. A.)
KLEIN Thérèse (Israël)
KLEISLI Heinrich (Suisse)
KLEPPNER Adam (U. S. A.)
KLINGENBERG Wilhelm (All. de l'Ouest)

KLUVANEK Igor (Australie)
KNAUER Ulrich (All. de l'Ouest)
KNAUFF Werner (All. de l'Ouest)
KNEEBONE Geoffrey (Grande-Bretagne)
KNESER Martin (All. de l'Ouest)
KNIGHT Dorothy (U. S. A.)
KNIGHT Lyman C. (U. S. A.)
KNILL Ronald (France) *
KNOPFMACHER John (Afrique du Sud) *
KNUS Max (Suisse)
KNUTH Donald (U. S. A.) (E7)
KNUTSON Donald I. (U. S. A.)
KOBAYASHI Shoshichi (U. S. A.) (C3)
KOCH Alois (Australie)
KOCH Wilfried (All. de l'Ouest)
KOCHER Franck (U. S. A.)
KOECHER Max (All. de l'Ouest) (B1)
KOEMHOFF Magclone
KOETHE Gottfried (All. de l'Ouest)
KOHNEN Walter (All. de l'Ouest)
KOITER Warner (Pays-Bas) (E3)
KOLAR Wonnfried (All. de l'Ouest) *
KOLIBIAR Milan (Tchécoslovaquie)
KOLIBIAROVA Blanka (Tchécoslovaquie)
KOLMOGOROV A. N. (U. R. S. S.) (E7)
KORANYI Adam (U. S. A.)
KORGANOFF André (France)
KORN D. G. (U. S. A.) (E3)
KOSCHMIEDER Lothar (All. de l'Ouest)
KOSHELEV A. I. (U. R. S. S.)
KOSINSKI Antoni (U. S. A.)
KOSKAS Maurice (France)
KOSMANN Yvette (France)
KOSNIOWSKI Czeslaw (Grande-Bretagne)
KOSTANT Bertram (U. S. A.) (D2)
KOSTRIKIN A. I. (U. R. S. S.) (B1)
KOSZUL J. L. (France)
KOVARI Thomas (Grande-Bretagne)
KOZOBROD V. P. (U. R. S. S.)
KRABBE Gregers (U. S. A.)
KRAINES David (U. S. A.)
KRAJA Osman (Albanie)
KRAJNAKOVA Dorota (Tchécoslovaquie)
KRAMER LASSAR Edna (U. S. A.)
KRASNER Marc (France) *
KRASOVSKY N. N. (U. R. S. S.) (E4)
KREE Paul (France)
KREISS Heinz O. (U. S. A.) (E8)
KRESS Rainer (All. de l'Ouest)
KRETTEK
KRIEF Henry (France)
KRIEGER Wolfgang (U. S. A.)
KRIPKE Saul A. (U. S. A.) (A)
KRISHNAN Viakalath (U. S. A.)
KRISTENSEN Leif (Danemark)
KRONHEIMER Erwin (Grande-Bretagne)
KRUSE Arthur (U. S. A.)
KRUSKAL Martin (U. S. A.)
KRYGOWSKA Zofia (Pologne) (F2)
KUBILIUS J. P. (U. R. S. S.) *
KUBOTA Tomio (Japon) (B4)
KUHNERT (All. de l'Est)
KUICH Werner (Autriche)
KUIPER Nicolaas (Pays-Bas) (C2)
KUIPERS L. (U. S. A.) *
KULIKOVSKII A. G. (U. R. S. S.) (E3)
KULKARNI Bavindra (All. de l'Ouest)
KUNZ Ernst (All. de l'Ouest)
KURAN Ulku (Grande-Bretagne)
KURANISHI Masatake (U. S. A.) (C4)
KURATOWSKI Kazimierz (Pologne)
KUREPA Svetozar (Yougoslavie)
KURODA S. T. (Japon) (D3)
KURODA Sigekatu (U. S. A.)
KURSMAN Robert P. (U. S. A.)
KURSS Hebert (U. S. A.)
KURZWEIL Jaroslav (Tchécoslovaquie)
KUTTNER Brian (Grande-Bretagne)
KUYK Willem (Belgique)
KUZNETZOV Yu. A. (U. R. S. S.) *
KVESELAVA D. A. (U. R. S. S.)
KWAPIEN S. (Pologne)

L

LABARRE Jr. Anthony (U. S. A.)
LACHAUD Gilles (France)
LACROIX Norbert (Canada)
LADYJENSKAIA O. A. (U.R.S.S.)
LAFON Jean-P. (France)
LAFON Monique (France)
LAHA R. G. (U. S. A.) *
DE LA HARPE Pierre (Grande-Bretagne)
LAITOCH Miroslav (Tchécoslovaquie)
LALAGUÉ Pierre (France)
LAL DUGGAL Krishan (Canada)
LAMAN Gerald (Pays-Bas)
LAMBERT John (Grande-Bretagne)
LAMBERT John D. (Grande-Bretagne)
LAMBERT Pol V. (Pays-Bas)
LA MENZA Francisco (Argentine)
LA MOUCHE
LAMOUREUX Claude (France)
LANCASTER Peter (Canada) *
LANCE Christophe (Grande-Bretagne)
LANCHON Hélène A. (France)
LANDESMAN Peter (U. S. A.)
LANDMAN Alain (U. S. A.)
LANGE Horst (All. de l'Ouest) *
LANGLANDS Robert (U. S. A.) (C5)
LANKOVA (France)
LARDNER Robin (Canada)
LASCAUX Patrick (France)
LASCOUX Jean (France)
LASHOF Richard K. (U. S. A.) (C2)
LATOUR François (France)
LAUDAL Olav (Norvège)
LAUFER Henry (U. S. A.)
LAVELLE Arthur (Grande-Bretagne)
LAVENDHOMME R. (Belgique)
LAVIGNE J.-Pierre (France)
LAVOIE Jean L. (Canada)
LAVRENTIEV M. A. (U. R. S. S.)
LAVRENTIEV M. M. (U. R. S. S.) (D10)
LAVROV S. S. (U. R. S. S.) (E7)
LAW Alan (Canada)
LAWRUK B. (Canada)
LAWVERE F. William (Canada) (B2)
LAX Peter (U. S. A.) (D11)
LAXTON Ronald (Grande-Bretagne)
LAZZERI Fulvio
LEAVITT Jay A. (U. S. A.)
LEBAUD Georges (France)
LEBLANC Noel (France)
LEBON Georgy (Belgique) *
LE DOURNEUF Jean (France)
LÊ DUNG Trang (France)
LEE Chung Nim (U. S. A.)
LEE Shing-Meng (République de Chine)
LEEDHAM-GREEN C. R. (Grande-Bretagne)
LEFRANC Marcel (France)
LEGRAN D. J.
LEGRAND Denise (France)
LEGRAND Gilles (France)
LE GRAND Pieter (Pays-Bas)
LEGRAND Solange (France)
LEHMANN Daniel (France)
LEHMANN Mme Josiane (France)
LEHMANN N. Joachim (All. de l'Est)
LEHNER Guydo R. (U. S. A.)
LEHRER Gustav (Grande-Bretagne)

EHRER ILAMED Yehiel (Israël)
EHTO Olli (Finlande)
EIBOVIC Nicholas (U. S. A.)
EIGHTON Walter (U. S. A.)
EIMANIS Eugène (Canada)
EINDLER Lázló (Hongrie) *
EIPNIK Roy (U. S. A.)
EKKERKERKER C. G. (Pays-Bas)
EKO Marko (Yougoslavie) *
ELAND Kenneth O. (U. S. A.)
E LIONNAIS François (France)
ELONG Pierre (France)
ELONG-FERRAND Jacqueline (France)
EMAIRE Claude (Belgique) *
EMMENS Petrus W. (Grande-Bretagne)
ENAGAN Thomas (Grande-Bretagne)
ENGAGNE Guy (France)
ENZING Helmut (All. de l'Ouest)
EONARD Pierre (France)
EONOR Concepcion (U. S. A.)
ÉPINGLE Dominique (France)
E POTIER (France)
ERAY Jean (France)
ESIEUR Léonce (France)
ETAC Gérard (France)
E THANK-PHONG (France)
EVEQUE William (U. S. A.)
EVIN Frank (U. S. A.)
EVIN Martin (U. S. A.)
EVINE Jérôme (U. S. A.) (C2)
EVITAN B. M. (U. R. S. S.) (D3)
EVITT Normann
ÉVY Paul (France)
ÉVY-BRUHL Jacques (France)
EWIS Donald J. (U. S. A.)
EWIS Jeff E. (U. S. A.)
HEUREUX James (U. S. A.)
[BERMANN Paulette (France)
[CHNEROWICZ André (France) (E2)
[CKORISH W. B. Raym. (Grande-Bretagne)
[EBECK Hans (Grande-Bretagne)
[EBLEIN Julius (U. S. A.)
[GAUD Jean-Pierre (Maroc)
[GOZAT Gérard (France)
INDENSTRAUSS Joram (Israël) (D1)
[NGUA Pierre (Italie)
[NNIK Y. V. (U. R. S. S.) (E6)
[ONS Jacques-Louis (France) (D11)
[PINSKI J. (Pologne)
[U Shih-Chao (République de Chine)
[ULEVICIUS Arunas (U. S. A.)
[VERANI Francesco (Italie)

LJUNGGREN Wilhem (Norvège)
LLUIS Emilio (Mexique)
LOESCH Friedrich (All. de l'Ouest)
LOETTGEN Ulrich (All. de l'Ouest)
LOHOUE Noël
LOJASIEWICZ S. (Pologne) (C4)
LOMBARDI Yves
LONDON Hymie (Canada)
LONSTED Knud (Danemark)
LOPEZ DE MEDRANO Santiago (Mexique) (C2)
LORCH Edgar (U. S. A.)
LORCH Lee (Canada)
LORENZ Falko (All. de l'Ouest)
LORIS-TEGHEM Jacqueline (Belgique)
LOSEY Gérald (Canada)
LOSEY Nora (Canada)
LOSONCZI László (Hongrie)
LOUD Warren S. (U. S. A.)
LOVASZ Laszlo (Hongrie)
LOVORKA Tomasic (Yougoslavie)
LUBIN Clarence (U. S. A.)
LUCAS Keith (Grande-Bretagne)
LUCAS Thierry (Belgique)
LUDWIG Garry (Canada)
LUE Abraham (Grande-Bretagne)
LUKACS Eugène (Autriche) *
LUNA Domingo
LUNDSGAARD HANSEN Vagn (Grande-Bretagne)
LUPANOV O. B. (U. R. S. S.) (E7)
LUPO Filomena (U. S. A.)
LYNN Erbe (Canada)

M

MAC CLUER Charles (U. S. A.)
MACDONALD J. G. (Grande-Bretagne)(C5)
MAC DONNELL John (U. S. A.)
MACHADO Armando (Portugal)
MACHENRY Trueman (Canada)
MACHI A.
MACHIZ Joan (Grande-Bretagne)
MACINTYRE Angus (Grande-Bretagne)
MACK Cornelius (Grande-Bretagne)
MACKEY George W. (U. S. A.) (D2)
MAC LANE Saunders (U. S. A.)
MAC LEOD Robert (Canada)
MACLEOD Roderick (Grande-Bretagne)
MAC MAHON James (Irlande)
MACPHAIL Moray (Canada)
MADLENER Klaus E. (All. de l'Ouest)
MADORE John (France)
MADSEN Gutmann (Danemark)

MADSEN Kaj (Danemark)
MAEZAWA Seiichiro (Japon) *
MAFFIOLI Franco
MAGARIAN Elisabeth (U. S. A.)
MAGENES Enrico (Italie)
MAHAMMED Norredine (France)
MAHJOUB Bechir (Tunisie)
MAHOWALD Mark E. (U. S. A.)
MAILHOS Line (France)
MAIRE Henri M. (Suisse)
MAJUMDAR Samir R. (Canada)
MALET Henri (France)
MALGRANGE Bernard (France)
MALLIAVIN M.-Paule (France)
MALLIAVIN Paul (France)
MALON Stanislas (Tchécoslovaquie)
MAMATOV M. (U. R. S. S.)
MAMMITZSCH Volker (All. de l'Ouest)
MAMMOUTH Claude (France)
MAMOURIS Athanasios (Grèce)
MANACORDA Tristano (Italie)
MANDELBAUM Richard (U. S. A.)
MANDJAVIDZE G. F. (U. R. S. S.) *
MANDELKER Mark (U. S. A.) *
MANDRELLA Renate (All. de l'Ouest)
MANFREDI Bianca (Italie)
MANIA G. M. (U. R. S. S.) *
MANIN Y. I. (U. R. S. S.) (B4)
MANN Horst (All. de l'Ouest)
MANOLOV Spas (Bulgarie)
MANTEL Nathan (U. S. A.)
MANUCEAU Jérôme (France)
MARATHE Kishore (U. S. A.)
MARCHUK G. I. (U. R. S. S.) (G)
MARCONI Paulo (Italie)
MARDEN Morris (U. S. A.)
MARDEŠIC' Sibe (Yougoslavie)
MARÉCHAL Odile (France)
MARIC Vojislav (Yougoslavie)
MARIJA Vencelj (Yougoslavie)
MARINI Alberto (Italie)
MARINKA Feratic (Yougoslavie)
MARKSJÖ Bertil (Suède)
MARLEY Gerald (U. S. A.)
MARQUETTY Antoine
MARRY Pierre D. (France)
MARTENS Henrik H. (Norvège)
MARTIN Benjamin (U. S. A.)
MARTIN George (U. S. A.)
MARTIN Nigel (Grande-Bretagne)
MARTINDALE Wallace (U. S. A.) *
MARTINEAU André (France) (D8)
MARTINET Jacques (France) *
MARTINEZ NAVEIRA Antonio (Espagne)
MARTIN GUZMAN Maria P. (Espagne)
MARTINOV Nikola (Bulgarie)

MARTINS Philipp
MARTSHENKO V. A. (U. R. S. S.)
MASANI Pesi (U. S. A.)
MASCORT Olga (France)
MASLOV V. P. (U. R. S. S.) (D10)
MASSAZA Carla (Italie)
MATHER John (U. S. A.) (C4)
MATHIAK Karl (All. de l'Ouest)
MATHIAS Adrian R. (Grande-Bretagne)
MATHIEU Gérard (France)
MATHIS Robert (U. S. A.)
MATSUMOTO Hideya (France)
MATSUSHIMA Yozo (U. S. A.)
MATTHEWS Geoffrey (Grande-Bretagne)
MATIJASEVIČ Y. V. (U. R. S. S.) (A)
MAUDE Ronald (Grande-Bretagne)
MAURER Christian (Grande-Bretagne)
MAURO Santi A. (Côte-d'Ivoire)
MAUTNER Friederic (France)
MAVINGA Honoré (Belgique)
MAVRON Vassili (Grande-Bretagne
MAWHIN Jean (Belgique)
MAXWELL Edwin (Grande-Bretagne)
MAY Kenneth (Canada)
MAYER Karl (All. de l'Ouest)
MAYER Stephen (Grande-Bretagne)
MAYOH Grete (Danemark)
MAZARAKIS George (Grèce)
MAZAT Françoise (France)
MAZET Pierre (France)
MAZZOLA Venzo (Suisse)
MC ARTHUR Charles (U. S. A.)
MC CARTNEY James R. (Grande-Bretagne)
MC CONNEL James R. (Irlande)
MC CRORY Clinton (U. S. A.)
MC DONOUGH Thomas (Grande-Bretagne)
MC DUFF Dusa (Grande-Bretagne)
MC KILLIGAN Sheila (Grande-Bretagne)
MC LAUGHLIN Harry (U. S. A.)
MC NAME John (Canada)
MC QUEEN Paul C. (Canada)
MEDEK Vaclav (Tchécoslovaquie)
MEHRA K. L. (Canada)
MEIJERINK Koos (Pays-Bas)
MEISE Reinhold (All. de l'Ouest)
MEJER H. G. (Pays-Bas)
MELCHIOR Ulrich (All. de l'Ouest)
MELDRUM John D. (Grande-Bretagne)
MÉNARD Jean (Canada)
MENDEL
MENDÈS FRANCE Michel (France) *
MENY Georges (France)
MENZEL Klaus (All. de l'Ouest)
MEREDITH Patrick (Grande-Bretagne)
MERGUELIAN S. N. (U. R. S. S.) (D9)
MEROVCI Ymer (Yougoslavie)
METELLI Claudia (Italie)
MÉTIVIER Michel (France)
METZGER Pierre (France)
MEYER Yves (France) (D9)
MEYNIEUX Robert M. (France)
MICHAEL Ernest (U. S. A.)
MICHAUD Pierre C. (France)
MICHEL René (France)
MICHON Gérard (France)
MIGLIORATO Renato
MIHAI Alexandre (Roumanie)
MIKLOSKO Josef (Tchécoslovaquie) *
MIKOLAS Miklos (Hongrie) *
MILIC Svetozar (Yougoslavie)
MILLER D. D. (U. S. A.)
MILLER John J. H. (Irlande)
MILLER Leonhard (U. S. A.)
MILLETT Kenneth (U. S. A.)
MILLIONŠČIKOV V. M. (U.R.S.S.) (D12)
MILLOUX Henri (France)
MIMURA Yukio (Japon)
MINTZ George
MIRANDA Mario (Italie) (D11)
MIRBAGHERI Ahmad (Iran)
MISCHENKO A. S. (U. R. S. S.) (C2)
MIŠIK Ladislav (Tchécoslovaquie)
MISLIN Guido (U. S. A.)
MITCHELL Joséphine (U. S. A.)
MITROPOLSKY Iu. A. (U. R. S. S.) *
MITROVIĆ Dragisa (Yougoslavie) *
MITTAS Jean (Grèce)
MITTEAU J.-Claude (France)
MOCH François (France)
MOGYORODI Jozsef (Hongrie)
MOHN Karl H. (All. de l'Ouest)
MOISE Edwin E. (U. S. A.)
MOISHEZON Boris (U.R.S.S.) (D8)
MOKOBODZKI Gabriel (France) (D5)
MOLINARO Italico (France)
MOLINO Pierre (France)
MOLTSHANOV A. M. (U.R.S.S.)
MONJARDET Bernard (France)
MONK Donald (U. S. A.)
MONSKY Paul (U. S. A.) (B5)
MONTESINOS Vicente
MONTGOMERY Deane (U. S. A.)
MOODY Robert V. (Canada)
MOORE Berrien (U. S. A.)
MOORE Calvin C. (U. S. A.) (D2)
MOORE John (U. S. A.)
MOORE John C. (U. S. A.) (B2)
MORAWETZ Cathleen (U. S. A.)
MORDELL Louis J. (Grande-Bretagne)
MOREAU J.-Jacques (Canada)
MORENO Carlos J. (U. S. A.)
MORET-BAILLY Françoise (France)
MORGADO Jr José (Brésil)
MORGAN Kathryn (U. S. A.)
MORICZ Ferenc A. (Hongrie)
MORREY Charles (U. S. A.) (D11)
MORRIS Grainger (Australie)
MORRIS Rosa M. (Grande-Bretagne)
MOSER Jurgen (U. S. A.)
MOSS Cyril (Grande-Bretagne)
MOSS Robert M. (Grande-Bretagne)
MOSSINO Jacques (France)
MOSTOW George D. (U. S. A.) (C3)
MOTCHANE Léon (France)
MOTHON Bernard (France)
MOTZKIN Elhan (France)
MOTZKIN Theodore (U. S. A.)
MOUKOKO PRISO Paul (France)
MOULIS Michel (France)
MOULIS Nicole F. (France)
MSEVETT Allan (Grande-Bretagne)
MUHLRAD Greif C. (France)
MUHLY Paul (U. S. A.)
MULDOON Martin (Canada)
MULHALL Harold (Australie)
MÜLTHEI Heinrich (All. de l'Ouest) *
MUMFORD David (U. S. A.) (B5)
MUNROE Evans (U. S. A.)
DE MUNTER Paul (Belgique)
MURDESHWAR Mangesh (Indes)
MURPHY Timothy (Irlande)
MURRE Jacob P. (Pays-Bas)
MURTY Usr (Canada)
MUSKHELISHVILI N. I. (U.R.S.S.)
MUSTAFA Abdalla (Grande-Bretagne)
MUWAFI Amin (Liban)
MYERS Donald (U. S. A.)
MYERS Peter (U. S. A.)
MYSAK Lawrence (Canada)

N

NACHBIN Leopoldo (U. S. A.)
NAGAEV S. V. (U. R. S. S.)
NAGAMI Keio (Japon) (C1)
NAGASAWA Masao (Japon)
SZ-NAGY Bela (Hongrie) * (D3)

NAIMAR R. A. (U. R. S. S.)
NAIMARK M. A. (U. R. S. S.) (D2)
NAIMPALLY Som. A. (Indes)
NAKANO Takeo (Japon)
NAKASSIS Anastase (France)
NARASIMHAN M. S. (Indes) (C3)
NARASIMHAN Ramabhadran (All. de l'Ouest)
NASIM Cyril (Canada)
NASR Saad K. (Egypte) *
NASTOLD Hans (All. de l'Ouest)
NATHANSON Melvyn B. (U. S. A)
NEDERSKI Petar
NEF Walter (Suisse)
NEFTIDJI Phèdre (Grèce)
NEGREPONTIS Stelios (Grèce)
NEGRO Angelo (Italie)
NELIUS Christian (All. de l'Ouest)
NELSON Paul (U. S. A.)
NENG CHE YEH (Thaïlande)
NÊRON André (France)
NETANYAHU Elisha (Israël)
NEUBERGER John W. (U. S. A.)
NEUBRUNN Tibor (Tchécoslovaquie)
NEUMANN Bernhard (Australie)(B1)
NEUNZERT Helmut (All. de l'Ouest) *
NEUSTADT L. W. (U. S. A.) (E4)
NEVANLINNA Rolf (Finlande)
NEVES D'OLIVEIRA Graciano (Portugal)
NEVEU Jacques (France)
NEWELL David (U. S. A.)
NEWELL Martin (Grande-Bretagne)
NEWELL Virginia (U. S. A.)
NEWHOUSE Sheldon (U. S. A.)
NEYRAND Hugues (France)
NG Kung-Fu (Hong-Kong)
NGUYEN HUU VINH (France)
NGUYEN-PHONG Chau (France)
NGUYEN Thank Van (France)
NIANG S. (Sénégal)
NICHOLLS Peter J. (Grande-Bretagne)
NICHOLS Eugène (U. S. A.)
NICHOLSON Victor (U. S. A.)
NICOLACOPOULOU Jeanne (Grèce)
NICOLAS Jean L. (France)
NICOLESCU Miron (Roumanie)
NIELSEN Ole (Canada)
NIEMINEN Toivo (Finlande)
NIETO Joseph (Canada)
NIJDAM Wietze (Pays-Bas)
NIKOLSKII S. M. (U. R. S. S.)
NILSSON Nils (Suède)
NIRENBERG Louis (U. S. A.)
NIRMALA Prakash (Indes)
NITSCHE Johannes (U. S. A.)
NOBLE Mark E. (Grande-Bretagne)
NOEL Guy (Belgique)
NOHEL John A. (U. S. A.)
NORMAND Gérard (Canada)
NOSAL Miloslav (Canada)
NOTTROT Roel (Pays-Bas)
NOVERRAZ Philippe (France)
NOVIKOV S. (U. R. S. S.) (C1)
NUNEZ Maria Car (France)

O

OBATA Morio (Japon)
OBERAI Kirti (Canada)
OBERDOERFFER Jacques (France)
OBOLASHVILI E. I. (U. R. S. S.)
OBRETONOV Apostol (Bulgarie)
O'BRIEN Stephen (Irlande)
OEHMKE Robert (U. S. A.)
OGG Frank G.
OHEIX Madeleine (France)
OHKUMA Tadashi (U. S. A.)
OKILJEVIC Blazo (Yougoslavie)
OKUBO Tanjiro (Canada) *
OLAH Gyula (Hongrie)
O'LEARY Cornelius (Irlande)
OLECH Czeslaw (Pologne) (E4)
OLEINIK O. A. (U. R. S. S.) (D10)
OLIVEIRA BENDER Joana (Brésil)
OLKIN Ingram (U. S. A.)
OLSON Loren (Norvège)
OLSSON Jorn (Danemark)
OLUBUMMO Adegoke (Nigéria)
OMAHONY Rosalie (U. S. A.)
OMORI Hideki (Japon)
ONICESCU O. (Roumanie)
ONTIVEROS PINEDA August
OORT Frans (Pays-Bas)
OPEER Gerhard (All. de l'Ouest)
OPIAL Zdzislaw (Pologne)
OPPENHEIM Jos (U. S. A.)
ORLAND Georges H. (U. S. A.)
ORLOV Konstant (Yougoslavie)
ORNSTEIN Avraham (Israël)
ORNSTEIN Donald (U. S. A.) (D6)
ORZECH Gret (Canada)
ORZECH Mooris (Canada)
OSBORN Marshall (U. S. A.)
OSGOOD Charles (U. S. A.)
OSHEA Siobhan (Irlande)
OSHER Stanley (U. S. A.)
OSIUS Gerhard (All. de l'Ouest)
OSTIANU N. M. (U. R. S. S.)
OSTROM T. G. (U. S. A.)
OSTROWSKI Alexander (Suisse)
OTT Udo (All. de l'Ouest)
OVSIANNIKOV L. V. (U. R. S. S.) (E3)
OWENS Robert (Grande-Bretagne)

P

PAARDEKOOPER M. H. C. (Pays-Bas)
PACHECO de AMORIM José B. (Portugal)
PACIOREK Joseph W. (U. S. A.)
PACQUEMENT Charles (Madagascar)
PAIGE Lowell (U. S. A.)
PALAIS Richard (U. S. A.) (C4)
PALAJ Cyril (Tchécoslovaquie)
PALIS Jacob (France)
PALLAS Aristidis (Grèce)
PALMGUIST Janet (U. S. A.)
PALMGUIST Paul (U. S. A.)
PANDEY J. N. (Canada)
PANFILOV P. S. (U. R. S. S.)
PAPACOSTAS G.
PAPIC' Pavle (Yougoslavie)
PAPY Georges (Belgique)
PAQUETTE G. (Canada)
PARE Robert (Canada)
PAREIGIS Bodo (All. de l'Ouest)
PARKER Francis (U. S. A.)
PARKER Monique (Belgique)
PARRY William (Grande-Bretagne) (D12)
PARŠIN A. N. (U. R. S. S.) (B5)
PARTHASARATHY Kalyanapu (Grande-Bretagne)
PARTOUCHE Jacqueline (France)
PASZTOR ENDRENE Katalin (Hongrie)
PATKOWSKA H. (Pologne)
PATTERSON Edward (Grande-Bretagne)
PAYNE Lawrence (U. S. A.)
PEARS Alan R. (Grande-Bretagne)
PEDERSEN Gert (Danemark)
PEDOE Daniel (U. S. A.)
PEETRE Jaak (Suède) (D1)
PEINADO Rolando E. (Porto-Rico)
PEIXOTO Mauricio
PELCZYNSKI Alex (Pologne)
PELL Williams (U. S. A.)
PENEL Patrick (France)
PENOT Jean-Paul (France)
PENRY Mervyn (Grande-Bretagne)
PEPPER Jon V. (Grande-Bretagne)
PERCELL Peter (U. S. A.)
PERDICOURIS Agellos (Grèce)
PERDRIZET François (France)
PEREIRA-GOMES Alfredo (France)
PEREMANS Wouter (Pays-Bas)
PEREZ Francisco
PERFECT Hazel (Grande-Bretagne)
PERRIN Henri (France)
PERROT Bernard (France)

PERRY Roy (Grande-Bretagne)
PERSSON Jan (Italie)
PESAMOSCA Giancarlo (Italie)
PESCHL Ernst (All. de l'Ouest)
PETCANTCHINE Boiane (Bulgarie)
PETERS George (U. S. A.)
PETERS Klaus (All. de l'Ouest)
PETERS Meinhard (All. de l'Ouest)
PETERSON Franklin (U. S. A.) (C2)
PETIT Jean-Claude (France)
PETRAQ Pilika (Albanie)
PETRI Jan (Belgique)
PETRICH Mario (U. S. A.) *
PETRIE Ted (U. S. A.)
PETROVA Zlaszka S. (Bulgarie)
PETRY Walter (All. de l'Ouest) *
PETTINI Giovanna (Italie)
PFISTER Albrecht (All. de l'Ouest) (B1)
PFLUGER Albert (Suisse)
PFLUGFELDER Hala (U. S. A.)
PHAM Frédéric (France) (D8)
PHAM Mau Quan (France) *
PHAM Tan Hoang (France)
PHELPS Robert R. (U. S. A.)
PHILLIPS Ralph (U. S. A.) (D10)
PICCARD Sophie (Suisse) *
PICCININI Livio Cl. (Italie)
PICHAT Étienne (France) *
PICHLER Franz (Autriche)
PIEPER Irene (All. de l'Ouest)
PIER Jean-Paul (Luxembourg)
PIETSCH Albrecht (All. de l'Est) *
PIGNEDOLI Antonio (Italie)
PIMBLEY George H. (U. S. A.) *
PINL M. (All. de l'Ouest)
PINTACUDA Nicolo (Italie)
PIQUET Claude (France)
PISANELLI Domingos (Brésil)
PITCHER Everett,(U. S. A.)
PITTIE Harsh V. (U. S. A.)
PIXLEY Alden (U. S. A.)
PLA Jean-M. (France)
PLAFKER Stephen (U. S. A.)
PLANCHARD Jacques (France)
PLANS Antonio (Espagne)
PLANT Andrew (Grande-Bretagne)
PLATZKER Ovadia (Israël)
PLEIJEL Åke (Suède)
PLYMEN Roger J. (Grande-Bretagne)
POGORELOV A. V. (U. R. S. S.) (C3)
POGUNTKE Detlev (All. de l'Ouest)
POHL William F. (U. S. A.)
POITOU Georges (France)
POLLACZEK Felix (France)
POLLAK Henry O. (U. S. A.) (F2)
POLLINGHER Adoef (Israël)
POLY (France)
POMERANZ Janet Bellcourt (U. S. A.)
PONTRYAGIN L. (U. R. S. S.) (G)
POPOV Vasil (Bulgarie)
POPOVICIU Tiberiu (Roumanie)
PORITZ Alan B. (U. S. A.)
PORTE Jean (Congo)
PORTENIER Claude (Suisse)
PORTEOUS Hugh L. (Grande-Bretagne)
PORTEOUS Ian Rober (Grande-Bretagne)
PORTER Don (U. S. A.)
PORTER Gerald J. (U. S. A.)
POTAPOV M. K. (U. R. S. S.)
POURCHET Yves (France)
POUR-EL Marian B. (Grande-Bretagne)
POUZET Maurice (France)
POZNIAK E. G. (U. R. S. S.) *
POZZI-ARRIGO Gianni
PRELLER Anne (France)
PRETZEL Olivier (Grande-Bretagne)
PREUSS Gerhard (All. de l'Ouest) *
DE PRIMA Charles (U. S. A.)
PRIMROSE Erici J. (Grande-Bretagne)
PROCESI Aveasis
PROCESI Claudio (U. S. A.)
PRODANOV Ivan (Bulgarie)
PROKHOROV Iu. V. (U. R. S. S.)
PROSSER (U. S. A.)
PROSSER Reese (U. S. A.)
PROTTER Murray H. (U. S. A.)
PROUSE G. (Italie) *
PRVANOVIC Mileva (Yougoslavie)
PUGH Charles (U. S. A.) (D12)
PUKANSZKY Lajos (U. S. A.) (D2)
PUPIER René (France)
PUTNAM Alfred L. (U. S. A.)

Q

QUENNET Jean (France)
QUILLEN Daniel G. (U. S. A.) (C1)
QUINTERO Francisco (France)

R

RABECHAULT Michel (France)
RABIN Michael (Israël) (A)
RABINOWITZ Philip (Israël)
RACHFORD Henry Herbert (U. S. A.)
RADO Peter A. (Grande-Bretagne)
RADO Richard (Grande-Bretagne)
RAGHUNATHAN M. S. (Indes) (C5)
RAGOZIN David (U. S. A.)
RAIMI Ralph (U. S. A.)
RAMADANOV Ivan (Bulgarie)
RAMAKRISHNA RAO Darbha (Iran)
RAMASWAMY Sundarara (France)
RAMSPOTT Karl (All. de l'Ouest)
RANGER K. B. (Canada)
RANKIN Robert A. (Grande-Bretagne)
RAO M. M. (U. S. A.)
RAO Veldanda (Canada)
RAOULT Jean-Pierre (France)
RAPCSÁK András (Hongrie)
RAUDELIUNAS A. K. (U. R. S. S.)
RAUTMANN Reimund (All. de l'Ouest) *
RAVDIN Davon
RAY Ajit Kum (Canada)
RAY Nigel (Grande-Bretagne)
RAY-CHAUDHURI D. K. (U.S.A.) (E5)
RAYMOND Bernard (France)
RAYNAUD Hervé (France)
RAYNAUD Michel (France) (B5)
RAYNER Francis (Grande-Bretagne)
RAYNER Margaret (Grande-Bretagne)
READE Maxwell (U. S. A.) *
RECILLAS Félix (Mexique)
REE Rimhak (Canada)
REED Jon (Norvège)
REED Michael (U. S. A.)
REES Elmer (Grande-Bretagne)
REES Mary Reb. (Grande-Bretagne)
REEVE John (Grande-Bretagne)
REGGE Tullio (Italie) (E1)
REICH Edgar (U. S. A.)
REICHERT Marianne (All. de l'Ouest)
REID Miles A. (Grande-Bretagne)
REITBERGER Heinrich (Autriche)
REITER Hans (Pays-Bas)
RENAUD André (France)
RENAULT Guy (France)
VON RENTELN (All. de l'Ouest)
REŠETNYAK Y. G. (U. R. S. S.) (D7)
REUTTER Fritz Karl (All. de l'Ouest)
REVUZ André (France)
REYNAUD Gérard (France)
REZA Fazlollah (France)
REZNIKOFF Iegor (France)
DE RHAM Georges (Suisse)
RHEMTULLA Akbar H. (Canada)
RHIN Georges Robert (France)
RIABUKHINE Yu. M. (U.R.S.S.) *
RIAZA PEREZ Roman (Espagne)
RIBARIC Marjan (Yougoslavie)

.IBEIRO Hugo (U. S. A.)
'*IBEIRO GOMES Antonio* (Portugal)
.IBENBOIM Paulo (France)
.ICCA Giuseppe
.ICCI Giovanni (Italie)
'*ICE Peter M.* (U. S. A.)
.ICHARDS I. (U. S. A.)
'*ICHTER W.* (All. de l'Est)
.ICHTER Gunther (All. de l'Ouest)
'*ICHTER Hans* (All. de l'Ouest)
.IDEAU François (France)
.IDEAU Guy (France)
.IDER Daniel (U. S. A.) (D4)
IECAN Beloslav (Tchécoslovaquie)
IESEL Hans (Suède)
IGBY John F. (Grande-Bretagne)
IGOLOT Alain (France)
IGOLOT Mme (France)
INGEL Claus (All. de l'Ouest)
ISTO Ilic J. (Yougoslavie)
IVET Roger (France)
IVLIN Théodore (U. S. A.)
IZYANOLLI Fuat (Yougoslavie)
IZZA Giovanni (Italie)
OBERT Alain (U. S. A.)
OBERT Jacques (France)
OBERT Pierre (France)
OBERTSON Mark M. (Grande-Bretagne)
OBIN Guy (France)
OBINOW Richard (Grande-Bretagne)
OBINSON Abraham (U. S. A.) (A)
OBINSON William (Grande-Bretagne)
OBSON James (Grande-Bretagne)
OCHE Claude (France)
OCOS Pantelis (France)
ODGERS Dykes
ODRIGUEZ-SALINA Balthasar (Espagne)
OESSLER Alfred (All. de l'Ouest)
OGERS Hartley (U. S. A.)
OGOSINSKI Hans (Grande-Bretagne)
OHLEDER Hans (All. de l'Est)
OHRL Helmut (U. S. A.) (C1)
OJO MORALES Jorge (Chili)
OLLAND Robert (France)
OMILLY Nicholas (Grande-Bretagne)
ONVEAUX A. (Canada)
OONEY Paul G. (Canada)
OOS Guy (France)
OOS Jan Erik (Suède)
OPARS Alain (France)
OSA Alexander (Canada)
OSEAU Maurice (France) (E3)
OSEBLADE James (U. S. A.)

ROSEMAN Joseph (U. S. A.)
ROSÊNFELD Norman S. (U. S. A.)
ROSENLICHT M. (U. S. A.)
ROSENTHAL Edward (Canada)
ROSENTHAL Haskell (U. S. A.)
ROSENTHAL Peter (Canada)
ROSINI Maria Lydia (Italie)
ROSSKOPF Myron (U. S. A.)
ROTA Gian C. (U. S. A.) (E5)
ROTH Klaus F. (Grande-Bretagne)
ROTHBERGER Fritz (Canada)
ROTMAN Joseph (U. S. A.)
ROURKE C. P. (Grande-Bretagne) (C2)
ROUXEL Bernard (France)
ROWLEY Christoph (Grande-Bretagne)
ROZANOV Iu. A. (U. R. S. S.)
ROZSA Pal (Hongrie)
RUBEL Lee (U. S. A.)
RUBIO Baldomero (Espagne)
RUCKLE William (U. S. A.)
RUDIN Mary El. (U. S. A.)
RUDIN Walter (U. S. A.) (D4)
RUDOLFER Stephan (Grande-Bretagne) *
RUELLE David (France) (E1)
RUFFET Jean (Suisse)
RUGGERI Tomaso
RUSSE Assunta (Italie)
RUSSELL Dennis (Canada)
RUSSEV Peter (Bulgarie)
RÜSSMANN Helmut (All. de l'Ouest) *
RUSTON Antony F. (Grande-Bretagne)
RUTLEDGE William (U. S. A.)
RUTTER John (Grande-Bretagne)
RYSER Herbert (U. S. A.) (E5)

S

SABBAGH Gabriel (France)
SACKS Gerald E. (U. S. A.) (A)
SACKS Jonathan (Afrique du Sud)
SADOLIN Viggo (Danemark)
SAFIUL Haq M. (Canada)
SAINT-JEAN-PAULIN Jeannine (France)
SAINTLOUP Bernard (France)
SAINT-PIERRE Jacques (Canada)
SAITO Kyoji (All. de l'Ouest)
SAKUMA Motoyoshi (France)
SALAKHITDINOV M. S. (U.R.S.S.)
SALT Tibor (Tchécoslovaquie)
SAMARSKY A. A. (U. R. S. S.) (E8)
SAMELSON Hans (U. S. A.)
SAMUEL Christian (France)

SAMUEL Pierre (France)
SANCHEZ ALONSO Margarita (France)
SANCHEZ FERNAND Carlos (France)
SANCHEZ GIRALDA Tomas (Espagne)
SANCHEZ-PALENCIA Enrique (France)
SANCHO SAN ROMAN Juan (Espagne)
SANDS Arthur (Grande-Bretagne)
SANKARAN N. (Indes)
SANKARAN Subraman. (Grande-Bretagne)
SANSONE Giovanni (Italie)
SANSUC Jean J. (France)
SANTI Donato
SANTOBONI Luigi (Italie)
DE SAPIO Rodolfo (U. S. A.)
SARIMSAKOV T. A. (U. R. S. S.)
SARMENTO Maria F. (Grande-Bretagne)
SARRA Maria (Italie)
SATAKE Ichiro (U. S. A.)
SATO Hajime (Japon)
SATO Mikio (Japon) (D10)
SAUNDERS Frank (U. S. A.)
SAUX Marie-Thérèse (France)
SAVARIAU J. (France)
SAVITHRI Kappagant (U. S. A.)
SAXENA Subhash (U. S. A.)
SAYEKI Hidemitsu (Canada)
SAZONOV V. V. (U. R. S. S.) (D6)
SCHAAL Werner (All. de l'Ouest)
SCHAFER Alice (U. S. A.)
SCHAFER James (Danemark)
SCHAFER Richard (U. S. A.)
SCHEERER Hans (Grande-Bretagne)
SCHEFFER Carel (Pays-Bas)
SCHEIBA Jurgen (All. de l'Ouest)
SCHELTER William (Canada)
SCHEMMEL Hans (All. de l'Est)
SCHERER Karl (All. de l'Ouest)
SCHIEK Helmut (All. de l'Ouest)
SCHIFFELS Gerhard (All. de l'Ouest)
SCHILD Albert (U. S. A.)
SCHINZEL Andrzej (Pologne) (B6)
SCHIRMER Helga (Canada)
SCHLESINGER Ernest C. (U.S.A.)
SCHMETS Jean (Belgique)
SCHMID Wilfried (U. S. A.) (C5)
SCHMIDT Klaus (Autriche)
SCHMIDT Rita (All. de l'Ouest)
SCHMIDT Wolfgang (U. S. A.) (B6)
SCHNEIDER Hans (U. S. A.)
SCHNEIDER Hubert (U. S. A.)

SCHNEIDER Michael (All. de l'Ouest)
SCHNEIDER Rolf (All. de l'Ouest)
SCHNEIDER Walter (U. S. A.)
SCHNEIDER Walter (Suisse)
SCHNITZPAN Daniel H. (France)
SCHNORR Claus (All. de l'Ouest)
SCHOCHET Claude (Danemark)
SCHOENFELD Lowell (U. S. A.)
SCHOLZ Werner (All. de l'Ouest)
SCHON Bernhard (All. de l'Ouest)
SCHORI Richard (U. S. A.)
SCHOTTENLOHER Rudolf (All. de l'Ouest)
SCHREIBER Bertram (U. S. A.)
SCHREIBER Michel (France)
SCHRÖDER Kurt (All. de l'Est)
SCHUBART Hans (All. de l'Ouest)
SCHUDER Werner (All. de l'Ouest)
SCHUMACHER Barbara (All. de l'Ouest)
SCHUSTER Hans (All. de l'Ouest)
SCHUTTE Hendrik (Afrique du Sud)
SCHÜTZENBERGER M. P. (France) (E7)
SCHUUR Jerry (U. S. A.)
SCHWABHAEUSER Wolfram (All. de l'Ouest)
SCHWABHAUSER Inge (All. de l'Ouest)
SCHWARTZ Jacob (U. S. A.)
SCHWARTZ Laurent (France)
SCHWARTZ Marie (France)
SCHWARZ Binyamin (Israël)
SCHWARZ Stefan (Tchécoslovaquie)
SCHWEITZER Paul (U. S. A.)
SCHWERDTFEGER Hans (Canada)
SEAL Hilary (Grande-Bretagne)
SEED Margaret (Grande-Bretagne)
SEELEY Robert (U. S. A.) (D10)
SEGAL Graeme (Grande-Bretagne) (C1)
SEGAL Irving E. (U. S. A.) (D2)
SEGAL Sanford (U. S. A.)
SEGRE Beniamino (Italie)
SEIDEL J. J. (Pays-Bas)
SEIDEN Esther (U. S. A.)
SEINIGE Lothar (Suisse)
SELBERG Sigmund (Norvège)
SELDIN Jonathan (U. S. A.)
SELENIUS Clas-Olof (Suède)
SELIGSON Stuart A. (U. S. A.)
SEMADENI Zbigniew (Pologne)
SEN Dipak K. (Canada)
SEN R. N. (Israël)
SENDOV Blagovest (Bulgarie)
SEPER Kajetan (Yougoslavie)
SERNA Juana (U. S. A.)
SERRE Jean-Pierre (France)
SERRIN James (U. S. A.) (D11)
SESHADRI Conjeev. (Indes) (B5)
SETH Bhoj Raj (Indes)
SETHURAMAN Jayaram (U.S.A.)*
SEVASTIANOV B. A. (U. R. S. S.)
SEVERO Norman (U. S. A.)
SEWELL Walter (U. S. A.)
SEYDI Hamet (France)
SHACKELL John R. (Grande-Bretagne)
SHAFAREVICH I. R. (U. R. S. S.) (B4)
SHAFFER Dorothy (U. S. A.)
SHANESON Julius (U. S. A.)
SHANKS Merrill (U. S. A.)
SHAPIRO Harvey (U. S. A.)
SHAPIRO Victor (U. S. A.)
SHARP William (Canada)
SHARPE David (Grande-Bretagne)
SHEPP Lawrence (U. S. A.)
SHIDLOVSKII A. B. (U. R. S. S.)
SHIH Kung-Sing (République de Chine)
SHIMAMOTO (U. S. A.)
SHIMURA Goro (U. S. A.) (C5)
SHIOZAWA Yoshinori (France)
SHIPPAM G. K. (Pays-Bas)
SHIRYAYEV A. N. (U. R. S. S.) (D5)
SHKLOV Nathan (Canada)
SHORE Samuel D. (U. S. A.)
SIBIRSKII K. S. (U. R. S. S.)
SIBONY Moïse (France)
SIDDIQI J. A. (Canada) *
SIEBENMANN Laurence (U. S. A.) (C2)
SIEVEKING Malte (Suisse)
SIGMUND Karl (France)
SIGRIST François (Suisse)
SIKORSKI Roman (Pologne)
SILBERSTEIN Josef (Australie)
DE SILVA Carl (Portugal)
SIMHA Roddam R. (Indes)
SIMMONS Harold (Grande-Bretagne)
SIMOES PEREIRA José (Portugal)
SIMON Barry (U. S. A.)
SIMON Udo (All. de l'Ouest)
SIMONS Stephen (U. S. A.)
SINAÏ J. G. (U. R. S. S.) (D12)
SINGH Kuldip (Canada)
SINGH S. P. (Canada)
SINGH U. N. (Indes)
SION Maurice (Canada) (D6)
SIRAO Tunekiti (Japon)
SIU Yun-Tong (U. S. A.)
SJODIN Gunnar (Suède)
SJOLIN Per (Suède)
SKARDA Vencil (U. S. A.)
SKENDZIC Marija (Yougoslavie)
SKLAR A. (U. S. A.)
SKODA Henri (France)
SKORDEV Dimiter (Bulgarie)
SKOROHOD A. V. (U. R. S. S.) (D6)
SKOVGAARD Helge (Danemark)
SLATER Michael (Grande-Bretagne)
SLOSS James (U. S. A.)
SLOT J. V. D. (Pays-Bas)
SMALE Stephen (U. S. A.)
SMILEY Malcolm (U. S. A.)
SMITH Anthony (Grande-Bretagne)
SMITH Edwin (Grande-Bretagne)
SMITH Hammond D. (Grande-Bretagne)
SMITH Roland (Grande-Bretagne)
SMITH Willem (Pays-Bas)
SMYRNELIS Emmanuel (France)
SMYTH Christoph (Grande-Bretagne)
SMYTH Malcolm (Irlande)
SNAJDER Zagorka (Yougoslavie)
SOBOLEV S. L. (U. R. S. S.) (F2)
SOLOMON Louis (U. S. A.)
SOLOVAY Robert (U. S. A.) (A)
SOMEN André (France)
SONNENSCHEIN Jacob (Belgique)
SONS Linda (U. S. A.)
SOTO ANDRADE Jorge (France)
SOUBLIN Jean-P. (France)
SPAGNOLO
SPATHIS Spyros (Grèce)
SPECHT Edward J. (U. S. A.)
SPECTOR René (France)
SPENCER Donald C. (U. S. A.) (C4)
SPIJKER Marc (Pays-Bas)
SPIRA Gabriel
SPRECHER D. (U. S. A.)
SPRINDŽUK V. (U. R. S. S.) (B6)
SPRING David (U. S. A.)
SPRINGER George (U. S. A.)
SPRINGER Tonny A. (Pays-Bas)
SREBRO Uri (Israël)
SRINIVASAN Bhama Mrs (Indes)
SRIVASTAN Ram (U. S. A.)
SRIVASTAVA H. M. (Canada)
SRIVASTAVA R. S. L. (Indes) *
STAKGOLD Ivar (U. S. A.)
STALLINGS John (U. S. A.) (C2)
STALLMANN Friedem (U. S. A.)
STAMM Émile (Canada)
STAMPACCHIA Guido (Italie) (D11)
STANAITIS Otonas E. (U. S. A.)
STANKOVIC Bogoljub (Yougoslavie)
STAPLES John (Grande-Bretagne)
STARK David (Italie)
STARK Harold (U. S. A.) (B6)
STATULIAVIČIUS V. A. (U. R. S. S.) *

TEČKIN S. B. (U. R. S. S.) (D4)
TEEN Lynn A. (U. S. A.)
TEENROD Norman E. (U. S. A.)
TEENSHOLT Gunnar (Norvège) *
TEER Brian (France)
TEFAN Peter (Grande-Bretagne)
TEGEMAN Jan (Pays-Bas)
TEIN Elias M. (U. S. A.) (G)
TEINER Eugène (Canada)
TEINFELD Ottó (Hongrie)
TEINLAGE Ralph (U. S. A.)
TENSTROM Bo (Suède)
TEPHENS Nelson M. (Grande-Bretagne)
TEPHENSON William (Grande-Bretagne)
TEPIN A. M. (U. R. S. S.) (D12)
TERGHIOU Georges (Grèce)
TIEFEL Edouard (Suisse)
TIEGLER Karl (All. de l'Ouest)
TIEGLITZ Andreas (All. de l'Ouest)
TOJAKOVIC Mirko (Yougoslavie)
TOLL Wilhelm (U. S. A.)
TONE Marshall (U. S. A.)
TORMER Erling (Norvège)
TRASBERG,Marcel (Belgique)
TRELLYN Jean-Marie (France)
TROMMER Gyula (Hongrie)
TROOKER Jan R. (Pays-Bas)
TRUBECKER Karl (All. de l'Ouest)
UCCI Tamarco
UCHESTON Louis (U. S. A.)
UGIURA Mitsuo (U. S. A.)
ULLIVAN Dennis (U. S. A.) (C2)
ULLIVAN Theodore (U. S. A.)
UPRUNENKO D. A. (U. R. S. S.)
URANYI Janos (Hongrie)
URAY Saffet (Turquie)
URIN Aline (France)
UTHERLAND Frame (Thailande)
UTHERLAND Wilson A. (Grande-Bretagne)
UWA Tatsuo (Japon)
UZUKI Haruo (Japon)
UZUKI Michio (U. S. A.) (B3)
UZUKI Satoshi (Japon)
VESHNIKOV A. G. (U. R. S. S.) *
WAMINATHAN Srinivasa (Canada)
WAN Richard (U. S. A.) (G)
WANSON Ellen (U. S. A.)
WEENEY William (U. S. A.)
WIFT J. Dean (U. S. A.)
YNOWIEC John (U. S. A.)
YSKI Ryszard (U. S. A.)
ZANKOWSKI Andrzej (Danemark)
ZASZ Gabor (Hongrie)
ZEKERES Georges (Australie)
ZENDREI Janos (Hongrie)
SZENTHE Janos (Hongrie)
SZEP Jenoe (Hongrie)
SZMYDT Zofia (Pologne)

T

TAAM C. T. (U. S. A.)
TAFT Earl Jay (U. S. A.) *
TAGAMLITZKI Yaroslaw (Bulgarie)
TAIMANOV A. D. (U. R. S. S.)
TAKAHASHI Moto-O. (Japon) *
TAKAHASHI Reiji (France)
TAKENS Floris (Pays-Bas)
TAKESAKI Masamichi (U. S. A.) * (D2)
TAKETA Kiyosi (Japon) *
TAKEUCHI Junji (Japon)
TALALIAN A. A. (U. R. S. S.)
TALENTI Giorgio (Italie)
TAMARI Dov (Israël)
TAMASCHKE Olaf (All. de l'Ouest)
TAMBURINI Maria (Italie)
TAMRAZOV P. M. (U. R. S. S.)
TAMURA Takayuki (U. S. A.)
TANAKA Minoru (Japon) *
TANDORI Károly (Hongrie) *
TANGORA Martin (Grande-Bretagne)
TANI MOTO Taffee (U. S. A.)
TANNER Rosalind (Grande-Bretagne)
TAPE Walter (U. S. A.)
TARGONSKI György (Suisse)
TARSKI Alfred (U. S. A.) *
TARSKI Jan
TARTAR Luc (France)
TATE John (U. S. A.) (G)
TATON René (France)
TAYLOR J. Chr. (Canada)
TAYLOR William (U. S. A.)
TCHAKALOFF Vladimir (Bulgarie)
TCHONKANOF Vladimir
TEGHEM Jacques (Belgique)
TEGHEM Jean (Belgique)
TEICHER A.
TEISSIER Bernard (France)
TEIXIDER Joseph (Espagne)
TEMAM Roger (France) (E8)
TEMPERLEY David J. (Grande-Bretagne)
TENENBAUM Marian (U. S. A.)
TENNISON Barry Roy (Grande-Bretagne)
TEODORESCO M. (Roumanie)
TERJANIAN Guy (France)
TERPSTRA Teunis (Pays-Bas)
TERRIER J. H. (Canada)
THEODOR Raymond (France)
THIAM Magatte (Sénégal)
THIRY Yves (France)
THOFT Christense Npalle (Danemark) *
THOM René (France) (C4) *
THOMAS Garth H. M. (Canada)
THOMAS Richard (Grande-Bretagne)
THOMEE Vidar (Suède) (E8)
THOMEIER Siegfried (Canada)
THOMPSON Christoph (Grande-Bretagne)
THOMPSON John (U. S. A.) (B3)
THOMSEN Donald (U. S. A.)
THOMSEN Per Grove (Danemark)
THOMSON Brian (Canada)
THORIN Olof (Suède)
THORP Edward O. (U. S. A.)
THWAITES Bryan (Grande-Bretagne)
TIMONEY Jr (Irlande)
TIMOURIAN James (Canada)
TITS Jacques (All. de l'Ouest) (C5)
TOBERGTE Jurgen (All. de l'Ouest)
TOBIN Sean (Irlande)
TOCHEV Bogidar (Bulgarie)
TOGNOLI Alberto (Italie)
TOMIC Miodrag (Yougoslavie)
TOMTER Per (Norvège)
TONDEUR Philippe (U. S. A.)
TONG Van Duc (France)
TONOLLI Antonelia (Italie)
TON THAT LONG (France)
TONTI Enzo (Italie)
TOPSOE Flemming (Danemark)
TORALBALLA L. V. (U. S. A.) *
TORELLI Alessandr (Italie)
TORNHEIM Leonard (U. S. A.) *
TORRANCE Ellen (U. S. A.)
TORRANCE Esther (U. S. A.)
TORRES IGLESIAS Miguel (Afrique du Sud)
TORTRAT Albert (France)
TOTH Imre (Hongrie)
TOTOV Gueorgui (Bulgarie)
TOUGERON Jean-Claude (France) (C4)
TOURE Saliou (Côte-d'Ivoire)
TOWERS David (Grande-Bretagne)
TRANSUE William (U. S. A.)
TRAUTMANN Gunther (All. de l'Ouest)
TREBELS Walter (All. de l'Ouest) *
TREDER J. (All. de l'Est)
TREVES François (U. S. A.) (D10)
TRONEL Gérard (France)
TRPENOVSKI Branko (Yougoslavie)
TRUDINGER Neil S. (Australie)
TSAGAS Grigorios (All. de l'Ouest)
TSHERNIKH I. I. (U. R. S. S.)

TSHERNIKOV S. N. (U. R. S. S.)
TSHOGOSHVILI G. S. (U. R. S. S.)
TUCKER C. T. (U. S. A.)
TUCKER John (Canada)
TURÁN Paul (Hongrie) (B6)
TURNER Nura (U. S. A.) *
TURNER Robert (U. S. A.)
TURQUETTE Atwell R. (U. S. A.) *
TURRELL Franklin (U. S. A.)
TUTSCHKE W. (All. de l'Est) *
TWILT Frank (Pays-Bas)

U

UDESCHINI-BRINIS Elisa (Italie)
UHL J. J. (U. S. A.)
UHLENBECK Karen (U. S. A.)
UL'JANOV P. L. (U. R. S. S.) (D9)
ULLMAN Joseph L. (U. S. A.)
ULLOM Stephen (U. S. A.)
UNGER Heinz (All. de l'Ouest)
UPSCHUTZ
URALTSEWA N. N. (U. R. S. S.) (D11)
URBANIK K. (Pologne)
USTINA Fred (Canada)
UYBORNY Rudolf (Australie)
UZGOREN Nakibe (Turquie)

V

VACCARO Giuseppe (Italie)
VAILLANT Jean-Léon (France)
VALENCIA ARVIZU Marco A. (Mexique)
VALETTE Guy (Belgique)
VALLÉE Robert (France)
VAMOS Peter (Grande-Bretagne)
VAN ALBADA Pieter (Pays-Bas)
VAN BECKUM Frederick (Pays-Bas)
VAN DEN BERG Johann J. (Grande-Bretagne)
VAN DEN BOSSCHE Gilberte (Belgique)
VAN DEN BROM Lourens (Pays-Bas)
VANDERGRAFT James (U. S. A.)
VAN DER PUT (Pays-Bas)
VAN DER WAERDEN Bartel L. (Suisse) (F1)
VAN DIJK Gerrit (Pays-Bas)
VANDOOREN René (Belgique)
VAN DULST Dick (U. S. A.)
VAN ECK H. Nico (Pays-Bas)
VAN EST W. T. (Pays-Bas)
VAN GOETHEM Pierre (U. S. A.)
VANHAMME Jacqueline (Congo)
VANHAMME Willy (Congo)
VAN ISEGHEM François (France)
VAN KEMPEN Hubert (Pays-Bas)
VAN PRAAG Paul (Belgique) *
VAN SCHEEPEN Frans (Belgique)
VAN SPIEGEL Willem (Pays-Bas)
VAQUER Joseph (Espagne)
VARADHAN Srinivasa (U. S. A.)
VARGA Laszlo (Hongrie)
VAROPOULOS Nicholas (France) (D4)
VASIC Petar (Yougoslavie)
VASILACH Serge (Canada) *
VEKUA I. N. (U. R. S. S.)
VEKUA N. P. (U. R. S. S.)
VELDKAMP Ferdinand (Pays-Bas)
VELDMAN Willem (Pays-Bas)
VELPRY Christian (France)
VELU Jacques (France)
VENKOV B. B. (U. R. S. S.)
VERCUEIL Nicole (France)
VERDIER Jean-Louis (France)
VER EECKE Paul (France)
VERGNE Michèle (France)
VESELIC Kresimir (Yougoslavie)
VESNA Tomasic (Yougoslavie)
VETTER Udo (All. de l'Ouest)
VICENTE CORDOBA José (Espagne)
VIDAL Enrique (Espagne) *
VIDICI Christian (All. de l'Ouest)
VILLAMAYOR Orlando (Argentine)
VILLE Françoise (France)
DE VILLIERS Raoul A. (U. S. A.)
VINCENSINI Paul (France) *
VINCENT Georges (Suisse)
VINCENT-SMITH Graham (Suisse)
VINTI (Italie)
VIOLA Carlo (Italie)
VIORT Bernard (France)
VISHIK M. I. (U. R. S. S.)
VISSER Cornelius (Pays-Bas)
VITANOV Alexander (Bulgarie)
VITUŠKIN A. G. (U. R. S. S.) (D4)
VIVIENTE José L. (Espagne)
VIVIER Marcel (France)
VLADIMIROV V. S. (U. R. S. S.) (E1)
VOGEL Walter (All. de l'Ouest)
VOGT Dietmar (All. de l'Ouest)
VOLKMANN Bodo (All. de l'Ouest)
VOPĚNKA Petr. (Tchécoslovaquie) (A)
VOREADOU Rodiani (Grèce) *
VOWDEN Barry (Grande-Bretagne)
DE VRIES Hendrik (Pays-Bas)
DE VRIES Rudolf (Pays-Bas)
VUJICIC Veljko (Yougoslavie) *
VYTHOULKAS Denis (Grèce)

W

WADA Junzo (Japon)
WAELBROECK Lucien (Belgique)
WAESCHE Hans (All. de l'Ouest)
WAGONER J. B. (U. S. A.)
WAGSCHAL Claude M. (France)
WAKABAYASHI Isao (Japon)
WALDSCHMIDT Michel (France)
WALKER Arthur (Grande-Bretagne)
WALKER Gordon L. (U. S. A.)
WALL Charles T. C. (Grande-Bretagne) (G)
WALLBANK Sarah (Grande-Bretagne)
WALLINGTON John Eve (Grande-Bretagne)
WALLISSER Rolf (All. de l'Ouest)
WALSH Joseph L. (U. S. A.)
WALTER Jan (Pays-Bas)
WALTHER Heinrich (All. de l'Ouest) *
WANNER Gerhard (Autriche)
WARNER Frank W. (U. S. A.)
WASSEF Pierre
WATANABE Takesi (Danemark) (D5)
WATERMAN Daniel (U. S. A.)
WATKINS Mark (U. S. A.)
WATSON George (Grande-Bretagne)
WATTERS J. Francis (Grande-Bretagne)
WEBBER David B. (Grande-Bretagne)
WEBER Claude (Suisse)
WEFELSCHEID Heinrich (All. de l'Ouest)
WEIDENFELD Michèle (France)
WEILL Georges (France)
WEINGRAM Stephen (U. S. A.)
WEINMANN Alfred (Grande-Bretagne)
WEINSTEIN Alan (U. S. A.)
WEINSTEIN Alexander (U. S. A.)
WEISFELD Morris (U. S. A.)
WEISS Guido (U. S. A.)
WELLS G. S. (Grande-Bretagne)
WELLS J. C. (Canada)
WELLS Raymond (U. S. A.)
WENDEL James G. (U. S. A.)
WERMER John (U. S. A.)
WESSELING Pieter (Pays-Bas)
WESSELIUS Willem (Pays-Bas)
WEST Alan (Grande-Bretagne)
WEST James (U. S. A.)
WESTMANN Joel (U. S. A.)
WESTWATER Michael (U. S. A.)
WETS Roger (U. S. A.)
WETTE Eduard (All. de l'Ouest) *

WETTERLING Wolfgang (Pays-Bas)
WEVERS Jan (Pays-Bas)
WHEELER Roger (Grande-Bretagne)
WHITE David (Grande-Bretagne)
WHITE Derck (Suisse)
WHITEHEAD George W. (U. S. A.)
WHITMAN Andrew P. (U. S. A.)
WHITNEY Hassler (U. S. A.)
WICK Joachim (All. de l'Ouest) *
WIDOM Harold (U. S. A.)
WIEGMANN Klaus W. (All. de l'Ouest)
WIESNER Gunter (All. de l'Ouest)
WILANSKY A. (U. S. A.)
WILCOX Ch. (U. S. A.)
DE WILDE Marc (Belgique)
WILHELMI Gerhard (All. de l'Ouest)
WILKEN (U. S. A.)
WILKENS David L. (Grande-Bretagne)
WILKINSON James (Grande-Bretagne)
WILLE Friedrich (All. de l'Ouest) *
WILLIAMS Graham D. (Grande-Bretagne)
WILLIAMS Kenneth (Canada)
WILLIAMS R. F. (U. S. A.) (D12)
WILLIAMSON John H. (Grande-Bretagne)
WILLS Jorg M. (All. de l'Ouest) *
WILSON Robin (Grande-Bretagne)
WILSON Stephen (Grande-Bretagne)
WINKLER Jorg (All. de l'Ouest) *
WINOGRAD Samuel (U. S. A.) (E7)
WIRSZUT Issac (U. S. A.)
WITT Ernst (All. de l'Ouest)
WLODARSKI Lech (Pologne)
WOLF Joseph A. (U. S. A.)
WOLFF Georg (All. de l'Ouest)
WOLFOWITZ Jacob (U. S. A.) (E6)
WOLFSON Kenneth (U. S. A.)
WOLFSSON Richard (Grande-Bretagne)
WOLKE Dieter (All. de l'Ouest)
WOLSKA-BOCHENEK Janina. (Pologne)
WONG Yau-Chuen (Hong-Kong) *
WONG Yung-Chow (Hong-Kong)
WOODS (Canada)
WORONOWICZ S. (Pologne)
WOUK Arthur (U. S. A.)
WRIGHT John Dav. (Grande-Bretagne)
WRONA Wtodrimen (Nigéria)
WUERGLER Urs (Suisse)
WŪLFSOHN Aubrey (U. S. A.)
WURGES Gerhard (All. de l'Ouest)
WUYTS Piet (Belgique)

Y

YABLONSKY S. V. (U. R. S. S.)
YANENKO N. N. (U. R. S. S.) (E8)
YANO Kentaro (Japon)
YOSHIHIKO Ito (Japon)
YOSIDA Kosaku (Japon)
YOSIDA Yoiti (Japon)
YOUNG Leslie (Grande-Bretagne)

Z

ZAGIER Don (All. de l'Ouest)
ZAHIR Mohsen (France)
ZAHORSKI Zygmunt (Pologne)
ZAIDMAN Samuel (Canada) *
ZAKARIAN V. S. (U. R. S. S.)
ZAKS Abraham (U. S. A.) *
ZAMBELLI Vittorina (Italie)
ZARA François (France)
ZAREMBA Stanislaw (Canada) *
ZEDEK Mishael (U. S. A.)
ZELAZKO Wieslaw (Pologne)
ZELINSKY Daniel (U. S. A.)
ZELLER Karl L. (All. de l'Ouest)
ZELMER Graham K. (Canada)
ZERNER Martin (France)
ZERVOS Spiros (Grèce) *
ZEULI Tino (Italie)
ZIEGLER Hans (Grande-Bretagne) *
ZIEGLER Zvi (Israël)
ZIERMANN Margit (Hongrie)
ZIMMERBERG Hyman J. (U.S.A.)
ZISMAN Michel (France)
ZIZI Khelifa (France)
ZNÁM Štefan (Tchécoslovaquie)
ZOLOTAREV V. M. (U. R. S. S.) *
ZORITSH V. A. (U. R. S. S.)
ZUMBRUNN J. R. (U. S. A.)
ZVONIMIR Bothe (Yougoslavie)
ZYGMUND Antony (U. S. A.)

RAPPORTS
SUR LES
MÉDAILLES FIELDS

(Tome 1 : pages 1 à 16)

Actes, Congrès intern. math., 1970. Tome 1, p. 3 à 5.

RAPPORTS
SUR LES MÉDAILLES FIELDS

ON THE WORK OF ALAN BAKER

by Paul TURÁN

The theory of transcendental numbers, initiated by Liouville in 1844, has been enriched greatly in recent years. Among the relevant profound contributions are those of A. Baker, W. M. Schmidt and V. A. Sprindzuk. Their work moves in important directions which contrast with the traditional concentration on the deep problem of finding significant classes of functions assuming transcendental values for all non-zero algebraic values of the independent variable. Among these, Baker's have had the heaviest impact on other problems of mathematics. Perhaps the most significant of these impacts has been the application to diophantine equations. This theory, carrying a history of more than thousand years, was, until the early years of this century, little more than a collection of isolated problems subjected to ingenious *ad hoc* methods. It was A. Thue who made the breakthrough to general results by proving in 1909 that all diophantine equations of the form $f(x, y) = m$, where m is an integer and f is an irreducible homogeneous binary form of degree at least three, with integer coefficients, have at most finitely many solutions in integers. This theorem was extended by C. L. Siegel and K. F. Roth (himself a Fields medallist) to much more general classes of algebraic diophantine equations in two variables of degree at least three. They even succeeded in establishing general upper bounds on the number of such solutions. A *complete* resolution of such problems however, requiring a knowledge of *all* solutions, is basically beyond the reach of these methods, which are what are called " ineffective ". Here Baker made a brilliant advance. Considering the equation $f(x, y) = m$, where m is a positive integer, $f(x, y)$ an irreducible binary form of degree $n \geqq 3$, with integer coefficients, he succeeded in determining an *effective* bound B, depending only on n and on the coefficients of f, so that

$$\max(|x_0|, |y_0|) \leqq B$$

for any solution (x_0, y_0). Thus, although B is rather large in most cases, Baker has provided, in principle at least, and for the first time, the possibility of determining *all* the solutions explicitly (or the nonexistence of solutions) for a large *class* of equations. This is an essential step towards the positive aspects of Hilbert's tenth problem the interest of which is largely increased by the recent negative solution of the general problem by Ju. V. Matyaszevics. The significance of his theorem is also enhanced by the fact that the so-called elliptic and hyperelliptic equations fall, after appropriate transformation, under its scope and again he gave explicit upper bounds on the totality of their solutions.

Joint work of Baker with J. Coates made effective for curves of genus 1 Siegel's classical theorem. Elaborating these methods and results Coates found among others the first *explicit* lower bound tending to infinity with n for the maximal primefactor of $| f(n) |$ where $f(x)$ stands for an arbitrary polynomial with integer coefficients apart from a trivial exception. The more fact that the maximal primefactor of $| f(n) |$ tends to infinity with n (conjectured for polynomials of second degree by Gauss) was established by K. Mahler several decades ago as well as an *explicit* lower bound for $n = 2$ by him and S. Chowla.

In collaboration with H. Davenport, Baker has shown by some examples how the upper bounds thus obtained permit actually the determination of *all* solutions.

As another consequence of his results he gave an *effective* lower bound for the approximability of algebraic numbers by rationals, the first one which is better than Liouville's

As mentioned before, these results are all consequences of his main results on transcendental numbers. As is well known, the seventh problem of Hilbert asking whether or not α^β is transcendental whenever α and β are algebraic, certain obvious cases aside, was solved independently by A. O. Gelfond and T. Schneider in 1934. Shortly afterwards Gelfond found a stronger result by obtaining an *explicit* lower bound for $| \beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 |$ in terms of α'_νs's and of the degrees and heights of the β'_νs's when the log $\alpha'_\nu s$ are linearly independent. After Gelfond realised in 1948, in collaboration with Ju. V. Linnik, the significance of an *effective* lower bound for the three-term sum, he and N. I. Feldman soon discovered an *ineffective* lower bound for it. The transition from this important first step to *effective* bound for the three-term sum, and more generally for the k-term sum, resisted all efforts until Baker's success in 1966. This success enabled Baker to obtain a vast generalization of Gelfond-Schneider's theorem by showing that if $\alpha_1, \alpha_2, \ldots, \alpha_k$ ($\neq 0, 1$) are algebraic, $\beta_1, \beta_2, \ldots, \beta_k$ linearly independent, algebraic and irrational, then $\alpha_1^{\beta_1}\alpha_2^{\beta_2} \ldots \alpha_k^{\beta_k}$ is transcendental. Some further appreciation of the depth of this result can be gained by recalling Hilbert's prediction that the Riemann conjecture would be settled long before the transcendentality of α^β. The analytic prowess displayed by Baker could hardly receive a higher testimonial. On the other hand, his brilliant achievement shows, after Gelfond-Schneider once more, that mathematics offers no scope for a doctrine of papal infallibility concerning its future. Among his other results generalizing transcendentality theorems of Siegel and Schneider I shall mention only one special case, in itself sufficiently remarkable, according to which the sum of the circumferences of two ellipses, whose axes have algebraic lengths, is transcendental.

His pathbreaking role is not diminished but perhaps even emphasized by the fact that in 1968 Feldman found another important lower estimate for the k-term sum which is stronger in its dependence upon the maximal height of the β_ν coefficients; it is weaker in its dependence upon the maximal height of the α's which is relevant in most applications at present. It is reasonable to expect also new applications depending more on the former.

The 1948 discovery of Gelfond and Linnik, mentioned above, revealed an unexpected connection between such lower bounds for the three-term sum and a classical class-number problem. This has as its goal the determination of all algebraic extensions $R(\theta)$ of the rational field with class number 1. In its full generality this seems hopelessly out of reach at present. Restricting themselves to the imaginary quadratic case $R(\sqrt{-d})$, $d > 0$, H. Heilbronn and E. Linfoot showed in 1934 that at most ten such " good " fields can exist. Nine of these were found explicitly. Concerning the tenth it was known that its d would have to exceed exp (10^7). Hence, if it can be shown that there exists an upper bound $d_0 < \exp(10^7)$ for all " good " d's then the tenth possible field cannot exist. Now the Gelfond-Linnik discovery was that the afore mentioned *effective* lower bound for the three-term sum could furnish such an *effective* d_0. Baker found that one of his general results implies an upper bound $d_0 = 10^{500}$ enough by far for this purpose. This outcome provides a striking new example, illustrating once more how effectivity can play a *decisive* role in essential problems. Again, the value of this approach is of course not diminished by H. M. Stark's outstanding achievement in showing the non-existence of the tenth field, simultaneously and independently, by quite different methods.

To illustrate further the many-sided applicability of Baker's work I mention that it could be employed to make effective some ineffective results of Linnik on the coefficients of a complete reduced set of binary quadratic forms belonging to a fixed negative discriminant (Linnik had used ideas from ergodic theory).

As one can guess, obtaining such long-sought solutions was a very complicated task. It is very difficult to attempt even a sketch of the underlying ideas in the short time at my disposal beyond the remark that they are of hard-analysis type. Fortunately, you will have the opportunity of hearing about them in some detail from Baker himself in his address to this Congress. To conclude, I remark that his work exemplifies two things very convincingly. Firstly, that beside the worthy tendency to start a theory in order to solve a problem it pays also to attack specific difficult problems directly. Particularly is this the case with such problems where rather singular circumstances do not make it probable that a solution would fall out as an easy consequence of a general theory. Secondly, it shows that a direct solution of a deep problem develops itself quite naturally into a healthy theory and gets into early and fruitful contact with other significant problems of mathematics. So, let the two different ways of doing mathematics live in peaceful coexistence for the benefit of our science.

P. TURÁN
Mathematical Institute
of the Hungarian
Academy of Sciences,
Budapest, Hungary

Alan BAKER
Trinity College
Cambridge
(Grande-Bretagne)

Actes, Congrès intern. math., 1970. Tome 1, p. 7 à 9.

TRAVAUX DE HEISOUKÉ HIRONAKA SUR LA RÉSOLUTION DES SINGULARITÉS

par A. GROTHENDIECK

Le résultat principal de Hironaka est le suivant :

THÉORÈME DE HIRONAKA. — Soit X une variété algébrique sur un corps k de caractéristique nulle, U un ouvert (de Zariski) de X tel que U soit non singulier et partout dense. Il existe alors une variété algébrique *non singulière* X' et un morphisme *propre* $f : X' \to X$, tels que le morphisme $f^{-1}(U) \to U$ soit un isomorphisme, et que $D = X' - f^{-1}(U)$ soit un diviseur « à croisements normaux » dans X' (i. e. localement donné par une équation de la forme $f_1 f_2 \ldots f_k = 0$, où les f_i font partie d'un système de « coordonnées locales »).

En fait le théorème complet de Hironaka est plus précis : il donne une information très précise sur la façon d'obtenir une telle « résolution » du couple (X, U) à l'aide d'une suite « d'éclatements » de nature très particulière. Cette précision supplémentaire est inutile dans toutes les applications connues du rapporteur, sauf pour nous dire que si X est projective, on peut choisir X' également projective. Le théorème complet de Hironaka est aussi plus général : il s'applique à tous les « schémas excellents » de caractéristique nulle, et en particulier aux schémas de type fini sur les anneaux de séries formelles ou de séries convergentes (au-dessus d'un corps de caractéristique nulle). Cela implique par exemple facilement que le théorème énoncé reste vrai au voisinage d'un point de X, lorsqu'on suppose maintenant que X est un espace analytique complexe (ou sur un corps valué complet algébriquement clos, plus généralement), et U est le complémentaire d'une partie fermée analytique de X. Il semble que Hironaka ait démontré également la version globale de ce résultat local.

Contrairement à ce qui était l'impression générale chez les géomètres algébristes avant qu'on ne dispose du théorème de Hironaka, celui-ci n'est pas un résultat tout platonique, qui donnerait seulement une sorte de justification après coup d'un point de vue en géométrie algébrique (celui où les variétés sont plongées à tout prix dans l'espace projectif) qui est désormais dépassé. C'est au contraire aujourd hui un *outil* d'une très grande puissance, sans doute le plus puissant dont nous disposions, pour l'étude des variétés algébriques ou analytiques (en caractéristique zéro pour le moment). Cela est vrai pour l'étude des singularités d'une variété, mais également pour l'étude « globale » des variétés algébriques (ou analytiques) non singulières, notamment pour le cas des variétés non compactes. L'application du théorème de Hironaka pour ces dernières se présente généralement ainsi : X étant supposée quasi projective i. e. immergeable comme sous-variété (en général non fermée) dans l'espace projectif P, l'adhérence $\bar{X}$ de X dans P contient X comme ouvert partout dense non singulier, de sorte qu'on peut appliquer le théorème de Hironaka au couple $(\bar{X}, X)$. On en conclut que

X est le complémentaire, dans une variété non singulière *compacte* X', d'un diviseur D à croisements normaux. Un tel théorème de structure pour X, et diverses variantes qu'on prouve de façon analogue, sont extrêmement utiles dans l'étude de X.

Les théorèmes démontrés à l'aide du théorème de Hironaka ne se comptent plus. Pour la plupart, on a l'impression que la résolution des singularités est vraiment au fond du problème, et ne pourra être évitée par recours à des méthodes différentes. Citons quelques-uns de ces résultats (sur un corps de car. nulle).

a) Si $f : X' \to X$ est un morphisme birationnel et propre de variétés algébriques non singulières, alors les faisceaux $R^i f_*(O_{X'})$ sont nuls pour $i > 1$ (Hironaka).

b) Si X est une variété algébrique affine sur le corps des complexes, sa cohomologie complexe peut être calculée à l'aide du « complexe de De Rham algébrique », i. e. le complexe formé des formes différentielles algébriques sur X (Grothendieck ; divers raffinements, inspirés par une question soulevée par Atiyah et Hörmander, ont été développés par P. Deligne).

c) Si X est une variété algébrique sur le corps des complexes, alors ses « groupes de cohomologie étales » à coefficients dans des faisceaux de torsion sont isomorphes aux groupes de cohomologie de l'espace localement compact sous-jacent à X (M. Artin et A. Grothendieck).

d) La construction par P. Deligne d'une théorie de Hodge pour les variétés algébriques complexes quelconques (supposées ni compactes ni non singulières) utilise de façon essentielle la résolution des singularités.

e) Même remarque pour divers théorèmes de P. A. Griffiths et de ses élèves sur la « variation des structures de Hodge », ou pour divers théorèmes de E. Brieskorn sur l'étude locale de certains types de singularités (singularités de Klein des surfaces, points critiques isolés d'un germe de fonction holomorphe...).

Certains des résultats mentionnés dans *d*) et *e*) figureront sans doute dans des rapports des auteurs cités dans ce même Congrès.

Du point de vue technique, la démonstration du théorème de Hironaka constitue une prouesse peu commune. Le rapporteur avoue n'en avoir pas fait entièrement le tour. Aboutissement d'années d'efforts concentrés, elle est sans doute l'une des démonstrations les plus « dures » et les plus monumentales qu'on connaisse en mathématique. Elle introduit d'ailleurs, comme on peut s'en douter, diverses idées géométriques nouvelles, dont il est trop tôt d'évaluer le rôle dans le développement futur de la géométrie algébrique (*). Notons d'autre part que Hironaka souligne que plusieurs de ces idées étaient déjà en germe chez son maître, O. Zariski, qui avait beaucoup fait depuis longtemps pour populariser le problème de la résolution des singularités parmi un public réticent, et qui avait dans un travail classique traité le cas de la dimension 3.

Pour terminer, il faut souligner que le problème de la résolution des singularités est loin d'être résolu. En effet, seul le cas de la caractéristique nulle est actuellement réglé. La solution de nombreux problèmes de géométrie algébrique, en caractéristique $p > 0$ comme en inégales caractéristiques, dépend de la démonstration d'un

---

(*) Cela est d'autant plus vrai que le développement de la géométrie algébrique s'arrêtera court, comme tout le reste, si notre espèce devait disparaître dans les prochaines décades, — éventualité qui apparaît aujourd'hui de plus en plus probable.

théorème analogue pour n'importe quel « schéma excellent », par exemple pour n'importe quelle variété algébrique sur un corps k de caractéristique arbitraire. Le cas de la dimension 2 a été traité par Abhyankar, et a déjà été un outil indispensable dans diverses questions, par exemple dans la théorie de Néron de la dégénérescence des variétés abéliennes ou des courbes algébriques (« théorème de réduction semi-stable »), et ses applications par Deligne-Mumford aux variétés de modules des courbes algébriques, en caractéristique quelconque. Depuis plusieurs années déjà, Hironaka travaille sur le cas de la dimension quelconque. Nul doute que le problème mérite qu'un mathématicien du format de H. Hironaka lui consacre dix ans d'efforts incessants. Nul doute aussi que tous les géomètres lui souhaitent, de tout cœur : Bon succès !

A. GROTHENDIECK
Collège de France
11, Place Marcelin-Berthelot,
Paris 5^{e}
(France)

H. HIRONAKA
Harvard University
Department of Mathematics,
2 Divinity Avenue
Cambridge, Massachusetts 02138
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 11 à 13.

ON THE WORK OF SERGE NOVIKOV

by M. F. ATIYAH

It gives me great pleasure to report on the work of Serge Novikov. For many years he has been generally acknowledged as one of the most outstanding workers in the fields of Geometric and Algebraic Topology. In this rapidly developing area, which has attracted many brilliant young mathematicians, Novikov is perhaps unique in demonstrating great originality and very powerful technique both in its geometric and algebraic aspects.

Novikov made his first impact, as a very young man, by his calculation of the unitary cobordism ring of Thom (independently of similar work by Milnor). Essentially Thom had reduced a geometrical problem of classification of manifolds to a difficult problem of homotopy theory. Despite the great interest aroused by the work of Thom this problem had to wait several years before its successful solution by Milnor and Novikov. Many years later Novikov returned to this area and, combining cobordism with homotopy theory, he developed some very powerful algebraic machinery which gives one of the most refined tools at present available in Algebraic Topology. In his early work it was a question of applying homotopy to solve the geometric problem of cobordism; in this later work it was the reverse, cobordism was used to attack general homotopy theory.

On the purely geometric side I would like to single out a very beautiful and striking theorem of Novikov about foliations on the 3-dimensional sphere. Perhaps I should remind you that a foliation of a manifold is (roughly speaking) a decomposition into manifolds (of some smaller dimension) called the leaves of the foliation: one leaf passing through each point of the big manifold. If the leaves have dimension one then we are dealing with the trajectories (or integral curves) of a vector field, and closed trajectories are of course particularly interesting. In the general case a basic question therefore concerns the existence of *closed leaves.* Very little was known about this problem. Thus even in the simplest case of a foliation of the 3-sphere into 2-dimensional leaves the answer was not known until Novikov, in 1964, proved that every foliation in this case does indeed have a closed leaf (which is then necessarily a torus). Novikov's proof is very direct and involves many delicate geometric arguments. Nothing better has been proved since in this direction.

Undoubtedly the most important single result of Novikov, and one which combines in a remarkable degree both algebraic and geometric methods, is his famous proof of the topological invariance of the Pontrjagin classes of a differentiable manifold. In order to explain this result and its significance I must try in a few minutes to summarize the history of manifold theory over the past 20 years. Fortunately, during this Congress you will be able to hear many more detailed and comprehensive surveys.

There are 3 different kinds or categories of manifold: differentiable, piece-wise linear (or combinatorial) and topological. For each category the main problem is to understand the structure or to give some kind of classification. There was no clear idea about the distinction between these 3 categories until Milnor produced his famous example of 2 different differentiable structures on the 7-sphere. After that the subject developed rapidly with important contributions from many people, including Novikov, so that in a few years the distinction between differentiable and piece-wise linear manifolds, and their classification, was very understood. However, there were still no real indications about the status of topological manifolds. Were they essentially similar to piece-wise linear manifolds or were they quite different? Nobody knew. In fact, there were no known invariants of topological manifolds except homotopy invariants. On the other hand, there were many invariants known for differentiable or piece-wise linear manifolds which were finer than homotopy invariants. Notable among these were the Pontrjagin classes. For a differentiable manifold these are cohomology classes which measure, in some sense, the amount of global twisting in the tangent spaces. For a manifold with a global parallelism like a torus they are zero. In the context of Riemannian geometry there is a generalized Gauss-Bonnet theorem which expresses them in terms of the curvature. In any case their definition relies heavily on differentiability. Around 1957 it was shown by Thom, Rohlin and Svarc, using important earlier work of Hirzebruch, that the Pontrjagin classes are actually piece-wise linear invariants (provided we use rational or real coefficients). When Novikov, in 1965, proved their topological invariance this was the first real indication that topological manifolds might be essentially similar to piece-wise linear ones. It was a big break-through and was quickly followed by very rapid progress which, in the past few years, through the work of many mathematicians — notably Kirby and Siebenmann — has resulted in fairly complete information about the topological piece-wise linear situation. Thus we now know that nearly all topological manifolds can be triangulated and essentially in a unique way. You will undoubtedly hear about this in the Congress lectures.

Perhaps you will understand Novikov's result more easily if I mention a purely geometrical theorem (not involving Pontrjagin classes) which lies at the heart of Novikov's proof. This is as follows:

THEOREM (*). — If a differentiable manifold X is homeomorphic to a product $M \times R^n$ (where M is compact, simply-connected and has dimension ≥ 5) then X is diffeomorphic to a product $M' \times R^n$.

Here both M, M' are differentiable manifolds. The theorem thus asserts that a topological factorization implies a differentiable factorization: it is clearly a deep result. Combined with the earlier Thom-Hirzebruch work it leads easily to the invariance of the Pontrjagin classes.

I hope I have now indicated the importance of this result of Novikov's and its place in the general development of manifold theory. I would like also to stress the remarkable nature of the proof which combines very ingenious geometric ideas with considerable algebraic virtuosity. One aspect of the geometry is particularly worth mentioning. As is well-known many topological problems are very much easier if one

(*) This formulation is due to L. SIEBENMANN.

is dealing with simply-connected spaces. Topologists are very happy when they can get rid of the fundamental group and its algebraic complications. No so Novikov! Although the theorem above involves only simply-connected spaces, a key step in his proof consists in perversely introducing a fundamental group, rather in the way that (on a much more elementary level) puncturing the plane makes it non-simply-connected. This bold move has the effect of simplifying the geometry at the expense of complicating the algebra, but the complication is just manageable and the trick works beautifully. It is a real master stroke and completely unprecedented. Since then a somewhat analogous device has proved crucial in the important work of Kirby mentioned earlier.

I hope this brief report has given some idea of the real individuality of Novikov's work, its variety and its importance, all of which fully justifies the award of the Fields Medal. It is all the more remarkable when we remember that he worked in relative isolation from the main body of mathematicians in his particular field. We offer him our heartiest congratulations in the full confidence that he will continue, for many years to come, to produce mathematics of the highest order.

Michael ATIYAH
Institute for Advanced Study
Department of Mathematics,
Princeton, New Jersey 08540
(U. S. A.)

Serge NOVIKOV
Steklov Mathematical Institute
ul Vavilova 42,
Moscow V 333
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 15 à 16.

ON THE WORK OF JOHN THOMPSON

by R. BRAUER

It is an honor to be called upon to describe to you the brilliant work for which John Thompson has just been awarded the Fields medal. The pleasure is tempered by the feeling that he himself could do this job much better. But perhaps I can say some things he would never say since he is a modest person.

The central outstanding problem in the theory of finite groups today is that of determining the simple finite groups. One may say that this problem goes back to Galois. In any case, Camille Jordan must have been aware of it. Important classes of simple groups have been constructed as well as some individual types of such groups. French mathematicians, Galois, Jordan, Mathieu, Chevalley, have been the pioneers in this work. In recent years, mathematicians of many different countries have joined. However, the general problem is unsolved. We do not know at all how close we are to knowing all simple finite groups. I shall not discuss the present situation of the problem since this will be the topic of Feit's address at this congress. I may only say that up to the early 1960's, really nothing of real interest was known about general simple groups of finite order.

I shall now describe Thompson's contribution. The first paper I have to mention is a joint paper by Walter Feit and John Thompson and, of course, Feit's part in it should not be overlooked. Here, the authors proved a famous conjecture, to the effect that all non-cyclic finite simple groups have even order. I am not sure who was the first to observe this. Fifty years ago this was already referred to as a very old conjecture. While it was usually mentioned in courses on algebra, it is only fair to say that nobody ever did anything about it, simply because nobody had any idea how to get even started. It was not even clear that the whole problem made much sense. Was the role of the prime 2 simply a little accident; did 2 play an entirely exceptional role, or were there properties of other prime divisors of the group order which bore at least some resemblance to those of 2? It was only after the Feit-Thompson paper that one could be sure that the whole question has been a reasonable one.

Thompson's work which has now been honored by the Fields medal is a sequel to this first paper. In it, he determines the minimal simple finite groups, this is to say, the simple finite groups, whose proper subgroups are solvable. Actually, a more general problem is solved. It suffices to assume that only certain subgroups, the so-called local subgroups, are solvable. These are the normalizers of subgroups of prime power order larger than I.

These results are the first substantial results achieved concerning simple groups. A number of important corollaries show that one is now able to answer questions on finite groups which had been completely out of reach before. I mention one: a finite groups is solvable, if and only if every subgroup generated by two elements is solvable. You only have to try to prove this yourself if you want to see how deep the result lies.

Both investigations are very long and complicated and their logical structure is extremely intricate. Unfortunately, I cannot even give you a vague idea of the methods. Reading the papers, one reaches stages repeatedly that one feels caught in a hopeless situation, in an abyss from which there is no escape. Then, miraculously, a way out appears, an amazing turn, which saves us. A famous 19-th century mathematician once remarked that group theory could be done by people who did not know much else of mathematics. There may be some truth in this, but I think, this was not meant in a very nice way. However I believe it was overlooked that if you work in a field where you have few tools, you have to create your own tools. In order to reach positive achievements, mathematical imagination must replace knowledge from other fields.

There is other important work of Thompson in group theory which I cannot discuss here. His methods have already been used successfully by other mathematicians who have developed some of them further. In this way, Thompson has had a tremendons influence. Since he first appeared at the International Congress in Stockholm eight years ago, finite group theory simply is not the same any more.

Let me finish with a personal remark. One reaches a point in life where one wonders what one still expects of life, what one would still like to see happen. This applies to events in Mathematics too. I have passed the point I mentioned. I like to say that I would like to see the solution of the problem of the finite simple groups and the part I expect Thompson's work to play in it. Quite generally, I would like to see to what further heights Thompson's future work will take him. I feel I should also say the same about the three other Fields medallists.

Richard BRAUER
Harvard University
Department of Mathematics,
2 Divinity Avenue,
Cambridge, Mass. 02138
(U. S. A.)

John, G. THOMPSON
University of Cambridge
Department of Mathematics,
16 Mill Lane
Cambridge
(Grande-Bretagne)

G

CONFÉRENCES GÉNÉRALES

(Tome 1 : pages 17 à 219)

Actes, Congrès intern. math., 1970. Tome 1, p. 19 à 26.

G - CONFÉRENCES GÉNÉRALES

EFFECTIVE METHODS IN THE THEORY OF NUMBERS

by A. BAKER

1. Problems concerning the determination of the totality of integers possessing certain prescribed properties such as, for instance, solutions of systems of Diophantine equations or inequalities, have captured man's imagination since antiquity, and a wide variety of different techniques have been employed through the centuries to resolve a diverse multitude of problems in this field. Most of the early work tended to be of an *ad hoc* character, the arguments involved being specifically related to the particular numerical example under consideration, but gradually the emphasis has altered and the trend in recent times has been increasingly towards the development of general coherent theories. Two particular advances stand out in this connexion. First, investigations of Thue [39] in 1909 and Siegel [33] in 1929 led to the discovery of a simple necessary and sufficient condition for any Diophantine equation $F(x, y) = 0$, where F denotes a polynomial with integer coefficients, to possess only a finite number of solutions in integers; this occurs, namely, if and (reading " ganzartige " for " integer ") only if the curve has genus at least 1 or genus 0 and at least three infinite valuations. The proof depends upon, amongst other things, Weil's well-known generalization [40] of Mordell's finite basis theorem and the earlier pioneering work of Thue and Siegel [32] concerning rational approximations to algebraic numbers. Secondly, in answer to a question raised by Gauss in his famous Disquisitiones Arithmeticae, Hecke, Mordell, Deuring and Heilbronn [29] showed in 1934 that there could exist only finitely many imaginary quadratic fields with any given class number, a result later to be incorporated in the celebrated Siegel-Brauer formula. These theorems and all their many ramifications, though of major importance in the evolution of much of modern number theory, nevertheless suffer from one basic limitation that of their non-effectiveness. The arguments depend on an assumption, made at the outset, that the relevant aggregates possess one or more elements that are, in a certain sense, large, and they provide no way of deciding whether or not these hypothetical elements exist. Thus the work leads merely to an estimate for the number of elements in question and throws no light on the fundamental problem of determining their totality.

Some special effective results in the context of the Thue-Siegel theory were obtained in 1964 by means of certain properties peculiar to Gauss' hypergeometric function, in particular, the classic fact, certainly known to Padé, that quotients of such functions serve to represent the convergents to rational powers of $1 - x$ (see [1, 2, 3]), but the first effective results applicable in a general context came in 1966 from a completely different source. One of Hilbert's famous list of problems raised at the International Congress held in Paris in 1900 asked whether an irrational quotient of logarithms of algebraic numbers is transcendental. An affirmative answer was obtained independently by Gelfond [26] and Schneider [30] in 1934, and shortly afterwards Gelfond established an important refinement giving a positive lower bound for a linear form in two logarithms (cf. [27]). It was natural to conjecture that an analogous result would hold for linear forms in arbitrarily many logarithms of algebraic numbers and a theorem of this nature was proved in 1966 [4]. The techniques devised for the demonstration form the basis of the principal effective methods in number theory known to date. I shall first describe briefly the main arguments and shall then proceed to discuss some of their applications (*).

2. The key result, which serves to illustrate most of the principal ideas, states that if $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers such that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals then 1, $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the field of all algebraic numbers. This implies, in particular, that $e^{\beta_0}\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ is transcendental for all non-zero algebraic numbers $\alpha_1, \ldots, \alpha_n, \beta_0, \ldots, \beta_n$. It will suffice to sketch here the proof of a somewhat weaker result namely, if $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_{n-1}$ are non-zero algebraic numbers such that $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent, then the equation $\alpha_1^{\beta_1} \ldots \alpha_{n-1}^{\beta_{n-1}} = \alpha_n$ is untenable; it is under these conditions that our arguments assume their simplest form. We suppose the opposite and derive a contradiction. The proof depends on the construction of an auxiliary function of several complex variables which generalizes the function of a single variable employed originally by Gelfond. Functions of many variables were utilized by Schneider [31] in his studies concerning Abelian integrals but, for reasons that will shortly be explained, there seemed to be severe limitations to their serviceability in wider settings. The function that proved to be decisive in the present context is given by

$$\Phi(z_1, \ldots, z_{n-1}) = \sum_{\lambda_1=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_1, \ldots, \lambda_n)\, \alpha_1^{(\lambda_1+\lambda_n\beta_1)z_1} \ldots \alpha_{n-1}^{(\lambda_{n-1}+\lambda_n\beta_{n-1})z_{n-1}},$$

where L is a large parameter and the $p(\lambda_1, \ldots, \lambda_n)$ denote rational integers not all 0. By virtue of the initial assumption we see at once that

$$\Phi(z, \ldots, z) = \sum_{\lambda_1=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_1, \ldots, \lambda_n)\alpha_1^{\lambda_1 z} \ldots \alpha_n^{\lambda_n z}$$

and so, for any positive integer l, the value of Φ at $z_1 = \ldots = z_{n-1} = l$ is an algebraic number in a fixed field. Moreover, apart from a multiplicative factor given by products of powers of the logarithms of the α's, the same holds for any derivative

$$\Phi_{m_1,\ldots,m_{n-1}} = (\partial/\partial z_1)^{m_1} \ldots (\partial/\partial z_{n-1})^{m_{n-1}}\Phi.$$

It follows from a well-known lemma on linear equations that, for any integers h, k, with hk^{n-1} a little less than L^n, one can choose the $p(\lambda_1, \ldots, \lambda_n)$ such that

$$\Phi_{m_1,\ldots,m_{n-1}}(l, \ldots, l) = 0 \qquad (1 \leqslant l \leqslant h, m_1 + \ldots + m_{n-1} \leqslant k)$$

and, furthermore, an explicit bound for $|p(\lambda_1, \ldots, \lambda_n)|$ can be given in terms of h, k and L.

(*) For a fuller survey of the applications see [13].

The real essence of the argument is an extrapolation procedure which shows that the above equation remains valid over a much longer range of values for l, provided that one admits a small diminution in the range of values for $m_1 + \ldots + m_{n-1}$. Although interpolation arguments have long been a familiar feature of transcendental number theory, work in this connexion has hitherto always involved an extension in the order of the derivatives while leaving the points of interpolation fixed; when dealing with functions of many variables, however, this type of argument requires that the points in question admit a representation as a Cartesian product and, as far as I can see, the condition can be satisfied only with respect to special multiply-periodic functions. Our algorithm proceeds by induction and it will suffice to illustrate the first step. We suppose that $m_1 + \ldots + m_{n-1} \leqslant \frac{1}{2}k$ and we prove that then

$$f(z) = \Phi_{m_1,\ldots,m_{n-1}}(z, \ldots, z)$$

vanishes at $z = l$, where $1 \leqslant l \leqslant h^2$. Now the condition $hk^{n-1} \leqslant L^n$ allows one to take $L \leqslant k^{1-\varepsilon}$ for some $\varepsilon > 0$ and h about $k^{\frac{1}{2}\varepsilon}$. This " saving " by an amount ε is crucial for it leads to a sharp bound for $|f(z)|$ on a circle centre the origin and radius slightly larger than h^2, thus including all the points l as above. Further, apart from a trivial multiplicative factor, $f(l)$ represents an algebraic integer in a fixed field and a similar bound obtains for each of the conjugates. But, by construction, we have

$$f_m(r) = 0 \qquad \left(0 \leqslant m \leqslant \frac{1}{2}k, 1 \leqslant r \leqslant h\right),$$

and the maximum-modulus principle applied to the function $f(z)/F(z)$, where

$$F(z) = \{(z-1)\ldots(z-h)\}^{[\frac{1}{2}k]},$$

now shows that $|f(l)|$ is sufficiently small to ensure that the norm of the algebraic integer is less than 1. Hence $f(l) = 0$ as required. The argument is repeated inductively and after a finite number of steps we conclude that

$$\Phi(l, \ldots, l) = 0 \qquad (1 \leqslant l \leqslant (L+1)^n).$$

But these represent linear equations in the $p(\lambda_1, \ldots, \lambda_n)$. The determinant of coefficients is of Vandermonde type and since, by hypothesis, $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent, it does not vanish. The contradiction establishes our result.

3. The argument just described is capable of considerable refinement and generalization. In particular several other auxiliary functions can be taken in place of Φ, the points of extrapolation can be varied and greater use can be made in the latter part of the exposition of our information regarding the partial derivatives. Thus, for instance, results in the context of elliptic functions have been derived and, in particular, the transcendence has been established of any non-vanishing linear combination with algebraic coefficients of periods and quasi-periods associated with a Weierstrass $\wp$-function with algebraic invariants [10, 11, 12]. More relevant to the main theme of this talk, however, are refinements giving quantitative lower bounds for linear forms in logarithms. The main change in the preceding discussion required to obtain results

of this nature is the replacement of the maximum-modulus principle by the Hermite interpolation formula. With this device one can show that

$$|\beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n| > Ce^{-(\log H)^\kappa},$$

where $\alpha_1, \ldots, \alpha_n$ denote non-zero algebraic numbers such that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals, $\beta_0, \ldots, \beta_n$ denote algebraic numbers, not all 0, with degrees and heights at most d and H respectively, $\kappa > n + 1$ and $C > 0$ depends only on n, $\log \alpha_1, \ldots, \log \alpha_n$, κ and d; by the height of an algebraic number we mean the maximum of the absolute values of the relatively prime integer coefficients in its minimal defining polynomial [5]. With more complicated adaptations the number on the right can be strengthened to $CH^{-\kappa}$, where $\kappa > 0$ is specified like C above; this was shown by Feldman [22, 23]. In applications it frequently suffices to have simply a lower bound of the form $e^{-\delta H}$, valid for any $\delta > 0$ and all $H > C$, where C now depends on δ, and interest then attaches to the exact expression for C. Some explicit forms have been calculated (cf. [5, 6, 23, 24]) but there is certainly scope for improvement here and, indeed, the general efficacy of our methods seems to be closely linked to our progress in this connexion.

4. We now discuss some applications of our results in the theory of Diophantine equations. To begin with, they can be utilized to obtain a complete resolution of the equation originally considered by Thue, namely $f(x, y) = m$, where f denotes an irreducible binary form with integer coefficients and degree at least 3 [6]. Indeed our arguments enable us to find more generally all algebraic integers x, y in a given field K satisfying any equation $\beta_1 \ldots \beta_n = m$ where $\beta_j = x - \alpha_j y$, $n \geqslant 3$ and $\alpha_1, \ldots, \alpha_n$, m denote algebraic integers in K subject only to the condition that the α's are all distinct (cf. [15]). For denoting by $\theta^{(1)}, \ldots, \theta^{(d)}$ the field conjugates of any element θ of K and by $\eta_1, \ldots, \eta_r$ a fundamental system of units in K, it is readily seen that an associate

$$\gamma_i = \beta_i \eta_1^{b_{i1}} \ldots \eta_r^{b_{ir}}$$

of β_i can be determined such that

$$|\log |\gamma_i^{(j)}|| \leqslant C_1 \qquad (1 \leqslant j \leqslant d),$$

where $C_1, C_2, \ldots$ can be effectively computed in terms of f and m. Writing

$$H_i = \max |b_{ij}| \qquad \text{and} \qquad H_l = \max H_i$$

we have $|\beta_l^{(h)}| \leqslant C_2 e^{-H_l/C_3}$ for some h; and without loss of generality we can suppose that $\beta_l^{(h)} = \beta_l$. From the initial equation we see that $|\beta_k| \geqslant C_4^{-1}$ for some $k \neq l$ and if now j is any suffix other than k or l, the identity

$$(\alpha_k - \alpha_l)\beta_j - (\alpha_j - \alpha_l)\beta_k = (\alpha_k - \alpha_j)\beta_l$$

gives

$$\eta_1^{b_1} \ldots \eta_r^{b_r} - \alpha_{r+1} = \omega,$$

where

$$b_s = b_{ks} - b_{js}, \qquad 0 < |\omega| < C_5 e^{-H_l/C_6}$$

and α_{r+1} is an element of K with degree and height $\leqslant C_7$. Now $|b_s| \leqslant 2H_l$ and hence the work of § 3 can be applied to obtain a bound for H_l, whence also for all the conjugates of the β's and, finally, for the conjugates of x and y.

The last result enables one to solve many other Diophantine equations in two unknowns. In particular, one can now effectively determine all rational integers x, y satisfying $y^m = f(x)$, where m is any integer $\geqslant 2$ and f is a polynomial with integer coefficients possessing at least three simple zeros [8]. This includes the celebrated Mordell equation $y^2 = x^3 + k$, the hyperelliptic equation and the Catalan equation $x^n - y^m = 1$ with prescribed m, n. The demonstration involves ideal factorizations in algebraic number fields similar to those appearing in the first part of the proof of the Mordell-Weil theorem; in special cases one has readier arguments and, in particular, the elliptic equation has been efficiently treated by means of Hermite's classical theory of the reduction of binary quartic forms [7]. There is, moreover, little difficulty in carrying out the work more generally when the coefficients and variables represent algebraic integers in a fixed field, and, indeed, Coates and I have used this extension to give a new and effective proof of Siegel's theorem on $F(x, y) = 0$ (see § 1) in the case of curves of genus 1 [15, 21]. Here the equation of the curve is reduced to canonical form by means of a birational transformation similar to that described by Chevalley, the rational functions defining the transformation being constructed to possess poles only at infinity and thus be integral over a polynomial ring. Explicit upper bounds have been established in each instance for the size of all the solutions [6, 7, 8, 15]. The bounds tend to be large, with repeated exponentials, and current research in this field is centred on techniques for reducing their magnitude. In particular, Siegel [34] has recently given some improved estimates for units in algebraic number fields which should prove useful for this purpose, and, furthermore, devices have been obtained which, for a wide range of numerical examples, would seem to render the problem of determining the complete list of solutions in question accessible to practical computation (cf. [16]).

5. Finally we mention some further results that have been obtained as a consequence of these researches. One of the first applications was to establish an effective algorithm for resolving the old conjecture that there are only nine imaginary quadratic fields with class number 1 [4, 18]. The connexion between this problem and inequalities involving the logarithms of algebraic numbers was demonstrated by Gelfond and Linnik [28] in 1949 by way of an expression for a product of L-functions analogous to the well-known Kronecker limit formula. By a remarkable coincidence, Stark [38] established the conjecture at about the same time by an entirely different method with its origins in a paper of Heegner. Attention has subsequently focussed on the problem of determining all imaginary quadratic fields with class-number 2, and I am happy to report that an algorithm for this purpose was obtained very recently by means of a new result relating to linear forms in three logarithms [9, 14] (*). It seems likely that this latest development will lead to advances in other spheres.

Among the original motivations of our studies was the search for an effective improvement on Liouville's inequality of 1844 relating to the approximation of algebraic numbers by rationals; from the work described in § 4 we have now

$$|\alpha - p/q| > cq^{-n}e^{(\log q)^{1/\kappa}}$$

(*) See also Stark's address to this Congress.

for all algebraic numbers α with degree $n \geqslant 3$ and all rationals p/q $(q > 0)$ where $\kappa > n$ and $c = c(\alpha, \kappa) > 0$ is effectively computable [6, 25]. For some particular α, such as the cube roots of 2 and 17, sharper results in this direction have been obtained from the work on the hypergeometric function mentioned in § 1. Further, in the special case when p, q are comprised solely of powers of fixed sets of primes, a much stronger result can be obtained directly from the inequalities referred to in § 3; indeed we have then

$$| \alpha - p/q | > c (\log q)^{-\kappa}$$

where $c > 0$, $\kappa > 0$ are effectively computable in terms of the primes and α, and this in fact furnishes an improvement on Ridout's generalization of Roth's theorem.

Analogues of the arguments of § 3 and § 4 in the p-adic realm have been given by Coates [19, 20]; his work leads, in particular, to an effective determination of all rational solutions of the equations discussed earlier with denominators comprised solely of powers of fixed sets of primes and so, more especially, provides a means for finding all elliptic curves with a given conductor (see also [35, 36, 37]). Furthermore, Brumer obtained in 1967 a natural p-adic analogue of the main theorem on logarithms which, in conjunction with work of Ax, resolved a well-known problem of Leopoldt on the non-vanishing of the p-adic regulator of an Abelian number field [17].

6. And now I must conclude my survey. It will be appreciated that I have been able to touch upon only a few of the diverse results that have been established with the aid of the new techniques, and, certainly, many avenues of investigation await to be explored. The work has demonstrated, in particular, a surprising connexion between the apparently unrelated seventh and tenth problems of Hilbert, as well as throwing an effective light on both of the fundamental topics referred to at the beginning concerning Diophantine equations and class numbers. Though the strength of this illumination has been steadily growing, and indeed the respective regions of shadow in these contexts have been receding at a remarkably similar rate, it would appear nevertheless that several further ideas will be required before our theories can be regarded as, in any sense, complete. The main feature to emerge is, I think, that the principal passage to effective methods in number theory lies, at present, deep in the domain of transcendence, and it is to be hoped that the territory so far gained in this connexion will be much extended in the coming years.

REFERENCES

[1] A. Baker. — Rational approximations to certain algebraic numbers, *Proc. London Math. Soc.* (3), 4 (1964), pp. 385-398.

[2] —. — Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, *Quart. J. Math. Oxford Ser.* (2), 15 (1964), pp. 375-383.

[3] —. — Simultaneous rational approximations to certain algebraic numbers, *Proc. Cambridge Philos. Soc.*, 63 (1967), pp. 693-702.

[4] —. — Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13 (1966), pp. 204-216.

[5] —. — Linear forms in the logarithms of algebraic numbers II, III, IV, *Mathematika*, 14 (1967), pp. 102-107, 220-228; 15 (1968), pp. 204-216.

[6] —. — Contributions to the theory of Diophantine equations. I: On the representation

of integers by binary forms. II: The Diophantine equation $y^2 = x^3 + k$, *Philos. Trans. Roy. Soc. London*, A 263 (1968), pp. 173-208.

[7] —. — The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. London Math. Soc.*, 43 (1968), pp. 1-9.

[8] —. — Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.*, 65 (1969), pp. 439-444.

[9] —. — A remark on the class number of quadratic fields, *Bull. London Math. Soc.*, 1 (1969), pp. 98-102.

[10] —. — On the periods of the Weierstrass $\wp$-function, *Symposia Mathematica*, vol. IV (Bologna, 1970), pp. 155-174.

[11] —. — On the quasi-periods of the Weierstrass ζ-function, *Göttingen Nachrichten* (1969), No. 16, pp. 145-157.

[12] —. — An estimate for the $\wp$-function at an algebraic point, *American J. Math.*, 92 (1970), pp. 619-622.

[13] —. — Effective methods in Diophantine problems, *Proc. Symposia Pure Maths (American Math. Soc.)*, vol. 20 (1971), pp. 195-205.

[14] —. — Imaginary quadratic fields with class number 2, *Annals of Math.* (to appear).

[15] — and J. Coates. — Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.*, 67 (1970), pp. 595-602.

[16] — and H. Davenport. — The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math., Oxford Ser.* (2), 20 (1969), pp. 129-137.

[17] Armand Brumer. — On the units of algebraic number fields, *Mathematika*, 14 (1967), pp. 121-124.

[18] P. Bundschuh and A. Hock. — Bestimming aller imaginär-quadratischen Zahlkorper der Klassenzahl Eins mit Hilfe eines Satzes von Baker, *Math. Z.*, 111 (1969), pp. 191-204.

[19] J. Coates. — An effective p-adic analogue of a theorem of Thue, *Acta Arith.*, 15 (1969), pp. 279-305.

[20] —. — An effective p-adic analogue of a theorem of Thue. II: On the greatest prime factor of a binary form. III: The Diophantine equation $y^2 = x^3 + k$. *Acta Arith.*, 16 (1970), pp. 399-412, 425-435.

[21] —. — Construction of rational functions on a curve, *Proc. Cambridge Philos. Soc.*, 68 (1970), pp. 105-123.

[22] N. I. Feldman. — Estimate for a linear form of logarithms of algebraic numbers, *Mat. Sb.*, 76 (118) (1968), pp. 304-319; *Math. USSR Sb.*, 5 (1968), pp. 291-307.

[23] —. — An improvement of the estimate for a linear form in the logarithms of algebraic numbers, *Mat. Sb.*, 77 (119) (1968), pp. 423-436; *Math. USSR Sb.*, 6 (1968), pp. 393-406.

[24] —. — An inequality for a linear form in the logarithms of algebraic numbers, *Mat. Zametki*, 6 (1969), pp. 681-689.

[25] —. — Refinements of two effective inequalities of A. Baker, *Mat. Zametki*, 6 (1969), pp. 767-769.

[26] A. O. Gelfond. — On Hilbert's seventh problem, *Doklady Akad. Nauk SSSR*, 2 (1934), pp. 1-6; *Izv. Akad. Nauk SSSR*, 7 (1934), pp. 623-634.

[27] —. — *Transcendental and algebraic numbers* (New York, 1960).

[28] — and Yu V. Linnik. — On Thue's method and the problem of effectiveness in quadratic fields, *Doklady Akad. Nauk SSSR*, 61 (1948), pp. 773-776.

[29] H. Heilbronn. — On the class-number in imaginary quadratic fields, *Quart. J. Math. Oxford Ser.*, 5 (1934), pp. 150-160.

[30] Th. Schneider. — Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen. *J. reine angew. Math.*, 172 (1934), pp. 65-69.

[31] —. — Zur Theorie der Abelschen Funktionen und Integrale, *J. reine angew. Math.*, 183 (1941), pp. 110-128.

[32] C. L. Siegel. — Approximation algebraischer Zahlen, *Math. Z.*, 10 (1921), pp. 173-213.

[33] —. — Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.* (1929), No. 1.

[34] —. — Abschätzung von Einheiten, *Göttingen Nachrichten*, 9 (1969), pp. 71-86.
[35] V. G. Sprindzuk. — Concerning Baker's theorem on linear forms in logarithms, *Dokl. Akad. Nauk BSSR*, 11 (1967), pp. 767-769.
[36] —. — Effectivization in certain problems of Diophantine approximation theory, *Dokl. Akad. Nauk BSSR*, 12 (1968), pp. 293-297.
[37] — and A. I. Vinogradov. — The representation of numbers by binary forms, *Mat. Zametki*, 3 (1968), pp. 369-376.
[38] H. M. Stark. — A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.*, 14 (1967), pp. 1-27.
[39] A. Thue. — Über Annäherungswerte algebraischer Zahlen, *J. reine angew. Math.*, 135 (1909), pp. 284-305.
[40] A. Weil. — L'arithmétique sur les courbes algébriques, *Acta Math.*, 53 (1928), pp. 281-315.

Trinity College
Cambridge
(England)

Actes, Congrès intern. math., 1970. Tome 1, p. 27 à 36.

ON TOPOLOGICAL OBSTRUCTIONS TO INTEGRABILITY

by RAOUL BOTT [1]

§ 1. Introduction.

In this lecture I would like to describe the state of the art in the problem of " foliating " a manifold or, as I prefer to view it, the problem of constructing integrable fields on a manifold. This subject has seen some interesting developments in the past two years and is also contemporary in the sense that, as you will see, it leads to " huge spaces ". By a huge space I mean here simply one whose homotopy groups are not finitely generated in every dimension. In the past we—and I think quite rightly—have shied away from such objects, but recently they have cropped up in various contexts: notably in the index theory associated to Von Neumann algebras of type II, and also in the localization of spaces at a given prime, and I am confident that in the future these " huge " spaces will enter into many of the analysis inspired problems in topology.

§ 2. Integrability.

Let me start by recalling the basic facts concerning the local theory of integrability. Consider a C^∞-manifold M and let TM denote its field of tangent planes. By a section of TM one means a smooth function $p \to X_p$ which attaches to each $p \in M$ a tangent vector at p. These are therefore the " vector-fields " or " infinitesimal motions " of M. If x, y are any two such sections their Lie bracket $[x, y]$ is again a well determined vector-field on M and the bracket operation satisfies the Jacobi-identity:

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]]. \tag{2.1}$$

By a field of tangent k-planes on M one means a smooth family $E = \{ E_p ; p \in M \}$ of k-subspaces of T_pM. In short a k-dimensional " sub-bundle " of TM, and such a field is called integrable if its space of sections is closed under the bracket:

$$x, y \in \Gamma(E) \Rightarrow [x, y] \in \Gamma(E). \text{ (}^2\text{)} \tag{2.2}$$

The term integrable is here justified by the well-known theorem of Frobenius [7], Clebsch-Deahna to the effect that if E is integrable, then locally E is generated by

(1) This work was partially supported by National Science Foundation grant GP 9566.
(2) $\Gamma(E)$ denotes the set of smooth sections of E.

parallell translation—relative to some coordinate system—from a fixed k-plane E_0. Quite equivalently this may also be put in the following way:

There exists a covering $\{ U_\alpha \}$ *of* M *by coordinate patches* U_α, *with coordinates* $\{ x_1^\alpha, \ldots, x_n^\alpha \}$ *such that on* U_α, E *consists of the planes tangent to the slices*

$$x_{k+1}^\alpha = c_1 \ldots x_n^\alpha = c_q, \qquad q = n - k.$$

These slices are therefore local integral manifolds of maximal dimension, which fiber U_α into submanifolds of codimension q.

It follows that if one defines

$$f_\alpha : U_\alpha \to \mathbb{R}^q$$

by the formula

$$f_\alpha(p) = \{ x_{k+1}^\alpha(p), \ldots, x_n^\alpha(p) \}$$

then f_α defines a " submersion " of U_α in $\mathbb{R}^q$, in the sense that the differential of f_α,

$$df_\alpha : T_p U_\alpha \to T_{f(p)} \mathbb{R}^q$$

is *onto at each point of* U_α, and our previous slices now are simply the *fibers*, $f_\alpha^{-1}(p)$, of f_α.

The $\{ f_\alpha \}$ may therefore be thought of as a system of maximal local integrals of E, which completely describe E.

Now using the implicit function theorem, it is easy to see that because f_α and f_β are both submersions, one can, for each $x \in U_\alpha \cap U_\beta$, find diffeomorphisms:

$$g_{\alpha\beta}^x : W_\beta^x \to W_\alpha^x,$$

of a neighborhood of $f_\beta(x) \in \mathbb{R}^q$ into a neighborhood of $f_\alpha(x) \in \mathbb{R}^q$, such that near x

$$g_{\alpha\beta}^x \circ f_\beta = f_\alpha. \tag{2.3}$$

Finally, it follows from (2.3) and again the submersion property of f_α that for points near $x \in U_\alpha \cap U_\beta \cap U_j$:

$$g_{\alpha\beta}^x \circ g_{\beta j}^x = g_{\alpha j}^x. \tag{2.4}$$

I have written these equations mainly for future reference. At this point, I want you essentially only to understand that integrable subbundles E of TM can either be described by the integrability condition (2.2), or by a system of local integrals $\{ f_\alpha \}$ of E which are local submersions of M in $\mathbb{R}^q$. Then, in particular any global submersion $f : M \to N$ of one manifold on the other defines an integrable field or " foliation " on M. Thus, for instance, if f is a fibration, then the field of tangents along the fiber is always integrable. Integrable fields generated in this way may be thought of as the most trivial examples.

To show you what may happen in more interesting cases let me remind you of two classical examples.

The first is the foliation on the torus $\mathbb{R}^2/\mathbb{Z}$ induced by the " foliation " of $\mathbb{R}^2$ by lines of a given slope m:

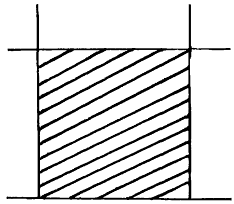


FIG. 1.

Thus, here I am drawing the " leaves ", i. e., *the maximal integral submanifolds* of the line field. If m is rational these leaves are all circles. If m is irrational they are all dense in T.

Next let me show you the beautiful Reeb foliation of the three sphere: First foliate the strip $|y| \leq 1$ in $\mathbb{R}^2$ as indicated in Figure 2:

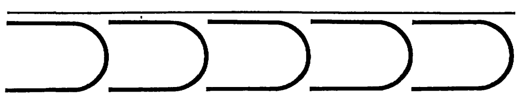


FIG. 2.

Next rotate this figure about the x-axis to obtain a foliation of a cylinder. There after identity points which differ by a integer x coordinate.

The result is a foliation of the anchor-ring,

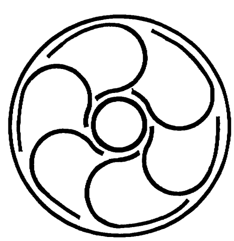


FIG. 3.

whose leaves are either planes coiling up to the bounding torus, or the bounding torus itself. Now if we take, for S^3 the set in complex 2-space $\mathbb{C}_2$, given by

$$| z_1 |^2 + | z_2 |^2 = 1,$$

it is easy to see that S^3 is the union of two anchor rings

$$S^3 = A_1 \cup A_2,$$

given by the equations $| z_1 | \leq | z_2 |$ and $| z_2 | \leq | z_1 |$ which intersect in the torus $T = \{ z_1 | = | z_1 | = 1/2 \}$. The foliations just described on A_1 and A_2 therefore fit together to form a foliation of S_3, which has one compact leaf, namely the torus T. All the other leaves are non-compact and curl up around this torus in opposite directions as we approach T from outside and inside. One may use this fact to show that this foliation though C^∞, is not *analytic*.

Concerning the higher spheres we know very little, in fact, we do not know whether any odd sphere S^n, of dim ≥ 3 admits an integrable $(n - 1)$ field (*). One only has A. Haefliger's beautiful result that: *analytic integrable $(n - 1)$-fields exist on a compact n-manifold only if its fundamental group is infinite.*

Another question which arises immediately in connection with this example is the existence of a compact leaf, and in this regard we have another beautiful result, due to Novikov, which asserts that every integrable 2-field on S^3 has a compact leaf. For 1-fields on S^3 it is not known whether a compact leaf has to exist. In fact, this is the famous Seifert problem. But these interesting and deep questions are really not pertinent to the problem (2.5) and I will have to leave them without further comment.

§ 3. On the nature of the global problem.

It is clear from the preceding that locally one can always construct integrable q-fields on a manifold M. The question therefore arises as to what difficulties one encounters in trying to construct a global field.

Now first of all, observe that difficulties will arise, because in general M does not admit a q-field, integrable or not. For instance, as is very well known, the 2-sphere S^2 admits no smooth line-field. On the other hand, the nature of this first question " does M admit a q-field ? " has been understood and much studied for many years. In particular, it has been converted into a purely homotopy-theoretic question.

Let me describe this translation to you, as it also points the way for our more refined question.

Please keep in mind during this development, that the homotopy theorist is a most singleminded person who treats only questions which can be phrased in terms of homotopy classes of continuous maps. Hence to please him we must convert all our geometric information into spaces and maps. In the present context this is not hard to do.

First of all one forms the Grassmanian variety

(3.1) $$G_m(\mathbb{R}^N) = \{ A \subset \mathbb{R}^N \}$$

consisting of the set of m-subspaces of $\mathbb{R}^N$, topologized by the requirement that two such subspaces A and B are close, if and only if the unit spheres of A and B are close in $\mathbb{R}^N$. Next one includes $\mathbb{R}^N \subset \mathbb{R}^{N+1}$ in a standard manner and takes the limit of the compact spaces $G_m(\mathbb{R}^N)$ under the induced inclusions, to obtain the space

(3.2) $$G_m = \lim_{N \to \infty} G_m(\mathbb{R}^N).$$

(*) Added November 10, 1970. Quite recently B. LAWSON has constructed such foliations on all spheres of dimension $2^k + 3$.

This " infinite Grassmanian " is of fundamental importance in topology, because it *classifies* the vector-bundle functor; that is, there is a natural m-vector bundle E_m over G_m, with the property that for any reasonable space X the set of isomorphism classes of m-vector bundles over X, say $\mathrm{Vect}_m(X)$, is naturally in one to one correspondance with the homotopy classes $[X, G_m]$ of maps of X into G_m.

(3.3) $$\mathrm{Vect}_m(X) \simeq [X, G_m].$$

This correspondence assigns to a map $f: X \to G_m$ the pullback $f^{-1}E_m$ of E_m to X.

In case some of you are lost at this point, let me describe for you a particular consequence of (3.3) in quite elementary terms.

First of all note that an imbedding of M in a Euclidean space, $M \subset \mathbb{R}^N$ induces a map

(3.4) $$\gamma : M \to G_m .$$

Indeed, simply let $\gamma(p)$ equal the subspace of $\mathbb{R}^N$ *parallel to the tangent plane to M at p.*

Now it turns out that these maps all belong to the same homotopy class $\gamma_M \in [M, G_m]$, and that this homotopy class which we refer to as the Gauss map of M, corresponds to the tangent bundle under the isomorphism (3.3).

The class γ_M is the first and fundamental homotopy theoretic invariant of the differentiable structure on M. Incidentally γ_M, also serves to define the *Pontrjagin ring* of M. This is the image of the cohomology $H^*(G_m; \mathbb{Q})$ under γ_M^* in $H^*(M; \mathbb{Q})$. In fact, quite generally, if E is any vector bundle over X, one defines its rational Pontrjagin ring by the formula

(3.5) $$\mathrm{Pont}\,(E) = f_E^* H^*(G_m; \mathbb{Q})$$

where $f_E : X \to G_m$ is the map corresponding to E under the isomorphism (3.3).

But to return to our problem of finding a k-plane field on M. The class γ_M is very pertinent to this question because, as is actually not hard to see, *constructing a k-field on M amounts to giving a " lifting " $\tilde{\gamma}$ of the Gauss map in the following diagram:*

$$\begin{tikzcd} & G_k \times G_{m-k} \arrow[d, "\pi"] \\ M \arrow[ur, dashed, "\tilde{\gamma}"] \arrow[r, "\gamma_M"'] & G_m \end{tikzcd}$$

Here π is induced by the direct sum maps

$$G_k(\mathbb{R}^N) \times G_{m-k}(\mathbb{R}^{N'}) \to G_m(\mathbb{R}^{N+N'})$$

sending (A, B) to $A + B$.

Problems of the type

(3.7) $$\begin{tikzcd} & Z \arrow[d] \\ X \arrow[ur, dashed] \arrow[r] & Y \end{tikzcd}$$

where the solid arrows are given homotopy classes of maps and a map from X to Z is sought which makes the diagram homotopy commutative, are called lifting problems and one has by now quite standard methods of treating them. Because, as we have just noted, the problem of constructing a k-field on M can be translated into such a lifting problem for the Gauss map, it is natural to ask whether our more refined question concerning the existence of integrable fields has a similar translation into a further lifting of γ_M. Now in the last two years Haefliger [5] and Milnor [7], using different approaches, but both based on deep results of Phillips [8, 9 and 10] and more generally Gromov [3], have essentially clarified the status of this question. Let me very briefly summarize Haefliger's point of view here.

Recall that an integrable E gave rise to *local* submersions

$$f_\alpha : U_\alpha \to \mathbb{R}^q,$$

and transition functions $g_{\alpha\beta}$ satisfying the equations (2.3) and (2.4). Haefliger now drops the condition that f_α be *submersions*, and considers more general systems $(f_\alpha, g_{\alpha\beta})$ satisfying only (2.3), and (2.4). Under a suitable equivalence relation, these systems give rise to a set-valued functor $\mathscr{H}_q(M)$, which one should think of as homotopy classes of foliations with singularities. The virtue of this construction is first of all that $\mathscr{H}_q$ makes sense on *all-spaces* (not just on manifolds!) is homotopy invariant and satisfies the " Meyer-Vietoris " condition of E. Brown [2]. Hence by Brown's general existence theorem there exists a space $B\Gamma_q$ which " classifies " $\mathscr{H}_q$. That is, there is a natural correspondence:

$$\mathscr{H}_q(X) = [X, B\Gamma_q]. \tag{3.8}$$

The space $B\Gamma_q$ thus plays the same role *relative* to $\mathscr{H}_q$ as the space G_q plays relative to the isomorphism classes of vector-bundles $\mathrm{Vect}_q(X)$. Furthermore, passing from Haefliger's " cocycle " $\{ f_\alpha, g_{\alpha\beta} \}$ to the differential $dg_{\alpha\beta}$ gives rise to a map

$$\nu : B\Gamma_q \to G_q \tag{3.9}$$

which expresses the fact that each element of $\mathscr{H}_q(M)$ has an associated " quotient-bundle ".

The construction of $\mathscr{H}_q$ and hence $B\Gamma_q$ now naturally leads to the questions:

A. How does the functor $\mathscr{H}_q(M)$ differ from the classes of integrable fields on M under a suitable equivalence relation?

B. To what extent does the homotopy of $B\Gamma_q$ differ from that of G_q?

For both these problems the Phillips-Gromov generalization of the Smale-Hirsch immersion theory it of fundamental importance. Essentially is enables one to push all the singularities of a " Haefliger structure " on open manifolds off to infinity. As a consequence on open manifolds any Haefliger structure compatible with the Gauss map is homotopic to an honest foliation! The precise result is as follows:

THEOREM I (Haefliger, Milnor). — *Let $\mathscr{E}_q(M)$ denote the classes of integrable plane fields on M of codimension q; under the following equivalence relation: two such fields E and E′ are equivalent if and only if there exists a field $\mathscr{E}$ of codimension q on $M \times I$,* *which is transversal to all the slices* $M \times$ const, *and induces* E (resp. E') *on the slice* $M \times 0$ (resp. $M \times 1$).

Then on open manifolds

(3.10) $$\mathscr{E}_q(M) = \textit{homotopy classes of liftings of } \gamma_M$$

in the diagram

(3.11)
$$\begin{tikzcd} & G_{m-q} \times B\Gamma_q \arrow[d, "1 \times \nu"] \\ & G_{m-q} \times G_q \arrow[d, "\pi"] \\ M \arrow[r, "\gamma_M"'] \arrow[uur, dashed] & G_m \end{tikzcd}$$

Concerning the second problem these same methods lead to the result.

THEOREM II (Haefliger, Milnor). — *The map* $\nu : B\Gamma_q \to G_q$ *induces isomorphisms in homotopy in dimension* $\leq q$ *and is onto in dimension* $\leq q + 1$.

Thus, in particular, combining these two theorems we see that if M is open and of the homotopy type of a complex of dimension $\leq q + 1$ then every plane field of codimension q on M is homotopic to an integrable one.

To summarize the situation, these developments show that first of all on open manifolds our problem reduces to a lifting problem, and secondly that in low dimensions integrability induces no new difficulty. In short, these theorems are both of the existence type.

I would finally like to report on the meager crop of *nonexistence* theorems which are at present known.

§ 4. Some global obstructions to integrability.

Classical obstruction-theory teaches one that a complete understanding of the obstructions to lifting a map from X to Y,

$$\begin{tikzcd} & Y \arrow[d, "\pi"] \\ M \arrow[r] \arrow[ur, dashed] & X \end{tikzcd}$$

involves, first of all, the homotopy groups of the " homotopy-theoretic fiber " of π. This is the space F which occurs as the inverse image of a point p in X under π, when π is replaced by a fibering in its homotopy class.

For instance if $F\Gamma_q$ denotes this fiber for the map $\nu : B\Gamma_q \to G_q$, so that we have the exact " sequence ":

(4.1) $$F\Gamma_q \to B\Gamma_q \to G_q ,$$

then Theorem II is quite equivalently expressed by the statement

(4.2) $$\pi_r(F\Gamma_q) = 0, \qquad \text{for} \qquad r \leq q.$$

The homotopy groups of the fiber are important because there is no impediment to lifting over successive skeletons as long as these homotopy groups are zero, while, in general the obstruction to lifting from t to the $(t+1)$st skeleton is in $H^{t+1}(M, \pi_t(F))$. Of particular interest therefore is the first nonvanishing homotopy group of F.

Now in many of the classical lifting problems one could get at this information because the universal spaces X and Y were given explicitly by some relatively easy constructions. For instance, in the classical problem $G_k \times G_{m-k} \xrightarrow{\pi} G_m$ all the spaces can be treated directly.

In the present instance, and this is really typical of all the more subtle modern universal spaces such as B_{Top}, B_{PL}, etc., the space $B\Gamma_q$ is not really known to us in any manageable manner, and one can therefore get at this type of information only by very roundabout methods.

At present only the following results are known about the higher homotopy of $F\Gamma_q$. First of all, J. Mather [6] has very recently constructed a surjection (*):

(4.3) $$\mathrm{Diff}_0(\mathbb{R}^1) \to \pi_2(F\Gamma_1) \to 0.$$

On the other hand, one can use the integrability condition which I noticed two years ago to prove that:

(4.4) *For $q \geq 2$, some $\pi_k(F\Gamma_q)$ is nonzero, and in fact not finitely generated.*

Let me remark briefly how this first nonexistence—or obstruction—result comes about.

First I recall the integrability criterion alluded to earlier [1].

INTEGRABILITY CRITERION: *A sub-bundle E of the tangent bundle TM is integrable only if the ring* Pont (T/E) *generated by the rational Pontrjagin classes of T/E vanishes in dimension greater than* $2 \times \dim (T/E)$

(4.5) $$\mathrm{Pont}^k (T/E) = 0 \quad \text{if} \quad k > 2 \dim T/E.$$

The proof of this proposition is very direct, provided only that one uses the geometric definition due to Pontrjagin, Chern, Weil of the Pontrjagin classes as real cohomology classes represented by differential forms. Indeed, to give a clue to the initiated in this geometric framework, the infinitesimal integrability condition can be exploited to define a connection on T/E which is flat *along the leaves*, and then the result follows immediately. Essentially the same construction can be used to strengthen this criterion as follows:

THEOREM III. — *The homomorphism*

(4.6) $$\nu^* : H^*\{G_q; \mathbb{Q}\} \to H^*(B\Gamma_q; \mathbb{Q})$$

is zero in dimensions greater than $2q$.

Now the rational cohomology of G_q is well known to be a polynomial algebra $\mathbb{Q}[P_1, \ldots, P_{[q/2]}]$ in the universal Pontrjagin classes $P_i \in H^{4i}(G_q, \mathbb{Q})$, and is therefore,

(*) $\mathrm{Diff}_0(\mathbb{R}^1)$ denotes the group of diffeomorphisms of $\mathbb{R}^1$ with compact support.

in particular, non-trivial in positive dimensions provided $q \geq 2$. By a standard spectral sequence argument it follows therefore that $\pi_k(F\Gamma_q)$ must be nontrivial for some k. To obtain the nonfinite generation, one still has to show that if one uses $\mathbb{Z}_p$ coefficients then:

$$(4.7) \qquad \nu^* : H^*(G_q, \mathbb{Z}_p) \to H^*(B\Gamma_q; \mathbb{Z}_p)$$

is injective.

To prove this one merely has to construct many examples of integrable fields E whose quotient bundles T/E have large mod p Pontrjagin rings, and such examples are easy to construct by taking E to be the horizontal space of flat vector bundles.

A question which seems to me of great interest is whether some of the groups $\pi_k(F\Gamma_q)$ are uncountable or not. In particular, one can relativize the integrability criterion to obtain homomorphisms of certain homotopy groups of $F\Gamma_q$ into the Reals and I would dearly like to know whether they are onto. The first case of interest occurs when $q = 3$ and in this situation the relative invariant gives rise to a homomorphism

$$(4.8) \qquad \theta : \pi_7(F\Gamma_3) \to \mathbb{R}.$$

Let me now conclude with a very brief remark about the complex analytic case, where some of these questions can be settled.

As is pointed out in Haefliger's paper [5], the space $B\Gamma_q$ should be thought of as the classifying space associated to the groupoid of *germs of diffeomorphisms of* $\mathbb{R}^q$. (Recall that the $g^x_{\alpha\beta}$ were local diffeomorphisms of $\mathbb{R}^q$). A corresponding construction for germs of *complex-analytic automorphism of* $\mathbb{C}^q$ is possible, and leads to a space $B\Gamma_q\mathbb{C}$. One also has a corresponding fibering

$$(4.9) \qquad F\Gamma_q\mathbb{C} \to B\Gamma_q\mathbb{C} \xrightarrow{\nu_{\mathbb{C}}} G\mathbb{C}_q$$

where now $G\mathbb{C}_q$ denotes the Grassmanian of complex subspaces of $\mathbb{C}^\infty$.

In this situation one can compute the relative invariants alluded to earlier and is then led to the

THEOREM IV. — *The homomorphism*

$$(4.10) \qquad \nu^*_{\mathbb{C}} : H^*\{G\mathbb{C}_q ; \mathbb{R}\} \to H^*(B\Gamma_q\mathbb{C}; \mathbb{R})$$

is zero in $\dim \geq 2q+1$.

Furthermore there exists a relative invariant θ_q *which maps* $\pi_{2q+1}(F\Gamma_q\mathbb{C})$ *onto* $\underbrace{\mathbb{C} \times \ldots \times \mathbb{C}}_{d(q)}$

$$(4.11) \qquad \pi_2(F\Gamma_q\mathbb{C}) \xrightarrow{\theta_q} \underbrace{\mathbb{C} \times \ldots \times \mathbb{C}}_{d(q)} \to 0$$

where $d(q) = \dim_{\mathbb{R}} H^{2(q+1)}(G\mathbb{C}_q, \mathbb{R})$.

In this case at least, I have therefore fulfilled my promise to introduce you to some genuinely huge spaces.

BIBLIOGRAPHY

[1] Raoul Bott. — On a topological obstruction to integrability, *Proceedings of Symposia in Pure Mathematics*, vol. XVI, Global Analysis, AMS, pp. 127-131.

[2] E. H. Brown. — Abstract homotopy theory, *Trans. Amer. Math. Soc.*, 119 (1965), pp. 79-85.

[3] M. L. Gromov. — *Izv. Akad. Nauk SSSR*, 33 (1969), pp. 707-734.

[4] A. Haefliger. — Structures feuilletées et cohomologie à valeur dans un faisceau de groupoïdes, *Comment. math. helvet.*, 32 (1958), pp. 248-329.

[5] —. — Feuilletages sur les variétés ouvertes, *Topology*, vol. 9, pp. 183-194.

[6] J. Mather. — *On Haefliger's classifying space* (in preparation).

[7] J. Milnor. — *Foilations and foliated vector bundles*, M. I. T., mimeographed notes, 1970.

[8] A. Phillips. — Submersions of open manifolds, *Topology*, 6 (1967), pp. 171-206.

[9] —. — Foliations on open manifolds. II, *Comment. math. helvet*, 44 (1969), pp. 367-370.

[10] —. — Smooth maps transverse to a foliation, to appear.

Department of Mathematics,
Harvard University
2 Divinity Avenue,
Cambridge, Mass. 02138
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 37 à 40.

MANIFOLDS AND HOMOTOPY THEORY (*)

by WILLIAM BROWDER (**)

If one considers the problem of classifying manifolds, as the dimension increases one soon finds even the homotopy type classification to be impossibly complex. For example, any finitely presented group is the fundamental group of some closed manifold for any dimension ≥ 4. Thus one is led to consider the problem of " relative classification ", such as (*a*) classifying up to diffeomorphism all the smooth manifolds of one fixed piecewise linear (*PL*) type, or (*b*) classifying up to homeomorphism all manifolds of one fixed homotopy type, etc. The prototype of such a theory is the theory of (*a*), which began with the work of Milnor on differential structures on spheres, and culminated in the smoothing theory developed by Hirsch, Mazur, Lashof and Rothenberg. Their theory may be described briefly as follows:

Given a *PL* manifold M^m, it has a *PL* stable tangent bundle τ_M, which is induced from the universal *PL* bundle over the classifying space B_{PL} by a map $f: M \to B_{PL}$. The classifying space for stable linear bundles B_0 maps into B_{PL}, $p: B_0 \to B_{PL}$, and if M has a smooth structure γ compatible with its *PL* structure, then the linear tangent bundle of the smooth M_γ defines a lift of f to $f': M \to B_0$ such that $pf' = f$.

THEOREM. — M has a compatible smooth structure if and only if τ_M has a linear structure, i. e., f lifts to $f': M \to B_0$, such that $pf' = f$. Furthermore, *concordance* classes of such structures correspond one to one to homotopy classes of lifts f' of f (homotopies lying over f).

COROLLARY. — If M is a smooth manifold, concordance classes of smooth structures on M compatible with a C^∞-triangulation are in 1-1 correspondence with elements in the homotopy set $[M, PL/0]$, where $PL/0$ is the fibre of the map $p: B_0 \to B_{PL}$.

(Two smooth structures on M are called concordant if there is a smooth structure on $M \times [0, 1]$ which restricts to the two structures at the two ends $M \times 0$ and $M \times 1$).

It remains a difficult problem to calculate the homotopy set $[M, PL/0]$, and in fact the calculation of $\pi_m(PL/0)$ depends on the homotopy groups of spheres. However, the neat and closed form of the result is attractive and useful for many applications. One would like to describe a similar theory for the problem of classifying manifolds

---

(*) A more detailed exposition on the subject of this talk is found in my article of the same title in the Proceedings of the Amsterdam Conference on Manifolds, 1970, Springer lecture notes.

(**) The author was partially supported by the National Science Foundation.

in a fixed homotopy type, and I will describe the analogous theory, and where the analogies break down.

A Poincaré pair is a pair $(X, \partial X)$ which satisfies Poincaré duality, i. e., there is an element $[X] \in H_n(X, \partial X)$ such that $[X] \cap : H^q(X) \to H_{n-q}(X, \partial X)$ is an isomorphism for all q. The *dimension* of X is defined to be n. If $\partial X = \emptyset$, X is called a Poincaré space, and for a Poincaré pair $(X, \partial X)$ of dimension n, it follows that ∂X is a Poincaré space of dimension $n - 1$.

Instead of a tangent bundle for a Poincaré pair $(X, \partial X)$, we define the Spivak normal fibre space of $(X, \partial X)$ which is the analog of the normal bundle of a smooth manifold $(M^m, \partial M) \subset (D^{m+k}, S^{m+k-1})$. If $(X, \partial X)$ is a connected Poincaré pair of dimension m, for $k > m + 1$ there is a $(k - 1)$ spherical fibre space ξ^k over X, and a pair of maps

$$(f, f_0) : (E_0(\xi), E_0(\xi \mid \partial X)) \to (Y, Y_0)$$

(where E_0 denotes the total space of the $(k - 1)$-spherical fibrations) such that

1) the pair $(X \bigcup_\pi E_0(\xi) \bigcup_f Y,\ \partial X \bigcup_\pi E_0(\xi \mid \partial X) \bigcup_{f_0} Y_0) = (A, B)$ is homotopy equivalent to (D^{m+k}, S^{m+k-1}), and

2) the map $f_{0*}: H_{m+k-2}(E_0(\xi \mid \partial X)) \to H_{m+k-2}(Y_0)$ is zero.

This fibre space is called the Spivak normal fibre space of $(X, \partial X)$ and it is unique up to fibre homotopy equivalence.

There is a classifying space B_G for stable spherical fibrations and maps

$$B_0 \to B_{PL} \to B_{\mathrm{Top}} \to B_G$$

(where B_{Top} is the classifying space for stable euclidean space bundles). If there is a smooth (PL, Top) manifold of the homotopy type of X then the classifying map of the Spivak normal fibre space ξ lifts to $B_0(B_{PL}, B_{\mathrm{Top}})$, but the converse is not true in general, which leads to a rich theory.

Note first that if one lift of ξ to B_H exists ($H = 0$, PL or Top) then the homotopy classes of lifts (homotopies covering a constant map into B_G) correspond 1-1 to elements of the set of homotopy classes of maps $[X, G/H]$, where G/H is the fibre of the map $B_H \to B_G$.

Let us define the set of concordance classes of homotopy H-structures ($H = 0$, PL or Top) on $X = \mathscr{S}^H(X)$ as follows. Consider pairs (M, h) where M is a manifold (in the category of H) and $h: (M, \partial M) \to (X, \partial X)$ is a homotopy equivalence of pairs. Two pairs (M_i, h_i), $i = 0, 1$, are concordant if there is a cobordism W, $\partial W = M_0 \cup M_1 \cup V$, $\partial V = \partial M_0 \cup \partial M_1$ and a homotopy equivalence of pairs

$$k: (W, V) \to (X \times [0, 1], \partial X \times [0, 1])$$

with

$$h(x) = (h_i(x), i) \qquad \text{for} \qquad x \in M_i.$$

Then $\mathscr{S}^H(X)$ is the set of concordance classes of such pairs.

The development of theory of surgery by Milnor, Kervaire, S. P. Novikov, the author, and Sullivan has culminated in the following theorem:

THEOREM. — Let X be a 1-connected Poincaré space of dimension $n \geq 5$ and suppose that its Spivak normal fibre space admits an H-structure ($H = 0$, PL or Top). Then there is an exact sequence of sets

$$P_{n+1} \xrightarrow{\omega} \mathscr{S}^H(X) \xrightarrow{\eta} [X, G/H] \xrightarrow{\sigma} P_n$$

where

$$P_n = \begin{cases} 0 & n \text{ odd} \\ Z & n = 4k \\ Z_2 & n = 4k + 2 \end{cases}$$

Here ω is defined if $\mathscr{S}^H(X) \neq \emptyset$, and in that case there is an action of P_{n+1} on $\mathscr{S}^H(X)$ such that $\eta(x) = \eta(x')$ if and only if x, x' are in the same orbit of the action.

In the case of pairs we have the result of Wall:

THEOREM. — If $(X, \partial X)$ is a Poincaré pair of dimension $m \geq 6$, with X, ∂X 1-connected, $\partial X \neq \emptyset$, and suppose the Spivak normal fibre space admits an H-structure ($H = 0$, PL or Top). Then $\mathscr{S}^H(X) = [X, G/H]$.

(The techniques used were proved first in the smooth case ($H = 0$), and extended to the PL case using the smoothing theory of PL manifolds above, and recently extended to the topological case using the work of Kirby and Siebenmann).

Thus we see an exact analogy with the smoothing theory of PL manifolds where $\partial X \neq \emptyset$, but in case $\partial X = \emptyset$ there is an obstruction to getting the analogous result, an obstruction lying in the group P_n. The underlying reasons for the difference in the theories arise from transversality. One has a Thom transversality theorem for either linear or PL bundles (or even Top bundles for higher dimensions) and this makes possible the exact correspondence between smoothings and lifts. But transversality fails for spherical fibre spaces and this failure is what creates the obstruction groups P_n. This relation has been precisely described in recent work of Levitt, which gives an obstruction theory to transversality for a map of a manifold M into a spherical fibre space, with values in cohomology $H^{j+1}(M : P_j)$.

The whole theory has been generalized by Wall to the non-simply connected case, where one assumes Poincaré duality with local coefficients, and other properties. Then one gets a similar exact sequence as above, and the obstruction groups depend only on the fundamental group system of X, ∂X and are again periodic of period 4. These obstruction groups are algebraically defined, for example, for $\partial X = \emptyset$, as certain Grothendieck groups of quadratic forms over $Z\pi$ or automorphisms of forms. This is analogous to the simply connected case where P_n is the Grothendieck group of even, unimodular Z-forms for $n = 4k$, or non-singular Z_2-quadratic forms for $m = 4k + 2$. The calculation of these groups (over $Z\pi$) has proven very difficult, and there is much work going on in this direction by both geometers and algebraic K-theorists.

For the term in the exact sequence $[X, G/H]$, the calculation is very difficult for $H = 0$, because again the homotopy groups of spheres are closely related. For $H = PL$ however, the homotopy properties of G/PL have been very well analyzed by Sullivan, and the work of Kirby-Siebenmann has enabled one to extend Sullivan's results to G/Top. The results make possible the explicit description of [X, G/Top], in terms of the cohomology and real K-theory of X, and have been used in the topological and PL classification of homotopy projective spaces, lens spaces, and many other manifolds.

Princeton University
Department of Mathematics,
Fine Hall, Box 37
Princeton, N. J. 08540
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 41 à 53.

DIFFERENTIAL GEOMETRY; ITS PAST AND ITS FUTURE

by SHIING-SHEN CHERN (*)

A. Introduction.

It was almost a century ago, in 1872, that Felix Klein formulated his Erlanger Program. The idea of unifying the geometries under the group concept is simple and attractive and its applications in the derivation of different geometrical theorems from the same group-theoretic argument are usually of great elegance. This leads to the development of differential geometries of submanifolds in homogeneous (or Klein) spaces: conformal, affine, and projective differential geometries. The latter had in particular an energetic development in the twenties.

It was also about a century ago that the greatest modern differential geometer Elie Cartan was born (on April 9, 1869). Among his contributions of a basic nature are his systematic use of the exterior calculus and his clarification of the global theory of Lie groups. Fiber spaces also find their origin in Cartan's work.

Differential geometry is the study of geometry by the methods of infinitesimal calculus or analysis. Among mathematical disciplines it is probably the least understood ([1]). Many mathematicians feel there is no geometry beyond two and three dimensions. The advent into higher and even infinitely many dimensions does make the intuition unreliable and the dependence on algebra and analysis mandatory. The basis of algebra is the algebraic operations and the basis of analysis is the topological structure. I would like to surmise that the core of differential geometry is the Riemannian structure (in its broad sense).

The main object of study in differential geometry is, at least for the moment, the differentiable manifolds, structures on the manifolds (Riemannian, complex, or other), and their admissible mappings. On a manifold the coordinates are valid only locally and do not have a geometrical meaning themselves. Historically the difficulty in achieving a proper understanding of this situation must have been tremendous (I wonder whether this was part of the reason which caused Hadamard to admit his

---

(*) This paper was written when the author held a Research Professorship of the Miller Institute and was under partial support of NSF grant GP 20096.

([1]) G. D. BIRKHOFF, « The second is a disturbing secret fear that geometry may ultimately turn out to be no more than the glittering intuitional trappings of analysis ». Fifty years of American mathematics, *Semicentennial Addresses of Amer. Math. Soc.* (1938), p. 307.

G. W. MACKEY, « Geometrical intuition, while very helpful, is not reliable and cannot be depended upon for rigorous arguments », *Lectures on the Theory of Functions of a Complex Variable*, p. 21, Van Nostrand, notes.

psychological difficulty in the mastery of Lie groups) ([2]). For technical purposes the Ricci calculus was a powerful tool, but it is inadequate for global problems. Global differential geometry, with the exception of a few isolated results, had to wait till algebraic topology and Lie groups have paved the way.

Global differential geometry must be considered a young field. The notion of a differentiable manifold should have been in the minds of many mathematicians, but it was H. Whitney who found in 1936 a theorem to be proved: the imbedding theorem. In the case of the richer complex structure a definition of a Riemann surface by overlapping neighborhoods was given and the theory rigorously treated by H. Weyl in his famous book " Idee der Riemannschen Fläche, Göttingen, 1913 " ([3]), following which Caratheodory gave the first definition of a high-dimensional complex manifold. More general pseudo-group structures were treated by Veblen and J. H. C. Whitehead in 1932 [34]. Only special cases of the general theory, such as Riemannian, conformal, complex, foliated structures, etc. have been found significant.

B. The development of some fundamental notions and tools.

Perhaps the most far-reaching achievement in differential geometry in the last thirty years lies in its foundation. Not only are the notions clearly defined, but notations are devised to treat manifolds which could be infinite-dimensional. The notations are up to now on the diversive side and are thus at an experimental stage. We believe in the survival of the fittest. Important as these foundational works are, no mathematical discipline can prosper without deeper study and simple challenging problems. We will comment briefly on a few fundamental developments in differential geometry and its related subjects, without endeavoring to make the list complete.

(1) *Lie Groups.* — It is one of the happiest incidents in the history of mathematics that the structure of Lie groups can be so thoroughly analyzed. The existence of the five exceptional simple Lie groups makes a deep study necessary and leads to a better understanding. Even so the subject has unity and is so much simpler than (say) finite groups. The quotient spaces of Lie groups give a multitude of examples of manifolds which are easy to describe. They include the classically important spaces and form a reservoir on which new conjectures can be tested.

(2) *Fiber Spaces.* — When a manifold has a differentiable structure, it can be locally linearized, giving rise to the tangent bundle and the associated tensor bundles. The first idea of a connection in a fiber bundle with a Lie group can be found in Cartan's " espaces généralisés ". It was algebraic topology which focused on the simplest problems, e. g., the problem of introducing invariants which serve to distinguish a general

([2]) J. Hadamard, *Psychology of Invention in the Mathematical Field*, Princeton (1949), p. 115.

E. Cartan, in his classical « Leçons sur la géometrie des espaces de Riemann » says, « La notion générale de variété est assez difficile à définir avec précision », p. 58.

([3]) Weyl's book was dedicated to Felix Klein, to whom he acknowledged for the fundamental ideas. Weyl's definition of a Riemann surface and Hausdorff's introduction of his axioms in 1914 must have made it superfluous to give formally a definition of a differentiable manifold. Chevalley's book on Lie groups (1946) exerted a great influence in the clarification of many concepts attached to it.

fiber bundle from a product bundle. Among them are the characteristic classes. Characteristic classes with real coefficients can be represented by the curvature of a connection, the simplest example being the Gauss-Bonnet formula. The bundle structure is now an integral part of differential geometry.

(3) *Variational Methods.* — The importance of the notion of measure (length, area, volume, curvature, etc.) makes the variational method a powerful and indispensable tool. The study of geodesics on a Riemannian manifold is a brilliant chapter of mathematics. It led to Morse's creation of the critical point theory whose scope extends far beyond differential geometry. Another example is the Dirichlet problem and its application to elliptic operators. Multiple integral variational problems open a vista whose terrain is still rocky. It promises, however, a fertile field of work. When a geomatrical problem involves a function, either over the given manifold or in some related functional space, it always pays to look at its critical values and the second variation at them. Much of differential geometry utilizes this idea, in its various ramifications. The importance of variational method in differential geometry can hardly be over-emphasized.

(4) *Elliptic Differential Systems.* — The geometrical properties of differential geometry are generally expressed by differential equations or inequalities. Contrary to analysis special systems with their special properties received more attention. While analysis is the main tool, geometry furnishes the variety. Differential systems on manifolds with or without boundary are the prime objects of study.

Elliptic systems occupy a central position because of their rich properties, which follow from the severe restrictions on the set of solutions. Hodge's harmonic differential forms, with their applications to Kahlerian manifolds, will remain a crucial landmark. A simple idea of Bochner relates them to curvature and leads to vanishing theorems when the curvature satisfies proper " positivity " conditions. This has remained a standard method in the establishment of such theorems, which in turn give rise to existence theorems. The indices of linear elliptic operators on a compact manifold include some of the deepest invariants of manifolds (Atiyah, Bott, Singer).

In the study of mappings an important problem consists in the analysis of the singularities. Important progress has been made recently on the singularities of differentiable mappings (Whitney, Thom, Malgrange, Mather). If the mappings are defined by elliptic differential equations, cases are known where the singularities take relatively simple form. Singularities in differential geometry remain a relatively untouched subject.

C. **Formulation of some problems with discussion of related results.**

We will attempt to discuss some areas where it is believed that fruitful researches can be carried out. The limited time at my disposal and, above all, my own limitation make it impossible for the treatment to be even remotely exhaustive. Any subject left out carries no implication that it is considered less significant.

My object is to amuse you by stating some very simple problems which have so far defied the efforts of geometers. The danger in formulating such problems is that the line distinguishing them from mathematical puzzles is thin. Personally I think there is no such line except that the " serious " problems concern with a new domain where the phenomena are not well understood and the basic concepts not well developped. Geometry and analysis on manifolds are still at this stage and will remain so for years to come. When such problems are solved, similar ones will tend toward puzzles.

Many of the problems to be given below are known. It is hoped that its collection may attract mathematicians not engaged in this field and lead to further progress.

1. Riemannian manifolds whose sectional curvatures keep a constant sign

It was known to Riemann that the local properties of a Riemannian structure are completely determined by its sectional curvature. The latter is a function $R(\sigma)$ of a two-dimensional subspace σ of the tangent space at a point x, which is equal to the gaussian curvature of the surface generated by the geodesics tangent to σ at x. Manifolds for which $R(\sigma)$ keeps a constant sign for all σ have a simple geometrical meaning. For their global study it is important to require that they are not proper open subsets of larger manifolds and, following Hopf and Rinow, it is customary to impose the stronger completeness condition: every geodesic can be indefinitely extended. In fact, without the completeness requirement the sign of the sectional curvature imposes hardly any condition on the manifold, as Gromov [21] proved that there exists on any non-compact manifold a Riemannian metric for which the range of the values of $R(\sigma)$ is any open interval on the real line.

For *complete* Riemannian manifolds M for which $R(\sigma)$ keeps the same sign the two classical theorems are:

(1) Theorem of Hadamard-Cartan. — If $R(\sigma) \leqslant 0$, the universal covering manifold of M is diffeomorphic to R^n, $n = \dim M$.

(2) Theorem of Bonnet-Myers. — If $R(\sigma) \geqslant c$ ($=$ const) > 0, M has a diameter $\leqslant \pi/c^{1/2}$ and is therefore compact.

The case of positive curvature turns out to be more elusive. Cheeger and Gromoll [9] achieved what is essentially a structure theory of non-compact complete Riemannian manifolds M with $R(\sigma) \geqslant 0$ (all σ) by proving the following theorem. There is in M a compact totally geodesic and totally convex submanifold S_M (to be called the soul of M) without boundary such that M is diffeomorphic to the normal bundle of S_M. If the sectional curvature is strictly positive, then Gromoll and Meyer [20] proved that the soul is a point and M is diffeomorphic to R^n. In particular, M must be simply connected.

Compact Riemannian manifolds of positive curvature obviously satisfy the stronger condition $R(\sigma) \geqslant c > 0$ (all σ). By the Bonnet-Myers Theorem they are identical with the complete Riemannian manifolds with the same property. They are not necessarily simply connected, as the example of the non-euclidean elliptic space shows. So far the simply connected compact differentiable manifolds known to admit a Riemannian metric of positive curvature are the following [3]: (1) the n-sphere; (2) the complex projective space; (3) the quaternion projective space; (4) the Cayley plane; (5) two manifolds discovered by Berger, of dimensions 7 and 13 respectively.

It is very unlikely that there are no others, but nothing more is known. The following question was asked by H. Hopf:

PROBLEM I. — Does the product of two 2-dimensional spheres admit a Riemannian metric of strictly positive curvature?

More generally, it is not known whether the exotic 7-spheres, some of which are bundles of 3-spheres over 4-spheres, admit Riemannian metrics of positive curvature. The answer to the question in Problem I is probably negative. A supporting evidence is furnished by the following theorem of Berger [5]: Let M and N be compact Riemannian manifolds. Let $g(t)$ be a family of Riemannian structures on $M \times N$, such that $g(0)$ is the product structure and such that the following condition is satisfied:

$$\left.\frac{dR(\sigma)}{dt}\right|_{t=0} \geqslant 0$$

for all σ spanned at $x \in M \times N$ by a tangent vector to M and a tangent vector to N. Then

$$\left.\frac{dR(\sigma)}{dt}\right|_{t=0} = 0$$

for all such σ.

To get deeper topological properties of a manifold of positive curvature Rauch introduced the notion of *pinching*. M is said to be β-pinched if $0 < \beta \leqslant R(\sigma) \leqslant 1$ for all σ. After the pioneering work of Rauch the following are the main theorems on the topology of compact pinched Riemannian manifolds of positive curvature:

(1) (Berger-Klingenberg) [4, 25]. If a simply connected Riemannian manifold of positive curvature is β-pinched, $\beta > \frac{1}{4}$, it is homeomorphic to the n-sphere; if $\beta = \frac{1}{4}$ and it is not homeomorphic to the n-sphere, it is isometric to a symmetric space of rank 1.

(2) (Gromoll-Calabi) [19]. Let M be an n-dimensional compact simply connected Riemannian manifold of positive curvature. There exists a universal constant $\beta(n) < 1$, depending only on n, such that if M is $\beta(n)$-pinched, it is diffeomorphic to the standard n-sphere.

Similar problems can be studied on the global implications of curvature properties of complex Kählerian manifolds. A new feature is the notion of holomorphic sectional curvature, i. e., sectional curvature $R(\sigma)$, where σ is the two-dimensional real space underlying a complex line in the complex tangent space. A most attractive question is the following one formulated by Frankel:

PROBLEM II. — Let M be a compact Kählerian manifold of positive sectional curvature. Is M biholomorphically equivalent to the complex projective space?

Andreotti and Frankel [17] proved that the answer is affirmative if M is of dimension 2. The proof makes use of the classification of algebraic surfaces. Partial results were recently obtained by Kobayashi and Ochiai [26] for 3 dimensions.

2. EULER-POINCARÉ CHARACTERISTIC

Among the important topological invariants of a manifold is the Euler-Poincaré characteristic. Its role is well-known on problems such as the Lefschetz fixed-point theorem, singularities of vector fields, and indices of some elliptic operators. Geometrically it is closely related to the total curvature (*curvatura integra*) as expressed by the Gauss-Bonnet formula

$$\chi(M) = \frac{(-1)^m}{2^{3m}\pi^m m} \int_M \left(\sum_{i,j} \varepsilon_{i_1 \dots i_{2m}} \varepsilon_{j_1 \dots j_{2m}} R_{i_1 i_2 j_1 j_2} \cdots R_{i_{2m-1} i_{2m} j_{2m-1} j_{2m}}\right) dv \qquad (1)$$

Here M is a compact orientable Riemannian manifold of even dimension $n = 2m$, $\chi(M)$ is its Euler-Poincaré characteristic, dv is the volume element, and R_{ijkl} are the components of the curvature tensor relative to ortho-normal frames. The $\varepsilon_{i_1 \dots i_{2m}}$ is the Kronecker symbol and is zero if $i_1, \dots, i_{2m}$ do not form a permutation of $1, \dots, 2m$ and is equal to $+1$ or -1 according as the permutation is even or odd.

In spite of the explicit expression for $\chi(M)$ the following has not been established:

Problem III and conjecture. — If M has sectional curvatures $\geqslant 0$, then $\chi(M) \geqslant 0$. If M has sectional curvatures $\leqslant 0$, then $\chi(M) \geqslant 0$ or $\leqslant 0$, according as $n \equiv 0$ or $2 \bmod 4$.

The above statement has been proved for $n = 4$ [10] and for the case that M has constant sectional curvature. A first approach would be to study the sign of the integrand in the Gauss-Bonnet formula, a purely algebraic problem. Even this algebraic problem seems to be of great interest [33].

As with the classical Gauss-Bonnet formula the relationship is more useful for compact manifolds with boundary (in which case a boundary integral should be added to make the formula (1) valid) and the problem is more interesting for non-compact manifolds, because a deeper study of the geometry will then be necessary. We will denote by $C(M)$ the right-hand side of (1) and we shall formulate the problem:

Problem IV. — Let M be a complete Riemannian manifold of even dimension. Suppose $\chi(M)$ and $C(M)$ both exist, the latter meaning that the corresponding integral converges. Find a geometrical interpretation of the difference

$$\delta(M) = \chi(M) - C(M).$$

Of course $\delta(M) = 0$ if M is compact. In two dimensions Cohn-Vossen's classical inequality says that $\delta(M) \geqslant 0$. For a class of two-dimensional manifolds Finn and A. Huber [16, 23] obtained a geometrical interpretation of $\delta(M)$, which implies that it is non-negative. Partial results on Problem IV have been obtained by E. Portnoy [30]. Perhaps the case of Kählerian manifolds has a simpler answer and should be studied first.

In a different direction Satake [31] obtained a Gauss-Bonnet formula for his V-manifolds and applied it to automorphic functions and number theory. V-manifolds are essentially manifolds with singularities of a relatively simple type.

Another problem on the Euler-Poincaré characteristic concerns compact affinely connected manifolds which are locally flat. These can be described as manifolds with a linear structure, i. e., having a covering by coordinate neighborhoods such that the coordinate transformation in overlapping neighborhoods is linear.

Problem V. — Let M be a compact manifold with an affine connection which is locally flat. Is its Euler-Poincaré characteristic equal to zero?

Bensecri proved that the answer is affirmative if M is of two dimensions (For proof and generalization cf. Milnor [27]). The high-dimensional case has been investigated by L. Auslander who proved the theorem [1]: suppose the affine connection be complete and suppose that the homomorphism $h : \pi_1(M) \to GL(n, R)$ defined by the holonomy group is not an isomorphism of the fundamental group $\pi_1(M)$ onto a discrete subgroup of $GL(n, R)$. Then $\chi(M) = 0$.

It is not known whether h can imbed $\pi_1(M)$ as a discrete subgroup of $GL(n, R)$.

In spite of great developments in algebraic topology there are simple problems on the Euler-Poincaré characteristic which remain unanswered.

3. Minimal submanifolds

A minimal submanifold is an immersion $x : M^n \to X^N$ of an n-dimensional differentiable manifold M^n (or simply M) into a Riemannian manifold X^N of dimension N, which *locally* solves the Plateau problem: Every point $x \in M$ has a neighborhood U such that U is of smallest n-dimensional area compared with other n-dimensional submanifolds having the same boundary ∂U. Analytically the condition can be expressed as follows: Let D^2x be the second differential on M in the sense of Levi-Civita. Then (D^2x, ξ), where ξ is a normal vector to M at x, is a quadratic differential form, the second fundamental form relative to ξ. The differential equation to be satisfied by M is

$$\mathrm{Tr}\,(D^2x, \xi) = 0, \qquad \text{all } \xi. \tag{2}$$

It is a system of non-linear elliptic partial differential equations of the second order, whose number is equal to the codimension $N - n$. A minimal submanifold of dimension one is a geodesic.

We wish to study the properties of complete minimal submanifolds in a given Riemannian manifold X^N (cf. [12]). Except for geodesics the interest has so far been restricted to the case when the ambient space X^N is either the Euclidean space E^N or the unit sphere $S^N(1)$ imbedded in E^{N+1}.

For a minimal submanifold $x : M^n \to E^N$ in the Euclidean space a condition equivalent to (2) is that the coordinate functions are harmonic (relative to the induced metric). It follows that for $n > 0$ a complete minimal submanifold in E^N is non-compact.

For various reasons the case of codimension one (i. e., the minimal hypersurfaces) is the most important. Let $x_1, \ldots, x_n, z$ be the coordinates in E^{n+1}. Consider minimal hypersurfaces defined by the equation

$$z = F(x_1, \ldots, x_n) \tag{3}$$

for all $x_1, \ldots, x_n$. The following fundamental theorem generalizes the classical theorem of Bernstein and was the combined effort of de Giorgi ($n = 3$), Almgren ($n = 4$), Simons ($n \leqslant 7$), Bombieri, de Giorgi, Giusti ($n \geqslant 8$) [6, 32]. The minimal hypersurface defined by (3) must be a hyperplane for $n \leqslant 7$ and is not always a hyperplane for $n \geqslant 8$.

The main reason for this difference is the existence of absolute minimum cones in high-dimensional Euclidean space, which in turn depends on properties of compact minimal hypersurfaces in $S^n(1)$. From a general viewpoint the study of compact minimal submanifolds in $S^N(1)$ is attractive for its own sake. The first uniqueness theorem is the theorem of Almgren-Calabi [11]. If a two-sphere is immersed as a minimal surface in $S^3(1)$, it must be the equator.

By a counter-example of Hsiang [22] this theorem is not true for the next dimension. However, the following question, which can be designated as the " spherical Bernstein problem ", is unanswered:

PROBLEM VI. — Let the n-sphere be *imbedded* as a minimal hypersurface in $S^{n+1}(1)$. Is it an equator?

Two-dimensional minimal surfaces in E^N and in $S^N(1)$ have been more thoroughly studied, because of the application of complex function theory. If the surface is itself a two-sphere (hence in $S^N(1)$), severe restriction is imposed for global reason and we have the following theorem (Boruvka, do Carmo, Wallach, Chern, but mainly Calabi [8, 14]). Let the two-sphere be immersed in $S^N(1)$ as a minimal surface, such that it does not belong to an equator. Then we have: (1) N is even; (2) The total area of the surface is an integral multiple of 2π; (3) If the induced metric is of constant Gaussian curvature, it is completely determined up to motions in $S^N(1)$ and the Gaussian curvature has the value

$$K = \frac{2}{m(m+1)}, \qquad N = 2m. \tag{4}$$

(4) There are minimal two-spheres in $S^N(1)$ of non-constant Gaussian curvature; all these with a given area form a finite-dimensional space.

The immersion of the n-sphere as a minimal submanifold of $S^N(1)$ is a fascinating problem. If the induced metric has constant curvature, the immersion is given by the spherical harmonics (Takahashi). For $n > 2$ two isometric minimal immersions $S^n(a) \to S^N(1)$ are not necessarily equivalent under the motions of the ambient space (do Carmo, Wallach [15]). In view of the precise results on the two-sphere we wish to propose the following problem:

PROBLEM VII. — Consider minimal immersions $S^n \to S^N(1)$ with total area $\leqslant A$ ($=$ const) and identify those which differ by a motion of the ambient space. Is the resulting set a finite-dimensional space with some natural topology?

4. ISOMETRIC MAPPINGS

A differentiable mapping f: M $\to$ V of Riemannian manifolds is called *isometric* if it preserves the lengths of tangent vectors. It is therefore necessarily an immersion, and $\dim M \leqslant \dim V$. Classical differential geometry deals almost exclusively with the case that V is the Euclidean space E^N of dimension N. We believe this is the most interesting case and we will adopt this restriction in our discussion.

The first problem is that of existence. Since the fundamental tensor on a Riemannian manifold of dimension n involves $n(n+1)/2$ components, Schläfli conjectured in 1871 that every Riemannian manifold of dimension n can be locally imbedded in E^N, with $N = \frac{1}{2}n(n+1)$. This was proved by Elie Cartan in 1927 for the real analytic case. For smooth non-analytic manifolds this local isometric imbedding problem is unsolved, even for $n = 2$, unless some restriction on the metric is imposed such as the Gaussian curvature keeping a constant sign. In other words, it is not known whether any smooth two-dimensional Riemannian manifold can be locally isometrically imbedded in E^3. The answer is probably negative.

The two important global imbedding theorems are:

(1) (Weyl's Problem). A compact two-dimensional Riemannian manifold of positive Gaussian curvature can be isometrically imbedded in E^3 (as a convex surface).

(2) (Nash's Theorem [18, 28]). A compact (resp. non-compact) C^∞ Riemannian manifold of dimension n can be isometrically imbedded in E^N,

$$N = \frac{1}{2}n(3n + 11) \quad (\text{resp. } N = 2(2n + 1)(3n + 7))\ (^4)$$

The second problem is the uniqueness of the isometric imbedding, also called rigidity, which is the problem whether an isometric immersion is determined up to a rigid motion of the ambient space E^N. Most interesting is the classical case of surfaces in E^3. Cohn-Vossen proved the rigidity of compact surfaces with Gaussian curvature $K > 0$ and the theorem was extended by Voss [35] to the case $K \geqslant 0$. Even before Cohn-Vossen, Liebmann proved that a smooth family of isometric compact convex surfaces (i. e., $K > 0$) is trivial, i. e., it consists of the surfaces obtained by the rigid motion of one member of the family. It is not known whether the same is true when the curvature condition is dropped and we believe the following problem is fundamental:

Problem VIII. — Let M be a compact surface and I be the interval $-1 < t < 1$. Let $f: M \times I \to E^3$ be a differentiable mapping such that $f_t : M \to E^3$ defined by $f_t(x) = f(x, t)$, $x \in M$, $t \in I$, is an immersion for each t. Suppose that the metric ds_t^2 induced by f_t on M is independent of t. Does there exist a rigid motion $g(t)$ such that

$$f_t(x) = g(t) f_0(x), \qquad x \in M, \tag{5}$$

where the right-hand side denotes the action on f_0 by $g(t)$?

The following remarks may be relevant to the problem. Cohn-Vossen [13] proved the existence of an unstable family of compact surfaces of revolution, i. e., that the above conclusion is not true if the hypothesis that ds_t^2 is independent of t is replaced by

$$\frac{\partial}{\partial t} ds_t^2 \,|_{t=0} = \frac{\partial^2}{\partial t^2} ds_t^2 \,|_{t=0} = 0 \tag{6}$$

There are well-known examples showing that Cohn-Vossen's rigidity theorem is not true without the convexity condition $K \geqslant 0$. A generalization of the latter condition to surfaces of higher genus is the notion of *tightness*. Let $f: M \to E^3$ be an immersed surface. The tangent plane at a point x is a local (resp. global) support plane if a neighborhood of the surface at x (resp. the whole surface $f(M)$) lies at one side of it. The surface is called tightly immersed if every local support plane is a global

(4) The value for N in the case of non-compact manifolds is an improvement of Nash's value by Greene [18].

support plane. A. D. Alexandrow proved that a real analytic tightly imbedded surface of genus one is rigid and Nirenberg [29] replaced the analyticity condition by some other conditions.

On the other hand, the notion of tightness has a meaning for polyhedral surfaces. In this case the rigidity problem asks whether the congruence of corresponding faces of two tightly imbedded polyhedral surfaces implies that they differ by a rigid motion. Cauchy's classical theorem says that this is true if the surfaces are of genus zero. But Banchoff [2] has constructed examples showing that this is untrue for surfaces of genus one. From these remarks it is anybody's guess whether the answer to the question in Problem VIII is affirmative or negative.

When M is of dimension greater than two, isometry is a strong condition and there are local rigidity theorems.

5. Holomorphic mappings

A holomorphic mapping $f: M \to V$ of complex manifolds is a continuous mapping which is locally defined by expressing the coordinates of the image point as holomorphic functions of those of the original point. The most significant example is the case when M is the complex line C and V is the complex projective line $P_1(C)$ (or the Riemann sphere), in which case the mapping is known as a meromorphic function. Much recent progress has been made in extending classical geometrical function theory to the study of holomorphic mappings.

A holomorphic mapping is called non-denegerate if the Jacobian matrix is of maximum rank at some point. For given M, V there may not exist a non-degenerate holomorphic mapping. Let B be a closed subset of V. Classically the following problem has been much studied.

Intersection or non-existence problem. Find B such that there is no non-degenerate holomorphic mapping $M \to V - B$, i. e., every non-degenerate holomorphic mapping $f: M \to V$ has the property $f(M) \cap B \neq \emptyset$.

The Picard theorem concerns the case $M = C$, $V = P_1(C)$, and B is the set of three distinct points. Clearly if the property holds for B, it holds for a subset containing B, so that a stronger theorem results from a smaller subset B. In view of the extreme importance and elegance of the Picard theorem, we wish to state the following conjecrure of Wu:

Problem and conjecture IX. — Let C_n be the n-dimensional complex number space and $P_n(C)$ the n-dimensional complex projective space. Let B be the set of $n + 2$ hyperplanes of $P_n(C)$ in general position (i. e., any $n + 1$ of them are the faces of a non-degenerate n-simplex). Then there is no non-degenerate holomorphic mapping $C_n \to P_n(C) - B$.

The Picard theorem says that this is true for $n = 1$. Wu has established this for $n \leqslant 4$. Moreover, if we set

$$\rho(n) = \begin{cases} \left(\dfrac{n}{2} + 1\right)^2 + 1, & n \text{ even} \\ \left(\dfrac{n+1}{2}\right)\left(\dfrac{n+3}{2}\right) + 1, & n \text{ odd,} \end{cases}$$

and let B' be the set of $\rho(n)$ hyperplanes in general position in $P_n(C)$, then Wu [36] proved that every holomorphic mapping $f: C_n \to P_n(C) - B'$ must reduce to a constant.

A far-reaching generalization of the Picard theory is the equi-distribution theory of Nevanlinna, which studies the frequency that a non-constant meromorphic function takes given values. In terms of vector bundles the problem can be generalized as follows [7]. Let M be a complex manifold and $p: E \to M$ a holomorphic vector bundle over M. A holomorphic mapping $s: M \to E$ is called a section if $p \cdot s =$ identity. Let W be a finite-dimensional vector space of holomorphic sections. Suppose the manifold and the bundle fulfill some convexity conditions (which are automatically satisfied in the classical case). Then we can define, to each $s(\neq 0) \in W$, a defect $\delta(s)$ satisfying the conditions: (1) $0 \leqslant \delta(s) \leqslant 1$; (2) $\delta(\lambda s) = \delta(s)$, $\lambda \in C - \{0\}$; (3) $\delta(s) = 1$ if s has no zero. The equi-distribution problem is to find an upper bound of an average of $\delta(s)$ (a sum in the case of a finite number of sections and an integral in the case of an infinite set). The problem has been studied recently by several authors.

Dual to the intersection problem is the extension problem: Given complex manifolds M, V and a closed subset $A \subset M$. When is a holomorphic mapping $M - A \to V$ the restriction of a holomorphic mapping $M \to V$?

Many extension theorems are known. In several complex variables the most famous are the Hartogs and Riemann extension theorems, which concern with the case that V is either the complex line or a bounded set of it. We wish to formulate the following problem of Hartogs type where the curvature of the image manifold enters into play:

PROBLEM X. — Let Δ be an n-ball in C_n, $n \geqslant 2$, and let V be a complete hermitian manifold of holomorphic sectional curvature $\leqslant 0$. Is it true that every holomorphic mapping of a neighborhood of the boundary $\partial\Delta$ of Δ into V extends into a holomorphic mapping of Δ into V?

It *is* known that without the curvature condition on V the assertion is not true [24]. The problem belongs to an area which might be described as " hyperbolic complex analysis ". The philosophy is that negative curvature of the receiving space limits the holomorphic mappings and allows strong theorems. In fact, a bounded holomorphic function is a mapping into a ball which has the non-euclidean hyperbolic metric.

REFERENCES

[1] L. AUSLANDER. — The structure of complete locally affine manifolds, *Topology*, 3 (1964), suppl. 1, pp. 131-139.

[2] T. BANCHOFF. — Non-rigidity theorems for tight polyhedra, to appear in *Archiv d. Math.*

[3] M. BERGER. — Les variétés riemanniennes homogènes normales simplement connexes a courbure strictement positive, *Ann. Scuola Norm. Sup. Pisa*, 15 (1961), pp. 179-246.

[4] —. — Sur quelques variétés riemanniennes suffisamment pincées, *Bull. Soc. Math. France*, 88 (1960), pp. 57-71.

[5] —. — Trois remarques sur les variétés riemanniennes à courbure positive, *Comptes Rendus* (Paris), 263 (1966), A 76-A 78.

[6] BOMBIERI, E. DE GIORGI and E. GIUSTI. — Minimal cones and the Bernstein problem, *Inventiones Math.*, 7 (1969), pp. 243-268.

[7] R. BOTT and S. S. CHERN. — Hermitian vector bundles and the equidistribution of the zeroes of their holomorphic sections, *Acta Math.*, 114 (1965), pp. 71-112.

[8] E. CALABI. — Minimal immersions of surfaces in euclidean spheres, *J. Diff. Geom.*, 1 (1967), pp. 111-125.

[9] J. CHEEGER and D. GROMOLL. — The structure of complete manifolds of non-negative curvature, *Bull. Amer. Math. Soc.*, 74 (1968), pp. 1147-1150.

[10] S. CHERN. — On curvature and characteristic classes of a Riemann manifold, *Abh. Math. Sem. Univ. Hamburg*, 20 (1955), pp. 117-126.

[11] —. — Simple proofs of two theorems on minimal surfaces, *L'Enseig. Math.*, 15 (1969), pp. 53-61.

[12] —. — Brief survey of minimal submanifolds, *Tagungsberichte, Oberwolfach* (1969).

[13] S. COHN-VOSSEN. — Unstarre geschlossene Flächen, *Math. Ann.*, 102 (1929), pp. 10-29.

[14] M. DO CARMO and N. WALLACH. — Representations of compact groups and minimal immersions into spheres, to appear in *J. Diff. Geom.*

[15] —. — Minimal immersions of spheres into spheres, *Proc. Nat. Acad. Sci.* (USA), 63 (1969), pp. 640-642.

[16] R. FINN. — On a class of conformal metrics, with application to differential geometry in the large, *Comm. Math. Helv.*, 40 (1965), pp. 1-30.

[17] T. FRANKEL. — Manifolds with positive curvature, *Pacific J. Math.*, 11 (1961), pp. 165-174.

[18] Robert E. GREENE. — Isometric embeddings of riemannian and pseudo-riemannian manifolds, *Memoirs Amer. Math. Soc.*, No. 97 (1970).

[19] D. GROMOLL. — Differenzierbare Strukturen und Metriken positiver Krummung auf Spharen, *Math. Annalen*, 164 (1966), pp. 353-371.

[20] — and W. MEYER. — On complete open manifolds of positive curvature, *Annals of Math.*, 90 (1969), pp. 75-90.

[21] M. L. GROMOV. — Stable mappings of foliations into manifolds, *Izvestia Akad. Nauk SSSR, Ser. Mat.*, 33 (1969), pp. 707-734.

[22] W. Y. HSIANG. — Remarks on closed minimal submanifolds in the standard riemannian *m*-sphere, *J. Diff. Geom.*, 1 (1967), pp. 257-267.

[23] A. HUBER. — On subharmonic functions and differential geometry in the large, *Comm. Math. Helv.*, 32 (1957), pp. 13-72.

[24] H. KERNER. — Über die Fortsetzung holomorpher Abbildungen, *Archiv d. Math.*, 11 (1960), pp. 44-47.

[25] W. KLINGENBERG. — Über Riemannsche Mannigfaltigkeiten mit nach oben beschränkter Krümmung, *Annali di Mat.*, 60 (1962), pp. 49-59.

[26] S. KOBAYASHI and T. OCHIAI. — On complex manifolds with positive tangent bundles, to appear in *J. Math. Soc. Japan.*

[27] J. MILNOR. — On the existence of a connection with curvature zero, *Comm. Math. Helv.*, 32 (1958), pp. 215-223.

[28] J. NASH. — The imbedding problem for riemannian manifolds, *Ann. of Math.*, 63 (1956), pp. 20-64.

[29] L. NIRENBERG. — Rigidity of a class of closed surfaces, Nonlinear Problems, R. E. Langer (Editor) (1963), pp. 177-193.

[30] E. PORTNOY. — Toward a generalized Gauss-Bonnet formula for complete open manifolds, Stanford thesis (1969).

[31] I. SATAKE. — The Gauss-Bonnet theorem for V-manifolds, *J. Math. Soc. Japan*, 9 (1957), pp. 464-492.

[32] J. SIMONS. — Minimal varieties in riemannian manifolds, *Ann. of Math.*, 88 (1968), pp. 62-105.

[33] J. THORPE. — The zeroes of non-negative curvature operators, to appear.

[34] O. VEBLEN and J. H. C. WHITEHEAD. — *Foundations of differential geometry*, Cambridge Univ. Press, New York (1932).
[35] K. VOSS. — Differentialgeometrie geschlossener Flächen im euklidischen Raum, *Jahresberichte deutscher Math. Ver.*, 63 (1960-1961), pp. 117-136.
[36] H. WU. — An *n*-dimensional extension of Picard's theorem, *Bull. Amer. Math. Soc.*, 75 (1969), pp. 1357-1361.

Department of Mathematics,
University of California
Berkeley, California 94720
(U. S. A.)

Added during proof, March 12, 1971: Problem X has been solved independently by P. Griffiths and B. Schiffman.

Actes, Congrès intern. math., 1970. Tome 1, p. 55 à 93.

THE CURRENT SITUATION IN THE THEORY OF FINITE SIMPLE GROUPS

by WALTER FEIT (*)

Dedicated to Richard Brauer on the occasion of his 70th Birthday

§ 1. Introduction.

As the title indicates the aim of this paper is to survey some of the known results concerning the structure of finite simple groups. All groups are assumed to be finite from now on.

This paper is concerned with exactly one problem.

MAIN PROBLEM. — *Give a reasonable description of all noncyclic simple groups.*

The key word here is " reasonable ". Thus this is not a well defined problem. What is wanted is a list of all known simple groups which makes it possible to prove or disprove various group theoretic statements by checking all groups on the list. Known simple groups are not really completely known. One cannot for instance give a complete description of all subgroups of all the alternating groups.

It should also be observed that it is not clear that there necessarily is an answer to the main problem. Conceivably an infinite number of simple groups may exist, each one of which owes its existence to a large number of arithmetical and group theoretical accidents.

Having stated some of the difficulties concerning the main problem I now wish to spend the rest of this paper in describing some of the results that have been obtained in answer to various special cases of the main problem. The results described below are mostly of the type that give a complete classification of all simple groups G which satisfy certain conditions. Possibly there are no such simple groups in which case the classification is vacuous. The conditions are of various sorts.

(I) Assumptions concerning the structure and imbedding of various subgroups of G.

(II) Assumptions about the order of G.

(III) Assumptions that G has a linear representation over a suitable field satisfying certain conditions.

(IV) Assumptions that G has a permutation representation of a special type.

(V) Assumptions concerning the multiplication table of G.

(VI) Various technical assumptions, such as that G has a given character table.

(*) This paper was written while the author was partially supported by the NSF.

I will attempt to give a (necessarily superficial) description of how one goes about proving results of this sort.

There are a large number of results which assert that if a group G contains certain special configurations of subgroups then G cannot be simple. Some of these date back to the nineteenth century, the most recent are the content of current research. There are more sophisticated theorems which assert that under suitable hypotheses a simple group *must* contain certain special configurations of subgroups.

Suppose that G is a simple group which satisfies certain hypotheses, call them (H). The results referred to in the previous paragraph can be brought to bear on G and, depending on (H), one may get a great deal of information concerning a large number of subgroups of G. This stage of the argument can loosely be called the purely group theoretic part of the argument since it consists in studying in great detail the structure of various subgroups of G.

After this has been done it is often possible by using the given information to construct a portion of the character table of G. The theory of modular characters developed by Brauer is frequently a useful tool here. The information from the character table can then be used to refine the information concerning subgroups of G. At this stage a contradiction may have been reached and so there are no simple groups satisfying (H).

If however no contradiction has been reached one may have to face the following situation. G is a simple group satisfying (H) many of whose subgroups are explicitly given and a large portion, possibly all, of its character table is known. One of the following questions has to be answered.

(1) (Existence Problem) If no known simple group satisfies (H) does G exist?

(2) (Recognition Problem) If some known simple groups satisfy (H) is G isomorphic to one of them?

One may be fortunate at this point and be able to find a linear representation of G over some field which makes it possible to recognize G, or more likely one may be able to construct a combinatorial configuration on which G acts as a group of automorphisms thus making it possible to recognize G. If these methods fail there is only one recourse left. Either construct the multiplication table of G or derive a contradiction from this multiplication table. In other words study generators and relations. Unfortunately there appear to be no general methods in this connection and each case needs to be handled individually.

This approach has in recent years (with the essential help of computers) led to the discovery of several new finite simple groups. At present there is a potential group investigated by Lyons [1] whose existence has not yet been established. A complete character table is known and an enormous amount of information about the structure of various subgroups is also known. A group satisfying all the appropriate conditions will be denoted by Ly. Conceivably there is more than one such group.

Similarly the recognition problem can be quite intractable. There is an infinite class of groups, known as groups of Ree type, which have many properties in common with the Ree groups ${}^2G_2(3^{2m+1})$. In spite of the efforts of various authors, e. g., Ree [3], Thompson [7], Ward [1] the question of whether these groups are isomorphic to the Ree groups has not yet been settled.

The pattern of proof outlined above is a bare skeleton which in itself is quite meaningless. To make it work it is necessary to have methods available that make it possible to use this pattern for the purpose of proving meaningful results for groups which satisfy appropriate hypotheses. *It is precisely the development of such methods that constitutes the achievement of the post war work in the theory of finite simple groups.*

The first critical step was taken by Brauer. It is quite trivial to prove and has been known for probably over a century that a group generated by two involutions is a dihedral group. Brauer [3] first observed that this fact, when combined with surprisingly simple counting arguments, has profound consequences concerning groups of even order. Amongst other things he showed that if t is an involution in the simple group G then $|G| \leq \{|\mathbb{C}_G(t)|^2\}!$ and so in particular there exist only finitely many simple groups which contain an involution with a given centralizer. Further results of this type, all quite elementary and yet of fundamental importance, can be found in Brauer-Fowler [1]. Related results were later proved by various authors. Some of these are described in Gorenstein [3].

This result of Brauer established the program of characterizing simple groups of even order in terms of centralizers of involutions and related conditions.

Independently of this the second critical step was taken by Thompson [3] a few years later in his thesis. Using the work of P. Hall and a theorem of P. Hall and G. Higman he introduced some completely novel purely group theoretic methods. Extensions of these methods when combined with some developments in the theory of characters made it possible to use the above described pattern of proof to show that noncyclic simple groups of odd order don't exist, Feit-Thompson [3]. It was to be expected that the group theoretic and character theoretic arguments would be enormously more complicated than they were in some previously proved special cases, Feit-Hall-Thompson [1], Suzuki [2]. However it is perhaps surprising that it was (and still is) necessary to actually look at the multiplication table of the group before reaching a contradiction from the assumption that G is noncyclic simple and has odd order.

The purely group theoretic methods which are continually being extended and generalized by many authors form a vital part of much of the current work on Brauer's program and other characterizations of simple groups. In many cases these methods now constitute the bulk of the proof. Surveys of some of these results and methods can be found in Glauberman [3] and Gorenstein [1], [3].

Since noncyclic simple groups have even order, the approach initiated by Brauer leads to a systematic attempt to provide an answer to the main problem. Whether it will ultimately be successful in providing such an answer remains to be seen. However the discovery of several new simple groups in this way has already vindicated this approach and indicates that it gets much closer to the heart of the problem than any previous attempts.

A subject as old as the theory of finite groups abounds with conjectures and unsolved problems. Many of these would easily be settled if one could answer the main problem. In fact this is one of the major reasons for attempting to solve the main problem since it lies at the heart of the theory of finite groups.

There is no point in attempting to list unsolved questions in group theory since the methods and results discussed in this paper are very singlemindedly aimed at solving the main problem and generally avoid looking at questions which are not related to it. The progress that has been made on some questions not directly concerned with the main problem is in the form of a bonus. See for instance Theorem 3.3 and Theorem 10.2 below. This singlemindedness is both the strength and weakness of this approach. Should this approach ultimately lead to the solution of the main problem many of these other questions will be settled. On the other hand if the main problem remains intractable more emphasis will be put in the future on attempting to answer some of the well known unsolved questions in the subject.

There are also many questions concerning simple groups which are independent of the main problem. For instance much work has been done in attempting to describe the characters of known simple groups, especially groups of Lie type. These questions fall outside the scope of this paper. They are only mentioned here to emphasize the fact that while the main problem is of great importance in the theory of finite simple groups it does not encompass the whole subject.

In the rest of this paper I will attempt to catalogue some of the known theorems concerning finite simple groups which give partial solutions to the main problem. These theorems are only the tip of the iceberg. Limitations of space unfortunately make it impossible to describe a great many results (for instance P. Hall's fundamental work on solvable groups) which are a necessary prerequisite for many of the listed theorems.

In the course of gathering material for this paper many people made valuable suggestions. In particular I wish to express my thanks to J. Alperin, B. Fischer, D. Gorenstein, R. Griess, A. Rudvalis, R. Steinberg and J. G. Thompson.

Standard notation and terminology from group theory is used freely throughout this paper. If G is a group then $\tilde{G}$ denotes some covering group of G. Numbers in square brackets refer to the bibliography. Results attributed to a person without bibliographical reference refer either to a personal communication or to an old well known result.

Added in proof. — Since this paper was written C. C. Sims has proved the existence of Ly on a computer. This will now be denoted by LyS. He has also proved the uniqueness of LyS by using the fact, proved by R. Lyons and L. Scott, that LyS contains $G_2(5)$.

§ 2. **The known simple groups.**

The existence of most of the known simple groups and the discovery of their properties is established by methods completely divorced from those discussed in the previous section. The use of Lie theory to show the existence of finite simple groups is due to C. Chevalley. The existence of finite groups of Lie type and the investigation of many of their properties is due to many authors, in particular Chevalley, Ree, Steinberg, Suzuki and Tits. Actually Suzuki discovered an infinite series of groups in trying to characterize some known groups and rather anticlimactically it later turned out that they really were groups of Lie type. Of course it should be mentioned that the classical groups over finite fields and finite analogues of G_2 and E_6 were found long ago by Galois, Jordan, Dickson and others. A detailed description of the groups of Lie type can be found in Carter [1], Tits [1].

In addition to the alternating groups and groups of Lie type there are 18 known sporadic groups and Lyons potential group whose existence has not yet been established. A description of these can be found in Tits [4] and his notation will be followed here. A sporadic group is a simple group that no one has yet been able to fit into an infinite class of simple groups in a natural way.

Five of the sporadic groups are the Mathieu groups which have been known for over a hundred years (though their existence was not incontrovertibly established until this century). The remaining 13 groups were discovered during the past decade.

Four of these groups were discovered by the methods described in the previous section with the help of a computer. Namely:

Ja, Janko [6], see also Livingston [1], Whitelaw [1].
HaJ, Hall [3], Janko [10], see also Tits [3], Wales [3], [4].
HJM, Higman-McKay [1], Janko [10].
HHM, Held [6], Higman-McKay.

The construction by M. Hall of HaJ as a rank 3 permutation group led to the discovery of 3 more groups by analogous methods.

HiS, Higman-Sims [1], see also G. Higman [3], Sims [2].
McL, McLaughlin [1].
Suz, Suzuki [20], see also Lindsey [3].

Three of the remaining groups, Co_1, Co_2, Co_3 were found by Conway by geometric methods. See Conway [1], where he also establishes some connections with other sporadic groups.

The remaining 3 known sporadic groups were found by Fischer [6] (see Theorem 4.5.2 below) by purely group theoretic methods related to those described in the previous section.

The properties of Ly whose existence has not yet been established can be found in Lyons [1].

The first table contains a list of all known sporadic groups, their orders, and whatever is known about the order of their groups of outer automorphisms and the structure of their Schur multipliers. A direct product of cyclic groups of order $n_1, n_2, \ldots$ is denoted by $(n_1, n_2, \ldots)$. In the table n is an unknown integer. The first five groups in the table are the Mathieu groups. Their automorphism groups have been known for a long time. Their Schur multipliers were computed by Burgoyne-Fong [1].

Let Aut (G) denote the automorphism group of G. It has been known for a long time that Aut $(\mathfrak{A}_n) = \mathscr{S}_n$ for $n \neq 6$ and $|\,\mathrm{Aut}\,(\mathfrak{A}_6) : \mathscr{S}_6\,| = 2$. In case G is a simple group of Lie type Aut (G) is also known except possibly for ${}^2F_4(2)'$, Ree [1], [2], Steinberg [1], Suzuki [11, I]. In all of these cases Aut (G) is uniformly described in terms of Lie goup theory.

The situation concerning Schur multipliers is more complicated. Let $\tilde{G}$ be the group of rational points over a finite field of a simply connected covering group of a simple algebraic group over an algebraically closed field. If $\tilde{G}$ is not solvable then Steinberg has shown that $\tilde{G}$ has no proper covering group except for the 11 cases in the second table. In each of these cases he found the upper bound for the order of the Schur multiplier. If $\tilde{G}_1$ is a nonsolvable Steinberg variation of $\tilde{G}$ then Steinberg also

Group	Order	Order of group of outer automorphisms	Schur multiplier
M_{11}	$2^4.3^2.5.11$	1	(1)
M_{12}	$2^6.3^3.5.11$	2	(2)
M_{22}	$2^7.3^2.5.7.11$	2	(6)
M_{23}	$2^7.3^2.5.7.11.23$	1	(1)
M_{24}	$2^{10}.3^3.5.7.11.23$	1	(1)
Ja	$2^3.3.5.7.11.19$	1 Janko [6]	(1)
Ha J	$2^7.3^3.5^2.7$	2 Hall [3]	(2) McKay-Wales [1]
HJM	$2^7.3^5.5.17.19$	$2n$	(3) McKay-Wales [1]
HHM	$2^{10}.3^3.5^2.7^3.17$		(1) Griess
HiS	$2^9.3^2.5^3.7.11$	$2n$	(2) Griess, McKay-Wales
McL	$2^7.3^6.5^3.7.11$	2	(3) Thompson
Suz	$2^{13}.3^7.5^2.7.11.13$	2 Lindsey [3]	(6) Griess
Co_1	$2^{21}.3^9.5^4.7^2.11.13.23$	1	order $2n$
Co_2	$2^{18}.3^6.5^3.7.11.23$		
Co_3	$2^{10}.3^7.5^3.7.11.23$	1 Fendel [1]	(1) Griess
Fi_{22}	$2^{17}.3^9.5^2.7.11.13$	2	(6) Griess
Fi_{23}	$2^{18}.3^{13}.5^2.7.11.13.17.23$	1	(1) Griess
Fi'_{24}	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$	$2n$, n odd	order 3^n, Griess
Ly ?	$2^8.3^7.5^6.7.11.31.37.67$	1 Thompson	(1) Thompson

showed that if $\tilde{\tilde{G}}_1$ is a universal covering group of $\tilde{G}_1$ then $|\tilde{\tilde{G}}_1 : \tilde{G}_1|$ is a power of p, where p is the characteristic of the underlying field, except possibly if $\tilde{G}_1$ is an odd dimensional unitary group. Griess has shown that $|\tilde{\tilde{G}}_1 : \tilde{G}_1|$ is prime to p except for the cases listed in the table below. The table below contains all the nonsporadic

Group	Schur multiplier
$\mathfrak{A}_5 \approx SL_2(4) \approx PSL_2(5)$	(2)
$\mathfrak{A}_6 \approx PSL_2(9)$	(6)
$\mathfrak{A}_7$	(6)
$\mathfrak{A}_8 \approx SL_4(2)$	(2)
$\mathfrak{A}_n$, $n \geq 9$	(2)
$SL_3(2) \approx PSL_2(7)$	(2)
$PSL_3(4)$	(4, 12) Burgoyne, Thompson
$Sp_6(2)$	(2) Steinberg
$O'_7(3)$	(6) Fischer, Rudvalis
$D_4(2)$	(2, 2) Steinberg
$G_2(4)$	(2) Griess, Steinberg
$G_2(3)$	(3) Griess
$F_4(2)$	(2) Griess
${}^2D_4(2)$	(1) Griess
$PSU_{2m+1}(p^m)$	a p'-group Griess
$PSU_4(2) \approx PSp_4(3)$	(2)
$PSU_4(3)$	(3, 12) Lindsey, Griess
$PSU_6(2)$	(2, 6) Fischer, Griess
$Sz(8)$	(2, 2) Alperin-Gorenstein [1]
$Sz(2^{2m+1})$, $m \geq 2$	(1) Alperin-Gorenstein [1]
${}^2G_2(3^{2m+1})$, $m \geq 1$	(1) Alperin-Gorenstein [1]
${}^2F_4(2^{2m+1})$, $m \geq 2$	(1) Ward [2]
${}^2F_4(8)$	
${}^2F_4(2)'$	(1) Griess

groups and whatever is known about their Schur multipliers except the Chevalley groups G for which it is known that $\tilde{G}$ has no proper covering group and the Steinberg variations G_1 for which it is known that $\tilde{G}_1$ has no proper covering group. The Schur multipliers of the alternating groups were found by Schur [1].

§ 3. N-groups.

One of the deepest results of the past few years is the following theorem.

THEOREM 3.1 (Thompson [8]). — *Let G be a simple group in which the normalizer of any solvable subgroup of G of order greater than 1 is solvable. Then G is one of the following groups.*

(i) $PSL_2(q)$, $q > 3$.
(ii) $Sz(2^{2m+1})$, $n \geq 1$.
(iii) $PSL_3(3)$.
(iv) M_{11}.
(v) $\mathfrak{A}_7$.
(vi) $PSU_3(3)$.
(vii) ${}^2F_4(2)'$ (*the* Tits *group*).

The author had originally overlooked case (vii). It was pointed out by T. Hearne that Tits' group satisfies the assumptions of the theorem. As an immediate corollary to this result one gets.

THEOREM 3.2 (Thompson [8]). — *Let G be a simple group in which all proper subgroups are solvable. Then G is one of the following groups.*

(i) $PSL_2(2^p)$, $PSL_2(3^p)$ *where p is any prime.*
(ii) $PSL_2(p)$ *where p is any prime with $p > 3$ and $p \equiv 2$ or 3 (mod 5).*
(iii) $Sz(2^p)$, *p any odd prime.*
(iv) $PSL_3(3)$.

These results can be used to give some characterizations of solvable groups.

THEOREM 3.3 (Thompson [8]). — *The following conditions are equivalent for a group G.*

(i) *G is solvable.*
(ii) *Every pair of elements of G generates a solvable group.*
(iii) *If x, y, z are three nonidentity elements of G of pairwise coprime order then* $xyz \neq 1$.
(iv) *If $x_1, x_2, \ldots$ are nonidentity elements of G of pairwise coprime order then* $x_1 x_2 \ldots \neq 1$.
(v) *For any nonprincipal irreducible character χ of G there exists a prime p and a S_p-group P of G such that the restriction of χ to P does not contain the principal character of P as a constituent.*

P. Hall first pointed out that every solvable group satisfies condition (iv). Gallagher [1] first proved the equivalence of conditions (iv) and (v).

§ 4. **Characterizations in terms of involutions and Sylow 2-groups.**

The results stated in this section are of various related types. They all consist of the classification, or steps toward the classification, of simple groups which satisfy a variety of conditions concerning involutions or S_2-groups.

§ 4.1. Strongly embedded subgroups

A subgroup H of G is *strongly embedded* if $|H|$ is even and $|H \cap H^x|$ is odd for all x in $G - H$.

THEOREM 4.1.1. — *Suppose that G contains a strongly embedded subgroup H with $H \neq G$. Then one of the following must occur.*

(i) *A S_2-group of G is either cyclic or (generalized) quaternion.*
(ii) *$G/\mathbb{O}_{2'}(G)$ has a normal subgroup of odd index which is isomorphic to one of the following groups.*

(a) $SL_2(2^n)$, $n \geq 2$.
(b) $PSU_3(2^n)$, $n \geq 2$.
(c) $Sz(2^{2n+1})$, $n \geq 1$.

This theorem, due to Bender [3], generalizes a result of Suzuki who reached the same conclusion under the assumption that a normalizer of a Sylow 2-group is distinct from G and is strongly embedded in G. The proof relies heavily on earlier work which can be found in Feit [1], [2], G. Higman [1], Suzuki [4, III], [6], [11], [13], [14], Zassenhaus [2]. Theorem 4.1.1 is of great importance for various characterization theorems since it disposes of the recognition problem for the classes of groups mentioned in the conclusion. Virtually every result which involves these classes of groups makes use of Theorem 4.1.1.

§ 4.2. Sylow 2-groups

For any positive integer n let Z_n, D_n denote a cyclic group or a dihedral group of order n. Let $Q_{2^{n+1}}$, $S_{2^{n+1}}$ respectively denote the quaternion and quasi-dihedral group of order 2^{n+1}. Observe that $D_4 \approx Z_2 \times Z_2$. Here

$$S_{2^{n+1}} = \langle x, y \mid x^2 = y^{2^n} = 1, x^{-1}yx = y^{-1+2^{n-1}} \rangle.$$

For any group G let $S_2(G)$ be the S_2-group of G.

THEOREM 4.2.1 (Gorenstein-Walter [1], [2], [3]). — *Let G be a simple group with $S_2(G) \approx D_{2^{n+1}}$ for some $n \geq 1$. Then either $G \approx \mathfrak{A}_7$ or $G \approx PSL_2(q)$ for some odd $q > 3$.*

The proof uses some results of Brauer [7, II] from the theory of modular characters in an essential way.

THEOREM 4.2.2 (Alperin-Brauer-Gorenstein [1], [2]). — *Let G be a simple group.*

(i) *If $S_2(G) \approx S_{2^{n+1}}$ with $n \geq 4$ then one of the following occurs.*

(a) *$G \approx PSL_3(q)$ with $q \equiv 3$* (mod 4).

(b) $G \approx PSU_3(q)$ *with* $q \equiv 1 \pmod 4$.
(c) $G \approx M_{11}$.

(ii) *If* $S_2(G) \approx Z_{2^n} \wr Z_2$ *with* $n \geq 2$ *then one of the following occurs.*

(a) $G \approx PSL_3(q)$ *with* $q \equiv 1 \pmod 4$.
(b) $G \approx PSU_3(q)$ *with* $q \equiv 3 \pmod 4$.

THEOREM 4.2.3 (Walter [2], [3]). — *Let G be a simple group with* $S_2(G)$ *abelian. Then one of the following occurs.*

(i) $G \approx PSL_2(q)$, $q \equiv \pm 3 \pmod 8$, $q > 3$.
(ii) $G \approx SL_2(2^n)$ *for some* $n \geq 2$.
(iii) *G is a group of* Ree *type.*
(iv) $G \approx$ Ja.

In particular $S_2(G)$ *is elementary abelian.*

In case $S_2(G)$ is generated by two elements in Theorem 4.2.3 Brauer [7, II] showed that it has order 4 and so in this case the result follows from Theorem 4.2.1. In case $S_2(G)$ has three generators earlier results of Gagen [2], Janko [6], [7], Janko-Thompson [1], Ree [1], Thompson [5] and Ward [1] are of relevance and are subsumed by Theorem 4.2.3. This result also includes as special cases earlier results in Brauer [6], Feit [2], Gagen [1], Gorenstein [2] and Suzuki [4, I], [4, II]. A simplification for part of this proof can be found in Bender [4].

The next result is a composite of several theorems.

THEOREM 4.2.4. — *Let G be a simple group.*

(i) (Collins [1]). *If* $S_2(G) \approx S_2(Sz(2^{2n+1}))$ *for* $n \geq 1$ *then* $G \approx Sz(2^{2n+1})$.
(ii) (Lyons [1]). *If* $S_2(G) \approx S_2(PSU_3(4))$ *then* $G \approx PSU_3(4)$.
(iii) (Gorenstein-Harada [1], Janko [10]). *If* $S_2(G) \approx S_2(\mathrm{HaJ})$ *then* $G \approx$ HaJ *or* $G \approx$ HJM.
(iv) (Gorenstein-Harada [4], Lyons [1]). *If* $S_2(G) \approx S_2(\mathrm{Ly})$ *then* $G \approx$ Ly.

In (i) the case $n = 1$ had previously been settled by Brauer and Goldschmidt.

THEOREM 4.2.5 (Glauberman [1]). — *Let* $T = Q_{2^{n+1}} \times T_0$ *where every involution in* T_0 *is in the* n^{th} *term of the upper central series of* T. *Then T cannot be a* S_2*-group of a simple group.*

The case that T_0 is a product of quaternion groups was proved independently, but later, by Mazurov [2]. The special case that $T_0 = \langle 1 \rangle$ which is the starting point for this result has to be handled separately. This case is due to Brauer-Suzuki [1]. Alternative proofs for this case can be found in Brauer [7, II], Suzuki [10]. Actually Theorem 4.2.5 is a consequence of Theorem 4.5.1 below which is of great importance for many of the results in this paper. A related result is the following.

THEOREM 4.2.6 (Goldschmidt [1]). — *Let T be a nonabelian* S_2*-groupe of a simple group. Suppose that T has nilpotence class n. Then* $\mathbb{Z}(T)$ *has exponent at most* 2^{n-1}. *Furthermore T has exponent at most* $2^{n(n-1)}$.

THEOREM 4.2.7 (Alperin-Brauer-Gorenstein [2]). — *Let G be a simple group. Assume that $S_2(G)$ contains no elementary abelian subgroup of order* 8. *Then G is isomorphic to one of the following groups:* $\mathfrak{A}_7$, $PSL_2(q)$, $PSL_3(q)$, $PSU_3(q)$ *with q odd or* $PSU_3(4)$.

This powerful result which is essentially an amalgam of some of the previously mentioned results in this section supersedes or has as simple corollaries a large number of previously proved theorems. For instance: Brauer [3], [8], Brauer-Suzuki-Wall [1], Camina-Gagen [1], Feit [2], Mazurov [1], Suzuki [1], [3], [4, I], Thompson [4], W. J. Wong [3], [4], [6].

The question of finding all simple groups G such that $S_2(G)$ contains no *normal* elementary abelian subgroup of order greater than 4 has not yet been settled. However a great deal of progress has been made. MacWilliams [1] has shown that $S_2(G)$ is one of a restricted class of 2-groups and under some additional assumptions on G this class of groups has been classified. See Theorem 4.3.3.

THEOREM 4.2.8 (Harada [2]). — *Let $T = A \times B$ where A is cyclic and B has a cyclic subgroup of index 2. If $A \neq \langle 1 \rangle$ and $T = S_2(G)$ for a simple group G then T is abelian (and hence G is determined by Theorem* 4.2.3).

THEOREM 4.2.9 (Gorenstein-Harada [2]). — *Let $T = D_{2^{n+1}} \times T_0$ where T_0 is either dihedral or a noncyclic abelian group generated by* 2 *elements. Then T is not a S_2-group of a simple group.*

The case that $T_0 = D_{2^{m+1}}$ with $m \neq n$ had previously been settled by Fong.

Two groups G and H have the *same involution fusion pattern* if $S_2(G) \approx S_2(H)$ and there exists an isomorphism f from $S_2(G)$ onto $S_2(H)$ such that for any involutions x, y in $S_2(G)$, x is conjugate to y in G if and only if $f(x)$ is conjugate to $f(y)$ in H.

THEOREM 4.2.10 (Gorenstein-Harada [3]). — *Let G be a simple group with $S_2(G) \approx S_2(\mathfrak{A}_8)$. Then either $G \approx \mathfrak{A}_8$ or $\mathfrak{A}_9$ or G has the involution fusion pattern of $PSp_4(q)$ with $q \equiv \pm 3 \pmod 8$.*

This result generalizes earlier results by Held [1], W. J. Wong [1] which are needed for the proof.

THEOREM 4.2.11 (Gorenstein-Harada [3]). — *Let G be a simple group with $S_2(G) \approx S_2(\mathfrak{A}_{10})$. Then either $G \approx \mathfrak{A}_{10}$ or $\mathfrak{A}_{11}$ or G has the involution fusion pattern of $PSL_4(q)$ with $q \equiv 3 \pmod 8$.*

THEOREM 4.2.12 (Gorenstein-Harada [4], S. K. Wong [2]). — *Let G be a simple group with $S_2(G) \approx S_2(M_{22})$. Then one of the following holds:*

(i) $G \approx M_{22}$, M_{23} *or* McL.

(ii) *G has only one class of involutions. If H is the centralizer of an involution in G then $H/\mathbb{O}_{2'}(H)$ is isomorphic to the centralizer of an involution in either $PSL_4(q)$, $q \equiv 5 \pmod 8$ or $PSU_4(q)$, $q \equiv 3 \pmod 8$.*

Theorems of a different nature due to Brauer asserts that certain types of 2-groups can only be the S_2-group of a finite number of simple groups. Results of this type are discussed in Brauer [6], [9].

§ 4.3. General conditions on centralizers of involutions

Theorem 4.3.1 (Suzuki [16]). — *Let G be a simple group in which the centralizer of every involution has a normal S_2-subgroup. Then G is isomorphic to one of the following groups:*

(i) $PSL_2(p)$, *p a Fermat or Mersenne prime*, $p > 3$.
(ii) $SL_2(2^n)$, $n \geq 2$.
(iii) $\mathfrak{A}_6 \approx PSL_2(9)$.
(iv) $PSL_3(q)$, $PSU_3(q)$ *or* $Sz(q)$ *where q is a power of* 2.

This powerful result is the end product of a large number of theorems which it generalizes. See Feit [2], Suzuki [4], [7], [8], [11], [14].

Theorem 4.3.2 (Gorenstein [4]). — *Let G be a simple group in which the centralizer of every involution has a normal 2-complement. Then G is isomorphic to one of the following groups:*

(i) $PSL_2(q)$, $q > 3$.
(ii) $Sz(2^n)$, $n \geq 3$.
(iii) $\mathfrak{A}_7$ *or* $PSL_3(4)$.

The proof of Theorem 4.3.2 make use of Theorem 4.3.1 as well as the next result.

Theorem 4.3.3 (Janko-Thompson [2], Lyons [1]). — *Let G be a simple group and let* $T = S_2(G)$. *Assume that T contains no normal elementary abelian subgroup of order* 8. *Assume further than if t is an involution in T such that* $|T : \mathbb{C}_T(t)| \leq 2$ *then* $\mathbb{C}_G(t)$ *is solvable. Then G must be isomorphic to one of the following groups:*

(i) $PSL_2(q)$, $q > 3$.
(ii) $\mathfrak{A}_7$, M_{11}, $PSL_3(3)$, $PSU_3(3)$ *or* $PSU_3(4)$.

Theorem 4.3.1 in particular includes the classification of all simple groups in which the centralizer of every involution is nilpotent. The problem of finding all simple groups in which the centralizer of every involution is solvable is still open. The answer to this would in particular have to include Theorem 3.1 as a special case. At this conference Janko has announced the following result in this connection.

Theorem 4.3.4. — *Suppose that G is a simple group in which the normalizer of every nonidentity 2-group is solvable with cyclic Sylow p-groups for all odd primes p. Then G is isomorphic to one of the following groups.*

(i) $PSL_2(q)$, $Sz(2^{2m+1})$, $PSU_3(2^m)$.
(ii) M_{11}, $PSU_3(3)$, $PSL_3(3)$, ${}^2F_4(2)'$.

§ 4.4. Precise conditions on centralizers of involutions

An involution in $\mathbb{Z}(S_2(G))$ is called a central involution of G. The following table lists a simple group G_0, a central involution t_0 in G_0 and all simple groups G which contain a central involution t such that $\mathbb{C}_G(t) \approx \mathbb{C}_{G_0}(t_0)$ and such that $\mathbb{C}_G(z) = \mathbb{C}_G(t)$ for every involution z in $\mathbb{Z}(\mathbb{C}_G(t))$. These conditions are sometimes redundant. For instance if $\mathbb{Z}(S_2(G_0))$ is cyclic it suffices to assume that G contains an involution t with $\mathbb{C}_G(t) \approx \mathbb{C}_{G_0}(t_0)$.

Since t is assumed to be a central involution it follows that in particular $S_2(G)$ is given. Results which follow directly from subsection 4.2 are not included in the list.

G_0	t_0	G
$SL_3(2)$, Kondo [2], Suzuki [4, II]	A transvection	$SL_3(2)$, $\mathfrak{A}_6$
$SL_4(2)$, Held [1], [4], Suzuki [4, IV], W. J. Wong [1]	A transvection	$SL_4(2) \approx \mathfrak{A}_8$, $\mathfrak{A}_9$
$SL_5(2)$, Held [6]	A transvection	$SL_5(2)$, M_{24}, HHM
$PSL_n(2^m)$ for $(n, m) \neq (3, 1), (4, 1), (5, 1)$, Suzuki [4, II], [4, IV], [19]	A transvection	$PSL_n(2^m)$
$PSp_{2n}(q)$, q odd $n \geq 2$, W. J. Wong [7], [8]	t_0 is represented in $Sp_{2n}(q)$ by an element with exactly two characteristic values equal to -1	$PSp_{2n}(q)$
$\mathfrak{A}_{12}$, Yamaki [2]	An involution of type 2^6	$\mathfrak{A}_{12}$, $\mathfrak{A}_{13}$, $Sp_6(2)$
$\mathfrak{A}_{4n+r}$, $n \geq 1$, $r = 2$ or 3, $4n + r \neq 6$ Kondo [1], [2], [3], Yamaki [1]	An involution of type 2^{2n}	$\mathfrak{A}_{4n+r}$.

In the remaining cases t_0 is any central involution.

$PSU_5(2^m)$, Thomas [2]	$PSU_5(2^m)$
$G_2(2^m)$, Thomas [1]	$G_2(2^m)$
${}^3D_4(2^m)$, Thomas [3]	${}^3D_4(2^m)$
$PSL_4(q)$, $q \equiv 3 \pmod 4$, Phan [1], [3]	$PSL_4(q)$
$G_2(q)$, $q > 3$, q odd, Fong [3]	$G_2(q)$
$G_2(3)$, Janko [11]	$G_2(3)$
$PSU_4(3)$, Phan [2]	$PSU_4(3)$
Co_3, Fendel [1]	Co_3
${}^2F_4(2)' =$ Tits group, Parrot (announced at this congress)	${}^2F_4(2)'$
${}^2F_4(2)$, (not simple), Hearne [1]	${}^2F_4(2)$

At this congress Suzuki has announced similar characterizations of the groups $PSU_n(2^m)$ and $PSp_{2n}(2^m)$.

The remaining results in this section are characterizations which are quite similar to those in the table above.

THEOREM 4.4.1 (Suzuki [4, III]). — *Let G be a simple group with one conjugate class of involutions. If t is an involution in G let $\mathbb{C}_G(t)$ be isomorphic to the centralizer of an involution in $PSU_3(2^m)$, $m > 2$. Then $G \approx PSU_3(2^m)$.*

THEOREM 4.4.2 (Guterman [1]). — *Let x_1, x_2, x_3 be central involutions in $F_4(2^m)$, no two of which are conjugate, such that $x_1x_2 = x_3$ and $\mathbb{C}(x_1) \cap \mathbb{C}(x_2) = \mathbb{C}(x_3)$. Suppose that G is a simple group which contains central involutions y_1, y_2, y_3 with $y_1y_2 = y_3$ and $\mathbb{C}_G(y_i) \approx \mathbb{C}(x_i)$ for $i = 1, 2, 3$. Then $G \approx F_4(2^m)$.*

THEOREM 4.4.3 (Asche [1]). — *A simple group cannot contain a central involution t with $\mathbb{C}_G(t) \approx D_{2^m} \times PSL_2(q)$ for odd q.*

THEOREM 4.4.4 (Harada [2], Janko-Thompson [1]). — *Suppose that t is an involution in the simple group G with $\mathbb{C}_G(t) = \langle t \rangle \times PSL_2(q)$. Then $S_2(G)$ is abelian.*

THEOREM 4.4.5 (Lyons-Thompson, Janko [12] for $n = 9$). — *Let G be a simple group which contains a central involution t with $\mathbb{C}_G(t) \approx \tilde{\mathfrak{A}}_n$. Then $n = 11$ or $n = 8$ (The cases $n = 8$, 11 occur for* McL, Ly *respectively).*

THEOREM 4.4.6 (Fong [1]). — *Let G be a simple group and let $T = S_2(G)$. Suppose that $| T | = 32$ and T contains a self centralizing cyclic subgroup of order 8. Assume further that the centralizer of every involution in G is solvable. Then $G \approx PSU_3(3)$.*

THEOREM 4.4.7 (Brauer-Fong [1]). — *Let G be a simple group and let $T = S_2(G)$. Assume that $| T | = 64$ and T contains a self centralizing cyclic subgroup $\langle x \rangle$ of order 8 all of whose generators are conjugate in G. Suppose that G has more than one class of involutions. Then $G \approx M_{12}$.*

THEOREM 4.4.8 (Held [3], [4], [5], Janko [9, I]). — *Let G be a simple group with $\mathbb{Z}(S_2(G))$ cyclic. Assume that if t is a central involution in G then $\mathbb{C}_G(t)$ is an extension of an elementary abelian group of order at most 16 by $\mathcal{S}_4$. Then G is isomorphic to one of the following groups.*

(i) $\mathfrak{A}_8$, $\mathfrak{A}_9$, $\mathfrak{A}_{10}$.
(ii) M_{11}, M_{12}, M_{22}.
(iii) $PSL_3(3)$.

THEOREM 4.4.9 (Janko [9, II]). — *Let G be a simple group with $\mathbb{Z}(S_2(G))$ cyclic. Assume that if t is a central involution in G then $\mathbb{C}_G(t)$ is an extension of an elementary abelian group of order 16 by $PSL_2(7)$. Then $G \approx M_{23}$.*

THEOREM 4.4.10 (Janko-Wong [1]). — *Let G be a simple group. Let H be the centralizer of a central involution. Assume that H has a normal nonabelian subgroup S of order 64 with $H/S \approx \mathcal{S}_5$. Assume further that if z is an element of order 3 in H then $\mathbb{C}_S(z) \subsetneq \mathbb{Z}(S)$. Then $G \approx$* HiS.

THEOREM 4.4.11 (Harada [5]). — *Let G be a simple group. Assume that $\mathbb{Z}(S_2(G)) = \langle t \rangle$ has order 2 and $S_2(G)/\langle t \rangle \approx S_2(\mathfrak{A}_8)$. Assume further that $\mathbb{C}_G(t)$ does not normalize any nonidentity subgroup of odd order. Then $\mathbb{C}_G(t)$ is isomorphic to the centralizer of a central involution in one of the following groups $\mathfrak{A}_{10}$, M_{22}, M_{23}, $PSL_4(5)$, $PSU_4(3)$,* HaJ, McL.

THEOREM 4.4.12 (Fong-Wong [1]). — *Let G be a simple group with subgroups L_1, L_2 such that $L_i \approx SL_2(q_i)$ for $i = 1, 2$, where q_1, q_2 are odd, $[L_1, L_2] = 1$ and $L_1 \cap L_2 = \langle t \rangle$ has order 2. Suppose that $| \mathbb{C}_G(t) : L_1 L_2 | = 2$. Then G is isomorphic to one of the groups $PSp_4(q)$, $G_2(q)$ or ${}^3D_4(q)$ where $q = \min \{ q_1, q_2 \}$.*

§ 4.5. PRODUCTS OF INVOLUTIONS

THEOREM 4.5.1 (Glauberman [1]). — *Let G be a finite group and let π be a set of odd primes. Suppose that G is generated by a conjugate class D of 2-elements such* *that the product of any two elements in D is a π-element. Then G' is a π-group and so in particular G is solvable.*

This strengthens earlier results of Fischer [4], [5] who first looked at problems of this type. The following remarkable result led to the discovery of the simple groups Fi_{22}, Fi_{23}, Fi'_{24}.

THEOREM 4.5.2 (Fischer [6]). — *Let D be the union of conjugate classes of G consisting of involutions such that $G = \langle D \rangle$. Assume that if $x, y \subseteq D$ then $|\langle xy \rangle| \leq 3$. Suppose further that G has no normal solvable nonidentity subgroup. Then G is isomorphic to one of the following groups.*

(i) *A semi-direct product of $D_4(2)$ or $D_4(3)$ by $\mathscr{S}_3$.*
(ii) $\mathscr{S}_n$, $Sp_{2n}(2)$ *or* $O^{\pm}_{2n}(2)$.
(iii) *A normal subgroup of* $O^{\pm}_n(3)$.
(iv) $PSU_n(2)$.
(v) Fi_{22}, Fi_{23}, Fi_{24} $(|Fi_{24} : Fi'_{24}| = 2)$.

Fischer and F. G. Timmesfeld are also studying groups G which are generated by a union of conjugate classes D of involutions and for which the following holds: If x, y are in D then xy has order at most 4 and in case xy has order 4 then $(xy)^2$ is in D. The work on these groups is not yet complete.

§ 4.6. RELATED TYPES OF CHARACTERIZATIONS

This subsection contains a sample of results which use properties of involutions but don't fit naturally into any of the earlier subsections. Some of these results can be considerably simplified by making use of some of the more recently proved theorems mentioned in the previous subsections.

THEOREM 4.6.1 (Suzuki [9]). — *A partition of a group G is a collection $\{U_i\}$ of subgroups such that $U_i \cap U_j = \langle 1 \rangle$ for all $i \neq j$. The partition is proper if $G \neq U_i$ for all i. Let G be a group with a proper partition which contains no solvable normal subgroup. Then $G \approx Sz(2^{2n+1})$ for some $n > 0$ or $G \approx PSL_2(q)$ or $PGL_2(q)$ for some $q > 3$.*

THEOREM 4.6.2 (Suzuki [18]). — *Suppose that G contains a subgroup H such that $H - A$ consists of involutions for some proper subgroup A of H. Assume that $4 \mid |H|$ and $H = \mathbb{C}_G(t)$ for any involution t in $\mathbb{Z}(H)$. Then either G is solvable or G has a normal subgroup N whose order is not divisible by 4 such that $G/N \approx PSL_2(q)$ or $PGL_2(q)$ for some $q > 3$.*

THEOREM 4.6.3 (Harada [1], Stewart [1]). — *A subgroup A of G is special if $|N_G(A) : A| = 2$ and $\mathbb{C}_G(x) \subseteq A$ for all nonidentity elements x in A. Suppose that G is simple.*

(i) *If G contains two nonconjugate special subgroups then $G \approx SL_2(2^m)$, $m > 1$.*
(ii) *If G contains a special subgroup A with $|G| \leq 4\,(|A| + 1)^3$ then $G \approx PSL_2(q)$, $q > 3$.*

THEOREM 4.6.4 (Fischer [1]). — *Let p be a prime. Assume*

(i) *Any two S_p-groups of G generate a solvable group.*
(ii) *Either $p = 2$ or if $N \lhd H$ are subgroups of G with H/N nonabelian then $p \mid |H:N|$. Then G is solvable.*

THEOREM 4.6.5 (Glauberman [4]). — *Let p be a prime and let P be a S_p-group of G. Assume*

(i) *If two elements of P are conjugate in G they are conjugate in $\mathbb{N}_G(P)$.*
(ii) *If x is in P, $x \neq 1$ then $\mathbb{C}_G(x)$ has a normal p-complement.*
(iii) *Any two elements of order p in G generate a p-solvable group.*
(iv) *P is not an elementary abelian group all of whose nonidentity elements are conjugate in G.*

If $\mathbb{O}_{p'}(G) = \langle 1 \rangle$ and P is not normal in G then $p = 2$ and $G = Sz(2^m)$ for some $m \geq 3$.

THEOREM 4.6.6 (Glauberman [4]). — *Let p be a prime and let G be a group with a cyclic S_p-subgroup. Then G is p-solvable if and only if any two p-elements generate a p-solvable group.*

THEOREM 4.6.7 (Martineau [1]). — *Let G be a simple group. Suppose that G contains a subgroup $H \approx D_{2m} \times D_{2n}$ with m, n odd and $m, n > 1$. Assume that H contains the normalizer of every nonidentity subgroup of H of odd order. Then $G \approx$* Ja.

A different type of result concerning involutions can be found in Walter [1].

§ 5. **Odd characterizations.**

If x, y are elements in a group G such that x, y and xy all have order 3 then $\langle x, y \rangle$ has a normal abelian subgroup. This can be exploited in a manner somewhat analogous to the way involutions are used. See Feit-Thompson [2]. G. Higman has used this and related relations in groups to systematically study certain questions about groups. He calls these results odd characterizations. A survey of many of these results can be found in G. Higman [2]. Here only three results will be mentioned to give an idea of the type of theorem to be expected.

THEOREM 5.1 (Stewart [1]). — *Suppose that the simple group G contains a subgroup A such that $3 \mid |A|$, $|\mathbb{N}_G(A) : A| = 2$ and $A = \mathbb{C}_G(x)$ for every nonidentity element x in A. Then $G \approx PSL_2(q)$ for some $q > 3$.*

The case $|A| = 3$ had previously been handled in Feit-Thompson [2]. See also Theorem 4.6.3.

THEOREM 5.2 (Fergusson [1], Herzog [1]). — *Suppose that the simple group G contains a subgroup M such that $3 \mid |M|$, $\mathbb{N}_G(M) \neq M$, $|\mathbb{N}_G(M) : M|$ is odd and $\mathbb{C}_G(x) \subseteq M$ for every nonidentity element x in M. Then $G \approx PSL_2(3^{2n+1})$ for some $n > 0$.*

Some variations on this result can also be found in Herzog [2], [3].

THEOREM 5.3 (G. Higman [2]). — *Let G be a group which contains a maximal subgroup isomorphic to D_{10}. Then $G \approx \mathfrak{A}_5$.*

§ 6. **Properties of subgroups.**

This section lists some results which do not refer to properties of involutions. However some of these results make use of the methods of section 4.

§ 6.1. Nilpotent subgroups

Theorem 6.1.1 (Thompson [1], [2], [3], [6]). — *Let G be a group which contains a maximal subgroup that is nilpotent of odd order. Then G is solvable.*

Janko [1], [5] and Deskins observed that this result can be generalized as follows.

Theorem 6.1.2. — *Let G be a simple group which contains a maximal subgroup M that is nilpotent. Then $M = S_2(G)$ and M has class at least* 3.

In all known cases of Theorem 6.1.2 M is a dihedral group. Harada [2] has verified that if $|M| \leq 64$ in Theorem 6.1.2 then M is a dihedral group.

Theorem 6.1.3 (Glauberman [5]). — *Let p be a prime and let P be a S_p-group of G. Suppose that $\mathbb{N}_G(P) = P$. If $p \geq 5$ then G is not simple.*

It remains an open question whether a simple group G can have a S_3-group P with $\mathbb{N}_G(P) = P$. If p is a Fermat prime or a Mersenne prime with $p > 5$ then a S_2-group is maximal and hence self normalizing in $PSL_2(p)$.

§ 6.2. Chains of subgroups

There are a variety of results which classify all groups satisfying some assumptions on chains of subgroups. Some examples will be given. A chain of subgroups is a set of subgroups which is linearly ordered by inclusion. The length of a chain is the number of distinct terms in it minus 1. A subgroup of G is k^{th} maximal if it is the k^{th} term in some chain of proper subgroups each of which is maximal in its predecessor and k is the smallest such integer.

Theorem 6.2.1 (Gagen [2], Harada [3]). — *Let G be a simple group in which every chain of subgroups has length at most 7. Then G is isomorphic to one of the following groups. $PSL_2(q)$ for some values of q, $PSU_3(3)$, $PSU_3(5)$, $\mathfrak{A}_7$, M_{11},* Ja.

This generalizes earlier results of Janko [3], [4].

Theorem 6.2.2 (Gagen-Janko [1], Janko [2]). — *Let G be a simple group in which every 3^{rd} maximal subgroup is nilpotent. Then either $G \approx Sz(8)$ or $G \approx PSL_2(q)$ for some values of q.*

Theorem 6.2.3 (Berkovic [3]). — *Let G be a simple group in which every 2^{nd} maximal subgroup is 2-nilpotent. Then $G \approx PSL_2(2^p)$ where p is a Fermat prime or $G \approx PSL_2(3^p)$ for some prime $p > 3$, or $G \approx PSL_2(p)$ for a prime $p > 3$ with $p^2 \equiv 9 \pmod{80}$.*

Various other results which characterize groups in similar terms can be found in Berkovic [1], [2], [3], [4], [5], [6], [7], [8], [9], Kohno-Vedernikov [1], Lelcuk [1], Mann [1], [2] and Winkler [1].

§ 6.3. Factorizable groups

Let A, B be subgroups of G such that $G = AB$. There are many results that assert that under various conditions on A and B, G must be solvable. A survey of some of these results can be found in W. R. Scott [1]. The following for instance generalizes Burnside's theorem which however is needed in the proof.

Theorem 6.3.1 (Kegel [1], Wielandt [1]). — *Suppose that $G = AB$ where A and B are nilpotent. Then G is solvable.*

Another result about factorizable groups can be found in Camina-Gagen [2].

§ 7. Orders of simple groups.

There are various theorems which assert that the order of a noncyclic simple group must have certain properties. One of the best known is Burnside's theorem which states that at least 3 distinct primes must divide $|G|$ if G is simple. The results of § 4.2 immediately yield a classification of all simple groups whose order is not divisible by 16 (modulo the question of groups of Ree type). In this section results of this type will be discussed.

Theorem 7.1 (Brauer-Fowler [1], Feit-Thompson [4]). — *Let G be a group of composite order. Then G contains a proper subgroup of order greater than $|G|^{1/3}$.*

It is an open question whether a noncyclic simple group G always contains a proper subgroup of order greater than $|G|^{1/2}$. Also it is not known whether a noncyclic simple group G always contains a real element x with $|\mathbf{C}_G(x)|^3 > |G|$.

Theorem 7.2 (Brauer-Tuan [1]). — *Let G be a simple group with $|G| = pq^a g_0$ where p, q are primes and $g_0 < p - 1$. Then $G \approx PSL_2(p)$ with $p = 2^m \pm 1$ or $G \approx PSL_2(p-1)$ with $p - 1 = 2^m$, $p > 3$.*

Theorem 7.3 (Brauer [12]). — *Let G be a simple group of order $p^a q^b g_0$, where p, q are distinct primes and $a > 0$. If $|G| \neq p$ then $g_0 - 1 > \log p/\log 6$.*

Theorem 7.4 (Brauer [2], Nagai [1], [2], [3]). — *See also* MR, 14 *p.* 843). *Let G be a simple group with $|G| = p\dfrac{(p-1)}{t}(1 + np)$ where p is a prime. Assume that a S_p-group of G is self centralizing and $t \mid (p-1)$.*

(i) *If $n \leq p + 2$ then $G \approx M_{11}$, $PSL_3(3)$, $PSL_2(p)$ or $PSL_2(2^m)$ where $2^m \pm 1 = p$.*

(ii) *If $2p - 3 < n \leq 2p + 3$ and t is odd, $t > 1$ then $2p + 1 = q^a \geq 23$ for some prime q where $q = 3$ for $a > 1$. Furthermore $G \approx PSL_2(2p + 1)$.*

(iii) *If $n = 2p + 3$ and $t = \dfrac{p-1}{2}$ then $2p+1$ is a prime power and $G \approx PSL_2(2p+1)$.*

Theorem 7.5 (Brauer-Reynolds [1]). — *Let G be a simple group whose order is divisible by the prime p. Suppose that $p^3 > |G|$. Then $G \approx PSL_2(p)$, $p > 3$ or $G \approx SL_2(2^m)$ with $p = 2^m + 1 > 3$.*

A variation on this result can be found in Herzog [6].

The only known simple groups whose order is not divisible by 4 distinct primes are the eight groups $PSL_2(5)$, $PSL_2(7)$, $PSL_2(8)$, $PSL_2(9)$, $PSL_2(17)$, $PSL_3(3)$, $PSU_3(3)$ and $O_5'(3)$. It is an open question whether any others exist. As a corollary of Theorem 3.2 one gets.

THEOREM 7.6 (Thompson [8]). — *Let G be a simple group whose order is not divisible by 4 distinct primes. Then* $|G| = 2^a 3^b p^c$ *where* $p = 5, 7, 13$ *or* 17.

THEOREM 7.7 (Brauer [13], Wales [5]). — *Let G be a simple group of order* $2^a 3^b p$ *where p is a prime. Then G is isomorphic to one of the eight groups listed above.*

Related results can be found in Herzog [4], [5]. A discussion of questions related to the theorems above can be found in Brauer [5].

There exist infinitely many pairs of nonisomorphic simple groups which have the same order. However various simple groups have been characterized by their orders. See for instance Theorem 7.5. In particular all the known simple groups of order at most 10^6 except $\mathfrak{A}_8$ and $PSL_3(4)$ which both have order 20, 160 have been characterized by their orders. Here are a few other results in this direction.

THEOREM 7.8. — *Each of the following groups is the unique simple group of its order.*

(i) (Stanton [1]), M_{12}, M_{24}.
(ii) (Parrot [1]), M_{11}, M_{22}.
(iii) (Bryce [1]), M_{23}.
(iv) (Hall-Wales [1]), HaJ.
(v) (S. K. Wong [1]), HJM.

Hall [3] has undertaken a systematic survey to find all simple groups of order at most 10^6. This work is not yet complete. However since this work was begun one new simple group, namely HaJ, with order in this range has been discovered.

While there may be two nonisomorphic groups of the same order it seems possible that a simple group is characterized by its character table. The following result is known.

THEOREM 7.9 (Nagao [1], Oyama [1]). — *The groups* $\mathfrak{A}_n$ *and* $\mathcal{S}_n$ *are characterized by their character table.*

To conclude this section let me mention one curious fact pointed out by M. Benard and A. Rudvalis in answer to a question I raised. The groups $PSp_6(2)$ and $D_4(2)$, which are isomorphic to the simple factors of the Weyl groups of E_7 and E_8 respectively, are the only known simple groups for which every character is rational valued.

§ 8. Linear groups.

One of the oldest results in group theory is the following.

THEOREM 8.1 (Jordan). — *There exists an integer valued function J defined on the positive integers such that if a group G has a faithful complex representation of degree n then* $|G:A| < J(n)$ *for some normal abelian subgroup A of G.*

Theorem 8.1 obviously implies the same conclusion with the same function J if the complex field is replaced by any field whose characteristic does not divide $|G|$. This has recently been generalized as follows.

THEOREM 8.2 (Brauer-Feit [1]). — *Let p be a prime. There exists an integer valued function f_p defined on ordered pairs of integers such that if G has a faithful representation of degree n over a field of characteristic p and p^m is the order of a Sylow p-group of G then $|G:A| < f_p(m, n)$ for some normal abelian subgroup A of G.*

The following result generalizes Theorem 8.1 in a different direction.

THEOREM 8.3 (Isaacs-Passman [1]). — *There exists an integer valued function f defined on the positive integers such that if the degree of every complex irreducible representation of G is at most n then $|G:A| < f(n)$ for some normal abelian subgroup A of G.*

Under special assumptions more precise conclusions can be obtained in Theorem 8.3. See Isaacs [1], Isaacs-Passman [2], [3] and Passman [1].

Theorems 8.1 and 8.2 assert that the degree of a faithful representation of G over some field and the order of a Sylow p-group in case the field has characteristic $p > 0$ restrict the nature of G. The remaining subsections of this section contain more precise results along these lines.

If p is a prime then G is of *type* $L_2(p)$ if every composition factor of G is either p-solvable or is isomorphic to $PSL_2(p)$.

§ 8.1. LINEAR GROUPS IN CHARACTERISTIC $p > 0$

Let p be a prime, let G be a group and let d be the degree of a faithful representation of G over a field of characteristic p. Let P be a S_p-group of G.

THEOREM 8.1.1 (P. Hall-G. Higman [1]). — *Suppose that G is p-solvable, $\mathbb{O}_p(G) = \langle 1 \rangle$ and P is cyclic. Then*

(i) *There exists an integer a with $1 \leq p^a \leq |P|$ depending on G such that*

$$d \geq |P| - p^a \geq \frac{p-1}{p}|P|.$$

(ii) *If either $p \neq 2$ or $p - 1 \neq 2^b$ for any integer b then $d \geq |P|$.*

THEOREM 8.1.2 (Blau [1], Feit [4]). — *Suppose that $p \geq 11$, P is cyclic, G is not of type $L_2(p)$ and $d \leq p$. Then $|P| = p$, $\mathbb{C}_G(P) = P \times \mathbb{Z}(G)$ and one of the following holds.*

(i) *$p = 11$ and $d \geq 7$.*

(ii) *$p > 11$ and $d \geq \max\left\{\frac{3}{4}(p-1), p - e\right\}$ where $e = |\mathbb{N}_G(P) : \mathbb{C}_G(P)|$.*

In case $p = 11$ Theorem 8.1.2 gives the best possible estimate since Ja has a 7 dimensional faithful representation over $GF(11)$. However in case $p > 11$ the result is far from satisfactory. A nonsolvable doubly transitive group on p letters satisfies the hypotheses of Theorem 8.1.2 with $d = p - 2$ but there is no known example of a group which satisfies these hypotheses with $d < p - 2$. Under various restrictions on e and $|\mathbb{Z}(G)|$ the inequality on d can be sharpened. A variety of results in this direction together with a detailed discussion of the cases $13 \leq p \leq 31$ can be found in Blau [1].

The fact that P is assumed to be cyclic is essential in Theorems 8.1.1 and 8.1.2. However Theorem 8.1.1 can be reformulated as follows.

THEOREM 8.1.3 (P. Hall-G. Higman [1]). — *Suppose that G is p-solvable and $\mathbb{O}_p(G) = \langle 1 \rangle$. Let M be a faithful $GF(p)[G]$ module. Let x be a p-element in G, $x \neq 1$ and let d be the degree of the minimum polynomial of x acting on M. If $P = \langle x \rangle$ then the conclusion of Theorem* 8.1.1 *holds.*

In this form the result has played a vital role in group theory during the past decade. If $|P| = 2$ or 3 in Theorems 8.1.1 or 8.1.3 the results are of course trivially true.

§ 8.2. Quadratic pairs

A *quadratic pair* $(G.M)$ consists of a group G and a faithful $GF(p)[G]$ module M such that G is generated by p-elements with a quadratic minimum polynomial on M.

Suppose that (G, M) is a quadratic pair with $p \geq 5$. If G is p-solvable and $\mathbb{O}_p(G) = \langle 1 \rangle$ then Theorems 8.1.3 implies that $G = \langle 1 \rangle$. The situation is however very different in case G is not p-solvable. In this connection the following profound result has recently been proved.

THEOREM 8.2.1 (Thompson [9]). — *Let (G, M) be a quadratic pair with $p \geq 5$. Assume that $G = G' \neq \langle 1 \rangle$ and $G/\mathbb{Z}(G)$ is simple. Then $G/\mathbb{Z}(G)$ is a simple group of Lie type other than E_8 defined over a field of characteristic p.*

For any simple group of Lie type other than E_8 a complete list of quadratic pairs (G, M) is given in Thompson [9] with M irreducible and G any covering group of the simple group. All types other than E_8 occur in some quadratic pair.

§ 8.3. Linear groups in characteristic 0

Let G be a group and let d be the degree of a faithful complex representation of G. Let π be the set of all primes p with $p - 1 > d$. A survey of some results related to the ones in this subsection can be found in Leonard [3].

THEOREM 8.3.1 (Blichfeldt, Burnside). — *G has an abelian* Hall *π-group.*

THEOREM 8.3.2 (Feit-Thompson [1]). — *If p is a prime with $d < \frac{p-1}{2}$ then the S_p-group of G is normal in G.*

THEOREM 8.3.3 (Feit [3]). — *Let H be a* Hall *π-group of G. Then one of the following holds.*

(i) *H is normal in G.*
(ii) *There exists a subgroup H_0 of prime index in H such that H_0 is normal in G.*

THEOREM 8.3.4. — *Suppose that $p \in \pi$ and a Sylow p-group P of G has order p. Assume that G is not of type $L_2(p)$. Then*

(i) $d > \frac{2}{3}(p-1)$. *If* $p \geq 11$ *then* $d \geq \frac{3}{4}(p-1)$.

(ii) (Feit [5]). *If* $|\mathbb{Z}(G)|$ *is odd then* $d \geq p-2$.

(iii) (Feit [5]). *If* $d = p-2$ *then* $p = 2^b + 1$ *for some b and* $G \approx SL_2(2^b) \times \mathbb{Z}(G)$.

(iv) (Blau [2], Brauer [7], Hayden [1]). *Let* $t \mid |\mathbb{N}_G(P) : \mathbb{C}_G(P)| = p-1$. *If* $3 \leq t$ *then* $6 \leq t$ *and* $p \leq t^2 - 3t + 1$.

Theorem 8.3.2 was conjectured by G. de B. Robinson and first proved by Brauer [1] in case $p^2 \nmid |G|$. Brauer conjectured Theorem 8.3.3. Theorem 8.3.4 (i) is an immediate consequence of Theorem 8.1.2 and is an improvement of earlier results of Brauer [1] and Tuan [1]. Theorem 8.3.4 (iii) is proved in Feit [5] under the assumption that $|\mathbb{Z}(G)| = 1$. This assumption can however easily be removed.

The estimate in Theorem 8.3.4 (ii) is clearly the best possible since any doubly transitive permutation group on p letters has a faithful irreducible complex representation of degree $p-1$. However it is an open question whether the assumption about $|\mathbb{Z}(G)|$ can be removed or not. If not then this would lead to (presumably) new simple groups. Under certain conditions the estimate on d can be improved as follows.

THEOREM 8.3.5. — *Let p be a prime and let P be a S_p-group of G. Assume that* $P \cap P^x = \langle 1 \rangle$ *for x in* $G - \mathbb{N}_G(P)$. *If* $d^4 \leq |P|$ *then* $P \lhd G$.

It seems possible that the same conclusion should hold for $d^2 \leq |P|$. Under additional assumptions this has been proved, Brauer-Leonard [1], Leonard [1], [2]. In a different direction the following has been proved.

THEOREM 8.3.6 (Lindsey [2]). — *Suppose that p is a prime and* $d = p-1$. *Assume that* $p^2 \mid \; |G : \mathbb{O}_p(G)|$. *Then* $G/\mathbb{Z}(G')$ *contains a normal subgroup of index at most* 2 *which is isomorphic to* $PSL_2(p) \times PSL_2(p)$.

Groups which have an irreducible complex representation of prime degree have been studied by Brauer [11] and Wales [1]. The following is a simple consequence of their results.

THEOREM 8.3.7. — *Suppose that G has an imprimitive irreducible faithful unimodular representation of prime degree p. Then* $p^3 \nmid |G : \mathbb{O}_p(G)|$.

If $p = 2$ or 3 this result is the best possible since $\mathfrak{A}_5$ and $\mathfrak{A}_6$ have representations of degree 2 and 3 respectively. It is not known whether it is possible to replace p^3 by p^2 in Theorem 8.3.7 for $p \geq 11$. Since all 5 and 7 dimensional finite linear groups have been classified it can be seen by inspection that p^3 can be replaced by p^2 in case $p = 5$ or 7.

The last two results in this subsection are more special in nature but the second of them is used in characterizing Co_3. The proofs depend on the arithmetic of cyclotomic fields.

THEOREM 8.3.8. — *Suppose that G has an irreducible faithful rational valued character of degree* 11. *Then G has a subgroup of index* 11 *or* 12.

THEOREM 8.3.9. — *Suppose that G has an irreducible faithful rational valued character of degree 23. Then one of the following possibilities must occur.*

(i) *G has a subgroup of index 23 or 24.*
(ii) *G' is isomorphic to a subgroup of* Co_2 *or* Co_3.

§ 8.4. THE 2 AND 3 DIMENSIONAL LINEAR GROUPS IN CHARACTERISTIC $p > 0$

Let p be a prime. A subgroup G of $GL_n(p^a)$ can be *lifted* if there exists a finite linear group of degree n whose coefficients are local integers with respect to some prime divisor of p in some algebraic number field and which maps onto G when read modulo this prime divisor. To list all subgroups of $SL_n(p^a)$ for $n = 2, 3$ it suffices to list those which cannot be lifted since all 2 and 3 dimensional finite complex linear groups are known (see the next subsection).

THEOREM 8.4.1 (Dickson). — *Let G be an irreducible subgroup of $SL_2(p^a)$ which cannot be lifted. Then G is isomorphic to $SL_2(p^b)$ for some $b \mid a$.*

THEOREM 8.4.2 (Bloom [1], Hartley [1], Mitchell [1]). — *Let G be an irreducible subgroup of $SL_3(p^a)$ which cannot be lifted. Then G is isomorphic to one of the following.*

(i) *$SL_3(p^b)$ for some $b \mid a$.*
(ii) *In case $3b \mid a$ and $3 \mid (p^b - 1)$ an extension of $SL_3(p^b)$ by a group of order 3.*
(iii) *$U_3(p^b)$ for some b with $2b \mid a$.*
(iv) *In case $6b \mid a$ and $3 \mid (p^b + 1)$ an extension of $U_3(p^b)$ by a group of order 3.*
(v) *If $p \neq 2$, $b \mid a$ and $p^b > 3$, either $PSL_2(p^b)$ or $PGL_2(p^b)$.*
(vi) *If $p = 5$ and a is even, a covering group of $\mathfrak{A}_7$.*

Mitchell [2] has also found all the subgroups of $PSp_4(q)$ for q odd.

§ 8.5. LOW DIMENSIONAL LINEAR GROUPS IN CHARACTERISTIC 0

The finite linear groups in dimension $n \leq 7$ have been completely classified. The tables below contains a complete list of primitive unimodular irreducible groups in dimension n with $\mathbb{Z}(G) \subseteq G'$. Let $z = |\mathbb{Z}(G)|$.

For any prime $p > 2$ let H_p be the split extension of a nonabelian group P of order p^3 and exponent p by $SL_2(p)$. Let (I_p) denote the class of all primitive unimodular subgroup of H_p containing P.

The results for $n = 2, 3$ are classical and can be found in Blichfeldt [1].

$n = 2$	G	$\lvert G \rvert$	z
(I)	$\tilde{\mathscr{S}}_4$, $SL_2(3)$	$24z$, $12z$	2
(II)	$SL_2(5)$	$60z$	2
$n = 3$			
(I_3)			
(II)	$\mathfrak{A}_5$	60	1
(III)	$\tilde{\mathfrak{A}}_6$	$360z$	3
(IV)	$PSL_2(7)$	$168z$	1

$n = 4$ (Blichfeldt [1])

(I)	$A \times B/Z$ where A, B occur for $n = 2$ and Z is the central subgroup of order 2 which is contained in neither A nor B.		
(II)	A subgroup of index 2 in $GL_2(3) \times GL_2(3)/Z$ which does not occur in (I).	$288z$	2
(III)	Let G_0 be the group in (II), there are two possible extensions of G_0 which interchange the factors	$576z$, $576z$	2
(IV)	An extension $SL_2(3) \times SL_2(3)/Z$ which interchanges the factors where Z is as in (I).	$288z$	2
(V)	$\mathfrak{A}_5$, $\mathscr{S}_5$	60, 120	1
(VI)	$\tilde{\mathfrak{A}}_6$, $\tilde{\mathscr{S}}_6$	$360z$, $720z$	2
(VII)	$\tilde{\mathfrak{A}}_7$	$\left(\frac{1}{2} 7!\right)z$	2
(VIII)	$SL_2(5)$	$60z$	2
(IX)	$SL_2(7)$	$168z$	2
(X)	$\tilde{O}_5'(3)$	$2^6.3^4.5z$	2
(XI)	G is a primitive subgroup containing T of the extension of an extra special group T of order 2^5 by its automorphism group.		

$n = 5$ (Brauer [11])

(I_5)			
(II)	$\mathfrak{A}_5$, $\mathfrak{A}_6$, $\mathscr{S}_5$, $\mathscr{S}_6$	60, 360, 120, 720	1
(III)	$PSL_2(11)$	660	1
(IV)	$O_5'(3)$	$2^6.3^4.5$	1

$n = 6$ (Lindsey [1])

(I)	$A \times B$ where A occurs for $n = 2$ and B for $n = 3$		
(II)	$SL_2(5)$	$60z$	2
(III)	$\tilde{\mathscr{S}}_5$	$120z$	2
(IV)	$\tilde{\mathfrak{A}}_6 \approx PS\tilde{L}_2(9)$, an extension by an automorphism of order 2 which is the product of the field automorphism by the automorphism from $GL_2(9)$	$360z$, $720z$	3
(V)	$\tilde{\mathfrak{A}}_6$	$360z$	6
(VI)	$\mathfrak{A}_7$, $\mathscr{S}_7$	$\frac{1}{2} 7!$, $7!$	1
(VII)	$\tilde{\mathfrak{A}}_7$	$\left(\frac{1}{2} 7!\right)z$	3
(VIII)	$\tilde{\mathfrak{A}}_7$	$\left(\frac{1}{2} 7!\right)z$	6
(IX)	$PSL_2(7)$, $PGL_2(7)$	168, 336	1
(X)	$SL_2(7)$, an extension by an automorphism of order 2 in $GL_2(7)$	$168z$, $336z$	2
(XI)	$SL_2(11)$	$660z$	2
(XII)	$SL_2(13)$	$1092z$	2
(XIII)	$O_5'(3)$, an extension by an automorphism of order 2	$2^6.3^4.5$, $2^7.3^4.5$	1
(XIV)	$SU_3(3)$, an extension by the field automorphism	6048, 12096	1
(XV)	$S\tilde{U}_4(3) = \tilde{O}_6^-(3)$ an extension by an automorphism of order 2	$2^7.3^6.5.7z$, $2^8.3^6.5.7z$	6
(XVI)	Ha$\tilde{\mathrm{J}}$	604, $800z$	2

(XVII)	$S\tilde{L}_3(4)$, an extension by an automorphism of order 2 which is the product of a graph automorphism and a field automorphism	$20, 160z, 40, 320z$	6
$n = 7$	(Wales [2]).		
(I_7)			
(II)	$PSL_2(13)$	1092	1
(III)	$PSL_2(8)$, an extension by the field automorphism	504, 1512	1
(IV)	$\mathfrak{A}_8$, $\mathscr{S}_8$	$\frac{1}{2} 8!$, $8!$	1
(V)	$PSL_2(7)$, $PGL_2(7)$	168, 336	1
(VI)	$PSU_3(3)$, an extension by the field automorphism	6048, 12096	1
(VII)	$Sp_6(2)$	$2^9.3^4.5.7$	1

§ 9. **Permutation groups.**

The theory of permutation groups is as old as group theory. See for instance Passman [2] and Wielandt [5] for systematic expositions. This section contains a list of some recently proved results. No attempt at completeness has been made, rather the emphasis is on results which are related to questions concerning the structure of simple groups.

Let G be a permutation group on a set Ω and let α be in Ω. Then G_α denotes the subgroup of G consisting of all permutations leaving α fixed.

§ 9.1. Doubly transitive groups

THEOREM 9.1.1. — *Let G be a 2-transitive permutation group on Ω. For α in Ω assume that G_α has a normal subroup which is regular on $\Omega - \{\alpha\}$. Then G has a normal subgroup M with $M \subseteq G \subseteq$ Aut (M) such that either M is a sharply doubly transitive group or M is isomorphic to one of the following groups and Ω is the set of S_p-groups of G.*

(i) $PSL_2(p^m)$, $PSU_3(p^m)$.
(ii) $Sz(2^{2m+1})$, $p = 2$.
(iii) *A group of* Ree *type*, $p = 3$.

(Sharply doubly transitive groups are completely known, Zassenhaus [3]*).*

This theorem appears in Hering-Kantor-Seitz [1], the proof incorporates the work of many authors who proved various special cases of Theorem 9.1.1. The earliest results in this connection are due to Burnside, Dickson and Frobenius. Essential contributions can be found in Feit [1], Ito [3], Shult [1], Suzuki [4], [6], [11], [14], [15], Zassenhaus [2], [3]. The groups $Sz(2^{2m+1})$ were discovered in proving a special case of this result. Some simplifications of part of the arguments can be found in Glauberman [6], Huppert [1]. Special cases of this theorem can also be found in Harada [6], Ito [11], Nagao [3, I].

THEOREM 9.1.2 (Kantor-O'Nan-Seitz [1]). — *Let G be a 2-transitive permutation group on Ω. Suppose that $G_{\alpha\beta}$ is cyclic for α, β in Ω. Then G is either sharply doubly* *transitive or G is isomorphic to one of the following groups and Ω is the set of S_p-groups of G.*

(i) $PGL_2(p^m)$, $PSL_2(p^m)$, $PGU_3(p^m)$, $PSU_3(p^m)$.
(ii) $Sz(2^{2m+1})$, $p = 2$.
(iii) *A group of* Ree *type*, $p = 3$.

Special cases and related results can be found in Iwasaki-Kimura [1], Kimura [1], Passman [3].

THEOREM 9.1.3 (Ree [3]). — *Let G be a 2-transitive permutation group on Ω. Assume that for α, β in Ω $G_{\alpha\beta}$ contains exactly one nonidentity element which leaves at least* 3 *letters fixed and every involution leaves at least* 3 *letters fixed. If $|\Omega|$ is even then G is a group of* Ree *type and Ω consists of the S_3-groups of G.*

THEOREM 9.1.4 (Harada [7]). — *Let G be a 2-transitive permutation group on Ω. Assume that for α, β in Ω, $|G_{\alpha\beta}|$ is even and $|G_{\alpha\beta} \cap G_{\alpha\beta}^x|$ is odd for x in $G - \mathbb{N}_G(G_{\alpha\beta})$.*

(i) *If $|\Omega|$ is odd then either G has a regular normal subgroup or $S_2(G)$ is dihedral, quasi-dihedral, $Z_{2^n} \wr Z_2$ or $Z_{2^n} \times Z_{2^n}$, $n \geq 2$.*
(ii) *If $|\Omega|$ is even then one of the following holds.*

(a) $PSL_2(p^m) \subseteq G \subseteq P\Gamma L_2(p^m)$, $p \neq 2$, *Ω is the set of S_p-groups of G and* $|\Omega| = p^m+1$.
(b) *G is isomorphic to an automorphism group of the* 1 *or* 2 *dimensional affine group over a field of characteristic* 2.
(c) $G \approx \mathfrak{A}_6$, $|\Omega| = 6$ *or* $G \approx P\Gamma L_2(8)$ *and* $|\Omega| = 28$.

See also Hering [2] and King [1].

THEOREM 9.1.5 (Harada [4]). — *Let G be a 2-transitive permutation group on Ω which contains no regular normal subgroup. Suppose that G contains an involution t such that every element in $\mathbb{C}_G(t) - \{1\}$ has the same number of fixed points. Then $G \approx PSL_2(p^m)$ and Ω is the set of S_p-groups of G or $G \approx Sz(2^{2m+1})$ and Ω is the set of S_2-groups of G.*

THEOREM 9.1.6. — *Let G be a 2-transitive permutation group on Ω. Let $m(G)$ be the maximum number of fixed points of an involution in G.*

(i) (Bender [2]). *If $m(G) = 0$ then either G is solvable or $PSL_2(p^m) \lhd G$ for some p and Ω is the set of S_p-groups of $PSL_2(p^m)$.*
(ii) (Hering [2], *see also Theorem* 9.1.4). *If $m(G) = 2$ and $|G_{\alpha\beta\gamma}|$ is odd for all α, β, γ in Ω then either $G \approx \mathfrak{A}_6$ and $|\Omega| = 6$ or $PSL_2(p^m) \subseteq G \subseteq P\Gamma L_2(p^m)$ for some p and Ω is the set of S_p-groups of G.*

THEOREM 9.1.7 (Tsuzuku [3]). — *Let G be a 2-transitive permutation group on Ω. Suppose that $|\Omega| = 1 + p + p^2$ for a prime p and $p^3 \mid |G|$. Then either $G \subseteq PGL_3(p)$ or $\mathfrak{A}_{1+p+p^2} \subseteq G$.*

THEOREM 9.1.8 (Appel-Parker [1]). — *Let G be a 2-transitive permutation group on Ω. Suppose that $|\Omega| = 1 + np$ for a prime p and $n < p$. If $p^2 \mid |G|$ then $\mathfrak{A}_{1+np} \subseteq G$. Furthermore $\mathfrak{A}_{1+np} \subseteq G$ for $|\Omega| = 29$, 53, 149, 173, 269, 293 or* 317.

Groups which have two inequivalent doubly transitive permutation representations with the same character lead to questions concerning block designs. See Feit [6], Ito [2], [13], [15]. It is not known whether a group can have three pairwise inequivalent doubly transitive permutation representations which afford the same character.

Other questions which relate doubly transitive permutation groups and combinatorial configurations are for instance discussed in Hall [2], Ito [16].

§ 9.2. Transitive extensions

Theorem 9.2.1 (Tits [2], Zassenhaus [1]). — *The only transitive extensions of $PGL_n(q)$ acting on projective space are the ones which give rise to the Mathieu groups unless $q = 2$.*

Theorem 9.2.2 (Suzuki [17]). — *Let G be one of the groups $PSU_3(p^m)$, $Sz(2^{2m+1})$ or a group of* Ree *type acting on the S_p-groups of G, where $p = 2$ or 3 respectively in the last two cases. Then G does not have a transitive extension unless $G = PSU_3(2)$ or $Sz(2)$.*

Related results can be found in Bender [1], Luneburg [1], [2]. By combining Theorems 9.1.1, 9.1.2 and 9.2.2 one easily gets.

Theorem 9.2.3 (Hering-Kantor-Seitz [1]). — *Let G be a 3-transitive group on Ω in which the stabilizer of 3 points is cyclic. Then $PGL_2(p^m) \subseteq G \subseteq P\Gamma L_2(p^n)$ where Ω is the set of S_p-groups of $PGL_2(p^m)$.*

§ 9.3. Permutation groups of prime degree

Throughout this subsection p is a prime and G is a permutation group on Ω with $|\Omega| = p$ such that a S_p-group of G is not normal in G. A theorem of Burnside implies that G is doubly transitive on Ω. By Ito [9], G has an irreducible character of degree p. The results of Brauer [2] are important for the study of these groups.

Theorem 9.3.1 (Ito [1], [5], [10]). — *Let P be a S_p-group of G. Let $N = \mathbb{N}_G(P)$.*

(i) (*See also* Feit [5] *and Theorem* 8.3.4 (iii)). *If $|N : P| = 2$ then $p = 2^b + 1$ and $G \approx SL_2(2^b)$.*

(ii) *If $|N : P| = q$ with $2 < q < p - 1$ and G is $2(q-1)-$ transitive on Ω then $G \approx \mathfrak{A}_p$.*

Theorem 9.3.2 (Ito [14]). — *If p is a Fermat prime and G contains an odd permutation then $G \approx \mathscr{S}_p$.*

A related result can be found in Fryer [1].

Theorem 9.3.3 (Ito [7], [8]). — *Suppose that $p = 2q + 1$ with q a prime.*

(i) *Either G is 4-transitive on Ω or $G \approx PSL_2(p)$ with $p = 5, 7$ or 11.*

(ii) *If $p > 23$, $\frac{1}{4}(p-3) = \frac{q-1}{2}$ and $p - 4$ are primes then $\mathfrak{A}_p \subseteq G$.*

§ 9.4. Permutation groups of degree $2p$

Let p be a prime. The only known examples of primitive permutation groups on $2p$ letters which are not doubly transitive occur for $p = 5$. The following results are known in this connection.

THEOREM 9.4.1. — *Let G be a primitive permutation group on 2p letters which is not doubly transitive.*

(i) (Wielandt [2], [5]). $2p = m^2 + 1$ *for some integer m.* $p^2 \not| \, |G|$. G_α *has* 3 *orbits of size* 1, $m\dfrac{(m-1)}{2}$, $m\dfrac{(m+1)}{2}$ *respectively. The irreducible constituents of the permutation character have degrees* 1, $p-1$, p *respectively.*

(ii) (L. Scott [1]). *If* $p > 5$ *then* $p \geq 313$ *and m in* (i) *is not a prime.*

(iii) (Ito [12]). *If* G_α *is not faithful on the orbit of size* $m\dfrac{(m-1)}{2}$ *then* $p = 5$.

(iv) (*See also Theorems* 8.3.4 (iii)). *Let P be a* S_p*-group of G. If* $|\mathbb{N}_G(P)| = 2p$ *then* $p = 5$.

For results of this type for groups of degree $3p$ see for instance Ito [6].

THEOREM 9.4.2 (Nakamura [1]). — *Let* p, $q = 2p - 1$ *be odd primes. A primitive permutation group on* $2p = q + 1$ *letters is either* 3*-transitive or is isomorphic to* $PSL_2(q)$.

§ 9.5. Primitive permutation groups

THEOREM 9.5.1 (Sims [1, I], W. J. Wong [5]). — *Let G be a primitive permutation group on* Ω. *If* G_α *has an orbit of length* 3 *then G is solvable.*

Related results concerning the structure of G under various hypotheses on G_α can be found in Cline-Keller [1], Keller [1], Sims [1, II], W. J. Wong [6].

§ 9.6. Rank 3-groups

Rank 3 permutation groups have recently played an important role in the discovery of several of the sporadic simple groups. The systematic study of these was begun by D. G. Higman [1], [2], [3]. See also Tsuzuku [2]. Since this topic was covered by D. G. Higman in his talk at this congress these results will not be mentioned here.

§ 9.7. Multiply transitive groups

Let G be a permutation group on Ω. The only known examples of groups G which are 5-transitive are the groups $\mathfrak{A}_n$, $\mathcal{S}_n$ with $|\Omega| = n$, M_{12} with $|\Omega| = 12$ or M_{24} with $|\Omega| = 24$.

THEOREM 9.7.1 (Nagao [2], [3], Wielandt [4]). — *Suppose that G is* 7*-transitive on* Ω. *If for any simple group G the group of outer automorphisms is solvable then* $\mathfrak{A}_n \subseteq G$ *where* $|\Omega| = n$.

THEOREM 9.7.2 (Hall [1], Nagao [3], Nagao-Oyama [1]). — *Suppose that G is* 4*-transitive on* Ω. *Let H be the subgroup of G leaving* 4 *letters fixed. If H leaves an additional letter fixed then* $G \approx \mathcal{S}_5$, $\mathfrak{A}_6$ *or* M_{11}.

THEOREM 9.7.3. — *Let G be* 4*-transitive on* Ω. *Let H be the subgroup of G leaving* 4 *letters fixed.*

(i) (Nagao [3]). *If every involution fixes at most* 5 *points then* G *is isomorphic to one of the following.* $\mathcal{S}_n$, $4 \leq n \leq 7$. $\mathfrak{A}_n$, $6 \leq n \leq 9$. M_{11}, M_{12}.

(ii) (Noda-Oyama [1]). *If* H *has a cyclic* S_2*-group then* $G \approx \mathcal{S}_6$ *or* $\mathcal{S}_7$.

(iii) (Oyama [2]). *If a* S_2*-group of* H *fixes exactly* 6 *points then* $G \approx \mathfrak{A}_6$.

(iv) (Oyama [2]). *If a* S_2*-group of* H *fixes exactly* 11 *points then* $G \approx M_{11}$.

(v) (Oyama [2]). *If a* S_2*-group* H *is semi-regular on the remaining points and distinct from* $\langle 1 \rangle$ *then* G *is isomorphic to one of the following* $\mathcal{S}_6$, $\mathcal{S}_7$, $\mathfrak{A}_8$, $\mathfrak{A}_9$, M_{12} *or* M_{23}.

Other conditions on 4-transitive groups can be found in Parker [1]. A result of this nature for 6-transitive groups is proved in Noda [1].

§ 10. **Automorphisms of groups.**

The central problem concerning automorphism groups of simple groups is to prove or disprove the Schreier conjecture which asserts that if G is simple then Out (G) is solvable. (Out (G) = Aut (G)/In (G) is the group of outer automorphisms of G). This conjecture has been verified for the known simple groups (except for a few of the most recently discovered sporadic groups), see section 2. However very little is known in general. The next two results and some variations on them contain almost everything known in this connection for general simple groups.

THEOREM 10.1 (Wielandt [6]). — *If* G *is a simple group which contains a subgroup of prime index then* Out (G) *is solvable.*

THEOREM 10.2 (Glauberman [2]). — *Let* G *be a simple group. If* Aut $(S_2(G))$ *is solvable then* Out (G) *is solvable.*

Related results can also be found in Glauberman [2], these are all consequences of Theorem 4.5.1 above. Special cases of Theorem 10.2 were first proved by Brauer [10].

In a different direction the following result of Brauer, which has been generalized by Wielandt [3], has played an important role in some of the previously mentioned work.

THEOREM 10.3. — *Suppose that* G *admits a noncyclic group* A *of order* 4 *as a group of automorphisms. Let* f_i *for* $i = 1, 2, 3$ *be the number of fixed points of the three nonidentity elements of* A *and let* f *be the number of fixed points of* A. *Then* $f_1 f_2 f_3 = f^2 \mid G \mid$.

An automorphism of a group which fixes only the identity element is said to be fixed point free. It is not known whether a nonsolvable group can admit a fixed point free automorphism though some results have been proved in this connection.

THEOREM 10.4 (Thompson [1], [2], [3], [6]). — *A group which admits a fixed point free automorphism of prime order is nilpotent.*

Related results can be found in Hughes-Thompson [1], Kegel [2]. For other results concerning groups which admit fixed point free automorphisms of special types see Fischer [2], [3], Ralston [1].

§ 11. **Generators and relations.**

An old conjecture states that a finite simple group is generated by two elements. This has been verified for most of the known simple groups. See for example Steinberg [2]. In general nothing is known although Theorem 3.3 above has a result in this connection.

Tits has defined a (B, N) pair to be a group containing subgroups B and N that satisfy various conditions. These conditions are modelled on the Bruhat decomposition of a semi-simple Lie group and have a very geometric flavor. He has succeeded in characterizing all groups of Lie type of rank at least 3 in these terms, see Tits [5]. Theorem 9.1.1 above may be interpreted as a characterization of groups of Lie type of rank 1 in related terms though the methods of proof are very different.

REFERENCES

FG = *Theory of Finite Groups*, A symposium, edited by R. Brauer and C. S. Sah, Benjamin, New York (1969).

J. L. Alperin, R. Brauer and D. Gorenstein. — [1] Finite Groups with quasi-dihedral and wreathed Sylow 2-subgroups, *Trans. A. M. S.*, 151 (1970), pp. 1-261 (Cf. FG 1-12, 13-20).

—. — [2]. To appear.

J. L. Alperin and D. Gorenstein. — [1] The multiplicators of certain simple groups, *Proc. Am. Math. Soc.*, 17 (1966), pp. 515-519.

K. I. Appel and E. T. Parker. — [1] On unsolvable groups of degree $p = 4q + 1$, p and q primes, *Can. J. Math.*, 19 (1967), pp. 583-589.

D. S. Asche. — [1] Some Finite Groups of Even Order, *Proc. L. M. S.* (III), 19 (1969), pp. 208-218.

H. Bender. — [1] Die Nichtexistenz transitiver Erweiterungen gewisser Permutations gruppen, *Arch. Math.* (Basel), 18 (1967), pp. 474-478.

—. — [2] Endliche zweifach transitive Permutationsgruppen, deren involutionen keine Fixpunkte haben, *Math. Z.*, 104 (1968), pp. 175-204.

—. — [3] Finite groups having a strongly embedded subgroup, FG, 21-24.

—. — [4] On groups with abelian Sylow 2-subgroups, *Math. Z.*, 117 (1970), pp. 164-176.

Ja. G. Berkovič. — [1] Some generalizations and applications of a theorem of Suzuki, *Mat. Sb* (N. S.), 64 (106) (1964), pp. 357-377.

—. — [2] On the existence of subgroups of finite non-solvable groups, *Izv. Akad. Nauk SSSR (Sér. Mat.)*, 28 (1964), pp. 583-606.

—. — [3] Finite groups with dispersive second maximal subgroups, *Dokl. Akad. Nauk SSSR*, 158 (1964), pp. 1007-1009 (Translation, *Soviet Math. Dokl.*, 5 (1964), pp. 1331-1334).

—. — [4] The existence of subgroups for a finite non-solvable group II, *Izv. Akad. Nauk SSSR (Sér. Mat.)*, 29 (1965), pp. 527-552.

—. — [5] Subgroup characterization of certain finite groups, *Dokl. Akad. Nauk SSSR*, 169 (1966), pp. 499-502 (Translation, *Soviet Math. Dokl.*, 7 (1966), pp. 940-943).

—. — [6] Finite Groups satisfying weakened Jordan-Dedekind conditions concerning chains, *Finite Groups* (Russian) (1966), pp. 14-23. Nauka i Tehnika Minsk.

—. — [7] A theorem on non-nilpotent solvable subgroups of a finite group, *Finite Groups* (Russian) (1966), pp. 24-39. Nauka i Tehnika Minsk.

—. — [8] Finite Groups in which any two solvable subgroups of equal order are isomorphic, *Sibirsk. Mat. Ž.*, 7 (1966), pp. 1194-1198.

—. — [9] A class of finite groups, *Sibirsk. Mat Ž.*, 8 (1967), pp. 734-740.

H. BLAU. — [1] Under the degree of some finite linear groups. To appear.

—. — [2] An inequality for complex linear groups of small degree. To appear.

H. F. BLICHFELDT. — [1] *Finite Collineation Groups*. University of Chicago Press, Chicago (1917).

D. M. BLOOM. — [1] The subgroups of $PSL_3(q)$ for odd q, *Trans. A. M. S.*, 127 (1967), pp. 150-178.

R. BRAUER. — [1] On groups whose order contains a prime number to the first power I, II, *Am. J. Math.*, 64 (1942), pp. 401-420, 421-440.

—. — [2] On permutation groups of prime degree and related classes of groups, *Ann. Math.*, 44 (1943), pp. 57-79.

—. — [3] On the structure of groups of finite order, *Proc. Int. Cong. of Math.*, Amsterdam (1954), vol. 1, pp. 209-217. Erven P. Noordhoff, N. V. Groninger, North Holland Publishing Co., Amsterdam (1957).

—. — [4] Investigation on groups of even order, *Proc. Nat. Acad. Sci.*, 47 (1961), pp. 1891-1893.

—. — [5] On some conjectures concerning finite simple groups, Studies in *Mathematical Analysis and related topics*. Stanford University Press, Stanford, Calif. (1962), pp. 56-61.

—. — [6] On groups of even order with an abelian 2-Sylow subgroup, *Arch. Math.*, 13 (1962), pp. 55-60.

—. — [7] Some applications of the theory of blocks of characters of finite groups I, II, III, *J. Algebra*, 1 (1964), 152-167, 207-334 ; 3 (1966), pp. 225-255.

—. — [8] On Finite Desarguesian planes I, II, *Math. Z.*, 90 (1965), pp. 117-123 ; 91 (1966), pp. 124-151.

—. — [9] Some results on finite groups whose order contains a prime to the first power, *Nagoya Math. J.*, 27 (1966), pp. 381-400.

—. — [10] Investigation on groups of even order II, *Proc. Nat. Acad. Sci.*, 55 (1966), pp. 254-259.

—. — [11] Über endliche lineare Gruppen von Primzahlgrad, *Math. Ann.*, 169 (1967), pp. 73-96.

—. — [12] On a theorem of Burnside, *Ill. J. Math.*, 11 (1967), pp. 349-351.

—. — [13] On simple groups of order $5.3^a.2^b$, *Bull. A. M. S.*, 74 (1968), pp. 900-903.

— and W. FEIT. — [1] An analogue of Jordan's theorem in characteristic p, *Ann. Math.*, 84 (1966), pp. 119-131.

— and P. FONG. — [1] A characterization of the Mathieu group $\mathfrak{M}_{12}$, *Trans. Am. Math. Soc.*, 122 (1966), pp. 18-47.

— and K. A. FOWLER. — [1] Groups of even order, *Ann. Math.*, 62 (1955), pp. 565-583.

— and H. S. Leonard. — [1] On finite groups with an abelian Sylow group, *Can. J. Math.*, 14 (1962), pp. 436-450.

— and W. E. REYNOLDS. — [1] On a problem of Artin, *Ann. Math.*, 68 (1958), pp. 713-720.

— and M. SUZUKI. — [1] On finite groups of even order whose 2-Sylow group is a generalized quaternion group, *Proc. Nat. Acad. Sci.*, 45 (1959), pp. 1757-1759.

— M. SUZUKI and G. E. WALL. — [1] A characterization of the one-dimensional unimodular projective groups over finite fields, *Ill. J. Math.*, 2 (1958), pp. 718-745.

— and H. F. TUAN. — [1] On simple groups of finite order I, *Bull. A. M. S.*, 51 (1945), pp. 756-766.

A. BRYCE. — [1] On the Mathieu Group M_{23}. Thesis, Monash University, 1969.

N. BURGOYNE and P. FONG. — [1] The Schur multipliers of the Mathieu groups, *Nagoya Math. J.*, 27 (1966), pp. 733-745, correction, 31 (1968), pp. 297-304.

A. R. CAMINA and T. M. GAGEN. — [1] Groups with metacyclic Sylow-2 subgroups, *Can. J. Math.*, 21 (1969), pp. 1234-1238.

—. — [2] Some non-soluble factorizable groups, *Ill. J. Math.*, 14 (1970), pp. 91-98.

R. W. CARTER. — [1] Simple groups and simple Lie-algebras, *J. London Math. Soc.*, 40 (1965), pp. 193-240.

E. CLINE and G. KELLER. — [1] A characterization of $PSL(2,8)$, *J. Algebra*, 13 (1969), pp. 393-408.

M. COLLINS. — [1] To appear.

J. H. CONWAY. — [1] A group of order 8, 315, 553, 613, 086, 720, 000, *Bull. London Math. Soc.*, 1 (1969), pp. 79-88 (Cf. *Proc. Nat. Acad. Sci.*, 61 (1968), pp. 398-400).

W. FEIT. — [1] On a class of doubly transitive permutation groups, *Ill. J. Math.*, 4 (1960), pp. 170-186 (Cf. *Proc. Sympos, Pure Math.*, vol. 1, *A. M. S.*, Providence, R. I. (1959), pp. 22-28).

—. — [2] A characterization of the simple groups $SL(2,2^a)$, *Am. J. Math.*, 82 (1960), pp. 281-300 (correction *Am. J. Math.*, 84 (1962), pp. 201-204).

—. — [3] Groups which have a faithful representation of degree less than $p - 1$, *Trans. Am. Math. Soc.*, 112 (1964), pp. 287-303.

—. — [4] Groups with a cyclic Sylow subgroup, *Nagoya Math. J.*, 27 (1966), pp. 571-584.

—. — [5] On finite linear groups, *J. Algebra*, 5 (1967), pp. 378-400.

—. — [6] Automorphisms of Symmetric Balanced Incomplete Block Designs, *Math. Z.*, 118 (1970), pp. 40-49.

— M. HALL and J. G. THOMPSON. — [1] Finite groups in which the centralizer of any non-identity element is nilpotent, *Math. Z.*, 74 (1960), pp. 1-17.

— and J. G. THOMPSON. — [1] Groups which have a faithful representation of degree less than $\frac{p-1}{2}$, *Pacific J. Math.*, 11 (1961), pp. 1257-1262.

—. — [2] Finite groups which contain a self-centralizing subgroup of order 3, *Nagoya Math. J.*, 21 (1962), pp. 185-197.

—. — [3] Solvability of groups of odd order, *Pacific J. Math.*, 13 (1963), pp. 755-1029.

—. — [4] A solvability criterion for finite groups and some consequences, *Proc. Nat. Acad. Sci.*, 48 (1962), pp. 968-970.

D. FENDEL. — [1] A characterization of Conway's group. 3. Thesis, Yale University, 1970.

P. A. FERGUSON. — [1] A theorem on CC subgroups. To appear.

B. FISCHER. — [1] Ein Auflösbarkeitskriterium für endliche Gruppen, *Arch. Math.*, 17 (1966), pp. 481-484.

—. — [2] Finite groups admitting a fixed-point-free automorphism of order $2p$, *J. Algebra*, 3 (1966), pp. 99-114.

—. — [3] *Idem* II, *J. Algebra*, 5 (1967), pp. 25-40.

—. — [4] Distributiv Quasigruppen endlicher Ordnung, *Math. Z.*, 83 (1964), pp. 267-303.

—. — [5] F-Gruppen endlicher Ordnung, *Archiv. Math.*, 56 (1965), pp. 330-336.

—. — [6] Finite Groups generated by 3-transpositions, Math. Inst. U. of Warwick.

P. FONG. — [1] Some Sylow subgroups of order 32 and a characterization of $U(3,3)$, *J. Algebra*, 6 (1967), pp. 65-76.

—. — [2] Sylow 2-subgroups of small orders. To appear.

—. — [3] On a characterization of the groups $G_2(q)$. To appear.

— and W. J. WONG. — [1] A characterization of the finite simple groups $PSp(4, p)$, $G_2(q)$, $D_4^2(q)I$. *Nagoya Math. J.*, 36 (1969), pp. 143-185 (Cf. FG 25-39).

K. D. FRYER. — [1] A class of permutation groups of prime degree, *Can. J. Math.*, 7 (1955), pp. 24-34.

T. M. GAGEN. — [1] On groups with abelian Sylow 2-groups, *Math. Z.*, 90 (1965), pp. 268-272.

—. — [2] A characterization of Janko's simple group, *Proc. A. M. S.*, 19 (1968), pp. 1393-1395.

— and Z. JANKO. — [1] Finite simple groups with nilpotent third maximal subgroups, *J. Austral. Math. Soc.*, 6 (1966), pp. 466-469.

P. X. GALLAGHER. — [1] Group characters and Sylow subgroups, *J. London Math. Soc.*, 39 (1964), pp. 720-722.

G. GLAUBERMAN. — [1] Central elements of core-free groups, *J. Algebra*, 4 (1966), pp. 403-420.

—. — [2] On the automorphism group of a finite group having no nonidentity normal subgroups of odd order, *Math. Z.*, 93 (1966), pp. 154-160.
—. — [3] Subgroups of finite groups, *Bull. Am. Math. Soc.*, 73 (1967), pp. 1-12.
—. — [4] A characterization of the Suzuki groups, *Ill. J. Math.*, 12 (1968), pp. 76-98.
—. — [5] Prime-power factor groups of finite groups I, II, *Math. Z.*, 107 (1968), pp. 159-172, *Math. Z.*, 117 (1970), pp. 46-56.
—. — [6] On a class of doubly transitive permutation groups, *Ill. J. Math.*, 13 (1969), pp. 394-399.
D. M. Goldschmidt. — [1] On the 2-exponent of a finite group. Thesis, U. of Chicago (1969).
D. Gorenstein. — [1] Some topics in the theory of finite groups, *Rend. Mat. e Appl.* (5), 23 (1964), pp. 298-315.
—. — [2] Finite groups in which Sylow 2-subgroups are abelian and centralizers of involutions are solvable, *Canad. J. Math.*, 17 (1965), pp. 860-906.
—. — [3] *Finite groups*, Harper and Row, New York (1968).
—. — [4] Finite groups the centralizer of whose involutions have normal 2-complements, *Canad. J. Math.*, 21 (1969), pp. 335-357.
— and K. Harada. — [1] A characterization of Janko's two new simple groups. To appear.
—. — [2] Finite groups whose Sylow 2-subgroups are the direct product of two dihedral groups. To appear.
—. — [3] On finite groups with Sylow 2-subgroups of type A_n, $n = 8, 9, 10, 11$, *Math. Z.*, 117 (1970), pp. 207-238.
—. — [4] On finite groups with Sylow 2-subgroups of type $\hat{A}_n$, $n = 8, 9, 10, 11$. To appear.
— and J. Walter. — [1] On finite groups with dihedral Sylow 2-subgroups, *Ill. J. Math.*, 6 (1962), pp. 553-593.
—. — [2] On the maximal subgroups of finite simple groups, *J. Algebra*, 1 (1964), pp. 168-213.
—. — [3] The characterization of finite groups with dihedral Sylow 2-subgroups, *J. Algebra*, 2 (1965), pp. 85-151, 218-270, 354-393.
M. Guterman. — [1] A characterization of the Groups $F_4(2^n)$. To appear.
M. Hall. — [1] On a theorem of Jordan, *Pacific J. Math.*, 4 (1954), pp. 219-226.
—. — [2] Current studies on permutation groups, *Proc. Sympos. Pure Math.*, vol. 1 (1959), pp. 29-41 ; *A. M. S.*, Providence R. I.
—. — [3] A search for simple groups of orders less than one million. To appear.
— and D. Wales. — [1] The simple group of order 604, 800, *J. Algebra*, 9 (1968), pp. 417-450 (Cf. FG, 79-90).
P. Hall and G. Higman. — [1] On the p-length of p-soluble groups and reduction theorems for Burnside's problem, *Proc. London Math. Soc.*, 6 (1956), pp. 1-40.
K. Harada. — [1] A characterization of the groups $LF(2, q)$, *Ill. J. Math.*, 11 (1967), pp. 647-659.
—. — [2] Groups with a certain type of Sylow 2-subgroups, *J. Math. Soc. Japan*, 19 (1967), pp. 303-307.
—. — [3] Finite simple groups with short chains of subgroups, *J. Math. Soc. Japan*, 20 (1968), pp. 655-672.
—. — [4] A characterization of the Zassenhaus groups, *Nagoya Math. J.*, 33 (1968), pp. 117-127.
—. — [5] Finite simple groups whose Sylow 2-subgroups are of order 2^7, *J. Algebra*, 14 (1970), pp. 386-404.
—. — [6] A characterization of the Simple Group $U_3(5)$, *Nagoya Math. J.*, 38 (1970), pp. 27-40.
—. — [7] On some doubly transitive groups. To appear.
R. W. Hartley. — [1] Determination of the ternary collineation groups whose coefficients Lie in $GF(2^n)$, *Ann. of Math.* (2), 27 (1925), pp. 140-158.
S. Hayden. — [1] On finite linear groups whose order contains a prime larger than the degree. Thesis, Harvard University (1963).
T. Hearne. — [1] On the finite group ${}^2F_4(2)$. Thesis, Northeastern University (1969).

D. HELD. — [1] A characterization of the alternating groups of degrees eight and nine, *J. Algebra*, 7 (1967), pp. 218-237.
—. — [2] Eine Bemerkung zur Kennzeichnung von $PSL(4,2)$, *Arch. Math.* (Basel), 18 (1967), pp. 580-581.
—. — [3] Eine Kennzeichnung der Mathieu-Gruppe M_{22} und der alternierenden Gruppe A_{10}, *J. Algebra*, 8 (1968), pp. 436-449.
—. — [4] A characterization of some multiply transitive permutation groups I, *Ill. J. Math.*, 13 (1969), pp. 224-240.
—. — [5] A characterization of some multiply transitive permutation groups II, *Arch. Math.* (Basel), 19 (1968), pp. 378-382.
—. — [6] The simple group related to M_{24}, *J. Algebra*, 13 (1969), pp. 253-296 (Cf. FG 121-124).
C. HERING. — [1] Eine Characterisierung der endlichen zweidimensionalen projektiven Gruppen, *Math. Z.*, 82 (1963), pp. 152-175.
—. — [2] Zweifach transitive permutationsgruppen, in denen 2 die maximale Anzahl von Fixpunkten von Involutionen ist, *Math. Z.*, 104 (1968), pp. 150-174.
—, W. M. KANTOR and G. M. SEITZ. — [1] Finite groups with a split *BN*-pair of rank 1. To appear.
M. HERZOG. — [1] On finite groups which contain a Frobenius subgroup, *J. Algebra*, 6 (1967), pp. 192-221.
—. — [2] A characterization of some projective special linear groups, *J. Algebra*, 6 (1967), pp. 305-308.
—. — [3] A characterization of the simple groups $PSL(2, p)$, $p > 3$, *Israël J. Math.*, 5 (1967), pp. 79-85.
—. — [4] On finite simple groups of order divisible by three primes only, *J. Algebra*, 10 (1968), pp. 383-388.
—. — [5] On finite groups with cyclic Sylow subgroups for all odd primes, *Israël J. Math.*, 6 (1968), pp. 206-216.
—. — [6] On finite groups with independent cyclic Sylow subgroups, *Pacific J. Math.*, 29 (1969), pp. 285-293.
D. G. HIGMAN. — [1] Finite permutation groups of rank 3, *Math. Z.*, 86 (1964), pp. 145-156.
—. — [2] Primitive rank 3 groups with a prime subdegree, *Math. Z.*, 91 (1966), pp. 70-86.
—. — [3] Intersection matrices for finite permutation groups, *J. Algebra*, 6 (1967), pp. 22-42.
—. — [4] Characterization of families of rank 3 permutation groups by the subdegrees I, *Archiv. der Math.*, 21 (1970), pp. 151-157.
— and C. C. SIMS. — [1] A simple group of order 44, 352, 000, *Math. Z.*, 105 (1968), pp. 110-113.
G. HIGMAN. — [1] Suzuki 2-groups, *Ill. J. Math.*, 7 (1963), pp. 79-96.
—. — [2] Odd characterization of finite simple groups, *Lecture notes*. University of Michigan (1968).
—. — [3] On the simple group of D. G. HIGMAN and C. C. SIMS, *Ill. J. Math.*, 13 (1969), pp. 74-80.
— and J. MCKAY. — [1] On Janko's simple group of order 50, 232, 960, *Bull. London Math. Soc.*, 1 (1969), pp. 89-94 (Cf. FG 65-77).
D. R. HUGHES and J. G. THOMPSON. — [1] The H_p-problem and the structure of H_p-groups, *Pacific J. Math.*, 9 (1959), pp. 1097-1102.
B. HUPPERT. — [1] Scharf dreifach transitive Permutationsgruppen, *Arch. Math.*, 13 (1962), pp. 61-72.
I. M. ISAACS. — [1] Finite groups with small character degrees and large prime divisors, *Pacific J. Math.*, 23 (1967), pp. 273-280.
— and D. S. PASSMAN. — [1] Groups with representations of bounded degree, *Can. J. Math.*, 16 (1964), pp. 299-309.
—. — [2] Groups whose irreducible representations have degrees dividing p^e, *Ill. J. Math.*, 8 (1964), pp. 446-457.

—. — [3] A characterization of groups in terms of the degrees of their character, *Pacific J. Math.*, 15 (1965), pp. 877-903.

N. Ito. — [1] Zur Theorie der permutationsgruppen vom grad pI, II, *Math. Z.*, 74 (1960), pp. 299-301; 75 (1961), pp. 127-135.

—. — [2] Über die Gruppen $PSL(n, q)$, die eine Untergruppe von Primzahlindex enthalten, *Acta Sci. Math. Szeged.*, 21 (1960), pp. 206-217.

—. — [3] On a class of doubly transitive permutation groups, *Ill. J. Math.*, 6 (1962), pp. 341-352.

—. — [4] On transitive simple permutation groups of degree $2p$, *Math. Z.*, 78 (1962), pp. 453-468.

—. — [5] A note on transitive permutation groups of degree p, *Osaka Math. J.*, 14 (1962), pp. 213-218.

—. — [6] On transitive simple groups of degree $3p$, *Nagoya Math. J.*, 21 (1962), pp. 123-158.

—. — [7] A note on transitive permutation groups of degree $p = 2q + 1$, p and q being prime numbers, *J. Math. Kyoto Univ.*, 3 (1963), pp. 111-113.

—. — [8] Transitive permutation groups of degree $p = 2q + 1$, p and q prime numbers I, II, III, *Bull. A. M. S.*, 69 (1963), pp. 165-192; *Trans. A. M. S.*, 113 (1964), pp. 454-487; 116 (1965), pp. 151-166.

—. — [9] Über die Darstellungen der Permutationsgruppen von Primzahlgrad, *Math. Z.*, 89 (1965), pp. 196-198.

—. — [10] Un teorema sui gruppi transitivi di grado primo, *Rend. Sem. Mat. Univ. Padova*, 35 (1965), pp. 132-133.

—. — [11] On doubly transitive groups of degree n and order $2(n - 1)n$, *Nagoya Math. J.*, 27 (1966), pp. 409-417.

—. — [12] On uniprimitive permutation groups of degree $2p$, *Math. Z.*, 102 (1967), pp. 238-244.

—. — [13] On a class of doubly, but not triply transitive permutation groups, *Arch. Math.* (Basel), 18 (1967), pp. 564-570.

—. — [14] On transitive permutation groups of Fermat prime degree, *Proc. Internat. Conf. Theory of Groups* (Canberra, 1965), pp. 191-202. Gordon and Breach, New York (1967).

—. — [15] On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p. I, II, *Rend. Sem. Mat. Univ. Padova*, 38 (1967), pp. 287-292; *Nagoya Math. J.*, 37 (1970), pp. 201-208.

—. — [16] A theorem on Jordan groups (FG 47-48).

S. Iwasaki and H. Kimura. — [1] On some doubly transitive permutation groups of degree n and order $6n(n - 1)$, *Nagoya Math. J.*, 37 (1970), pp. 25-33.

Z. Janko. — [1] Zur theorie der einfachen Gruppen, Glusnik Mat-Fiz., *Astronom. Drustvo. Mat. Fiz. Hrvatske (Ser. II)*, 16 (1961), pp. 167-169.

—. — [2] Endliche Gruppen mit lauter nilpotenten zweitmaximalen Untergruppen, *Math. Z.*, 79 (1962), pp. 422-424.

—. — [3] Finite groups with invariant fourth maximal subgroups, *Math. Z.*, 82 (1963), pp. 82-89.

—. — [4] Finite simple groups with short chains of subgroups, *Math. Z.*, 84 (1964), pp. 428-437.

—. — [5] Finite groups with a nilpotent maximal subgroup, *J. Australian Math. Soc.*, 4 (1964), pp. 449-451.

—. — [6] A new finite simple group with abelian 2-Sylow subgroups and its characterization, *J. Algebra*, 3 (1966), pp. 147-186 (Cf. *Proc. Nat. Acad. Sci.*, 53 (1965), pp. 657-658).

—. — [7] A characterization of the smallest group of Ree associated with the simple Lie-algebra of type (G_2), *J. Algebra*, 4 (1966), pp. 293-299.

—. — [8] A characterization of the finite simple group $PSp_4(3)$, *Can. J. Math.*, 19 (1967), pp. 872-894.

—. — [9] A characterization of the Mathieu simple groups I, II, *J. Algebra*, 9 (1968), pp. 1-19, 20-41.
—. — [10] Some new simple groups of finite order I, *Ist. Naz. Alta Math., Symposia Mathematica*, vol. vol. I, Odensi, Gubbio (1968), pp. 25-64 (Cf. FG 63-64).
—. — [11] A characterization of the simple group $G_2(3)$, *J. Algebra*, 12 (1969), pp. 360-372.
—. — [12] The nonexistence of a certain type of finite simple group. To appear.
— and J. G. THOMPSON. — [1] On a class of finite simple groups of Ree, *J. Algebra*, 4 (1966), pp. 274-292.
—. — [2] On finite simple groups whose Sylow 2-subgroups have no normal elementary subgroup of order 8, *Math. Z.*, 113 (1970), pp. 385-397.
— and S. K. WONG. — [1] A characterization of the Higman-Sims simple group, *J. Algebra*, 13 (1969), pp. 517-534.
W. M. KANTOR, M. O'NAN and G. M. SEITZ. — [1] 2-transitive groups in which the stabilizer of two points is cyclic. To appear.
O. H. KEGEL. — [1] Produkte nilpotenter Gruppen, *Arch. Math.*, 12 (1961), pp. 90-93.
—. — [2] Die Nilpotenz der H_p-Gruppen, *Math. Z.*, 75 (1961), pp. 373-376.
G. KELLER. — [1] A characterization of A_6 and M_{11}, *J. Algebra*, 13 (1969), pp. 409-421.
H. KIMURA. — [1] On doubly transitive permutation groups of degree n and order $4(n - 1)n$, *J. Math. Soc. of Japan*, 21 (1969), pp. 234-243.
J. D. KING. — [1] A characterization of some doubly transitive groups, *Math. Z.*, 107 (1968), pp. 43-48 (Corrections *Math. Z.*, 112, pp. 393-394).
A. P. KOHNO and V. A. VEDERNIKOV. — [1] The effect of subgroup chains on the properties of finite groups, *Vesci Akad. Navak BSSR Ser. Fiz.-Mat. Navuk* (1967), No. 3, pp. 75-81.
T. KONDO. — [1] On a characterization of the alternating group of degree eleven, *Ill. J. Math.*, 13 (1969), pp. 528-541.
—. — [2] On the alternating groups, I, II, III, *J. Fac. Sci. Univ. Tokyo* (Sect. I), 15 (1968), pp. 87-97 ; *J. Math. Soc. Japan*, 21 (1969), pp. 116-139 ; *J. Algebra*, 14 (1970), pp. 35-69 (Cf. FG 49-53).
A. I. KOSTRIKIN. — [1] Finite groups, *Algebra* (Russian) (1964), pp. 7-46 ; *Akad. Nauk SSSR Inst. Nauĕn Informacii*, Moscow (1966).
M. P. LELČUK. — [1] Nonsolvable groups structurally close to solvable ones, *Finite groups* (Russian) (1966), pp. 55-71. Nauka i Tehnika Minsk.
H. LEONARD. — [1] On finite groups which contain a Frobenius factor group, *Ill. J. Math.*, 9 (1965), pp. 47-58.
—. — [2] On finite groups whose p-Sylow subgroup is a T. I. set, *Proc. A. M. S.*, 19 (1968), pp. 667-670.
—. — [3] Finite complex linear groups of small degree. To appear.
J. H. LINDSEY II. — [1] On a projective representation of the Hall-Janko group, *Bull. A. M. S.*, 74 (1968), p. 1094 (Cf. FG 97-100).
—. — [2] A correlation between $PSU_4(3)$, the Suzuki group, and the Conway group. To appear.
D. LIVINGSTON. — [1] On a permutation representation of the Janko group, *J. Algebra*, 6 (1967), pp. 43-55.
H. LÜNEBURG. — [1] Some remarks concerning the Ree groups of type (G_2), *J. Algebra*, 3 (1966), pp. 256-259.
—. — [2] Transitive Erweiterungen endlicher Permutationsgruppen, *Lecture notes in mathematics*, No. 84, Springer-Verlag, Berlin-New York (1969).
R. N. LYONS. — [1] On some finite simple groups of small 2-rank. Thesis, U. of Chicago (1970).
A. MACWILLIAMS. — [1] On 2-groups with no normal abelian subgroups of rank 3 and their occurrence as Sylow 2-subgroups of finite simple groups, *Trans. Amer. Math. Soc.*, 150 (1970), pp. 345-408.
A. MANN. — [1] Finite groups with maximal normalizers, *Ill. J. Math.*, 12 (1968), pp. 67-75.
—. — [2] Simple groups having p-nilpotent 2nd-maximal subgroups, *Israël J. Math.*, 6 (1968), pp. 233-245.

R. P. MARTINEAU. — [1] A characterization of Janko's simple group of order 175, 560, *Proc. London Math. Soc.* (III), 19 (1969), pp. 709-729.
V. D. MAZUROV. — [1] On finite groups with a given Sylow 2-subgroup, *Dokl. Akad. Nauk SSSR*, 168 (1966), pp. 519-521 (Translation, *Soviet Math. Dokl.*, 7 (1966), pp. 681-682).
—. — [2] Finite groups of which a Sylow 2-subgroup is a direct product of quaternions, *Algebra i Logiker Sem.*, 5 (1966), No. 5, pp. 55-57.
—. — [3] Finite groups with metacyclic Sylow 2-subgroups, *Sibirsk. Mat. Ž.*, 8 (1967), pp. 966-982.
J. MCKAY and D. WALES. — [1] The multipliers of the simple groups of order 604, 800 and 50, 232, 960. *J. algabra*, 17 (1971), pp. 262-272.
J. MCLAUGHLIN. — [1] A simple group of order 898, 128, 000 (FG 109-111).
H. H. MITCHELL. — [1] Determination of the ordinary and modular ternary linear group, *Trans. A. M. S.*, 12 (1911), pp. 207-242.
—. — [2] The subgroup of the quaternary abelian linear group, *Trans. A. M. S.*, 15 (1914), pp. 379-396.
O. NAGAI. — [1] Note on Brauer's theorem of simple groups, *Osaka Math. J.*, 4 (1952), pp. 113-120.
—. — [2] Supplement to « Note on Brauer's theorem of simple groups », *Osaka Math. J.*, 5 (1953), pp. 227-232.
—. — [3] On simple groups related to permutation group of prime degree I, *Osaka Math. J.*, 8 (1956), pp. 107-117.
H. NAGAO. — [1] On the groups with the same table of characters as symmetric groups, *J. Inst. Polytech. Osaka City Univ. (Ser. A)* (8) (1957), pp. 1-8.
—. — [2] On a theorem of Wielandt, *Proc. Japan Acad.*, 40 (1964), pp. 793-794.
—. — [3] On multiply transitive groups I, IV, V, *Nagoya Math. J.*, 27 (1966), pp. 15-19 ; *Osaka J. Math.*, 2 (1965), pp. 327-341 ; *J. Algebra*, 9 (1968), pp. 240-248.
— and T. OYAMA. — [1] On multiply transitive groups II, III, *Osaka J. Math.*, 2 (1965), pp. 129-136, 319-326.
K. NAKAMURA. — [1] Über Permutationsgruppen von Grad $2p$, *Math. Z.*, 94 (1966), pp. 307-308.
R. NODA. — [1] On 6-fold transitive groups, *Osaka J. Math.*, 4 (1967), pp. 257-260.
— and T. OYAMA. — [1] On multiply transitive groups VI, *J. Algebra*, 11 (1969), pp. 145-154.
T. OYAMA. — [1] On the groups with the same table of characters as alternating groups, *Osaka J. Math.*, 1 (1964), No. 1, pp. 91-101.
—. — [2] On multiply transitive groups VII, VIII, IX, *Osaka J. Math.*, 5 (1968), pp. 155-164 ; 6 (1969), pp. 315-319 ; 7 (1970), pp. 41-56.
E. T. PARKER. — [1] On quadruply transitive groups, *Pacific J. Math.*, 9 (1959), pp. 829-836.
D. PARROTT. — [1] On the Mathieu groups M_{22} and M_{11}, *J. Australian Math. Soc.*, 11 (1970), pp. 69-82.
D. S. PASSMAN. — [1] Groups whose irreducible representations have degrees dividing p^2, *Pacific J. Math.*, 17 (1966), pp. 475-496.
—. — [2] *Permutation groups*. W. A. Benjamin, Inc., New York, Amsterdam (1968).
—. — [3] Some 5/2 transitive permutation groups, *Pacific J. Math.*, 28 (1969), pp. 157-171.
K. W. PHAN. — [1] A characterization of the finite simple group $L_4(3)$, *J. Australian Math. Soc.*, 10 (1969), pp. 51-76.
—. — [2] A characterization of the finite simple group $U_4(3)$, *J. Australian Math. Soc.*, 10 (1969), pp. 77-94.
—. — [3] A characterization of four-dimensional unimodular group, *J. Algebra*, 15 (1970), pp. 252-279 (Cf. FG 39-42).
E. RALSTON. — [1] Solvability of finite groups admitting fixed-point-free automorphisms of order *rs*. Thesis Yale U. (1970).
R. REE. — [1] A family of simple groups associated with the simple Lie algebra of type F_4, *Am. J. Math.*, 83 (1961), pp. 401-420.

—. — [2] A family of simple groups associated with the simple Lie algebra of type G_2, *Am. J. Math.*, 83 (1961), pp. 432-462.
—. — [3] Sur une famille de groupes de permutations doublement transitifs, *Can. J. Math.*, 16 (1964), pp. 797-820.
I. SCHUR. — [1] Über die Darstellungen der symmetrischen und alternierenden Gruppen durch gebrochene lineare Substitutionen, *J. Math.*, 139 (1911), pp. 155-250.
L. SCOTT. — [1] Uniprimitive permutation groups (Cf. FG 55-62).
W. R. SCOTT. — [1] *Group theory*. Englewood Cliffs (New Jersey), Prentice-Hall, Inc. (1964).
E. SHULT. — [1] On a class of doubly transitive groups. To appear.
C. C. SIMS. — [1] Graphs and finite permutation groups I, II, *Math. Z.*, 95 (1967), pp. 76-86; 103 (1968), pp. 276-281.
—. — [2] On the isomorphism of two groups of order 44, 352, 000 (Cf. FG 101-108).
R. G. STANTON. — [1] The Mathieu groups, *Can. J. Math.*, 3 (1951), pp. 164-174.
R. STEINBERG. — [1] Automorphisms of finite linear groups, *Can. J. Math.*, 12 (1960), pp. 606-615.
—. — [2] Generators for simple groups, *Can. J. Math.*, 14 (1962), pp. 277-283.
—. — [3] Algebraic groups and finite groups, *Ill. J. Math.*, 13 (1969), pp. 81-86.
W. B. STEWART. — [1] Thesis, Oxford University (1967).
M. SUZUKI. — [1] On finite groups with cyclic Sylow subgroups for all odd primes, *Am. J. Math.*, 77 (1955), pp. 657-691.
—. — [2] The non-existence of a certain type of simple groups of odd order, *Proc. Am. Math. Soc.*, 8 (1957), pp. 686-695.
—. — [3] On finite groups containing an element of order four which commutes only with its powers, *Ill. J. Math.*, 3 (1959), pp. 255-271.
—. — [4] On characterizations of linear groups I, II, III, IV, *Trans. A. M. S.*, 92 (1959), pp. 191-204, 205-219; *Nagoya J. Math.*, 21 (1961), pp. 159-183; *J. Algebra*, 8 (1968), pp. 223-247.
—. — [5] Applications of group characters, *Proc. Sympos. Pure Math.*, 1 (1959), pp. 88-99.
—. — [6] A new type of simple groups of finite order, *Proc. Nat. Acad. Sci.*, 46 (1960), pp. 868-870.
—. — [7] Investigations on finite groups, *Proc. Nat. Acad. Sci.*, 46 (1960), pp. 1611-1614.
—. — [8] Finite groups with nilpotent centralizers, *Trans. Am. Math. Soc.*, 99 (1961), pp. 425-470.
—. — [9] On a finite group with a partition, *Arch. Math.*, 12 (1961), pp. 241-254.
—. — [10] Contributions to the theory of finite groups, *Proc. Sympos. Pure Math.*, vol. VI, pp. 101-109; *A. M. S.*, Providence R. I. (1962).
—. — [11] On a class of doubly transitive groups I, II, *Ann. of Math.*, 75 (1962), pp. 105-145; 79 (1964), pp. 514-589 (Cf. *Proc. Int. Congr. Stockholm* (1962), pp. 285-287. Institute Mittag-Leffler, Djursholm (1963)).
—. — [12] On generalized ZT-groups, *Arch. Math.*, 13 (1962), pp. 199-202.
—. — [13] Two characteristic properties of ZT-groups, *Osaka Math. J.*, 15 (1963), pp. 143-150.
—. — [14] Finite groups of even order in which Sylow 2-subgroups are independent, *Ann. Math.*, 80 (1964), pp. 58-77.
—. — [15] A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic, *J. Algebra*, 2 (1965), pp. 1-14.
—. — [16] Finite groups in which the centralizer of any element of order 2 is 2-closed, *Ann. Math.*, 82 (1965), pp. 191-212.
—. — [17] Transitive extensions of a class of doubly transitive groups, *Nagoya Math. J.*, 27 (1966), pp. 159-169.
—. — [18] A characterization of the simple groups $PSL(2, q)$, *J. Math. Soc. Japan*, 20 (1968), pp. 342-349.
—. — [19] Characterizations of linear groups, *Bull. A. M. S.*, 75 (1969), pp. 1043-1091.

—. — [20] A simple group of order 448, 345, 497, 600 (FG, 113-119).
G. THOMAS. — [1] A characterization of the groups $G_2(2^n)$, *J. Algebra*, 13 (1969), pp. 87-119.
—. — [2] A characterization of the unitary groups $PSU_5(q^2)$, $q = 2^n$, *J. Algebra*, 14 (1970), pp. 245-259.
—. — [3] A characterization of the Steinberg group $D_4^2(q^3)$, $q = 2^n$, *J. Algebra*, 14 (1970), pp. 373-385.
J. G. THOMPSON. — [1] Finite groups with fixed point free automorphisms of prime order, *Proc. Nat. Acad. Sci.*, 45 (1959), pp. 578-581.
—. — [2] Finite groups with normal p-complements, *Proc. Symp. Pure Math.*, vol. 1, pp. 1-3 ; *A. M. S.*, Providence, R. I. (1959).
—. — [3] Normal p-complements for finite groups, *Math. Z.*, 72 (1960), pp. 332-354.
—. — [4] A special class of non-solvable groups, *Math. Z.*, 72 (1960), pp. 458-462.
—. — [5] 2-signalizers of finite groups, *Pac. J. Math.*, 14 (1964), pp. 363-364.
—. — [6] Normal p-complements for finite groups, *J. Alg.*, 1 (1964), pp. 43-46.
—. — [7] Toward a characterization of $E_2^*(q)$, *J. Algebra*, 7 (1967), pp. 406-414.
—. — [8] Non-solvable finite groups all of whose local subgroups are solvable, *Bull. A. M. S.*, 74 (1968), pp. 383-437 (Cf. *Proc. Int. Cong. Math. Moscow* (1966), pp. 158-162. Izdat « Mir », Moscow (1968)).
—. — [9] Quadratic Pairs. To appear.
J. TITS. — [1] Groupes simples et géométries associées, *Proc. Int. Cong. Math. Stockholm* (1962), pp. 197-221.
—. — [2] Sur les systèmes de Steiner associés aux trois « grands » groupes de Mathieu, *Rend. Mat. e Appl.* (5), 23 (1964), pp. 166-184.
—. — [3] Le groupe de Janko d'ordre 604, 800 (Cf. FG 91-95).
—. — [4] Groupes finis simples sporadiques, *Séminaire Bourbaki* (1969-1970), n° 375.
—. — [5] Notes on finite BN pairs. To appear.
T. TSUSUKU. — [1] On multiply transitivity of permutation groups, *Nagoya Math. J.*, 18 (1961), pp. 93-109.
—. — [2] Transitive extension of certain permutation groups of rank 3, *Nagoya Math. J.*, 31 (1968), pp. 31-36.
—. — [3] On doubly transitive permutation groups of degree $1 + p + p^2$ where p is a prime number, *J. Algebra*, 8 (1968), pp. 143-147.
H. F. TUAN. — [1] On groups whose order contain a prime number to the first power, *Ann. Math.* (2), 45 (1944), pp. 110-140.
D. B. WALES. — [1] Finite linear groups of prime degree, *Can. J. Math.*, 21 (1969), pp. 1025-1041.
—. — [2] Finite linear groups of degree seven I, *Can. J. Math.*, 21 (1969), pp. 1042-1056 (Cf. *Bull. A. M. S.*, 74 (1968), pp. 197-198).
—. — [3] The uniqueness of the simple group of order 604, 800 as a subgroup of $SL_6(4)$, *J. Algebra*, 11 (1969), pp. 455-460.
—. — [4] Generators of the Hall-Janko group as a subgroup of $G_2(4)$, *J. Algebra*, 13 (1969), pp. 513-516.
—. — [5] Simple Groups of order $p.3^a.2^b$, *J. Algebra*, 16 (1970), pp. 183-190; Simple Groups of order $7.3^a.2^b$, *J. Algebra*, 16 (1970), pp. 575-596.
J. H. WALTER. — [1] On the characterization of linear and projective linear groups I, II, *Trans. A. M. S.*, 100 (1961), pp. 481-529; 101 (1961), pp. 107-123.
—. — [2] Finite groups with abelian Sylow 2-subgroups of order 8, *Invent. Math.*, 2 (1967), pp. 332-376.
—. — [3] The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. of Math.*, 89 (1969), pp. 405-514 (Cf. FG 43-46).
H. N. WARD. — [1] On Ree's series of simple groups, *Trans. A. M. S.*, 121 (1966), pp. 62-89.
—. — [2] On the triviality of primary parts of the Schur multiplier, *J. Algebra*, 10 (1968), pp. 377-382.

T. A. WHITELAW. — [1] Janko's group as a collineation group in $PG(6,11)$, *Proc. Camb. Philos. Soc.*, 63 (1967), pp. 663-677.
H. WIELANDT. — [1] Über das Produkt von paarweise vertauschbaren nilpotenten Gruppen, *Math. Z.*, 55 (1951), pp. 1-7.
—. — [2] Primitive Permutationsgruppen vom Grad $2p$, *Math. Z.*, 63 (1956), pp. 478-485.
—. — [3] Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichenGruppe, *Math. Z.*, 73 (1960), pp. 146-158.
—. — [4] Über den Transitivitätsgrad von Permutationsgruppen, *Math. Z.*, 74 (1960), pp. 297-298.
—. — [5] *Finite permutation groups*. New York and London, Academic Press (1964).
—. — [6] On automorphisms of doubly transitive permutation groups, *Proc. Int. Conf. Theory of Groups* (Canberra, 1965), pp. 389-393, Gordon and Breach, New York (1967).
G. WINKLER. — [1] Eine Charakterisierang der Gruppen $PSL(2,5)$, $SL(2,5)$ und $PSL(2,8)$, *Arch. Math.* (Basel), 18 (1967), pp. 230-234.
S. K. WONG. — [1] On a new finite nonabelian simple group of Janko, *Bull. Austr. Math. Soc.*, 1 (1969), pp. 59-80.
—. — [2] A characterization of McLaughlin's simple group. To appear.
W. J. WONG. — [1] A characterization of the alternating group of algebra 8, *Proc. London Math. Soc.* (3), 13 (1963), pp. 359-383.
—. — [2] A characterization of the Mathieu group M_{12} , *Math. Z.*, 84 (1964), pp. 378-388.
—. — [3] On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, *J. Australian Math. Soc.*, 4 (1964), pp. 90-112.
—. — [4] On finite groups with semidihedral Sylow 2-subgroups, *J. Algebra*, 4 (1966), pp. 52-63.
—. — [5] Determination of a class of primitive permutation groups, *Math. Z.*, 99 (1967), pp. 235-246.
—. — [6] Finite groups with a self-centralizing subgroup of order 4, *J. Australian Math. Soc.*, 7 (1967), pp. 570-576.
—. — [7] A characterization of the finite simple groups $PSp_6(q)$, q odd, *J. Algebra*, 12 (1969), pp. 494-524.
—. — [8] Characterization of the finite simple groups $PSp_{2n}(q)$, *J. Algebra*, 14 (1970), pp. 531-551.
H. YAMAKI. — [1] A characterization of the alternating groups of degrees 12, 13, 14, 15, *J. Math. Soc. Japan*, 20 (1968), pp. 673-694.
—. — [2] A characterization of the simple group $Sp(6,2)$, *J. Math. Soc. Japan*, 21 (1969), pp. 334-356.
H. ZASSENHAUS. — [1] Über transitive Erweiterungen gewisser Gruppen aus Automorphismen endlicher mehrdimensionaler Geometrien, *Math. Ann.*, 111 (1935), pp. 748-759.
—. — [2] Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, *Abhandl. Math. Seminar Hamburg. Univ.*, 11 (1936), pp. 17-40.
—. — [3] Über endliche Fastkörper, *Abhandl. Math. Seminar Hamburg. Univ.*, 11 (1936), pp. 187-220.

Yale University
Department of Mathematics,
Box 2155. Yale Station
New Haven,
Connecticut 06520 (U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 95 à 111.

THE COHOMOLOGY OF INFINITE DIMENSIONAL LIE ALGEBRAS; SOME QUESTIONS OF INTEGRAL GEOMETRY

by I. M. GEL'FAND

This report is concerned with certain results and problems arising in the theory of the representation of groups. In the last twenty years much has been achieved in this field and—most important—its almost boundless possibilities have become apparent.

Indeed, its problems, touching on the interests of algebraic geometry, on many questions of the algebraic number theory, analysis, quantum field theory and geometry, as well as its inner symmetry and beauty have resulted in the growing popularity of the theory of representations.

It is impossible to list even briefly its main achievements, and this is not the aim of this communication. Nevertheless, one cannot omit mentioning the outstanding papers by Harish-Chandra, Selberg, Langlands, Kostant, A. Weil, which considerably advanced the development of the theory of representations and opned up new relationships; and, since we do not go into these questions, we will not be able to touch upon many of the deep notions and results of the theory of representations.

We feel that the methods which have arisen in the theory of representation of groups may be used in a considerably more general non-homogeneous situation. We will give some examples:

1. The proof of the fact that the spectrum of a flow on symmetric spaces of constant negative curvature is a Lebesgue spectrum [1] was based on methods of the theory of representations, namely the decomposition of representations into irreducible ones. One of the most useful methods of decomposing representations into irreducible representations is the orisphere method [5]. In the works of Sinai, Anosov, Margulis [2], [3], [4], only the orispheres are considered and groups symmetries are left out. This rendered possible the study of the spectrum of dynamic systems in a considerably more general situation.

2. The theorem of Plancherel and the method of orispheres gives rise to the consideration of more general problems of integral geometry, taking place in a non-homogeneous situation [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17].

3. If we have a manifold and its mapping, the study of distributions " constant on the inverse image of each point " of this mapping is an extremely interesting problem, special examples of which were studied in the homogeneous situation (functions in

four-dimensional space, invariant relative to the Lorenz group, functions constant on classes of conjugate elements of a semi-simple Lie group [18], etc.). There are various aspects of this problem which are considerably more interesting and important than may seem at first glance. Of course, the main interest of the problem is the study of these distributions at singularies of the mapping. To be more precise, suppose X is a manifold (C^∞-analytical, algebraic) and $\mathscr{G}$ is some (perhaps infinitely dimensional) Lie algebra of smooth vector fields. One wishes to describe the space of unvariant distributions.

A more natural statement of the problem is obtained by replacing the distributions by generalised sections of a vector bundle which vary according to a given finite dimensional representation. Unfortunately consideration of length prevent me from giving a series of existing examples. Those examples are particularly interesting when X has only a finite number of orbits relative to $\mathscr{G}$. For interesting example in the non-homogeneous situation see [34].

4. The theory of representation of groups makes the consideration of interesting examples possible and shows the importance of studying the ring of all the regular differential operators on those algebraic manifolds which are homogeneous spaces. It is quite natural to wish to describe the structure of the ring R of regular differential operators on any algebraic manifold. Perhaps, as in [19], [20], it would be helpful to consider the quotient skew-field of the ring R. Another interesting problem is the description of the involutions of this ring R.

In this report I would like to tell about certain problems which were studied by my friends and myself while thinking about questions connected with representation theory.

I. Representations of semisimple Lie algebras.

0. Suppose $\mathscr{G}$-is a semisimple Lie algebra. The study of representations is essentially the study of a category of $\mathscr{G}$-modules. The choice of the particular category of $\mathscr{G}$-modules considered in the algebraic problems of the theory of representations is essential. Suppose $\mathscr{k}$ is a fixed subalgebra of $\mathscr{G}$. $\mathscr{G}$-the module will be called $(\mathscr{g}, \mathscr{k})$ finite iff 1° it is a finitely generated $\mathscr{U}(\mathscr{G})$-module and 2° as an $\mathscr{U}(\mathscr{G})$-module it is the algebraic direct sum of finite dimensional irreducible representations of $\mathscr{k}$ and in this decomposition each of the irreducible representation appears only a finite number of times.

The following two cases are very interesting:

1° $\mathscr{G}$ is a real semisimple algebra, $\mathscr{k}$ is the subalgebra corresponding to the maximum compact subgroup. The corresponding $(\mathscr{g}, \mathscr{k})$-modules were considered by V. A. Ponamaryov and the author and were called by them " Harish-Chandra modules ".

2° $\mathscr{G}$ is a real Lie algebra, $\mathscr{k}$ is a Cartan subalgebra or, more generally, the semisimple part of the parabolic subalgebra.

1. Let us consider in more detail the category of Harish-Chandra modules in the case when $\mathscr{G}$ is the algebra of a complex semisimple Lie group.

Further, each module is the direct sum of modules on each of which the Laplace operators have only one eigen-value.

Consider an example. Suppose G is a simply connected Lie group over the algebra $\mathcal{G}$, B – its Borel subgroup, $\mathcal{N}$ is a unipotent radical of B, H – a Cartan subgroup. Consider the indecomposable finite dimensional representation ρ of the group H. Note that since $H = C^* \times C^* \times \ldots \times C^*$ the question of the finite dimensional representations of H is reduced to the determination of a finite number of pairwise commutative matrices. Let us extend this representation ρ of the group H to a representation of the group B and consider, further, the representation of the group G induced by this representation B. The representation thus obtained will be called a Jordan representation. In the case when ρ is of dimension one, we obtain the well-known representation of the principal series. Thus we have constructed, using the representation of the group H, a representation of the group G. Note that the description of the canonical form of the representation of H is in some sense an unsolvable problem if the rang of H is greater than 1 [21].

If we consider the representation of the algebra $\mathcal{G}$ thus constructed only on the space of vectors which vary over the finite dimensional representation of the maximum compact subgroup, we will obtain Harish-Chandra modules. Apparently the following hypothesis holds: at the points of general position all the indecomposable Harish-Chandra modules are all Jordan representations (*).

For $SL(2, \mathbb{C})$ this statement follows from work of Zhelobenko. The most interesting is the study of Harish-Chandra modules at singular points. Of course, the problem of listing all the Jordan modules is already a badly stated (unsolvable) problem, since it is based on the classification of systems of pairwise commutative matrices. However, it is not clear whether it is possible to solve this problem at a singular point, considering the Jordan modules as given. If such a solution were possible, it would have exceptional interest.

The problem of describing Harish-Chandra modules was completely solved by V. A. Ponomaryov and the author for the Lie algebra of the group $SL(2, \mathbb{C})$ [22], [23], [24]. Then these representations were constructed as a group representation (and not only as an algebra representation) by M. I. Graev and the authors cited above [25].

The classification of indecomposable Harish-Chandra modules is carried out in two stages.

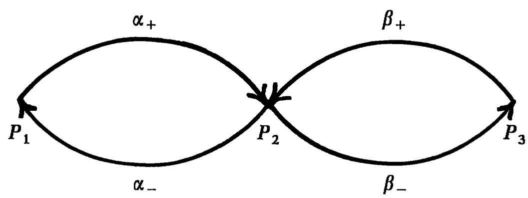
1. The problem is reduced to a problem in linear algebra.
2. The linear algebra problem obtained for $SL(2, \mathbb{C})$ generalises the problem of describing the canonical form of pairs of matrices A, B such that $AB = BA = 0$. To solve this problem we apply the Maclane relation theory, which allows us to use the relations $A^{\#}$ and $B^{\#}$, inverse to the degenerate operators A and B, as well as the monomials $A^{\#k_1}B^{\#k_2}A^{\#k_3}\ldots$.

The Harish-Chandra modules at a singular point may be divided into two classes.

(*) To be more precise, each HARISH-CHANDRA module is decomposed into direct sum of submodules on which the Laplace operators have precisely one eigen-value. The set of eigenvalues thus obtained is called singular if the representation of the fundamental series with the same eigen-values of the Laplace operator are reducible. The points of general position will be exactly the non-singular points.

The modules of first class are uniquely defined by any set of natural numbers, the modules of the second class are determined by any set of natural numbers together with one complex number λ. It is thus interesting to note that at singular points the module space is not discrete. The most convenient canonical form of Harish-Chandra modules are given in [25].

In the case of $SL(2, \mathbb{R})$ the problem of classifying Harish-Chandra modules is easily reduced to a problem in linear algebra; explicitely the category of Harish-Chandra modules at a given singular point is isomorphic to the following category of diagrams in the category of finite dimensional linear spaces:



with the condition $\alpha_+\alpha_- = \beta_+\beta_- = \gamma$, where γ is nilpotent. The question of the classification of the objects of this category is aparantly solvable but leads to considerable difficulties.

Conjecture. — The category of Harish-Chandra modules for any semisimple group with given eigen-values of Laplace operators is equivalent to a certain category of diagrams in the category of finite dimensional linear spaces.

2. This and the following section of the report summarise some results of I. N. Bernstein, S. I. Gel'fand and the author.

Suppose $\mathscr{G}$ is a semisimple Lie algebra over $\mathbb{C}$, b is its Borel subalgebra, $\mathfrak{u}$ is a radical and $\mathscr{h}$ is a Cartan subalgebra. Consider the following category $\mathscr{O}$. Its objects are $(\mathscr{G}, \mathscr{h})$ – finite modules M, satisfying the following condition: for every vector $\xi \in M$ the space $\mathscr{U}(u)\xi$ is finite dimensional. This category is most useful for the application of the theory of highest weights. In this category, let us chose a class of objects which will be called elementary. All the others will be constructed from them and their factor modules by step by step extensions.

Suppose χ is a linear functional over $\mathscr{h}$. Denote by $M_\chi \mathscr{U}(\mathscr{G})$-module, generated by f_χ, with the relations $nf_\chi = 0$ and $hf_\chi = (\chi - \rho, h).f_\chi$ for all $h \in \mathfrak{h}$ and $n \in \mathfrak{u}$. Here ρ denotes the half-sum of the positive roots. By studying the modules M_χ we get extensive information on the representation of the algebras $\mathscr{G}$, including finite dimensional ones. We now state a few theorems on M_χ modules and their morphisms.

Theorem 1 (Verma). — Let the modules M_{χ_1} and M_{χ_2} be given. Two cases are possible:

1° $$\operatorname{Hom}(M_{\chi_1}, M_{\chi_2}) = 0;$$

and

2° $$\operatorname{Hom}(M_{\chi_1}, M_{\chi_2}) \approx \mathbb{C},$$

then any non-trivial homomorphism M_{χ_1} into M_{χ_2} is an embedding.

To state the next theorem we must introduce a partial ordering in the Weyl group W. Suppose $s_1, s_2 \in W$. We shall say that $s_1 > s_2$ iff there exist reflexions $\sigma_1, \ldots, \sigma_r$ in W such that $s_1 = \sigma_1 \ldots \sigma_r s_2$ and $l(\sigma_{i+1} \ldots \sigma_r s_2) = l(\sigma_{i-1} \ldots \sigma_r s_2) + 1, i = 1, \ldots, r$, where $l(s)$ is the length of the element $s \in W$.

THEOREM 2. — Let M_{χ_1} and M_{χ_2} be given. M_{χ_1} imbeds into M_{χ_2} if and only if,

1. There exists such an χ that $\operatorname{Re} \chi$ lies in the positive Weyl chamber and such a pair of elements $s_1, s_2 \in W$, $s_1 > s_2$ that $\chi_1 = s_1\chi$, $\chi_2 = s_2\chi$.

2. $\chi_1 - \chi_2 = \Sigma n_i \alpha_i$, where n_i are integers, α_i are simple roots.

The module M_{χ_0} is richest in submodules for integer values of χ_0 from the positive Weyl chamber. It follows from theorem 2 that M_{χ_0} contains a submodule $M_{s\chi_0}$ for all $s \in W$. In this case the embedding of $M_{s\chi_0}$ into M_{χ_0} is determined in the following way. Suppose s_{α_i} is the reflection with respect to the simple roots α_i, $s = s_{\alpha_i} \ldots s_{\alpha_k}$ is the decomposition of minimum length. Let

$$\chi_i = s_{\alpha_i} s_{\alpha_{i+1}} \ldots s_{\alpha_k} \chi_0 .$$

Then

$$f_{s\chi_0} = a f_{\chi_0},$$

where

$$a = E_{-\alpha_1}^{\frac{(\chi_2-\chi_1,\alpha_1)}{(\alpha_1,\alpha_1)}} . E_{-\alpha_2}^{\frac{(\chi_3-\chi_2,\alpha_2)}{(\alpha_2,\alpha_2)}} \ldots E_{-\alpha_k}^{\frac{(\chi_0-\chi_k,\alpha_k)}{(\alpha_k,\alpha_k)}}$$

Since the minimum representation s in the form of the product of s_{α_i} is not unique, whereas the injection $M_{s\chi_0}$ into M_{χ_0} is uniquely determined, the theorem gives relations between " chains " of the type described. In the general case the embedding is more complicated.

The relations between $M_{s\chi_0}$ may easily be shown by the following commutative diagram. The vertices of the diagram are numbered by the elements s of the Weyl group and correspond to the modules $M_{s\chi_0}$. If $s_1 < s_2$, then an arrow going from s_2 to s_1 is drawn. The mapping is defined by the embedding of $M_{s_2\chi_0}$ into $M_{s_1\chi_0}$. We obtain a commutative diagram. It is not difficult, using this diagram, to get in particular, a resolution of the finite dimensional representation by free $\mathscr{U}(u)$-modules.

The finite dimensional representation with highest weight $\chi_0 - \rho$ is of the form

$$M = M_{\chi_0} / \sum_{s \neq l} M_{s\chi_0} .$$

The theorems stated above and this diagram contain, in this case, the formulas of Kostant, Weyl's formulas for characters, the Borel-Weil theorem and the Harish-Chandra theorem concerning the left ideals of enveloping algebras.

3. *The ring of differential operators on the principal affine space and the generalisation of the Segal-Bargman representation to any compact group.*

Suppose G is a complex semisimple Lie group, $\mathscr{N}$ is the maximum unipotent subgroup, H — a Cartan subgroup. The manifold $A = \mathscr{N} \backslash G$ is called the principal affine space of the group G. It is an algebraic quasi affine manifold. It is interesting to consider the ring $\mathcal{D}$ of regular differential operators on A. Suppose $f(g)$ ranges over all the regular algebraic functions (polynomials) on the group G. We will give a method allowing to construct for any such function a differential operator on A. Since H normalises $\mathcal{N}$, the transformation $g \to hg$ may be carried over to A (left translations [5]). Using these left translations we can assign to every element of the Lie algebra $\not{h}$ of the group H a differential operator on A. The commutative ring of differential operators on A generated by these operators will be denoted, following [20], by W_u. Suppose π is the natural map of G into A. Denote by π^* extension of the functions over A to functions over G induced by π. The operation π_*, mapping the functions on G into functions on A is less obvious and supplements, in our case, the operation of averaging the function over the subgroup. The construction of π_* is carried out in the following way.

Suppose $f(g)$ is a regular algebraic function on G. Consider it as the linear combination of matrix elements of finite dimensional irreducable representations in the basis of weight vectors H. Threw out all the elements of this sum except the summands corresponding to those matrix elements whose first index is the highest weight of the corresponding representations. Denote by $\pi_* f$ the function thus obtrained.

Suppose f is a fixed function on G. Define the operator f in the functions by the formula

$$\bar{f}(\varphi) = \pi_*(f\pi_*(\varphi))$$

THEOREM 1. — There exists an element $w \in W_u$ such that $w_0 f$ is a regular differential operator on A. Conversely, every regular differential operator on A may be represented in the form $\Sigma w_i \,.\, \bar{f_i}$, $w_i \in W_u$ where f_i are functions on G.

Suppose $\mathcal{K}$ is the quotient field of the W_u ring, $\mathcal{F}(G)$ is the ring of regular algebraic functions on G. The map constructed in theorem 1 may be expanded to the map

$$i : \mathcal{D} \bigotimes_{W_u} \mathcal{K} \to \mathcal{F}(G) \bigotimes_{\mathbb{C}} \mathcal{K}$$

THEOREM 2. — i is a linear space isomorphism over $\mathcal{K}$, compatible with the right translations by elements of G.

Note that the fact of the existence of an isomorphism of the spaces above was obtained earlier in a joint paper of A. A. Kirillov and the author [20].

For the group $SU(2)$ there exists an extremely useful realisation of the whole series of representations of this group due to Segal and Bargmann. This realisation is in the Hilbert space of analytic functions of two complex variables, square, integrable with weight $e^{-|z_1|^2 - |z_2|^2}$. We will point out a generalisation of this construction for any compact Lie group.

Suppose K is a simply connected compact Lie group of rang r, G — its complexification, A — the principal affine space of the group G. Introduce the weight function $e^{-H(a)}$, $a \in A$. Suppose ρ_i is the i'-th fundamental representation of G, let ξ_i denote the vector of highest weight in ρ_i. Put

$$H_i(g) = (\rho_i(g)\xi_i, \rho_i(g)\xi_i),$$

where (,) is the scalar product in the space of the representation ρ_i invariant relative to K. It is clear that $H_i(g)$ is a function on A and we can then put

$$H(a) = \sum_{i=1}^{r} H_i(a).$$

Now consider the analytic functions on A which are square integrable with weight $e^{-H(a)}$. Call the Hilbert space of all these functions a " generalised Segal-Bargmann space ". The group K thus obtained acts on it in a natural way and the unitary representation thus obtained contains every irreducible one exactly once. Let us call any operator with polynomial regular algebraic coefficients a " differential operator on A ".

CONJECTURE. — The operator conjugate (in the generalised Segal-Bargmann space) with a regular differential operator is again a regular differential operator.

The involutions which arise in the ring of regular differential operators are far from trivial. Thus, for the case of $SU(n)$ the operator, say, conjugate with multiplication by a simple first order function, is a differential operator of the $(n-1)$-st order. The techniques developed in the previous section apparently will turn out to be very useful in the study of the ring of differential operators on A, in particular, for the proof of the conjecture stated aboce. The fact of the matter is that the construction of the involution itself is most conveniently carried out in the terms developed there. Using this method the conjecture was checked for $SU(3)$.

We state another problem. Let the real form of the group G be given. Its unitary representation naturally gives rise to an involution in the enveloping algebra $\mathcal{U}(\mathcal{G})$. We must find all the possible extensions of this involution from $\mathcal{U}(\mathcal{G})$ to the ring of all the regular differential operators on A. In the simpliest examples these extended involutions correspond to series of unitary representations (of real groups) contained in the regular one. It would be interesting to list the involutions in the ring of regular differential operators on any quasiaffine algebraic manifold.

It would also be interesting to consider the factor space of the group G, not only over the maximal unipotent group, but also over any orispherical subgroup.

II. Integral geometry.

In this paragraph I will only consider one elementary example [17]. The derivation of the Plancherel formula for $G = GL(n, \mathbb{C})$ is based on the following problem in integral geometry. Denote by $\mathcal{N} \in G$ the set of all the upper triangular matrices with units on the diagonal. Suppose the function $f(x)$, $x \in G$ is given. Let

$$\varphi(x_1, x_2) = \int_{\mathcal{N}} f(x_1^{-1} z x_2) dz,$$

where x_1 and x_2 are any matrices. The problem is: given $\varphi(x_1, x_2)$ find $f(x)$. It suffices to solve the problem when $x = e$ is the unit matrix. We can assume that the fonction f is given on $\mathbb{C}^{n^2}$ and the equation $y = x_1^{-1} z x_2$ for fixed x_1 and x_2 defines in $\mathbb{C}^{n^2}$ a plane of dimension $\dfrac{n(n-1)}{2}$.

Now replace our problem with the following, at first glance meaningless, problem. Consider the space $H_{n^2,k}\left(k = \dfrac{n(n-1)}{2}\right)$ of all the k-dimensional planes in $\mathbb{C}^{n^2}$. For all $h \in H_{n^2,k}$ consider the function

$$\varphi(h) = \int_h f(x)dx.$$

We must now recover $f(x)$. In the paper [10] this problem is solved in the following manner. Using the function φ and its derivatives construct a differential (k, h) form $\mathscr{H}\varphi$ on the Grassman manifold $G_{n^2,k}$ of k-dimensional planes containing the point x. This form $\mathscr{H}\varphi$ is closed and the value of $f(x)$ is equal to $\int_{\gamma_0} \mathscr{H}\varphi$, where γ_0 is any cycle homologic to the set of all k-dimensional planes containing the point x and lying in a fixed $k+1$-dimensional plane passing through the point (Euler's cycle (*)). As to the integral over the other k-dimensional cycles in the basis of Schubert cells in $G_{n^2,k}$, it is equal to zero.

In our case the function $\varphi(x_1, x_2)$ is known not on the whole manifold $H_{n^2,k}$ but only on a certain submanifold. The submanifold of $H_{n^2,k}$ will from now on be called the " complex of k-dimensional planes ". The complex is called permissible if the form $\mathscr{H}\varphi$ on this complex is determined by the values of the function φ on this complex only. In the case when φ is given on a permissible complex we can recover $f(x)$ by using the formula

$$f(x) = C_\gamma \int_\gamma \mathscr{H}\varphi,$$

where γ is a cycle lying in the complex; thus to find C_γ it suffices to decompose the cycle γ over the Schubert cell basis. In our case the complex will consist of planes of the form $h_{x_1,x_2} = \{\, y/y = x_1^{-1}zx_2 \,\}$ and has dimension n^2. It turns out to be permissible. The set of these planes of this complex which contain the point e has the necessary dimension k and forms a cycle. The coefficient of the Euler cycle is equal to $n!$ Considering the form $\mathscr{H}\varphi$ only on the complex, we will obtain the classical inversion formula

$$f(e) = [(2i)^k \pi^{2k} n!]^{-1} \int \prod_{q<p} \left(\frac{\partial}{\partial \delta_p} - \frac{\partial}{\partial \delta_q}\right)\left(\frac{\partial}{\partial \bar{\delta}_p} - \frac{\partial}{\partial \bar{\delta}_q}\right) \times \varphi(\mathscr{C}^{-1}\delta\mathscr{C})\,|_{\delta=e} \bigwedge_{q<p} d\mathscr{C}_{qp} \bigwedge_{q<p} d\overline{\mathscr{C}}qp.$$

Apparently one can obtain the Paley-Wiener theorem for $GL(n, \mathbb{C})$, in a similar manner; in other words, obtain conditions on φ, which imply the decrease of f at infinity. To do this we embed $GL(n, \mathbb{C})$ not into $\mathbb{C}^{n^2}$ but into $\mathbb{CP}^{n^2}$ and consider the problem as a projective problem of integral geometry (see [15]). Since in this case we can recover $f(x)$ in the points at infinity as well, the Paley-Wiener conditions will consist in the

(*) Note that other problems of integral geometry give rise to integration over other cycles in $G_{n^2,k}$; see, for example [16].

following: the function f' and its derivatives (recovered by using φ) must be equal to zero at all the points of infinity.

III. **Cohomology of infinite algebras.**

0. *This part of the report contains results obtained jointly by D. B. Fuks and the author.*

We know how difficult it is to describe any reasonable category of representations. On the other hand, the problem of determining cohomology groups is a sumpler one. Here we list results about the cohomology of Lie algebras of vector spaces, which show that these cohomologies are reasonable, are not equal to zero and are not infinite dimensional.

Recall that the cohomology $H^*(\mathscr{G}; M) = \sum_q H^q(\mathscr{G}; M)$ of the topological algebra $\mathscr{G}$ with coefficients in the $\mathscr{G}$-module is defined as the cohomology of the complex $C(\mathscr{G}; M) = \{c^q(\mathscr{G}; M), d^q(\mathscr{G}; M)\}$ where $c^q(\mathscr{G}; M)$ is the space of continuous skew-symetric q-linear functionals on $\mathscr{G}$ ranging over M, and the differential $d^q = d^r(\mathscr{G}; M)$ is defined by the formula

$$(d^qL)(\xi_1, \ldots, \xi_{q+1}) = \sum_{1 \leqslant s < t \leqslant q+1} (-1)^{s+t-1} L([\xi_s, \xi_t], \xi_1, \ldots, \hat{\xi}_s, \ldots, \hat{\xi}_t, \ldots, \xi_{q+1}) - \sum_{1 \leqslant s \leqslant q} (-1)^s \xi_s L(\xi_1, \ldots, \hat{\xi}_s, \ldots, \xi_{q+1}).$$

If M is a ring, and the operators on $\mathscr{G}$ are its differentials, then the complex $C(\mathscr{G}; M)$ has a natural multiplicative structure.

1. *Problems and examples.*

The main example of an infinitely dimensional Lie algebra will be the algebra of smooth vector fields on a smooth manifold.

Suppose M is a closed orientable connected smooth (*) manifold. Denote by $\mathfrak{A}(M)$ the Lie algebra of smooth tangent vector fields on M with Poisson brackets for commuting. The first of the problems considered is a follows. Define the cohomology ring $\mathfrak{H}^*(M) = H^*(\mathfrak{A}(M); \mathbb{R})$ of the algebra $\mathfrak{A}(M)$ with coefficients in the unit representation, i. e., in the field $\mathbb{R}$ of real numbers with a trivial $\mathfrak{A}(M)$-module structure. This ring obviously is a differential invariant of the manifold M. Looking ahead we shall say that the space $H^q(\mathfrak{A}(M); \mathbb{R})$ will turn out to be finite dimensional for any q (see [28]). The problem of computing the ring $\mathfrak{H}^*(M)$ is not as of yet completely solved.

We would like to point out the difference between the method of constructing invarients of manifolds by using objects of differential geometry (the Lie algebra of vector fields) and the usual method of constructing differential invariants. Whereas usually the differential form representing a Pontryagin of Chern class on the manifold X is built up from the individual object (by using the metric) on the manifold,

(*) By smooth we always mean of class C^∞.

in our case the invariants are constructed using the infinite dimensional set of all smooth vector fields on the manifold.

As an example consider the case when M is the circle S^1. We can show that the ring $H^*(S^1)$ is generated by a two-dimensional generator a and a three-dimensional generator, the two being related only by the skewsymetry condition.

Further the generators $a \in \mathfrak{H}^2(S^1)$, $\mathscr{C} \in \mathfrak{H}^3(S^1)$ are represented by cocycles $A \in C^2(\mathfrak{A}(S^1); \mathbb{R})$, $B \in C^3(\mathfrak{A}(S^1); \mathbb{R})$ given by the formulas

$$A(f, g) = \int_{S^1} \begin{vmatrix} f'(x) & f''(x) \\ g'(x) & g''(x) \end{vmatrix} dx$$

$$B(f, g, h) = \int_{S^a} \begin{vmatrix} f(x) & f'(x) & f''(x) \\ g(x) & g'(x) & g''(x) \\ h(x) & h'(x) & h''(x) \end{vmatrix} dx$$

When the dimension of the manifold M increases the ring $\mathfrak{H}^*(M)$ becomes considerably richer; thus the ring $\mathfrak{H}^*(S^2)$ has 10 generators, and the ring $\mathfrak{H}^*(S^1 \times S^2)$, 20 generators (see [29]).

The cohomology of the Lie algebra of smooth vector fields is intimately connected with the cohomology of Lie algebras of formal vector fields. By a formal vector field at the point O of the space R^n we mean a linear combination of the form $\Sigma p_i(x_1, \ldots, x_n)e_i$ where $e_1, \ldots, e_n$ are the standard basis vectors of the space R^n and $p_i(x_1, \ldots, x_n)$, the formal power series with real coefficients in the coordinates $x_1, \ldots, x_n$ of the space. The set of formal vector fields is, in an obvious sense, a linear topological space, and a natural commutation operation transforms it into a topological Lie algebra. This algebra is denoted by W_n.

2. *The algebra of formal vector fields. The cohomology of the algebra W_n with coefficients in,R.*

In order to state the final result it is necessary to describe a certain auxilliary topological space X_n $(n = 1, 2, \ldots)$. Suppose $\mathscr{N} \geqslant 2n$ and let $p_i E(N, n) \to G(N, n)$ be the canonical $U(n)$ bundle over the (complex) Grasman manifold $G(\mathscr{N}, n)$. The usual (W-complex of the manifold $G(\mathscr{N}, n)$ has the following property: the $2n$-th skeleton $[G(\mathscr{N}, n)]_{2n}$ does not depend on $\mathscr{N}$ when $\mathscr{N} \geqslant 2n$. The inverse image of the set $[G(\mathscr{N}, n)]$ under the map p will be denoted by X_n.

The space X_1 is a three-dimensional sphere, the other spaces do not have such a simply visualised description. We have the following.

THEOREM 2.1. — For all q, n there is an isomorphism

$$H^q(W_n; R) = H^q(X_n; R).$$

Multiplication in the ring $H^*(W_n; R)$ (as well as in the ring $H^*(X_n; R)$) is trivial, i. e., the product of any two elements of positive dimension is equal to zero.

The cohomology of the space X_n may be computed by using standard topological methods. For example, it is trivial for $0 < q \leq 2n$ and for $q > n(n + 2)$.

Theorem 2.1 is the central result of the article [30]. Its proof uses a somewhat modified version of the Serre-Hoschild spectral sequence [31] corresponding to the subalgebra of the algebra W_n, generated by the elements $x_i e_j$ (*); this subalgebra is isomorphic to $\mathscr{G}l(n, R)$. Beginning with the second member, this spectral sequence turns out to be isomorphic to the Leray-Serre spectral sequence of the bundle $X_n \to [G(\mathscr{N}, n)]_{2n}$ with fibre $U(n)$.

It turns out also that each element $\alpha \in H^q(W_n; \mathbb{R})$ is represented by such a cocycle $A \in C^q(W_n; \mathbb{R})$, that $A(\xi_1, \ldots, \xi_q)$ depends only on the 2-jets of formal vector fields $\xi_1, \ldots, \xi_q$ (see [30]).

To study the cohomology of W_n with coefficients in other modules (and to describe those modules) it is important to know the structure of the subalgebras

$$\ldots \subset L_k \subset \ldots \subset L_0 \subset W_n$$

where L_k consists of vector spaces whose components are series without terms of power less than or equal to K.

The relation between the cohomology of the algebras W_n and L_0. The following general fact is easily generalised to the case of the cohomology of infinite dimensional Lie algebras.

Suppose B is an subalgebra of Lie algebra A; M – some B-module; $\hat{M}$ – an induced A-module (i. e. $\hat{M} = \mathrm{Hom}_{[B]}(M, [A])$ where $[A]$, $[B]$ are enveloping algebras for A, B). Then

$$H^*(A; \hat{M}) = H^*(B; M).$$

We will apply this statement in the case when M is a tensor representation of the algebra L_0 (i. e. a finite dimensional representation obtained from the representation of the algebra $\mathscr{G}l(n; R)$ by means of the projection $L_0 \to L_0/L_1 = \mathscr{G}l(n; R)$). At the same time the induced representation $\hat{M}$ of the algebras W_n is none other than the space of the corresponding formal tensor fields. For example, if $M = R$ is the unit representation of the algebra L_0, then $\hat{M}$ is the space $F(R^n)$ of formal power series in n variables with the natural action of the algebra W_n; if M is the space $\Lambda^r(R^n)'$ of skewsymetric r-linear forms in R^n, then $\hat{M}$ is the space Ω^r of formal exterior differential forms of r order in R^n.

The cohomology of the algebra W_n with coefficients in the spaces of formal exterior differential forms. The space

$$H^*(W_n, \Omega^*) = \sum_{q,\mathfrak{A}} H^q(W_n; \Omega^r)$$

is obviously a bigraduated algebra (over R), isomorphic, as we just found out, to $H^*(L_0; \Lambda^*(R^n)')$.

THEOREM 2.2. — The bigraduated ring $H^*(W_n; \Omega^*) = H^*(L_0; \Lambda^*(R^n)')$ is multiplicatively generated by $2n$ generators

$$\begin{array}{lll} \rho_i \in H^{2i-1}(L_0; \Lambda^0(R^n)') & & (i = 1, \ldots, n) \\ \tau_i \in H^i \quad (L_0; \Lambda^i(R_n)') & & (i = 1, \ldots, n) \end{array}$$

These generators are connected only by the following relations $\rho_i\rho_k = -\rho_k\rho_i$; $\rho_k\tau_i = \tau_i\rho_k$; $\tau_i\tau_k = \tau_k\tau_i$; $\tau_1^{i_1}\tau_2^{i_2} \ldots \tau_n^{i_n} = 0$ if $i_1 + 2i_2 + \ldots + ni_n > n$.

(*) $i, j = 1, \ldots, n$.

In particular, the ring $H^*(L_0\,;\,R) = H^*(L_0\,;\,\Lambda^0(R^n)') = H^*(W_n\,;\,F(R^n))$ is an exterior algebra in generators of dimension $1, 3, 5, \ldots, 2n-1$. i. e.

$$H^*(W_n\,;\,F(R^n)) = H^*(gl(n, R)\,;\,R).$$

Moreover,

$$H^q(L_0\,;\,\Lambda^r(R^n)') = \begin{cases} 0 & \text{where} \quad q < r \\ H^r(L_0\,;\,\Lambda^r(R^n)') \otimes H^{q-r}(gl(n, R)\,;\,R) & \text{where} \quad q \geqslant r \end{cases}$$

while the dimension of the space $H^r(L_0, \Lambda^r(R^n)')$ is equal to the number of ways in which the number r may be represented as the sum of natural numbers.

The computation of the cohomology of L_0 with coefficients in the tensor representation reduces to the computation of the cohomology of the algebra L_1 with coefficients in $\mathbb{R}$. In a similar way for jets, to the cohomology of L_k with coefficients in $\mathbb{R}$.

Apparently the following statement holds.

CONJECTURE. — For any n the spaces $H^q(L_k\,;\,R)$ are finite dimensional.

For $n=1$ the dimension of the space $H^q(L_k; R)$ equals $C_q^{k-1}+C_{q+1}^{k-1}$, $q, k=0, 1, \ldots$).

Using previously mentioned results to compute the cohomology of the algebra L_0 with tensor coefficients we can deduce that the classes of cohomology of the algebra W_n (even W_1) with coefficients in tensor fields is not always representable by cocycles depending only on 2-jets of their arguments (in contrast with the cases of constant and skewsymetric coefficients).

We have been unsuccessful, so far, in computing the cohomology $H^*(A, \mathbb{R})$ for other Cartan algebras. Note that all these cohomologies are connected with very important standard complexes. For this complex consists of the polynomials $P(\alpha_1, \ldots, \alpha_q)\,;\,(\beta_1, \ldots, \beta_q)$, $\alpha_i \in \mathbb{R}^n$, $\beta_i \in (\mathbb{R}^n)'$; the polynomial P is skewsymetric under the simultaneous interchange of α_i, β_i with α_j, β_j. The differential is given by the formula

$$\begin{aligned} dP(\alpha_1, \ldots, \alpha_{q+1}\,;\,\beta_1, \ldots, \beta_{q+1}) \\ = \Sigma(-1)^{s+t}(\alpha_s, \beta_t) - (\alpha_t, \beta_s))P(\alpha_f + \alpha_t, \alpha_f, \ldots, \hat{\alpha}_f, \ldots, \hat{\alpha}_t, \ldots\,; \\ \beta_f + \beta_t, \beta_1, \ldots, \hat{\beta}_f, \ldots, \hat{\beta}_t, \ldots, \beta_{q+1}). \end{aligned}$$

Usually, the infinite dimensional Lie algebras which arise in the formal theory are factor subcomplexes of this complex.

3. *The algebra of smooth vector fields. Cohomology with coefficients in R.*

Suppose M is a compact connected orientable smooth n-dimensional manifold without boundary, $\mathfrak{A}(M)$ – the Lie algebra of smooth tengent yest fields on M. In the standard complex $C(M) = \{\, C^a(M) = C(\mathfrak{A}(M)\,;\,R)d^a \,\}$ we introduce a filtration $0 = C_0(M) \subset C_1(M) \subset \ldots \subset C(M)$ where $C_k(M) = \{\, C_k^q(M) \,\}$ is a subcomplex of the complex $C(M)$, defined in the following way. A cochain $L \in C^a(M)$ belongs to $C_k^q(M)$ if it equals zero on any C^a the vector fields $\xi_1, \ldots, \xi_q$ such that for any k points of the manifold M one of the fields $\xi_1, \xi_2, \ldots, \xi_q$ equals zero in the neighbourhood of each of these points. For example, $C_0^q(M) = 0$; $C_1^q(M)$ consists of such cochains L that $L(\xi_1, \ldots, \xi_q) = 0$ when the supports of the fields $\xi_1, \ldots, \xi_q$ are pairwise nonintersecting; $C^a_{q-1}(M)$ consists of such cochains L that $L(\xi_1,\ldots,\xi_q)=0$ when the supports of the fields $\xi_1,\ldots,\xi_q$ have no common intersection to all of them; $C^a_k(M)=C^a(M)$ when $k\geqslant q$. It is clear that $C_k(M)$ for all k is a subcomplex of the complex $C(M)$ and that $C^q_k(M)C^r_l(M)\subset C^{q+r}_{k+l}(M)$.

To compute the cohomology of the factor complex $C_k(M)/C_{k-1}(M)$ we have defined a spectral sequence, the first term of which may be expressed by using the cohomology of the manifold M and the algebra W_n. A special role is played by the complex $C_1(M)$. This complex we shall call a diagonal complex.

CONJECTURE. — The image of the cohomology of the diagonal complex $C_1(M)$ in $\mathfrak{H}^*(M)$ under the embedding $C_1(M)\to C(M)$ multiplicatively generates all of the ring $\mathfrak{H}^*(M)$. In particular the ring $\mathfrak{H}^*(M)$ is always finitely generated.

Remark. — This is true for the second term of the spectral sequence.

Let us describe a spectral sequence which converges to the cohomology of the diagonal complex. It arises in connection with two different filtrations of the diagonal complex of the manifold. In order to describe the first filtration, note that the q-cochains of the diagonal complex $C_1(M)$ are determined by distributions (more precisely, by the generalized sections of a certain fibre bundle) on M^q which are supported by the diagonal. The m-th term $C^q_{1,m}$ of the first filtration consists of those distributions which have an order (relative to Δ) less than or equal to m.

To define the second filtration fix a triangulation of the manifold

$$M=M_n\supset M_{n-1}\supset\ldots\supset M_0$$

where M_i is the i-dimensional skeleton, and the m-th term $C_{1,m}$ of the filtration consider those q-cochains which are realised by distributions whose support is $M_m\subset\Delta$.

Knowing the cohomology of W_n can construct a spectral sequence which allows us to compute the cohomology of the diagonal complex.

THEOREM 3.1. — There exists a spectral sequence $\mathscr{E}=\{E^{p,q}_r, d^{p,q}_r\}$ which converges to the cohomology of the diagonal complex $\mathfrak{H}^*(M)$ such that

$$E^{p,q}_r=H^{p+n}(M)\otimes H^q(W_n\,;R);$$

$E^{p,q}_r$, in particular, can be different from zero only when $-n\leqslant p\leqslant 0$.

Let us clarify the operation of " globalizing " the formal cohomology: construct a mapping of the space $E^{-r,q+r}_r=H^{n-r}(M)\otimes H^{q+r}(W_n, R)$ into $C^q_1(M)$. This mapping is not uniqual determined: it depends on the choice of the system of local coordinates on M. Suppose $\Gamma=\{U_1,\ldots,U_{\mathscr{N}}\}$ is a coordinate covering of M with coordinates $y_{k_1},\ldots,y_{k_n}$ on U_i and $\{\rho_i\}$ is a decomposition of unity consistent with this covering. In order to construct the element $\mathscr{I}(a\otimes\Psi)(a\in H^{n+r}(W_n, R), \Psi\in H^{n-v}(M))$ find a cochain $\alpha\in C^{n+v}(W_n\,;R)$ representing the closed form ω from the class Ψ. Set

$$\mathscr{I}(a_n\otimes\Psi)(\xi_1,\ldots,\xi_q)=\int_M\omega\Lambda[\sum_{k=1}^{N}\rho_k\varphi(\alpha, U_k\,;\xi_1,\ldots,\xi_q)]$$

where $\varphi(\alpha, U_i; \xi_1, \ldots, \xi_q)$ is a form on U_k, which equals

$$\sum_{1 \leqslant i < \ldots < i_r \leqslant n} \alpha(\xi_1(u, U_k), \ldots, \xi_q(u, U_i), e_{k,i_1 \ldots} e_{k,i_r}) \times dy_i \wedge \ldots \wedge dy_{i_v}$$

at the point $u \in U_i$, where the ξ_i are considered as a formal field in the neighbourhood of the point u under the coordinates y_{k_i}. The theorem is proved in [29] (statement 1.4).

The cohomology with coef cients in the spaces of smooth sections of smooth vector bundles. Suppose A is a finite dimensional $GL(n, R)$ module and suppose M is a smooth connected manifold (we do not assume M either orientable, or compact, or without boundary). Denote by α the vector bundle over M with fiber isomorphic to A, induced by the tangent bundle and by means of the representation of the group $CL(n, R)$ in A. By $\mathscr{A}$ denote the space of smooth sections of the fiber bundle α. The space $\mathscr{A}$ has an obvious $\mathfrak{A}(M)$ module structure. Our goal is the study of the cohomology of the algebra $\mathfrak{A}(M)$ with coefficients in the $\mathfrak{A}(M)$ module $\mathscr{A}$.

In the complex $C(M; A) = \{ C^a(\mathfrak{A}(M); \mathscr{A}); d^a \}$ we will introduce a filtration similar to the one considered above for $C(M)$. We shall say that the cocycle $L \in C^q(\mathfrak{A}(M); \mathscr{A})$ has filtration no greater than k if the section $L(\xi_1, \ldots, \xi_q)$ of the bundle α is equal to zero for any point $x \in M$ with the following property: for any points $x_1, \ldots, x_k \in M$ one of the vector fields $\xi_1, \ldots, \xi_q$ equals zero in the neighbourhood of each of the points $x_1, \ldots, x_k, x$.

The space of q-dimensional cocycles which have filtration no greater than k is denoted by $C_k^q(\mathfrak{A}(M); \mathscr{A})$. It is clear that $C_k(M; \mathscr{A}) = \{ C_k^q(\mathfrak{A}(M); \mathscr{A}) \}$ is a subcomplex of the complex $C(M; \mathscr{A})$.

The subcomplex $C_0(M; \mathscr{A})$ is called " diagonal ". We denote it by $C_\Delta(M; \mathscr{A})$.

THEOREM 3.5. — We have the following spectral sequence $\{ E_r^{p,q}, d_r^{p,q} \}$ which converges to $\mathfrak{H}_\Delta^*(M; \mathscr{A})$ and is such that $E_r^{p,q} = H^p(M; R) \otimes H^q(L_0; A)$. In the multiplicative case the spectral sequence is a multiplicative one and the isomorphism considered above is an isomorphism of rings.

CONJECTURE. — $H_\Delta^*(M, \mathscr{A}) = H(T_M, R) \otimes \mathrm{Hom}_{CL(n)}(A, H^*(L, R))$ where T is the principal $U(n)$ bundle over M induced by the complexification of the tangent bundle.

This conjecture has been proved in the case when $A = \Lambda^q$ is the exterior power of the standard representation. The case $q = 0$ was independently studied by Locik [33].

In the end of this part of the report I would like to introduce a general concept of formal differential geometry. It arises when one formalises and generalises the methods of construction of Pontryagin and Chern classes (by means of metrics and connections); also in the expression of the index of a differential operator in terms of the symbol and the metric of the manifold.

Suppose we have an algebra W_n of formal vector fields. Consider the jet space and, in it, a invariant algebraic submanifold X. Examples of such manifolds are the space of all symmetric tensors of rang 2, the set of all affine connections.

Let us define the complex $\Omega(X)$. Any rational map of X into the complex of formal differential forms will be called a chain of $\Omega(X)$, the differential will be obtained by differentiation in the image. Set $\Omega(X) = \mathrm{Hom}(X, \Omega)$, where Ω is the complex of formal differential forms, and call the maps of the rational cohomology of $\Omega(X)$-generalised Chern classes. It can be shown, in the case when X is the manifold of symmetric tensors of rang 2, that they coincide with Pontryagin classes ($q < n$).

REFERENCES

[1] I. M. Gel'fand, S. V. Fomin. — Geodesic flows on surfaces of constant negative curvature (Геодезические потоки на поверхностях постоянной отрицательной кривизны). Успехи математически ких наук, т. ХУІ, 1 (1952), pp. 118-137.

[2] Y. G. Sinai. — Classical dynamic systems with countable Lebesgue spectrum (2) (Классические динамические системы со счетнократным лебеговым спектром). Изв. АН СССР, сер. матем. 30, 1 (1966), pp. 15-68.

[3] D. V. Anosov. — Geodesic flows on closed Riemann manifolds of negative curvature (Геодезические потоки на замкнутых римановых многообразиях отрицательной кривизны). Труды Матем. ин-та АН СССР, 90 (1967), pp. 1-210.

[4] G. A. Margulis. — On some applications of ergodic theory to the study of manifolds of negative curvature (О некоторых применениях эргодической теории к изучению многообразий отрицательной кривизны). Функц. анализ, 3, вып. 4 (1969), pp. 89-90.

[5] I. M. Gel'fand, M. I. Graev. — The geometry of homogeneous spaces, representation theory in homogeneous spaces and related questions of integral geometry (Геометрия однородных пространств, представления групп в однородных пространствах и связанные с ними вопросы интегралвной геометрии). Труды Моск. матем. об-ва, 8 (1959), pp. 321-390.

[6] I. M. Gel'fand. — Automorphic functions and the theory of representations (Автоморфные функции и теория представлений). *Proceedings of the International Congress of Mathematicians*, Stockholm (1962), pp. 74-85.

[7] I. M. Gel'fand, M. I. Graev, I. I. Pyatetskii-Shapiro. — Representation theory and automorphic functions (Теория представлений и автоморфные функции). Изд. « Наука » (1966), pp. 1-512.

[8] Harish-Chandra. — *Eisenstein series over finite fields*. Stone Jubilee volume, Springer.

[9] Helgason. — *Seminare Bourbaki* (1965).

[10] I. M. Gel'fand, M. I. Graev, Z. Y. Shapiro. — Integral geometry on κ-dimensional planes (Интегральная геометрия на κ-мерных плоскостях). Функц. анал., т. 1, вып. 1 (1967), pp. 15-31.

[11] I. M. Gel'fand, M. I. Graev. — Permissible complexes of planes in C^n (Допустимые комилексы прямых в пространстве C^n). Функц. анализ, т. 2, вып. 3 (1968).

[12] —, —, Z. Y. Shapiro. — Differential forms and integral geometry (Дифференциальные формы и интегральн ная геометрия). Функц. анализ, т. 3, вып. 2 (1969).

[13] Langlands. — *On the functional equations satisfied by Eisenstein series* (1967).

[14] I. M. Gel'fand, M. I. Graev, N. Y. Vilenkin. — Integral geometry and related questions of representation theory (Интегральная геометрия и связанные с ней вопросы теории представлений). Гос. изд. физ.-мат. лит. (1962), pp. 1-656.

[15] —, —, Z. Y. — SHAPIRO. Integral geometry in projective space (Интегральная геометрия в проективном пространстве). Функц. анализ, т. 4, вып. 1 (1970), pp. 14-32,

[16] —, —, —. — Problems of integral geometry related with a pair of Grassman manifolds (Задачи интегральной геометрии, связанные с парой грассмановых многообразий). ДАН СССР, 193, N° 2 (1970).

[17] —, —. — Complexes of κ-dimensional planes and the Plancherel formula for GL(n, $\mathbb{C}$) (Комплексы κ-мерных плоскостей и формула Планшереля для GL(n, $\mathbb{C}$)). ДАН СССР, 179 N° 3 (1968).

[18] HARISH-CHANDRA. — Invariant distributions on Lie algebras. *Am. J. Math.*, LXXXVI, 2 (1964), pp. 272-309.

[19] I. M. GEL'FAND, A. A. KIRILLOV. — Sur les corps liés aux algèbres enveloppantes des algèbres de Lie (О телах, связанных с обертывающими алгебрами алгебр Ли). Institut des hautes études scientifiques, Publications Mathématiques, (1966).

[20] —, —. — Structure of the Lie skew-field, related to a semisimple split Lie algebra (Структура тела Ли, связанного с полупростой расщепимой алге брой Ли). Функц. анализ, 3, вып. 1 (1969).

[21] I. M. GEL'FAND, V. A. PONOMAREV. A remark on the classification of pairs of commuting linear operators in finite dimensional space (Замечания о классификации пары коммутирующих линейных преобразований в конечномерном пространстве). Функц. анализ, 3, вып. 4 (1969), pp. 81-82.

[22] —, —. — Undecomposable representations of the Lorenz group (Неразложимые представления группы Лоренца). Успехи матем. наук, XXIII, вып. 2 (140), 1968 г.

[23] —, —. — The category of Harish-Chandra modules over the Lie algebra of the Lorenz group (Категория модулей Хариш-Чандры над алгеброй Ли группы Лоренца). ДАН СССР, N° 2, 176 (1967), pp. 243-246.

[24] —, —. — The classification of undecomposable infinitesimal representations of the Lorenz group. (Классификация неразложимых инфинитезимальных представлений группы Лоренца). ДАН СССР, N° 3, 176 (1967).

[25] —, —, M. I. GRAEV. — The classification of linear representations of the group SL (2, C) (Классификация линейных представлений группы SL (2, C)). ДАН СССР, N° 5, 194 (1970).

[26] I. N. BERNSTEIN, I. M. GEL'FAND, S. I. GEL'FAND. — Differential operators on the principal affine space (Дифференциальные операторы на основном пространстве). ДАН СССР, N° 6, 195 (1970).

[27] V. BARGMANN. — On a Hilbert space of analytic functions and an associated integral transform. I, II. *Com. Pure and Appl. Math.*, XIV, 3 (1961), pp. 187-214 and XX, 1 (1967), pp. 1-101.

[28] I. M. GEL'FAND, D. B. FUKS. — The cohomology of the Lie algebra of tangent vector fields of a smooth manifolds, I (Когомологии алгебры Ли касательных векторных полей гладкого многообразия). Функц. анализ, 3, вып. 3, pp. 32-52.

[29] —, —. — The cohomology of the Lie algebra of tangent vector fields of a smooth manifolds, II (Когомологии алгебры Ли касательных векторных полей гладкого многообразия). Функц. анализ, вып. 2, 4 (1970), pp. 23-32.

[30] —, —. — The cohomology of the Lie algebra of formal vector fields (Когомологии алгебры Ли формальных векторных полей). Изв. АН СССР, сер. мат., 34 (1970), pp. 322-337.

[31] I. P. SERRE, C. HOCHSHILD. — Cohomology of group extensions. *Trans. Am. Math. Soc.*, 74 (1953), pp. 110-134.

[32] I. M. GEL'FAND, D. B. FUKS. — The cohomology of the Lie algebra of vector fields with non-trivial coefficients (Когомологии алгебры Ли векторных полей с нетривиальными коэффициентами). Функц. анализ, вып. 3, 4 (1970).
[33] M. V. LOCIK. — Concerning the cohomology of infinite dimensional Lie algebras of vector fields (О когомологиях бесконечномерных алгебр Ли векторных полей). Функц. анал., вып. 2, 4 (1970), pp. 43-53.
[34] I. N. BERNSTEIN, S. I GEL'FAND. — The function ρ^λ meromorphic (Мероморфность функции ρ^λ). Функц. анал., вып. 1, 3 (1969).

University of Moscow,
Department of Mathematics,
Moscow V 234 (U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 113 à 119.

A TRANSCENDENTAL METHOD IN ALGEBRAIC GEOMETRY

by PHILLIP A. GRIFFITHS

1. Introduction and an example from curves.

It is well known that the basic objects of algebraic geometry, the smooth projective varieties, depend continuously on parameters as well as having the usual discrete invariants such as homotopy and homology groups. What I shall attempt here is to outline a procedure for measuring this continuous variation of structure. This method uses the periods of suitably defined rational differential forms to construct an intrinsic " continuous " invariant of arbitrary smooth projective varieties. The original aim in defining this " period matrix " of an algebraic variety was to give, at least in some cases, a complete invariant (i. e. " moduli ") of the algebraic structure, as turns out to happen for curves. It is too soon to evaluate the success of this program, but a few interesting things have turned up, and there remain very many attractive unsolved problems. In presenting this talk, I shall not give references as these, together with a more detailed discussion of the material discussed, may be found in my survey paper which appeared in the March (1970) *Bulletin of the American Mathematical Society.*

Let me begin by discussing the example of hyperelliptic curves. Consider the family of affine curves with the equation

$$y^2 = (x - s_1) \dots (x - s_{2g+2}).$$

Denoting by V_s the complete curve corresponding to $s = (s_1, \dots, s_{2g+2})$ and letting

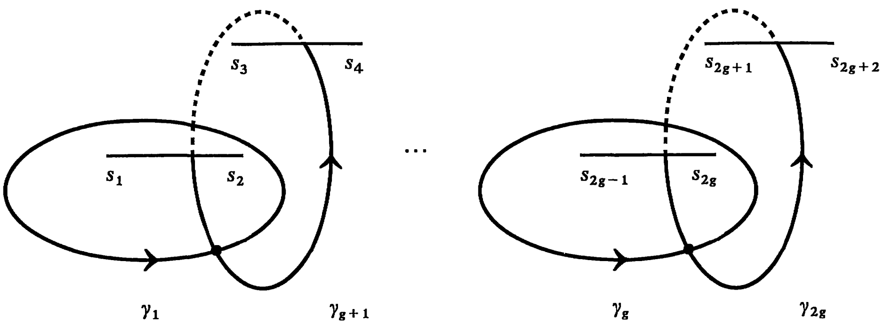
$$S = \{ s : \prod_{j<k} (s_j - s_k) \neq 0 \},$$

we see that $\{ V_s \}_{s \in S}$ forms an algebraic family of non-singular curves of genus g. Furthermore, for a suitable *smooth completion* $\bar{S}$ of S (e. g. $\bar{S} = \mathbb{P}_{2g+2}$), we may enlarge our family to $\{ V_s \}_{s \in \bar{S}}$ by adding suitable degenerate curves $V_{\bar{s}}$ corresponding to the points $\bar{s} \in \bar{S} - S$. The notations $\{ V_s \}_{s \in S}$ and $\{ V_s \}_{s \in \bar{S}}$ will be used throughout this talk to represent respectively an algebraic family of smooth, projective varieties V_s with smooth parameter space S, and a completion of this family where $\bar{S}$ is smooth and $\bar{S} - S = D_1 \cup \dots \cup D_l$ is a divisor with normal crossings. The varieties $V_{\bar{s}}$ ($\bar{s} \in D_j$) may be thought of as singular specializations of the general V_s.

On the curve V_s we consider a basis $\varphi_1, \dots, \varphi_g$ for the holomorphic differentials and a *canonical basis* $\gamma_1, \dots, \gamma_{2g}$ for the first homology $H_1(V_s, \mathbb{Z})$. Thus we might choose

$$\varphi_\alpha = \frac{x^{\alpha-1}dx}{y} \qquad (\alpha = 1, \dots, g)$$

and, upon representing V_s as a 2-sheeted covering of the x-line, we have the picture



The choice of the $\{\varphi_\alpha\}$ is determined up to a substitution $\varphi_\alpha \to \sum_{\beta=1}^{g} A_\alpha^\beta \varphi_\beta$, $\det(A_\alpha^\beta) \neq 0$, and the $\{\gamma_\rho\}$ are determined up to a transformation $\gamma_\rho \to \sum_{\sigma=1}^{2g} T_\rho^\sigma \gamma_\sigma$ where $T = (T_\rho^\sigma)$ is a $2g \times 2g$ integral matrix which preserves the intersection matrix $Q = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ of the $\{\gamma_\rho\}$. Thus $A \in GL(g, \mathbb{C})$ and $T \in Sp(g, \mathbb{Z})$.

We now form the period matrix

$$\Omega(s) = \underbrace{\begin{pmatrix} \int_{\gamma_1} \varphi_1 & \cdots & \int_{\gamma_{2g}} \varphi_1 \\ \vdots & & \vdots \\ \int_{\gamma_1} \varphi_g & \cdots & \int_{\gamma_{2g}} \varphi_g \end{pmatrix}}_{2g} \Bigg\} g,$$

which is determined up to the equivalence relation

$$\Omega \sim A\Omega T$$

arising from the indeterminacy of the $\{\varphi_\alpha\}$ and $\{\gamma_\rho\}$. Because of the obvious relations

$$\begin{cases} \int_{V_s} \varphi_\alpha \wedge \varphi_\beta = 0 \\ \sqrt{-1} \int_{V_s} \varphi_\alpha \wedge \bar{\varphi}_\alpha > 0, \end{cases}$$

the period matrix $\Omega(s)$ satisfies the *Riemann bilinear relations*

$$\begin{cases} \Omega Q {}^t\Omega = 0 \\ \sqrt{-1}\Omega Q {}^t\bar{\Omega} > 0. \end{cases}$$

Thus, if we let D be the set of all $g \times 2g$ matrices Ω which satisfy the Riemann bilinear relations and with the equivalence $\Omega \sim A\Omega$ ($A \in GL(g, \mathbb{C})$), we see that the periods of the holomorphic differentials on V_s lead to the period mapping

$$\Omega: \quad S \to D/Sp(g, \mathbb{Z}),$$

where $Sp(g, \mathbb{Z})$ acts on D by sending Ω into $\Omega {}^tT^{-1}$. We recall that D is a complex manifold which is biholomorphic to the Siegel-upper-half-plane of all $g \times g$ matrices $Z = X + \sqrt{-1}Y$ with $Z = {}^tZ$, $Y > 0$. Furthermore, D is a homogeneous complex manifold with automorphism group $Sp(g, \mathbb{R})$ which acts in the same way as $Sp(g, \mathbb{Z})$ above. For $g = 1$, D is of course the usual upper half plane.

Here are a few properties of the period mapping:

(*a*) The point $\Omega(s)$ depends only on the intrinsic structure of V_s. Furthermore, $\Omega(s) = \Omega(s')$ if, and only if, the curves V_s and $V_{s'}$ are isomorphic (Torelli's theorem). Thus the period matrix gives a complete invariant for non-singular curves.

To discuss the next two properties, we need to digress a little about the monodromy group of a family of smooth algebraic varieties. In the case of our family of hyperelliptic curves, the canonical basis $\{ \gamma_\rho \}$ of $H_1(V_s, \mathbb{Z})$ will change when we displace V_s around a closed path in the parameter space S. More precisely, fixing a base point $s_0 \in S$ and letting $V = V_{s_0}$, the fundamental group $\pi_1(S)$ acts on the homology $H_1(V, \mathbb{Z})$. As is always the case, this action preserves the intersection pairing on homology, and we have then the monodromy representation

$$\begin{tikzcd} \pi_1(S) \arrow[r] \arrow[rr, bend left, dashed, "\rho"] & \operatorname{Aut}(H_1(V, \mathbb{Z})) \arrow[r] \arrow[d, phantom, "\wr\|"] & \operatorname{Aut}(D) \\ & Sp(g, \mathbb{Z}) & \end{tikzcd}$$

The image $\Gamma = \rho(\pi_1(S))$ will be called the *monodromy group.*

(*b*) For $g = 1$, the monodromy group is of finite index in $SL(2, \mathbb{Z}) \cong Sp(1, \mathbb{Z})$ (For an arbitrary family of elliptic curves, Γ is either a finite group or is of finite index in $SL(2, \mathbb{Z})$). This result should be interpreted as being a first suggestion that the monodromy group in an algebraic family of algebraic varieties has extremely remarkable properties.

(*c*) A further indication of this is the " rigidity property ", due to Grothendieck in this case. This states that if we have two families of curves $\{ V_s \}_{s \in S}$, $\{ V'_s \}_{s \in S}$ with the same parameter space S, with $V_{s_0} = V'_{s_0}$, and with the same monodromy representations ρ and ρ', then the period mappings Ω and Ω' are the sȃme. In other words, the period mapping is determined by the monodromy representation plus its value at one point.

(*d*) The next property may perhaps be thought of as relating algebraic geometry to group representations. We recall that the study of the discrete series representations of the automorphism group $Sp(g, \mathbb{R})$ is intimately related to the construction of certain Γ-invariant meromorphic functions on D. If ψ is one such *automorphic function*, then the composite

$$\psi \circ \Omega$$

turns out to be a *rational* function on S. Roughly speaking, we may say that the study of $L^2(Sp(g, \mathbb{R}))$ leads to functions which uniformize the period mapping (" automorphic function property ").

The proofs of properties (*b*), (*c*), (*d*) above may be based on studying asymptotically the period matrix $\Omega(s)$ as s tends to a point $\bar{s} \in \bar{S} - S$. More precisely, a neighborhood in S of a point $s \in S - S$ will be a *punctured polycylinder*

$$P^* \cong \underbrace{\Delta^* \times \ldots \times \Delta^*}_{k} \times \underbrace{\Delta \times \ldots \times \Delta}_{m-k}$$

where Δ is a unit disc in $\mathbb{C}$, $\Delta^* = \Delta - \{0\}$ is the punctured disc, and $\dim S = m$. By localizing the period mapping at infinity, we will have a holomorphic mapping

$$\Omega: \quad P^* \to D/\Gamma$$

where we are interested in the behavior of $\Omega(s)$ as $\|s\| \to 0$ $(s = (s_1, \ldots, s_m) \in P^*)$. This asymptotic analysis of the period mapping is a purely function-theoretic problem which, in the end, should provide the best general method for proving the various global properties of Ω including the analogues of (*b*)-(*d*) above.

2. Construction and elementary properties of the period mapping.

We first observe that giving a $g \times 2g$ matrix Ω with the condition rank $(\Omega) = g$ and the equivalence relation $\Omega \sim A\Omega$ $(A \in GL(g, \mathbb{C}))$ is the same as giving a point $\Omega \in G(g, 2g)$, the Grassmann variety of g-planes in $\mathbb{C}^{2g}$. In fact, the point Ω is the point in $\mathbb{C}^{2g}$ spanned by the row vectors of the matrix Ω. Thus, giving the period matrix $\Omega(s)$ above is the same as giving a g-dimensional subspace of $H^1(V, \mathbb{C})$, this subspace being determined up to the monodromy group Γ. It is now easy to see that this g-dimensional subspace is simply the g-plane

$$H^{1,0}(V_s) \subset H^1(V_s, \mathbb{C})$$

spanned by the holomorphic 1-forms, followed by the identification

$$H^1(V_s, \mathbb{C}) \cong H^1(V, \mathbb{C})$$

which is determined up to Γ. Thus, giving the period matrix $\Omega(s)$ is equivalent to giving the g-dimensional subspace $H^{1,0}(V_s, \mathbb{C})$ of $H^1(V, \mathbb{C})$, and both of these are determined up to the monodromy group.

In general, let $\{V_s\}_{s \in S}$ be a family of smooth, projective algebraic varieties, and introduce the notations, $E = H^n(V_{s_0}, \mathbb{C})$, $E_{\mathbb{R}} = H^n(V_{s_0}, \mathbb{R})$, $E_{\mathbb{Z}} = H^n(V_{s_0}, \mathbb{Z})$. Using standard Kähler manifold theory we find that the cup product on $H^*(V, \mathbb{C})$ together with the Kähler class of the projective embedding give rise to a non-degenerate bilinear form

$$Q: \quad E \otimes E \to \mathbb{C}$$

which is rational on $E_{\mathbb{Z}}$, is invariant under the monodromy group Γ, and satisfies $Q(e, e') = (-1)^n Q(e', e)$. We will denote by G, $G_{\mathbb{R}}$, $G_{\mathbb{Z}}$ respectively the automorphism groups of E, $E_{\mathbb{R}}$, $E_{\mathbb{Z}}$ which preserve the bilinear form Q. $G_{\mathbb{C}}$ is a complex semi-simple algebraic group, $G_{\mathbb{R}}$ is a real form of $G_{\mathbb{C}}$, and $G_{\mathbb{Z}}$ is an arithmetic subgroup of $G_{\mathbb{R}}$ such that the monodromy group $\Gamma \subset G_{\mathbb{Z}}$.

From Hodge theory we recall the *Hodge decomposition*

$$H^n(V_s, \mathbb{C}) = \bigoplus_{p+q=n} H^{p,q}(V_s) \qquad (H^{p,q}(V_s) = \overline{H^{q,p}(V_s)}),$$

and using this we define the *Hodge filtration* $F^0(V_s) \subset \ldots \subset F^n(V_s) = H^n(V_s, \mathbb{C})$ by the formula

$$F^p(V_s) = H^{n,0}(V_s) + \ldots + H^{n-p,p}(V_s).$$

Using the Kodaira-Spencer continuity theorem, it follows that $F^p(V_s)$ is a continuously varying subspace of $H^n(V_s, \mathbb{C})$. Consequently, if we identify all $H^n(V_s, \mathbb{C})$ with $E = H^n(V_{s_0}, \mathbb{C})$ and let $F(E)$ be the *flag manifold* of all filtrations $F^0 \subset \ldots \subset F^n = E$, $\dim F^p = \dim F^p(V_s)$, then we have a continuous mapping

$$\Omega: \; S \to F(E)/\Gamma$$

which is the first form of the general period mapping. It will be convenient to write $\Omega(s) = (\Omega^0(s), \ldots, \Omega^n(s))$ where the $\Omega^p(s)$ are subspaces of $F(E)$ taken modulo Γ. Using the structure equations of the Kodaira-Spencer-Kuranishi theory of deformation of complex structure, it follows that $\Omega(s)$ varies holomorphically with $s \in S$.

The period mapping Ω will satisfy three bilinear relations, two of which are classical and generalize the Riemann-bilinear relations, and one which is non-classical but which is crucial for understanding the general period mapping. Recalling the bilinear form Q mentioned above, these bilinear relations are

$$\left.\begin{array}{ll} \text{(I)} & Q(\Omega^p, \Omega^{n-p-1}) = 0 \\ \text{(II)} & (\sqrt{-1})^n Q(\Omega^p, \bar{\Omega}^p) > 0 \end{array}\right\} \text{ Hodge-Riemann bilinear relations}$$

$$\text{(III)} \quad Q(d\Omega^p, \Omega^{n-p-2}) = 0 \quad \text{infinitesimal bilinear relation.}$$

The first relation is self-explanatory; the second means that, for any choice of basis $\{ e_\alpha \}$ for Ω^p, the Hermitian matrix

$$(\sqrt{-1})^n Q(e_\alpha, e_\beta)$$

is non-singular and has a fixed signature; and the third bilinear relation means that

$$Q\left(\frac{\partial}{\partial s_j}\{ \Omega^p(s) \}, \; \Omega^{n-p-2}(s)\right) = 0$$

where $(s_1, \ldots, s_n)$ are local coordinates on S.

Suppose now that we let $\check{D}$ be the algebraic variety of all points $(F^0, \ldots, F^n) \in F(E)$ which satisfy (I), and let D be the open set in $\check{D}$ of all points which satisfy (II). Then $\check{D}$ is acted on transitively by the group $G_{\mathbb{C}}$, and D turns out to be the $G_{\mathbb{R}}$ orbit of a suitable point in $\check{D}$. Thus we have a diagram

$$\begin{array}{ccc} D & \subset & \check{D} \\ \| & & \| \\ G_{\mathbb{R}}/H & \subset & G_{\mathbb{C}}/B \end{array} \qquad (H = G_{\mathbb{R}} \cap B)$$

where B is a parabolic subgroup of $G_{\mathbb{C}}$ and H is a compact subgroup of $G_{\mathbb{R}}$. In the case of elliptic curves, $D \subset \check{D}$ is the upper-half-plane $z = x + iy$, $y > 0$ embedded in $\mathbb{P}_1 = \mathbb{C} \cup \{ \infty \}$. The group $G_{\mathbb{C}}$ is the group of linear fractional transformations

$z \to az + b/(cz + d)$, $G_{\mathbb{R}}$ is the subgroup of real transformations, and D is the $G_{\mathbb{R}}$ orbit of $\sqrt{-1}$. Since $\Gamma \subset G_{\mathbb{Z}}$, the monodromy group is a discrete subgroup of $G_{\mathbb{R}}$ and acts properly discontinuously on D. Consequently, D/Γ is an analytic space and the period mapping is a holomorphic mapping

$$\Omega: \quad S \to D/\Gamma.$$

In the case of curves, D is biholomorphic to a bounded domain in $\mathbb{C}^{g(g+1)/2}$. However, for $n > 1$, D is no longer a bounded domain and consequently the holomorphic mappings into D will *not* have the strong function-theoretic properties (e. g. normal families) which are present when D is a bounded domain. However, if we consider only the mappings into D which satisfy the infinitesimal bilinear relation (III), then it is increasingly becoming clearer that these have the qualitative properties of mappings into a bounded domain. Thus, e. g., a holomorphic mapping

$$\Phi: \quad \Delta^* \to D$$

of the punctured disc $0 < |t| < 1$ in D which satisfies (III) will extend continuously across $t = 0$. A much deeper recent result is due to Wilfried Schmid, who has proved that an arbitrary holomorphic mapping

$$\Phi: \quad \Delta^* \to D/G_{\mathbb{Z}}$$

which satisfies (III) is, when $|t| \to 0$, strongly asymptotic to an orbit

$$\exp\left(\frac{\log t}{2\pi\sqrt{-1}} N\right)\Omega_0$$

where N is a very special nilpotent transformation of $E_{\mathbb{Z}}$ and Ω_0 is a point in D. From this it follows that the asymptotic analysis of these periods of algebraic integrals is reduced to a problem in Lie groups.

3. Deeper properties and open questions concerning the period mapping.

We want to discuss the analogues of the properties (*a*)-(*d*) for the periods of the elliptic curve in the general case of a period mapping

$$\Omega: \quad S \to D/\Gamma$$

arising from an algebraic family $\{ V_s \}_{s \in S}$ of algebraic varieties.

(*a*) Of course the point $\Omega(s) \in D/\Gamma$ depends only on the intrinsic structure of V_s. However, except for curves there is essentially nothing general known about the global equivalence relation determined by Ω. There is some heuristic evidence that, in general, the equivalence relation might be closely related to birational equivalence; i. e. the " Torelli property " should hold in general. Along these lines, it is perhaps an easier problem to determine the equivalence relation infinitesimally; i. e. to find the kernel of the differential $d\Omega$. The best example known here seems to be when the V_s are smooth hypersurfaces in projective space. Then, except for the obvious example of cubic surfaces, the differential $d\Omega$ is injective on the biregular moduli space of the V_s (" local Torelli property ").

The dual problem to finding the equivalence relation of Ω is to determine which points of D come from algebraic varieties. When D is the Siegel upper-half-plane, even though not every point $\Omega \in D$ is the period matrix of a curve, it is obviously the case that every Ω is the period matrix of an abelian variety and therefore may be said to come from algebraic geometry. However, this is essentially the only case when all points are a period matrix of some algebraic variety, and to my knowledge there is not yet even a plausible candidate for the set of points in D which arise from algebraic geometry.

(*b*) Concerning the " size " of the monodromy group Γ, we have Deligne's theorem that Γ is semi-simple and the result that the image $\Omega(S)$ has finite volume in D/Γ. From this it follows that if Γ' is any larger discrete subgroup of $G_{\mathbb{R}}$ which leaves invariant the inverse image $\pi^{-1}(\overline{\Phi(S)})$ for $\pi : D \to D/\Gamma$ the projection, then Γ is of finite index in Γ'. These facts, plus a few examples, indicate that it might be the case that there is a semi-simple subgroup $G'_{\mathbb{Q}}$ of $G_{\mathbb{Q}}$ such that the monodromy group is commensurable with $G'_{\mathbb{Z}} = G_{\mathbb{Z}} \cap G'_{\mathbb{Q}}$ (recall that this means that $\Gamma \cap G'_{\mathbb{Z}}$ is of finite index in both Γ and $G'_{\mathbb{Z}}$). The available evidence certainly indicates that Γ should be large.

(*c*) Matters are somewhat better regarding the " rigidity property ", which states that the period mapping $\Omega : S \to D/\Gamma$ is determined by its value at one point together with the induced map $\Omega_* : \pi_1(S) \to \Gamma$. This property was proved by myself for an arbitrary holomorphic mapping Ω satisfying the infinitesimal bilinear relation (III) but making the strong assumption that S is complete. Then Deligne proved the result in case Ω arises from a family $\{ V_s \}_{s \in S}$ of algebraic varieties. The result for a general holomorphic mapping Ω satisfying (III) follows from Schmid's nilpotent orbit theorem mentioned above.

(*d*) Given a period mapping Ω: $S \to D/\Gamma$, it is expected that the equivalence relation given by Ω is at least an algebraic equivalence relation; i. e. there should exist a sub-field $\mathscr{R}_{\Omega}$ of the field $\mathscr{R}$ of rational functions on S such that $\Omega(s) = \Omega(s')$ if, and only if, $\psi(s) = \psi(s')$ for all $\psi \in \mathscr{R}_{\Omega}$. Furthermore, by analogy with the classical case $n = 1$, it is to be hoped that $\mathscr{R}_{\Omega}$ arises by composing the mapping Ω with something on D/Γ. More precisely, we should like it to be the case that the discrete series representations in $L^2(G_{\mathbb{R}})$ lead to the construction of some " analytic objects " on D/Γ which, upon composition with Ω, yield $\mathscr{R}_{\Omega}$. This is a problem of fundamental importance, which may well be related to the question mentioned above of saying which points of D come from algebraic geometry, and about which nothing really is known. What is known is that the discrete series part of $L^2(G_{\mathbb{R}})$ seems to lead to " automorphic cohomology " on D/Γ, but it is a mystery as to what this might have to do with algebraic geometry.

These problems mentioned here are discussed in more details in the survey paper referred to at the beginning of this talk. This survey paper also contains some conjectures not discussed above as well as the references for all of the material presented.

Institute for Advanced Study
Department of Mathematics,
Princeton, N. J. 08540
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 121 à 133.

LINEAR DIFFERENTIAL OPERATORS

by LARS HÖRMANDER

At the Edinburgh congress 12 years ago Gårding [1] gave a general survey of the theory of linear partial differential operators. I shall take his lecture as my starting point and try to give some idea of the later development. Naturally it is necessary to concentrate on a few topics and ignore others which are as interesting. I shall not try to list the omissions but wish to specify the limitation to questions concerning the existence and structure of solutions of differential equations with constant, C^∞ or analytic coefficients.

1. **Operators with constant coefficients.**

1.1. *Interaction with complex analysis.*

Let $P(D)$ where P is a polynomial and $D = -i\partial/\partial x$ be a partial differential operator in an open convex set $X \subset \mathbb{R}^n$, and let $u \in C^\infty(X)$, $P(D)u = 0$. Already Malgrange [1] proved that u can then be approximated by exponential solutions of the same equation. A significant improvement of this result was made by Ehrenpreis [1] who found that u is actually a superposition of exponential solutions. If we assume for simplicity that P is irreducible, this means that

$$u(x) = \int e^{i\langle x,\zeta\rangle} d\mu(\zeta)$$

where $d\mu$ is a measure carried by $\{ \zeta \in \mathbb{C}^n,\ P(\zeta) = 0 \}$ and

$$\int e^{-\langle x, \operatorname{Im}\zeta\rangle}(1 + |\zeta|)^N |d\mu(\zeta)| < \infty$$

for all N and $x \in X$. A slightly weaker result is proved as follows. For a fixed convex compact set $K \subset X$ we consider the form

$$L: \quad \mathscr{E}'(K) \ni v \to \langle u, v \rangle.$$

For any v we have if H is the supporting function of K

$$|L(v)| \leqq C \sup |\hat{v}(\zeta)| e^{-H(\operatorname{Im}\zeta)}(1 + |\zeta|)^{-\nu}.$$

That $P(D)u = 0$ means that $L(P(-D)v) = 0$ if $v \in \mathscr{E}'(K)$, or since P is irreducible that $L(v) = 0$ if $v \in \mathscr{E}'(K)$ and $\hat{v} = 0$ on $N = \{ \zeta \in \mathbb{C}^n,\ P(-\zeta) = 0 \}$. Thus $L(v)$ depends only on the restriction of $\hat{v}$ to N. Now the global theory of analytic functions (theorem B of Cartan) gives that if f is an analytic function on N (that is, locally the restriction of a function analytic in a neighborhood) then f is the restriction of an entire analytic function F. Ehrenpreis proved that one can give bounds for a suitable extension F: for every $\nu > 0$ one can find C and $\nu' > 0$ so that for a suitable choice of F

$$\sup |F(\zeta)| e^{-H(\operatorname{Im}\zeta)}(1 + |\zeta|)^{-\nu'} \leqq C \sup_N |f(\zeta)| e^{-H(\operatorname{Im}\zeta)}(1 + |\zeta|)^{-\nu}.$$

Taking f to be the restriction of $\hat{v}$ to N, where $v \in \mathscr{E}'(K)$, we obtain $F = \hat{w}$ where $w \in \mathscr{E}'(K)$ also, and since $L(v) = L(w)$ we obtain

$$|L(v)| \leqq C \sup_N |\hat{v}(\zeta)| e^{-H(\operatorname{Im}\zeta)}(1 + |\zeta|)^{-\nu}.$$

Hence there is a measure μ supported by N such that

$$\int e^{H(\operatorname{Im}\zeta)}(1 + |\zeta|)^{\nu} |d\mu(\zeta)| < \infty,$$
$$L(v) = \int \hat{v}(\zeta) d\mu(\zeta), \quad v \in \mathscr{E}'(K).$$

This implies that on K

$$u(x) = \int e^{-i\langle x,\zeta\rangle} d\mu(\zeta).$$

We have given this argument in some detail to show that the decisive point is the application of a variant, involving bounds, of theorem B of Cartan. We shall refer to this as theorem B with bounds. Ehrenpreis [1, 2], Malgrange [2] and Palamodov [1] have pushed this technique very far and given existence theorems for general over-determined systems with constant coefficients

$$\sum_1^K P_{jk}(D)u_k = f_j, \qquad j = 1,\dots, J \tag{1.1.1}$$

where u_k, $f_j \in \mathscr{D}'(X)$ and X is a convex open set in $\mathbb{R}^n$. They have also proved that solutions of the homogeneous system can be represented by integrals over exponential polynomial solutions. Obviously solutions of (1.1.1) cannot exist unless we have the compatibility conditions

$$\sum_1^J Q_j(D)P_{jk}(D) = 0, \quad k = 1,\dots, K \Rightarrow \sum_1^J Q_j(D)f_j = 0; \tag{1.1.2}$$

the existence theorems state that these conditions are sufficient. (It is clear that they are finitely generated.) The results obtained in this way sum up a very substantial part of our knowledge of differential operators with constant coefficients.

The proof of theorem B with bounds follows the lines of the Oka-Cartan theory starting from existence theorems for the differential equation

$$\bar{\partial} u = f \tag{1.1.3}$$

where u is a $(0, p)$ form in $\mathbb{C}^n$ and f a $(0, p + 1)$ form. The compatibility conditions are here $\bar{\partial} f = 0$. The proof of the sufficiency of this condition with methods from the theory of partial differential equations was first achieved by Morrey [1] and Kohn [1] (see also Kohn-Nirenberg [1]) in relatively compact strongly pseudo-convex domains in $\mathbb{C}^n$ (or Stein manifolds). Actually one solves a certain boundary problem for the Laplacean on forms, called the $\bar{\partial}$ Neuman problem. A variant of this approach was used by Hörmander [2, 3] to prove that if φ is plurisubharmonic in $\mathbb{C}^n$ and $f \in L^2_{\text{loc}}$, then a solution of (1.1.3) exists when $\bar{\partial} f = 0$, with the bound

$$2\int |u|^2 e^{-\varphi}(1 + |z|^2)^{-2} d\lambda \leqq \int |f|^2 e^{-\varphi} d\lambda, \tag{1.1.4}$$

where $d\lambda$ is the Lebesgue measure. Starting from this result and local results on analytic functions one can give a proof of theorem B with bounds (see Hörmander [2, section 7.6]).

1.2. *Convexity with respect to an operator.*

The restriction to convex open sets X in section 1.1 cannot be relaxed if one wants to have an existence theory for arbitrary operators. However, for a fixed operator $P(D)$ one can consider more general sets X, and since the study of the appropriate conditions on X is a source of interesting problems we shall discuss them briefly assuming that P is scalar.

Malgrange [1] proved that a solution of the equation $P(D)u = f$ exists for all $f \in C^\infty(X)$ (or $L^2_{\mathrm{loc}}(X), \ldots$) if and only if for every compact set $K \subset X$ there is another compact set $K' \subset X$ such that

$$(1.2.1) \qquad u \in \mathscr{E}'(X), \quad \operatorname{supp} P(-D)u \subset K \Rightarrow \operatorname{supp} u \subset K'.$$

To have solutions for arbitrary $f \in \mathscr{D}'(X)$ one must have in addition (see Hörmander [1])

$$(1.2.2) \qquad u \in \mathscr{E}'(X), \quad \operatorname{sing\,supp} P(-D)u \subset K \Rightarrow \operatorname{sing\,supp} u \subset K'.$$

Here $\operatorname{supp} u$ ($\operatorname{sing\,supp} u$) is the smallest closed subset of X such that u vanishes (is C^∞) in the complement with respect to X. These results are essentially functional analytic but the question of finding the geometric meaning of (1.2.1), (1.2.2) which we shall now discuss is not.

Conditions (1.2.1) resp. (1.2.2) mean that if u is a distribution in a fixed neighborhood of the boundary in X satisfying the equation $P(D)u = 0$ resp. $P(D)u \in C^\infty$ and if $u = 0$ resp. $u \in C^\infty$ in an unspecified neighborhood of ∂X, then this last property is valid in a fixed neighborhood of the boundary. Such results are called theorems on unique continuation (of singularities). For operators with constant (or more generally analytic) coefficients the basic uniqueness theorem is the classical one of Holmgren giving uniqueness across a non-characteristic surface, that is, a surface with $p(N) \neq 0$ if N is the normal and p the principal part of P, the homogeneous part of highest degree. That this breaks down for certain characteristic surfaces can be shown by solving a Goursat problem. Combining these facts with essentially geometric arguments one concludes (Malgrange [3], Hörmander [1]) if $\partial X \in C^2$ and P is of real principal type that (1.2.1) is valid if at characteristic points $x \in \partial X$ the normal curvature in the direction of the corresponding bicharacteristic is positive while (1.2.1) is false if it may become negative. That P is of real principal type means that p is real and that $p'(\xi) = \partial p/\partial \xi \neq 0$ for $\xi \in \mathbb{R}^n \backslash 0$. Lines with the direction $p'(\xi)$ are then called bicharacteristics. More precise results along the same lines have also been given by Trèves [2, section 6.7] and Zachmanoglou [1, 2]. (After the congress the author has proved using the results on propagation of singularities mentioned below that (1.2.1) is valid if $\partial X \in C^1$, P is of real principal type, and no bicharacteristic emanating from a characteristic point $x \in \partial X$ contains an interval $I \ni x$ with $\partial I \subset X$ and I in the closure of X.)

Results of Zerner [1], Hörmander [1] and Grušin [1] show that for the same class of operators the condition (1.2.2) is essentially equivalent to convexity of X in the direction $p'(\xi)$ for all $\xi \in \mathbb{R}^n \backslash 0$ with $p(\xi) = 0$. We shall now describe a partial generalization of these theorems to general operators (see Hörmander [10]). To do so we first introduce the set $L(P)$ of all limits

$$Q(\xi) = \lim c_i P(\xi + \xi_i) \tag{1.2.3}$$

where $c_i \in \mathbb{C}$ and $\xi_i \to \infty$ in $\mathbb{R}^n$. One should think of Q as a localization of P at infinity. We denote by B_Q the smallest subspace of $\mathbb{R}^n$ along which Q acts and call an affine subspace parallel to some B_Q with $\dim B_Q > 0$ a bicharacteristic subspace. For operators of real principal type this agrees with the earlier definition, and the bicharacteristic subspaces carry the singularities as one would like them to do. More precisely, for any $Q \in L(P)$ one can find $u \in \mathscr{D}'(\mathbb{R}^n)$ with $P(D)u = 0$ and sing supp $u = B_Q$, provided that $\dim B_Q > 0$. Furthermore, for any closed cone F containing a half space of every bicharacteristic subspace and the origin we can construct a fundamental solution (that is, solution of $P(D)E = \delta$, the Dirac measure at 0) which is as smooth as we like outside F. Gabrielov [1] has proved that the closed union of all B_Q is semi-algebraic of codimension $\geqq 1$ so this statement is never empty. As a corollary one concludes that (1.2.2) is always valid if $X \cap B$ is convex for all bicharacteristic subspaces, a condition which is also necessary when $n = 2$. However, when $n > 2$ the results known are far from complete.

When P is of real principal type Andersson [1] has recently obtained analogous results with singular support replaced by analytic support, defined as the complement of the largest domain of real analyticity. In particular, these imply that (1.2.1) is then a consequence of (1.2.2). (See also the lecture by M. Sato in these proceedings as well as section 2.4 below.) Also for general operators one should expect results similar to those described above for analytic supports or " Gevrey supports ". It is clear that the localizations (1.2.3) must then be modified by allowing ξ_i to tend to ∞ in an appropriate complex neighborhood of $\mathbb{R}^n$.

1.3. *Supports of fundamental solutions.*

To continue the work described in section 1.2 one seems to need additional information on the supports and singular supports of fundamental solutions. More precisely, given a closed set $F \subset \mathbb{R}^n$ we would like to know which operators $P(D)$ have a fundamental solution with support or singular support in F. The question concerning singular supports should be closely related to the question on supports for all localizations so we shall only discuss the latter.

When F is a closed convex cone which is proper, that is, contains no straight line, the existence of a fundamental solution with support in F means that P is hyperbolic with respect to the proper supporting planes of F, and algebraic conditions for this are known (see e. g. Hörmander [1]). If F is a subset of such a cone we have the problem of lacunas for hyperbolic differential operators where in addition to the classical work of Petrowsky we now have extensive recent work of Atiyah, Bott and Gårding [1]. Another case which has been completely solved is that where $F = \{ x; \langle x, N \rangle \geqq 0 \}$ is a half space. A classical sufficient condition for the existence of a fundamental solution with support in F is the Petrowsky condition that there is a constant C such that the zeros of $P(\xi + \tau N) = 0$ for $\xi \in \mathbb{R}^n$ lie in the half plane $\operatorname{Im} \tau > -C$. The necessary and sufficient condition turns out to be that by analytic continuation from ξ to a point as distance $\leqq C$ from ξ one can bring τ into this half plane (see Hörmander [9]). For general convex cones F we also have some sufficient conditions (see Gindikin [1]).

Further results can be obtained using the methods of Hörmander [9] but the general situation is far from clear yet.

2. Operators with C^∞ coefficients.

2.1. *Pseudo-differential operators.*

The theory of (singular) integral operators has always been closely connected with the theory of differential operators. A complete merger with the theory of differential operators has been achieved by the notion of pseudo-differential operator (Kohn-Nirenberg [2]). This development has been greatly stimulated by the solution of the index problem for elliptic operators by Atiyah and Singer [1] where the restriction to differential operators is awkward from the topological point of view. Actually this work was originally based on the earlier techniques of singular integral operators (see e. g. Calderón and Zygmund [1], Calderón [1]).

If X is an open set in $\mathbb{R}^n$, an operator $A\colon C_0^\infty(X) \to C^\infty(X)$ is called pseudo-differential of degree m if A can be written in the form

$$Au(x) = (2\pi)^{-n}\int e^{i\langle x,\xi\rangle}a(x, \xi)\hat{u}(\xi)d\xi, \quad u \in C_0^\infty(X), \tag{2.1.1}$$

where $a \in C^\infty(X \times \mathbb{R}^n)$ and the functions $(x, \xi) \to t^{-m}a(x, t\xi)$ belong to a bounded subset of $C^\infty(X \times (\mathbb{R}^n\backslash 0))$ when $t \to \infty$ (Actually it is preferable to use less restrictive hypotheses on a as in Hörmander [6]). One calls a the symbol of A. Often it is possible to write $a = a^0 + a^1$ where $a^0(x, \xi)$ is homogeneous with respect to ξ of degree m and a^1 is of degree $m - 1$. Then one calls a^0 a principal symbol. If a is a polynomial in ξ it is clear that A is the differential operator $a(x, D)$ obtained by replacing ξ by $D = -i\partial/\partial x$, put to the right of the coefficients. We shall therefore use the notation $a(x, D)$ in general to suggest the analogy with differential operators. In fact, most rules of calculus valid for differential operators remain true for pseudo-differential operators with very small modifications. It is this ease of manipulation which makes pseudo-differential operators so useful and not their generality; the algebra of pseudo-differential operators is essentially generated by differential operators and say the Newtonian potential operator. In particular, the calculus leads to the definition of pseudo-differential operators on manifolds X and shows that the principal symbol is invariantly defined on the cotangent bundle. Let us also note that pseudo-differential operators can be extended to continuous operators $\mathscr{E}'(X) \to \mathscr{D}'(X)$ and in fact $\mathscr{D}'(X) \to \mathscr{D}'(X)$ if one is somewhat careful with questions concerning supports. Finally,

$$\text{sing supp } Au \subset \text{sing supp } u, \qquad u \in \mathscr{D}'(X),$$

which is called the pseudo-local property.

A (pseudo-) differential operator is called elliptic if the principal symbol never vanishes in $T^*(X)\backslash 0$. To every elliptic operator A of order m one can construct a parametrix B of order $-m$, that is, an operator such that AB and BA differ from the identity only by an operator with a C^∞ kernel. Starting from this fact it is easy to reduce the study of boundary problems for elliptic differential operators to the study of (systems) of pseudo-differential operators inside the boundary (Calderón [2], Hörmander [5], Seeley [1]). Consider for example the Laplace equation $\Delta u = 0$ in $X \subset \mathbb{R}^n$ with a differential boundary condition $Bu = f$ on the smooth boundary

∂X. If u_0 is the restriction of u to ∂X, then u is the Poisson integral of u_0 and the boundary condition $Bu = f$ becomes a pseudo-differential equation

$$\tilde{B}u_0 = f$$

whose principal symbol is easy to calculate. In this way the study of elliptic boundary problems (Agmon-Douglis-Nirenberg [1], see also Hörmander [1, chap. X]) is reduced to the study of an elliptic system of pseudo-differential operators on the compact manifold ∂X. The same reduction of more general boundary problems for elliptic differential equations leads to the study of non-elliptic systems of pseudo-differential operators (see also section 2.3). Another important conclusion is that mixed boundary problems for elliptic differential equations, such as the boundary problem $\Delta u = 0$, in X, $u = f$ and $du/dn = g$ on complementary parts of ∂X, are essentially equivalent to boundary problems for pseudo-differential systems on ∂X, the new boundary being the manifold where the shift of boundary condition occurs. A thorough study of such questions has been given by Višik and Eškin [1-5] and Boutet de Monvel [1, 2].

2.2. *Hypoelliptic operators.*

If a pseudo-differential operator A has a (left) parametrix (see section 2.1), if follows that A is hypoelliptic, that is, $Au \in C^\infty$ implies that $u \in C^\infty$. In fact, $u = BAu - (BA - I)u$ where both terms are in C^∞. Using sufficiently large classes of pseudo-differential operators one can prove the hypoellipticity of wide classes of differential operators in this way. However, more subtle arguments are required for such operators as the Kolmogorov operator

$$Au = \partial^2 u/\partial x^2 + x\partial u/\partial y - \partial u/\partial t \tag{2.2.1}$$

at least in the present state of the theory of pseudo-differential operators. For (2.2.1) it is easy to construct a fundamental solution explicitly but this is no longer the case if one modifies A slightly. Starting from the hypoellipticity of (2.2.1), due to Kolmogorov himself, a rather complete study of hypoellipticity for second order differential equations with real coefficients was made by Hörmander [7]. A remarkable simplification and extension of this work has been given recently by Radkevič [1, 2]. He proved in [1] that A is hypoelliptic if

$$A = \sum_1^r P_j^* P_j + iP_0 + Q$$

where $P_0, \ldots, P_r$ are pseudo-differential operators of order $2m - 1, m, \ldots, m$ with real principal symbols $p_0, \ldots, p_r$; Q is of order $2m - 2$ and the functions

$$p_j,\ \{p_i, p_j\},\ \{p_i, \{p_j, p_k\}\}, \ldots;\quad i, j, k, \ldots = 0, 1, \ldots, r;$$

have no common zero in $X \times (\mathbb{R}^n \backslash 0)$. Here

$$\{p, q\} = \Sigma(\partial p/\partial \xi_j \partial q/\partial x_j - \partial p/\partial x_j \partial q/\partial \xi_j)$$

is the Poisson bracket of functions in $X \times (\mathbb{R}^n \backslash 0)$ (or rather $T^*(X)\backslash 0$), and repeated Poisson brackets of all orders should be considered. We recall that $\{p, q\}$ is the derivative of q along the Hamiltonian vector field defined by p, whose integral curves are the bicharacteristic strips given by the Hamilton-Jacobi equations

$$dx/dt = \partial p/\partial \xi, \qquad d\xi/dt = -\partial p/\partial x.$$

$\{p, q\}$ is the principal symbol of $i[P, Q] = i(PQ - QP)$ if p, q are principal symbols of P, Q. When P_0 can be omitted in the condition above the same result was also obtained by J. J. Kohn in 1968 (unpublished). Even somewhat more general results have been announced by Radkevič (See also the lectures by Bony and Olejnik in these proceedings as well as a forthcoming book by Olejnik and Radkevič).

Closely related theorems on hypoellipticity have been obtained by Egorov [2, 3] and by Trèves [1]. Since they are discussed in their lectures in these proceedings we just remark that their conditions involve the repeated Poisson brackets of the principal symbol a and its complex conjugate $\bar{a}$ at the zeros of a. Clearly more work should be done to unify all these new results.

In this connection we should also refer to the extensive work on boundary problems for certain degenerating elliptic equations related to (2.2.1) (Kohn-Nirenberg [3], Olejnik [1], Višik and Grušin [1, 2]).

2.3. *Local solvability of pseudo-differential equations.*

The close analogy between pseudo-differential and differential operators allows one to extend the existence and non-existence theorems originally given for differential operators by Hans Lewy and the author (see Hörmander [1, chap. VI, VIII]). The result is (Hörmander [5]):

a) If for some $(x, \xi) \in X \times (\mathbb{R}^n \backslash 0)$ the principal symbol a of A vanishes but $\operatorname{Im}\{a, \bar{a}\} < 0$, then the equation $Au = f$ has no solution in any neighborhood of x if $f \in C^\infty$ avoids a certain set of the first category.

b) If $\operatorname{Im}\{a, \bar{a}\} \geqq \operatorname{Re} ba$ for some smooth homogeneous b, it follows that A is solvable, that is, there exist at least local solutions of the equation $Au = f$.

There is of course a wide gap between the conditions *a*) and *b*) above. This has now been filled to a large extent by work of Nirenberg-Trèves [1, 2] and of Egorov [2, 3]. Since reports on these results are given by F. Trèves and Yu. V. Egorov in these proceedings, we shall not give any details here. Instead we shall give an application of the results above to boundary problems. As an example we take the boundary problem

$$\Delta u = 0 \quad \text{in} \quad X, \qquad \partial u/\partial \nu = f \quad \text{on} \quad \partial X$$

where ν is a non-vanishing vector field on ∂X such that the equation $\langle \nu, N \rangle = 0$ defines a non-singular submanifold Y of ∂X, if N is the interior normal of ∂X. If on Y the derivative of $\langle \nu, N \rangle$ in the direction ν (which is tangential to ∂X on Y) is negative, we obtain (local) solvability but no regularity theorem whereas there is a strong non-existence theorem but regularity of solutions (when they exist) in the opposite case (cf. Borelli [1], Hörmander [5]). This strange result was explained by Egorov and Kondrat'ev [1] who found that in the two cases one should respectively introduce an additional boundary condition on Y or allow a discontinuity on Y. The problem then becomes well posed and solutions are smooth apart from a smooth jump. Using the reduction described in section 2.1 one can view this as a result on a certain pseudo-differential operator which is elliptic outside a submanifold Y of codimension one. A general theorem of this type has been proved by Eškin (to appear in *Mat. Sbornik*). More generally still J. Sjöstrand has shown (to appear in *C. R. Acad. Sci. Paris*) that if $\{a, \bar{a}\} \neq 0$ and $\partial a/\partial \xi$ is proportional to a real vector when $a = 0$, then it is possible to modify the requirements on u in a similar way on an immersed submanifold so that an essentially correctly posed problem is obtained.

2.4. *Propagation of singularities.*

For differential operators with variable coefficients or more generally pseudo-differential operators we shall now discuss an analogue of the result of Grušin [1] mentioned in section 1.2. The first point is to refine the notion of singular support.

If $u \in \mathscr{D}'(X)$ we have by definition

$$\text{sing supp } u = \cap \{ x;\ \varphi(x) = 0 \}$$

the intersection being taken over all $\varphi \in C^\infty(X)$ with $\varphi u \in C^\infty(X)$. Replacing the function φ by a compactly supported pseudo-differential operator A, with principal symbol denoted by a, we introduce

$$WF(u) = \bigcap_{Au \in C^\infty} \{ (x, \xi) \in T^*(X)\backslash 0,\ a(x, \xi) = 0 \}. \tag{2.4.1}$$

It is clear that this is a closed cone in $T^*(X)\backslash 0$ with projection in X contained in sing supp u, and the regularity of solutions of elliptic equations gives easily that the projection is precisely equal to sing supp u. It may be useful to think of $WF(u)$ as the set of all wave fronts contributing to the singularities of u. A similar concept has been given by M. Sato in the case of hyperfunctions (see his lecture in these proceedings). Indeed, he identifies a hyperfunction modulo analytic functions with a section of a certain sheaf on the sphere bundle of $T^*(X)$, and the support of this section has properties analogous to $WF(u)$.

If $u \in \mathscr{D}'(X)$ and $Pu \in C^\infty$, where P is a pseudo-differential operator of order m with principal symbol p, it follows from the definition that

$$WF(u) \subset \{ (x, \xi);\ p(x, \xi) = 0 \}.$$

When p is real and $\partial p/\partial \xi \neq 0$ when $p = 0$ we claim that $WF(u)$ is in fact the union of bicharacteristic strips for p which of course contains the result of Grušin [1] discussed in section 1.2. In sketching the proof we may assume that $X \subset \mathbb{R}^n$ for it suffices to make a proof locally. (This would not have been the case if we had not passed to $WF(u)$.)

Assume that $(x^0, \xi^0) \in WF(u)$. This means that for some pseudo-differential operator A with $Au \in C^\infty$ the principal symbol a does not vanish at (x^0, ξ^0). We shall exhibit another operator with the same property relative to all points on the bicharacteristic strip through (x^0, ξ^0). To do so we shall construct a pseudo-differential operator B such that $[B, P] = BP - PB$ is of order $-\infty$ and $Bu \in C^\infty$ near the plane $x_n = x_n^0$, assuming that $\partial p/\partial \xi_n \neq 0$ at (x^0, ξ^0). The first condition requires first of all that if b is the principal symbol of B then $\{b, p\} = 0$, that is, b is constant on the bicharacteristic strips of p. Clearly we can choose b in this way so that b is 1 at (x^0, ξ^0) but vanishes outside a small conical neighborhood of the bicharacteristic strip through (x^0, ξ^0). The support of b will then lie in the set where $a \neq 0$ if x_n is close to x_n^0. The lower order terms of B can then be chosen successively with the same support so that $[B, P]$ is of order $-\infty$. Thus

$$PBu = BPu + [P, B]u \in C^\infty.$$

Now it is easy to find an elliptic operator R such that the symbol of RP differs from that of a hyperbolic pseudo-differential operator $Q = D_n - \tau_1(x, D') + \tau_0(x, D')$ only by a term of order $-\infty$ in the support of all terms in the symbol of B. Here

τ_1 is a homogeneous real valued function of degree 1 and τ_0 is of degree 0, $D' = (D_1, \ldots, D_{n-1})$. Hence $QBu \in C^\infty$. The standard construction of a parametrix finally shows that there is a pseudo-differential operator C such that $B - CA$ is of order $-\infty$ near the plane $x_n = x_n^0$. Thus $Bu = CAu + (B - CA)u \in C^\infty$ for x_n near x_n^0, so the simplest results on hyperbolic operators suffice to show that $Bu \in C^\infty$. Since the principal symbol of B is 1 on the bicharacteristic strip through (x^0, ξ^0) it cannot meet $WF(u)$, which proves the assertion.

We remark that the preceding result improves the existence theorems given in Hörmander [1, section 8.7] for operators of real principal type.

2.5. *Fourier integral operators.*

The calculus of pseudo-differential operators has to be extended if one wants to construct a (left) parametrix for an operator which is not hypoelliptic. The form which such an extension should take is suggested by the approximate solutions given by the asymptotic expansions of geometrical optics. These were adapted by Lax [1] to determine the location of the singularities of the solutions of the Cauchy problem for a hyperbolic operator of arbitrary order. His local result was globalized by Ludwig [1], and his constructions were developed and applied by Hörmander [8] to give improved and in a sense optimal error estimates in the asymptotic formulas for the spectral function of an elliptic operator. The best earlier results due to Agmon and Kannai [1], Hörmander [12] were based, roughly speaking, on the approximations to fundamental solutions given by the techniques of pseudo-differential operators. Closely related ideas have been developed by some Russian mathematicians (Maslov [1, 2], Eškin [1], Egorov [1]) and they play an essential role in the work of Egorov and Nirenberg-Trèves mentioned in section 2.3. The work of Maslov seems to be quite farreaching but is very inaccessible and perhaps not quite rigorous so we must content ourselves with a reference to the explanations given by him at this congress. A systematic development of an enlarged operator calculus has also been undertaken recently by Hörmander [11], and in joint work with J. J. Duistermaat, still unpublished, it has been applied to give a global construction of a parametrix for arbitrary operators of real principal type, and of solutions with a given bicharacteristic strip as wave front set. This work also shows that the condition $\partial p/\partial\xi \neq 0$ can be dropped in section 2.4.

2.6. *Over-determined systems.*

In section 1.1 we mentioned how existence theorems for the system $\bar\partial u = f$ of Cauchy-Riemann equations in the theory of functions of several complex variables are obtained from the solution of the $\bar\partial$ Neuman problem. The same technique can be applied to various related equations (see Sweeney [1], McKichan [1]) but the hopes of obtaining a general theory of overdetermined systems with variable coefficients from this approach have not been fulfilled so far. For a generic overdetermined system Spencer [1] introduced a sequence of first order operators, now called the Spencer sequence, which is formally exact. The desired local existence theorems for the original equation are equivalent to exactness of the Spencer sequence on the sheaf of germs of C^∞ functions. The algebraic machinery for the study of the Spencer sequence has been highly polished (see the survey article by Spencer [2] and the references there) but analytic results on exactness of the desired generality have not yet been obtained (For very recent progress we refer to the lectures by Guillemin and Kuranishi in these proceedings). However, an interesting new line of investigation is suggested by the recent progress by Henkin [1, 2], Kerzman [1], Grauert and Lieb [1], Lieb [1], Øvrelid [1], Ramierez de Arellano [1] concerning the construction of kernels which reproduce solutions of $\bar{\partial}u = 0$ or solve the equation $\bar{\partial}u = f$. If these constructions could be adapted to more general systems with constant coefficients it seems reasonable to expect that the techniques of Fourier integral operators mentioned in section 2.5 would allow the study of suitable classes of systems with variable coefficients.

3. Equations with analytic coefficients.

3.1. *Hyperfunctions.*

In the study of differential operators with C^∞ coefficients it is natural to work with Schwartz distributions which form the largest class on which all such operators are defined. However, when the coefficients are real analytic it is possible to work within the larger frame of Sato hyperfunctions (Sato [1], Martineau [1]). During the past few years much work has been done along such lines which has given many results parallel to those for Schwartz distributions. We must content ourselves here with referring to the survey by Schapira [1] and the lecture by M. Sato in these proceedings.

3.2. *Uniformization.*

A study of the Cauchy problem with data on a hypersurface which is partly characteristic was initiated by Leray [1]. He found that the solution ramifies around the variety generated by the bicharacteristics passing through the characteristic points of the initial surface. A detailed analysis was given by Gårding, Kotake and Leray [1] in the case of linear systems. Later Choquet-Burhat [1] has simplified the proofs and extended the general result to non-linear equations.

REFERENCES

S. Agmon, A. Douglis and L. Nirenberg. — [1] Estimates near the boundary for solutions of elliptic partial differential equations satisfying general boundary conditions. I. *Comm. Pure Appl. Math.*, 12 (1959), pp. 623-727. II. *Comm. Pure Appl. Math.*, 17 (1964), pp. 35-94.

S. Agmon and Y. Kannai. — [1] On the asymptotic behavior of spectral functions and resolvent kernels of elliptic operators, *Israel J. Math.*, 5 (1967), pp. 1-30.

K. G. Andersson. — [1] Propagation of analyticity of solutions of partial differential equations with constant coefficients, *Ark. för Matematik*, 8 (1970).

M. Atiyah, R. Bott and L. Gårding. — [1] Lacunas for hyperbolic differential operators with constant coefficients I *Acta Math.*, 124 (1970), pp. 109-189.

M. F. Atiyah and I. M. Singer. — [1] The index of elliptic operators I, III, *Ann. Math.*, 87 (1968), pp. 484-530 and 546-604.

R. L. Borelli. — [1] *A priori* estimates for a class of second order non-regular boundary problems. Thesis, U. of California, Berkeley (1963).

L. Boutet de Monvel. — [1] Comportement d'un opérateur pseudo-différentiel sur une variété à bord, *J. Anal. Math.*, 17 (1966), pp. 241-304.

—. — [2] Boundary problems for pseudo-differential operators. To appear.

A. P. Calderón. — [1] Uniqueness in the Cauchy problem for partial differential equations, *Amer. J. Math.*, 80 (1958), pp. 16-36.

—. — [2] Boundary value problems for elliptic equations, *Outlines of the joint Soviet-American symposium on partial differential equations*, Novosibirsk 1963, pp. 303-304.
— and A. ZYGMUND. — [1] Singular integral operators and differential equations, *Amer. J. Math.*, 79 (1957), pp. 901-921.
Y. CHOQUET-BRUHAT. — [1] Uniformisation de la solution d'un problème de Cauchy non linéaire, à données holomorphes, *Bull. Soc. Math. France*, 94 (1966), pp. 25-48.
Yu. V. EGOROV. — [1] On canonical transformations of pseudo-differential operators, *Uspehi Mat. Nauk*, 25 (1969), pp. 235-236.
—. — [2] On subelliptic pseudo-differential operators, *Dokl. Akad. Nauk SSSR*, 188 (1969), pp. 20-22. Also in *Soviet Math. Dokl.*, 10 (1969), pp. 1056-1059.
—. — [3] Non-degenerate subelliptic pseudo-differential operators, *Mat. Sbornik*, 82 (124) (1970), pp. 324-342.
— and V. A. KONDRAT'EV. — [1] The oblique derivative problem, *Mat. Sbornik*, 78 (120) (1969). Also in *Math. USSR Sbornik*, 7 (1969), pp. 139-169.
L. EHRENPREIS. — [1] A fundamental principle for systems of linear differential equations with constant coefficients and some of its applications, *Proc. Intern. Symp. on Linear Spaces*, Jerusalem 1961, pp. 161-174.
—. — [2] Fourier analysis in several complex variables. Wiley-Interscience publishers, New York, 1970.
G. I. EŠKIN. — [1] The Cauchy problem for hyperbolic systems in convolutions, *Mat. Sbornik*, 74 (116) (1967), pp. 262-297. Also in *Math. USSR, Sbornik*, 3 (1967), pp. 243-277.
—. — [2] Degenerating elliptic pseudodifferential equations of principal type. *Mat. Sbornik*, 82 (124) (1970), pp. 585-628.
A. M. GABRIELOV. — [1] On a theorem of Hörmander, *Funkt. anal. i evo pril.*, 4 (1970), pp. 18-22.
L. GÅRDING. — [1] Some trends and problems in linear partial differential equations, *Proc. Int. Congr. Math. Edinburgh*, 1958, pp. 87-102.
—, T. KOTAKE and J. LERAY. — [1] Uniformisation et développement asymptotique de la solution du problème de Cauchy linéaire à données holomorphes; analogie avec la théorie des ondes asymptotiques et approchées (Problème de Cauchy I *bis* et VI), *Bull. Soc. Math. France*, 92 (1964), pp. 263-361.
S. G. GINDIKIN. — [1] A generalization of parabolic differential operators to the case of multi-dimensional time, *Dokl. Akad. Nauk SSSR*, 173 (1967), pp. 499-502. Also in *Soviet Math. Dokl.*, 8 (1967), pp. 410-414.
H. GRAUERT and I. LIEB. — [1] Das Ramirezsche Integral und die Gleichung $\bar{\partial} f = \alpha$ im Bereich der Beschränkten Formen. To appear in *Rice Univ. Studies*.
V. V. GRUŠIN. — [1] The extension of smoothness of solutions of differential equations of principal type, *Dokl. Akad. Nauk SSSR*, 148 (1963), pp. 1241-1244. Also in *Soviet Math. Dokl.*, 4 (1963), pp. 248-252.
G. M. HENKIN. — [1] Integral representations of functions holomorphic in strictly pseudo-convex domains and some applications, *Mat. Sbornik*, 70 (120) (1969), pp. 611-632.
—. — [2] Integral representations of functions in strictly pseudoconvex domains and applications to the $\bar{\partial}$ problem, *Mat. Sbornik*, 82 (124) (1970), pp. 300-308.
L. HÖRMANDER. — [1] Linear partial differential operators, *Grundl. d. Math. Wiss.*, 116, Springer Verlag, 1963.
—. — [2] *An introduction to complex analysis in several variables*. D. van Nostrand Publ. Co., Princeton, N. J., 1965.
—. — [3] L^2 estimates and existence theorems for the $\bar{\partial}$ operator. *Acta Math.*, 113 (1965), pp. 89-152.
—. — [4] Pseudo-differential operators, *Comm. Pure Appl. Math.*, 18 (1965), pp. 501-517.
—. — [5] Pseudo-differential operators and non-elliptic boundary problems, *Ann. Math.*, 83 (1966), pp. 129-209.
—. — [6] Pseudo-differential operators and hypoelliptic equations, *Amer. Math. Soc. Symp. on Singular Integral Operators*, 1966, pp. 138-183.

—. — [7] Hypoelliptic second order differential equations, *Acta Math.*, 119 (1967), pp. 147-171.
—. — [8] The spectral function of an elliptic operator, *Acta Math.*, 121 (1968), pp. 193-218.
—. — [9] On the characteristic Cauchy problem, *Ann. Math.*, 88 (1968), pp. 341-370.
—. — [10] On the singularities of solutions of partial differential equations, *Comm. Pure Appl. Math.*, 23 (1970), pp. 329-358.
—. — [11] The calculus of Fourier integral operators. To be published in « *Prospects in Mathematics* » by Princeton University Press.
—. — [12] On the Riesz means of spectral functions and eigenfunction expansions for elliptic differential operators, *Belfer Graduate School Science Conference*, November 1966, pp. 155-202, New York, 1970.
N. KERZMAN. — [1] Hölder and L^p estimates for solutions of $\bar{\partial} u = f$ in strongly pseudo-convex domains, *Bull. Amer. Math. Soc.*, 76 (1970), pp. 860-864.
J. J. KOHN. — [1] Harmonic integrals on strongly pseudo-convex manifolds I, *Ann. Math.*, 78 (1963), pp. 206-213; II, *Ann. Math.*, 79 (1964), pp. 450-472.
— and L. NIRENBERG. — [1] Non-coercive boundary problems, *Comm. Pure Appl. Math.*, 18 (1965), pp. 443-492.
—. — [2] On the algebra of pseudo-differential operators, *Comm. Pure Appl. Math.*, 18 (1965), pp. 269-305.
—. — [3] Degenerate elliptic parabolic equations of second order, *Comm. Pure Appl. Math.*, 20 (1967), pp. 797-872.
P. D. LAX. — [1] Asymptotic solutions of oscillatory initial value problems, *Duke Math. J.*, 24 (1957), pp. 627-646.
J. LERAY. — [1] Uniformisation de la solution du problème linéaire analytique de Cauchy près de la variété qui porte les données de Cauchy, *Bull. Soc. Math. France*, 85 (1957), pp. 398-429.
I. LIEB. — [1] Beschränktheitsaussagen für den d'' Operator. To appear.
D. LUDWIG. — [1] Exact and asymptotic solutions of the Cauchy problem, *Comm. Pure Appl. Math.*, 13 (1960), pp. 473-508.
B. MALGRANGE. — [1] Existence et approximation des solutions des équations aux dérivées partielles et des équations de convolution, *Ann. Inst. Fourier Grenoble*, 6 (1955-1956), pp. 271-355.
—. — [2] Sur les systèmes différentiels à coefficients constants, *Coll. C. N. R. S.*, pp. 113-122, Paris, 1963.
—. — [3] Sur les ouverts convexes par rapport à un opérateur différentiel, *C. R. Acad. Sci. Paris*, 254 (1962), pp. 614-615.
A. MARTINEAU. — [1] Les hyperfonctions de M. SATO, *Sém. Bourbaki*, 214 (1960-1961).
V. P. MASLOV. — [1] Theory of perturbations and asymptotic methods, *Moskov. Gos. Univ.*, Moscow 1965 (Russian).
—. — [2] Regularization of the Cauchy problem for pseudo-differential equations, *Dokl. Akad. Nauk SSSR*, 177 (1967), pp. 1277-1280. Also in *Soviet Math. Dokl.*, 8 (1967), pp. 1588-1591.
B. MCKICHAN. — [1] A generalization to overdetermined systems of the notion of diagonal operators. I. Elliptic operators. To appear in *Acta Math.*
C. B. MORREY. — [1] The analytic embedding of abstract real analytic manifolds, *Ann. Math.*, 68 (1958), pp. 159-201.
L. NIRENBERG and F. TRÈVES. — [1] Solvability of a first order linear partial differential equation, *Comm. Pure Appl. Math.*, 14 (1963), pp. 331-351.
—. — [2] On local solvability of linear partial differential equations. Part I: Necessary conditions. Part II: Sufficient conditions, *Comm. Pure Appl. Math.*, 23 (1970), pp. 1-38 and 459-510.
O. A. OLEJNIK. — [1] On linear second order equations with non-negative characteristic form, *Mat. Sbornik*, 69 (1966), pp. 111-140.

N. ØVRELID. — [1] Integral representations and L^p estimates of differential forms for the $\bar{\partial}$ operator. To appear in *Math. Scand.*

V. P. PALAMODOV. — [1] *Linear differential operators with constant coefficients.* Moscow, 1967 (Russian). Also *Grundl. d. Math. Wiss.*, 168, Springer Verlag, 1970.

E. V. RADKEVIČ. — [1] On a theorem of L. Hörmander, *Uspehi Mat. Nauk SSSR*, 24, 1 (145) (1969), pp. 199-200.

—. — [2] *A priori* estimates and hypoelliptic operators with multiple characteristics, *Dokl. Akad. Nauk SSSR*, 187 (1969), pp. 274-277.

E. RAMIEREZ DE ARELLANO. — [1] Ein Divisionsproblem und Randintegraldarstellungen in der komplexen Analysis, *Math. Ann.*, 184 (1970), pp. 172-187.

M. SATO. — [1] Theory of hyperfunctions, I-II, *Journ. Fac. Sci. Univ. Tokyo*, 8 (1959-1960), pp. 139-193 and 387-437.

P. SCHAPIRA. — [1] Théorie des hyperfonctions. *Springer lecture notes in mathematics*, 126 (1970).

R. T. SEELEY. — [1] Singular integrals and boundary problems, *Amer. J. Math.*, 88 (1966), pp. 781-809.

D. C. SPENCER. — [1] Deformation of structures on manifolds defined by transitive, continuous pseudogroups I-II, *Ann. Math.*, 76 (1962), pp. 306-445.

—. — [2] Overdetermined systems of linear partial differential equations, *Bull. Amer. Math. Soc.*, 75 (1969), pp. 179-239.

W. J. SWEENEY. — [1] A uniqueness theorem for the Neumann problem, *Ann. Math.*, 90 (1969), pp. 353-360.

F. TRÈVES. — [1] Hypoelliptic partial differential equations of principal type with analytic coefficients. To appear.

—. — [2] *Linear partial differential equations with constant coefficients.* Gordon and Breach, New York, 1966.

M. I. VIŠIK and G. I. EŠKIN. — [1] Convolution equations in bounded domains, *Usp. Mat. Nauk*, 20, 3 (123) (1965), pp. 89-152 (Russian).

—. — [2] Convolution equations in bounded domains in spaces with weighted norms, *Mat. Sb.*, 69 (111) (1966), pp. 65-110 (Russian).

—. — [3] Elliptic convolution equations in bounded domains and their applications, *Usp. Mat. Nauk*, 22, 1 (133) (1967), pp. 15-76 (Russian).

—. — [4] Convolution equations with variable order, *Trudy Moskov. Mat. Obsc.*, 16 (1967), pp. 25-50 (Russian).

—. — [5] Normally solvable problems for elliptic systems of convolution equations, *Mat. Sb.*, 74 (116) (1967), pp. 326-356 (Russian).

M. I. VIŠIK and V. V. GRUŠIN. — [1] On a class of degenerating elliptic equations of higher order, *Mat. Sb.*, 79 (121) (1969), pp. 3-36 (Russian).

—. — [2] Boundary problems for elliptic equations degenerating on the boundary of the domain, *Mat. Sb.*, 80 (122) (1969), pp. 455-491 (Russian).

E. C. ZACHMANOGLOU. — [1] Uniqueness of the Cauchy problem when the initial surface contains characteristic points, *Arch. Rat. Mach. Anal.*, 23 (1966), pp. 317-326.

—. — [2] Non-uniqueness of the Cauchy problem for linear partial differential equations with variable coefficients, *Arch. Rat. Mech. Anal.*, 27 (1968), pp. 373-384.

University of Lund
Department of Mathematics,
Fack 725, S-220 07 Lund
(Suède)

Actes, Congrès intern. math., 1970. Tome 1, p. 135 à 140.

SCATTERING THEORY AND PERTURBATION OF CONTINUOUS SPECTRA

by Tosio KATO

At this Congress in 1950 the late Professor F. Rellich [49] gave a lecture entitled " Störungstheorie der Spektralzerlegung ". It was a survey of results known at that time regarding the perturbation of the spectral properties of linear operators. The emphasis was laid on the behavior of isolated eigenvalues and the associated eigenvectors. There was no detailed account of continuous spectra, although the results [18, 19] of Friedrichs were described; in fact there were rather few results known. During the past twenty years, however, there has been great progress in this direction. It is my pleasure to be able to give a survey of the major developments.

To begin with, I have some remarks concerning the nature of the problem. We are not considering a sharply defined mathematical problem; rather the problem itself evolves with the development of the methods to solve it. Also, it is closely connected with physical problems, in particular, scattering theory (classical as well as quantum-mechanical). It is my aim to survey those results concerning the perturbation of continuous spectra that are more or less related to scattering theory, with some applications to differential equations. But I shall restrict myself to *abstract scattering theory*, which works in the framework of operator theory, thereby omitting results obtained by more concrete analytical methods. For very recent results I refer you to the lecture by Professor Kuroda. Also there will be a lecture by Professor Phillips on scattering theory.

1. Let me start by reviewing what was known in 1950. It had long been known that the *essential spectrum* was stable under perturbation by a compact operator but the *continuous spectrum* was rather unstable. (Here and in what follows all operators are assumed to be linear.) But these results are not in the direction of our interest here.

Another result, far more important for our purpose, was given by Friedrichs [18] in 1938 and was mentioned in Rellich's lecture. I repeat it in a specialized form. In the Hilbert space $\mathbf{H} = L^2(a, b)$ consider the operator H_1 of multiplication: $H_1 u(\lambda) = \lambda u(\lambda)$, and perturb it by the addition of a symmetric integral operator:

$$H_2 = H_1 + \varepsilon V, \quad Vu(\lambda) = \int_a^b k(\lambda, \mu)u(\mu)d\mu, \quad \overline{k(\lambda, \mu)} = k(\mu, \lambda).$$

Friedrichs shows that H_1 and H_2 are unitarily equivalent (so that H_2 has a pure continuous spectrum ranging over $[a, b]$) if the kernel k is Hölder-continuous, vanishes on the boundary of the square $[a, b] \times [a, b]$, and if $|\varepsilon|$ is sufficiently small. This is done by constructing two unitary operators $U_\pm$ that implement the unitary equivalence: $H_2 = U_\pm H_1 U_\pm^{-1}$.

This result is not so special as might appear at first sight. All subsequent developments I am going to discuss are more or less related to it.

The significance of Friedrichs' result became clear later, when gereral scattering theory was developed by physicists. In 1943 Heisenberg [23] introduced the notion of the *S-matrix*, or *scattering operator* as mathematicians now prefer to call it. The formal theory of scattering was further developed by Møller [45], who introduced the *wave operators.* As was shown by Friedrichs [19], his model of 1938 contained essentially all the proofs necessary to define these notions rigorously. The operators $U_\pm$ which he constructed were exactly the wave operators, by which the scattering operator is expressed as $S = U_+^{-1}U_-$. These results were greatly generalized by Friedrichs in [19] and [21].

Here we have another example of a recurrent phenomenon. The mathematical tools were ready when physicists needed them, although this was not recognized immediately. Friedrichs remarked in [20] that it was strange that such a natural notion as the scattering operator had not appeared earlier. It seems to me no less remarkable that the paper of Friedrichs, written before the advent of this notion, contained all the tools necessary for its rigorous construction.

2. Let me sketch a formulation of scattering theory in the simple case of *single-channel scattering*, following Jauch [29] but with a slight modification. Consider two unitary groups e^{-itH_j}, $j = 1, 2$, $-\infty < t < \infty$, in a Hilbert space $\mathbf{H}$, with selfadjoint generators $H_j = \int_{-\infty}^{\infty} \lambda dE_j(\lambda)$. Let P_j be the orthogonal projection onto the *subspace of absolute continuity* for H_j (the set of all $u \in \mathbf{H}$ such that $(E_j(.)u, u)$ is absolutely continuous with respect to Lebesgue measure). P_j commutes with H_j.

Suppose that the strong limits

$$(W) \qquad W_\pm = W_\pm(H_2, H_1) = \lim_{t\to\pm\infty} e^{itH_2}e^{-itH_1}P_1$$

exist; we call them the (generalized) *wave operators* for the pair H_1, H_2. $W_\pm$ are partial isometries with the initial set $P_1\mathbf{H}$ and intertwine H_1 and H_2: $H_2W_\pm \supset W_\pm H_1$. It follows that the final sets (ranges) of $W_\pm$ are subsets of $P_2\mathbf{H}$. If they coincide with $P_2\mathbf{H}$, we say that the wave operators $W_\pm$ are *complete.* In this case the absolutely continuous parts of H_1 and H_2 are unitarily equivalent; this is why the wave operators are interesting mathematically.

The *scattering operator* is defined by $S = W_+^*W_-$; it commutes with H_1, and is unitary in $P_1\mathbf{H}$ if $W_\pm$ are complete. S contains all information about scattering, and is physically most important. In accordance with the canonical direct integral decomposition $P_1\mathbf{H} = \int\oplus\, \mathbf{H}(\lambda)d\lambda$ of $P_1\mathbf{H}$ by which the absolutely continuous part of H_1 is diagonalized: $H_1P_1 = \int\oplus\, \lambda I(\lambda)d\lambda$, where $I(\lambda)$ is the identity operator in $\mathbf{H}(\lambda)$, S is expressed as the direct integral $S = \int\oplus\, S(\lambda)d\lambda$, where $S(\lambda)$ is unitary in $\mathbf{H}(\lambda)$. $S(\lambda)$ is called the *S-matrix* or the *scattering suboperator.*

In most applications H_1 is absolutely continuous so that $P_1 = I$, but it has been found convenient to define $W_\pm$ as above in the general case. There is no *a priori* reason why $P_j\mathbf{H}$ should be the subspaces of *absolute* rather than mere continuity. As it turns out, however, more existence theorems can be proved by the above definition than otherwise, which indicates that it is an adequate definition. In fact, one of the important results of scattering theory is the discovery that the absolutely continuous spectrum is rather stable under perturbation, whereas the continuous spectrum is quite unstable (cf. Aronszajn [1]).

Thus the first mathematical questions are the existence and completeness of the wave operators. They have been answered affirmatively in the Friedrichs model, but it does not cover all interesting applications. Many attempts have been made to give useful sufficient conditions. I would like to discuss some of the methods and results, together with some typical applications.

3. There have been proposed two different methods: *time-dependent* and *stationary*, although these are often used in conjunction. The time-dependent method works with the groups e^{-itH_j} directly. In this way it is rather easy to deduce general properties of the wave operators and give useful sufficient conditions for their existence, as was shown by Cook [13], Kuroda [39], and others. The completeness is more difficult to establish. But a very simple condition for the existence and completeness was obtained by Rosenblum [50] and Kato [31, 34] in the form $H_2 = H_1 + V$, $V \in B_1(\mathbf{H})$, where $B_1(\mathbf{H})$ is the *trace class* of compact operators in $\mathbf{H}$. It is interesting to note that $B_1(\mathbf{H})$ is practically the only class with this property (Kuroda [38]). This condition was later generalized by many authors. Here we mention the useful criterion, due to Birman and Krein [10] and de Branges [11], that $R_2(z) - R_1(z) \in B_1(\mathbf{H})$ for some $z \in \rho(H_1) \cap \rho(H_2)$, where $R_j(z) = (H_j - zI)^{-1}$ and ρ denotes the resolvent set. It was also shown [10] that in this case $S(\lambda) - I(\lambda) \in B_1(\mathbf{H}(\lambda))$ for almost all real λ.

In this connection I note the *invariance principle* for the wave operators. It asserts that $W_\pm(\phi(H_2), \phi(H_1)) = W_\pm(H_2, H_1)$ holds for any real-valued, piecewise monotone increasing function ϕ with a certain continuity property. The invariance principle has not been proved in general, but it has been shown to hold in most of the cases in which the existence and completeness of $W_\pm(H_2, H_1)$ has been proved (Birman [5], Kato [32, 34], Kuroda [40], Kato and Kuroda [37]). It easily leads to many new and old criteria, for example $H_2^{-\alpha} - H_1^{-\alpha} \in B_1(\mathbf{H})$ for some $\alpha > 0$ when H_1, H_2 have positive lower bounds (Birman [3]).

These criteria have been applied successfully to differential operators, including single-particle Schrödinger operators. For example, consider the operators in $\mathbf{H} = L^2(R^n)$

$$(A_n) \qquad \begin{aligned} H_1 &= -\Delta, \\ H_2 &= -\sum_{j,k=1}^{n} \frac{\partial}{\partial x_j} a_{jk}(x) \frac{\partial}{\partial x_k} + \frac{1}{i} \sum_{j=1}^{n} \left[b_j(x) \frac{\partial}{\partial x_j} + \frac{\partial}{\partial x_j} b_j(x) \right] + q(x), \end{aligned}$$

where $a_{jk}(x)$, $b_j(x)$, $q(x)$ are real-valued and the symmetric matrix $(a_{jk}(x))$ is positive-definite. We refer to the special case $a_{jk}(x) = \delta_{jk}$, $b_j(x) = 0$ as (A_n^0). It was shown in [39] that $q \in L^1 \cap L^2$ is sufficient for the existence and completeness of $W_\pm$ for (A_3^0). Ikebe and Tayoshi [28] show that, roughly, a similar decay rate for the $a_{jk} - \delta_{jk}$, b_j, and q is sufficient for (A_3), certain smoothness conditions being assumed for the a_{jk} and b_j. The existence of $W_\pm$ has been proved under weaker conditions. Another interesting result, due to Birman [4], is the invariance of the absolutely continuous spectrum of a differential operator on an exterior domain when the boundary and the boundary conditions are changed.

4. The stationary method, on the other hand, has many variants. In general they work with the resolvents $R_j(z)$ rather than the groups e^{-itH_j}, of which the resolvents

are the Laplace transforms. Roughly speaking, one tries to define two operators $U_\pm$ by

$$(U)\quad U_\pm = \int_{-\infty}^{\infty} E_2'(\lambda)(I + VR_1(\lambda \pm i0))P_1 d\lambda = \int_{-\infty}^{\infty} (I - VR_2(\lambda \pm i0))E_1'(\lambda)P_1 d\lambda,$$

where $V = H_2 - H_1$ formally, and show that they have all (or some of) the properties of the wave operators. (U) may be deduced by a formal Fourier transformation from (W), but it has no precise meaning as it stands. The various stationary methods arise from different attempts to interpret (U) rigorously. Since the derivatives $E_j'(\lambda)$ and the boundary values $VR_j(\lambda \pm i0)$ do not exist in the ordinary topologies, one has to introduce new topologies in certain spaces of operators. There are many ways to do this but it is impossible to describe them in detail here. Unfortunately there are few theorems in the stationary methods that can be stated concisely.

It has turned out, however, that the stationary methods are on the whole more powerful than the time-dependent one. The main advantages are the following. 1) One may prove the unitary equivalence of H_1P_1 and H_2P_2 without proving $U_\pm = W_\pm$ completely. 2) Possibility of *localization*: one may define $U_\pm$ only on a subspace $E_1(\Gamma)\mathbf{H}$ to $E_2(\Gamma)\mathbf{H}$, where $\Gamma \subset R^1$. 3) Often one can obtain some information on the *singular parts* $H_j(I - P_j)$, for example their non-existence.

The stationary methods have been studied vigorously in the recent years. The original method of Friedrichs may be regarded as one of them, although it cannot be written directly in the form (U). The perturbations V permitted in this method are called *gentle perturbations*. They were further studied by Faddeev [17] and Rejto [47], who later arrived at the very general notion of *partly gentle* perturbations [48]. An analogous notion was introduced by Howland [25] independently. Roughly speaking, V is partly gentle if there is a Banach space $\mathbf{X}$, partly contained in $\mathbf{H}$, such that *i)* $d(E_j(\lambda)u, v)/d\lambda$ exist as continuous sesquilinear forms in $u, v \in \mathbf{X}$ for each $\lambda \in \Gamma$ and *ii)* the $VR_j(z)$ map $\mathbf{X}$ into itself continuously and have boundary values when z approaches the two edges of the part Γ of the real axis.

Birman and Entina [9], on the other hand, give a more direct interpretation of (U), assuming the trace condition $V \in B_1(\mathbf{H})$ or its generalizations. Birman [6] gives " local " criteria, which are most useful in applications to differential operators as shown in [7]. For example, sufficient conditions analogous to those of [28] are deduced for (A_n); one can even admit as H_2 differential operators of higher order than H_1 if one does not insist on the completeness of $W_\pm$.

Another interpretation of (U) is given by Kuroda [40] using the *factorization method.* A recent paper [37] by Kuroda and myself gives a rather general theorem that covers gentle (or " smooth ") as well as trace-type perturbations. It has been found useful in many applications. For example, in (A_n^0) it suffices to assume

$$|q(x)| \leq c(1 + |x|)^{-\beta}, \qquad \beta > 1,$$

to ensure the existence and completeness of $W_\pm$ [36]. (This is optimal in a certain sense in view of the result of Dollard [14] for the Coulomb potential.) Kuroda [41] generalizes it to cases when q need not be locally bounded. He further applies the theorem to (A_n), assuming the decay rate $O(|x|^{-\beta})$, $\beta > 1$, of the $a_{jk} - \delta_{jk}$, b_j, and q; this is a substantial improvement over the results of [7] and [28] stated above. For details I refer to Kuroda [41 *a*].

I should note that some of these results pertaining to differential operators were obtained also by more concrete methods.

5. Finally I want to list other related problems and open questions.

(*a*) Two space theory. The formulation presented above is adapted to single-channel scattering for quantum-mechanical systems. For applications to classical wave equations and to more general hyperbolic systems of partial differential equations, one needs a more general formulation in which the two groups e^{-itH_j} act in different Hilbert spaces $\mathbf{H}_j$. See Belopol'skii and Birman [2], Birman [8], Kato [35], Kuroda [41 *a*], Schulenberger and Wilcox [51], Wilcox [52]. Some of these results have points of contact with the theory of Lax and Phillips [42].

(*b*) Multi-channel scattering. An abstract formulation was given by Jauch [30]. It has been verified in certain typical cases of many-particle Schrödinger operators by Hack [22], Faddeev [16], Hepp [24], Combes [12], and others. To give a more abstract treatment of this problem would seem to be one of the major open questions in scattering theory.

(*c*) Eigenfunction expansions for the absolutely continuous spectrum. In concrete problems like (A_n), one can construct eigenfunctions of H_1 and H_2 explicitly and then define the wave operators, cf. Povzner [46], Ikebe [27]. In the abstract theory one reverses this order and constructs eigenfunctions for H_2 by a refinement of the stationary method, assuming the existence of eigenfunctions for H_1. Cf. Howland [26], Kato and Kuroda [37].

(*d*) Scattering theory has been developed, though rather incompletely, for certain non-selfadjoint problems in Hilbert and Banach spaces. Cf. Kato [33], Lin [43], Mochizuki [44].

(*e*) The inverse problem. Consider the map $H_2 - H_1 = V \to S$ for a fixed H_1. One expects that the map is one-one and onto between certain classes of V and S (which should be sufficiently large) and wants to give the inverse map $S \to V$ explicitly. Unfortunately, the situation is not so simple in general; it depends greatly on H_1 and the classes employed. (For example, if H_1 is fixed arbitrarily and V is allowed to vary on $B_1(\mathbf{H})$, then the map $V \to S$ is not one-one.) Thus it does not seem easy to develop an abstract theory of the inverse problem. But many interesting results have been obtained for Schrödinger operators, especially for $n = 1$ (cf. Faddeev [15]).

BIBLIOGRAPHY

[1] N. Aronszajn. — *Amer. J. Math.*, 79 (1957), pp. 597-610.

[2] A. L. Belopol'skii and M. Sh. Birman. — *Izv. Akad. Nauk SSSR*, 32 (1968), pp. 1162-1175.

[3] M. Sh. Birman. — *Dokl. Akad. Nauk SSSR*, 143 (1962), pp. 506-509.

[4] —. — *Vestnik Leningrad. Univ.*, 1 (1962), pp. 22-55.

[5] —. — *Izv. Akad. Nauk SSSR*, 27 (1963), pp. 883-906.

[6] —. — *Ibid.*, 32 (1968), pp. 914-942.

[7] —. — *Functional Anal. Appl.*, 3 (1969), pp. 1-16.

[8] —. — *Dokl. Akad. Nauk SSSR*, 185 (1969), pp. 735-738.

[9] — and S. B. Entina. — *Izv. Akad. Nauk SSSR*, 31 (1967), pp. 401-430.

[10] — and M. G. Krein. — *Dokl. Akad. Nauk SSSR*, 144 (1962), pp. 475-478.
[11] L. de Branges. — *Amer. J. Math.*, 84 (1962), pp. 543-560.
[12] J. M. Combes. — *Nuovo Cimento*, 64A (1969), pp. 111-144.
[13] J. M. Cook. — *J. Math. Phys.*, 36 (1957), pp. 82-87.
[14] J.-D. Dollard. — *J. Mathematical Phys.*, 5 (1964), pp. 729-738.
[15] L. D. Faddeev. — *Uspehi Mat. Nauk SSSR*, 14, 4 (88) (1959), pp. 57-119.
[16] —. — *Trud. Mat. Inst. Steklov.*, 69 (1963), pp. 1-122.
[17] —. — *Ibid.*, 73 (1964), pp. 292-313.
[18] K. O. Friedrichs. — *Math. Ann.*, 115 (1938), pp. 249-272.
[19] —. — *Comm. Pure Appl. Math.*, 1 (1948), pp. 361-406.
[20] —. — The theory of wave propagation, *NYU Notes*, 1951-1952.
[21] —. — Perturbation of spectra in Hilbert space, *Amer. Math. Soc.* (1965).
[22] M. N. Hack, *Nuovo Cimentó*, 13 (1959), pp. 231-236.
[23] W. Heisenberg. — *Z. Phys.*, 120 (1943), pp. 513-538.
[24] K. Hepp. — *Helv. Phys. Acta*, 42 (1969), pp. 425-458.
[25] J. S. Howland. — *J. Math. Anal. Appl.*, 20 (1967), pp. 22-47.
[26] —. — *J. Functional Anal.*, 2 (1968), pp. 1-23.
[27] T. Ikebe. — *Arch. Rational Mech. Anal.*, 5 (1960), pp. 1-34.
[28] — and T. Tayoshi. — *Publ. RIMS Kyoto Univ.*, 4 (1969), pp. 483-496.
[29] J. M. Jauch. — *Helv. Phys. Acta*, 31 (1958), pp. 127-158.
[30] —. — *Ibid.*, pp. 661-684.
[31] T. Kato. — *Proc. Japan Acad.*, 33 (1957), pp. 260-264.
[32] —. — *Pacific J. Math.*, 15 (1965), pp. 171-180.
[33] —. — *Math. Ann.*, 162 (1966), pp. 258-279.
[34] —. — *Perturbation theory for linear operators*, Springer, 1966.
[35] —. — *J. Functional Anal.*, 1 (1967), pp. 342-369.
[36] —. — *Proc. Internat. Conf. on Functional Anal. and Related Topics*, Tokyo (1969), pp. 206-215.
[37] — and S. T. Kuroda. — *Functional Anal. and Related Fields*, Springer (1970), pp. 99-131.
[38] S. T. Kuroda. — *Proc. Japan Acad.*, 34 (1958), pp. 11-15.
[39] —. — *Nuovo Cimento*, 12 (1959), pp. 431-454.
[40] —. — *J. d'Anal. Math.*, 20 (1967), pp. 57-117.
[41] —. — *J. Fac. Sci. Univ. Tokyo*, Sec. IA, vol. 17 (1970), pp. 315-329.
[41*a*] —. — These proceedings, t. 3, D 3.
[42] P. D. Lax and R. S. Phillips. — *Scattering theory*, Academic Press (1967).
[43] S. C. Lin. — *Trans. Amer. Math. Soc.*, 139 (1969), pp. 469-494.
[44] K. Mochizuki. — *J. Math. Soc. Japan*, 19 (1967), pp. 123-158.
[45] C. Møller. — *Kgl. Danske Vid. Selsk. Mat. Fys. Medd.*, 23 (1945), pp. 2-48.
[46] A. Ya. Povzner. — *Dokl. Akad. Nauk SSSR*, 104 (1955), pp. 360-363.
[47] P. Rejto. — *Comm. Pure Appl. Math.*, 16 (1963), pp. 279-303; 17 (1964), pp. 257-292.
[48] —. — *J. Math. Anal. Appl.*, 17 (1967), pp. 453-462; 20 (1967), pp. 145-187; 27 (1969), pp. 21-67.
[49] F. Rellich. — *Proc. Internat. Congr. Math.* (1950), vol. 1, pp. 606-613.
[50] M. Rosenblum. — *Pacific J. Math.*, 7 (1957), pp. 997-1010.
[51] J. R. Schulenberger and C. H. Wilcox. — *J. Functional Anal.*, to appear.
[52] C. H. Wilcox. — *Arch. Rational Mech. Anal.*, 22 (1966), pp. 37-78.

University of California
Department of Mathematics,
Berkeley, California 94720
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 141 à 150.

MODEL THEORY

by H. JEROME KEISLER

1. Introduction

Twenty years ago, A. Robinson and A. Tarski lectured on the subject of model theory to the International Congress at Cambridge, Massachusetts. At that time the subject was just beginning, and only two real theorems were known. Since then progress has been so spectacular that today it takes years of graduate study to reach the frontier. In this lecture I will try to give an idea of what the subject is like and where it is going.

Model theory is a combination of universal algebra and logic. We start with a set L of symbols for operations, constants, and relations, called a *language*; for example, $L = \{ +, ., 0, 1, < \}$. The language L is assumed to be finite or countable except when we specify otherwise. A *model* $\mathfrak{A}$ for the language L is an object of the form

$$\mathfrak{A} = \langle A, +_{\mathfrak{A}}, \cdot_{\mathfrak{A}}, 0_{\mathfrak{A}}, 1_{\mathfrak{A}}, <_{\mathfrak{A}} \rangle.$$

A is a non-empty set, called the set of *elements* of $\mathfrak{A}$, $+_{\mathfrak{A}}$ and $\cdot_{\mathfrak{A}}$ are binary operations on $A \times A$ into A, $0_{\mathfrak{A}}$ and $1_{\mathfrak{A}}$ are elements of A, and $<_{\mathfrak{A}}$ is a binary relation on A.

EXAMPLES. — The field of rationals, $\langle Q, +, ., 0, 1 \rangle$, is a model for the language $\{ +, ., 0, 1 \}$. So is every other ring, lattice with endpoints, etc. The ordered field $\langle Q, +, ., 0, 1, < \rangle$ is a model for the language $\{ +, ., 0, 1, < \}$. Each group, partially ordered set, graph, etc., is a model for the appropriate language.

Most results in model theory apply to an arbitrary language. We frequently shift from one language to another, for instance a new theorem about a given language is often proved by applying an old theorem to a different language.

Many facts about models can be expressed in *first order logic*. In addition to the operation, relation, and constant symbols of L, first order logic has an infinite list of *variables*

$$x, y, z, v_0, v_1, v_2, \ldots,$$

the *equality symbol* $=$, the *connectives*

$$\wedge \text{ (and)}, \quad \vee \text{ (or)}, \quad \neg \text{ (not)},$$

and the *quantifiers*

$$\forall \text{ (for all)}, \quad \exists \text{ (there exists)}.$$

Certain finite sequences of symbols are counted as *terms*, *formulas*, and *sentences*. The class of *terms* is defined as follows:

Every variable or constant is a term;

If t, u are terms, so are $t + u$, $t \cdot u$.

The *formulas* are defined by the rules:

If t, u are terms, then $t = u$, $t < u$ are formulas.

If φ, ψ are formulas and v is a variable, then $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\forall v\varphi$, $\exists v\varphi$ are formulas.

A *sentence* is a formula all of whose variables are bound by quantifiers. For example, the sentence

$$\forall x\ (x = 0 \vee \exists y\ (x \cdot y = 1)) \tag{1}$$

states that every non-zero element has a right inverse.

Hereafter $\mathfrak{A} = \langle A, \dots \rangle$, $\mathfrak{B} = \langle B, \dots \rangle, \dots$ denote models for L, and φ, ψ, $\theta, \dots$ denote sentences.

The central notion in model theory is that of a sentence φ being *true* in a model $\mathfrak{A}$, in symbols $\mathfrak{A} \models \varphi$. This relation between models and sentences is defined mathematically by an induction on the subformulas of φ. It coincides exactly with the intuitive concept. For example, the sentence (1) is true in the field of rationals but not in the ring of integers. A set of sentences is called a *theory*. $\mathfrak{A}$ is a *model of* a theory T, in symbols $\mathfrak{A} \models T$, if every sentence $\varphi \in T$ is true in $\mathfrak{A}$.

Examples. — The theory of rings is the familiar finite list of ring axioms found in any modern algebra text, and each ring is a model of this theory. The theory of real closed ordered fields is an infinite set of sentences, consisting of the axioms for ordered fields, the axiom stating that every positive element has a square root, and for each odd n an axiom stating that every polynomial of degree n has a root.

For each model $\mathfrak{A}$, the *theory of* $\mathfrak{A}$, Th ($\mathfrak{A}$), is the set of all sentences true in $\mathfrak{A}$.

Model theory is a rich subject which studies the interplay between various kinds of sentences and various kinds of models.

2. Two classical theorems.

Model theory traces its beginnings to two basic theorems which come out of the 1930's. The mathematicians who proved them are the founders of the subject.

Compactness theorem. — If every finite subset of a set T of sentences has a model, then T has a model.

This theorem was first proved by Gödel, 1930 for countable languages. Malcev, 1936 extended the theorem to the case where T is a set of sentences in an uncountable language. The compactness theorem has many applications to algebra (see Robinson, 1963).

Example. — Suppose the sentence φ is true in every field of characteristic zero. Then there is an n such that φ is true in all fields of characteristic $p > n$.

Proof. — Consider the set T of sentences consisting of the field axioms, the sentence $\neg\varphi$, and the infinite set

$$\neg(1 + 1 = 0), \quad \neg(1 + 1 + 1 = 0), \quad \neg(1 + 1 + 1 + 1 = 0), \dots$$

By the hypothesis, T has no models, so some finite subset of T has no models, and the conclusion follows.

By the *cardinal* of a model $\mathfrak{A}$ we mean the cardinal of the set A of elements of $\mathfrak{A}$.

LÖWENHEIM-SKOLEM-TARSKI THEOREM. — If T has at least one infinite model, then T has a model of every infinite cardinality.

Example. — Let T be the theory of real closed fields. Then T has a model of cardinal $2^{\aleph_0}$, namely the field of real numbers. There are countable real closed fields and also real closed fields of every other infinite cardinality. The LST theorem shows that this happens in general.

Both of the theorems above assert that a certain kind of model exists, and their proofs depend on techniques for constructing models. Indeed, almost all the deeper results in model theory depend on the construction of a model. We shall indicate some of the most useful methods of constructing models and state some of the theorems which they yield.

3. The method of diagrams.

This method, due to Henkin, 1949 and Robinson, 1951, is the basis of Henkin's proof of the Gödel compleneness theorem. It also has many other uses.

The *diagram language* for $\mathfrak{A}$ is obtained by adding to L a new constant symbol $\bar{a}$ for each element a of A. The *elementary diagram* of $\mathfrak{A}$, denoted by Diag ($\mathfrak{A}$), is the set of all sentences in the diagram language of $\mathfrak{A}$ which are true in $\mathfrak{A}$. The difference between Th ($\mathfrak{A}$) and Diag ($\mathfrak{A}$) is that Diag ($\mathfrak{A}$) has new constant symbols for the elements of $\mathfrak{A}$ while Th ($\mathfrak{A}$) does not.

In many situations it is possible to construct a model of a set T of sentences by extending T to a set of sentences T' which happens to be an elementary diagram of some model $\mathfrak{A}$. In this construction one is always working with sentences, and constant symbols are used for the elements of $\mathfrak{A}$. The compactness and LST theorems can be proved by this method. The construction has many other applications; we shall state three of them without proofs.

The notation $\varphi \models \psi$ means that every model of φ is a model of ψ.

THEOREM 1 (Craig interpolation theorem, Craig, 1957, A. Robinson, 1956). — Suppose $\varphi \models \psi$. Then there is a sentence θ such that $\varphi \models \theta$, $\theta \models \psi$, and every operation, constant, or relation symbol which occurs in θ occurs in both φ and ψ.

The next theorem concerns homomorphisms. A mapping h of A onto B is called a *homomorphism*, and $\mathfrak{B}$ is called the *homomorphic image* of $\mathfrak{A}$ by h, if for all a, b, $\in A$,

$$h(a +_{\mathfrak{A}} b) = h(a) +_{\mathfrak{B}} h(b), \quad h(1_{\mathfrak{A}}) = 1_{\mathfrak{B}},$$
$$a <_{\mathfrak{A}} b \quad \text{implies} \quad h(a) <_{\mathfrak{B}} h(b),$$

etc. If h is one-one and h^{-1} is also a homomorphism, then h is called an *isomorphism*. It is obvious that every sentence φ is preserved under isomorphic images, that is, every isomorphic image of a model of φ is a model of φ. But which sentences are preserved under homomorphic images?

A sentence φ is said to be *positive* if it contains no negation symbol $\neg$, i. e. it is built using only $\wedge$, $\vee$, $\forall$, $\exists$.

THEOREM 2 (Lyndon homomorphism theorem, 1959). — A sentence φ is preserved under homomorphic images if and only if there is a positive sentence ψ which has exactly the same models as φ.

The hard direction is " only if ".

Examples. — The theories of groups, abelian groups, rings, and fields (if we allow the one element field) are preserved under homomorphic images because their axioms are positive. But the theory of integral domains is not preserved under homomorphic images. It has the axiom

$$\forall x \ \forall y \ (x = 0 \vee y = 0 \vee \neg\, x \cdot y = 0),$$

and this axiom cannot be replaced by a positive sentence.

A theory is *complete* if it is equal to Th $(\mathfrak{A})$ for some $\mathfrak{A}$. Let us consider the number of (non-isomorphic) countable models of a complete theory T.

Examples. — We have examples of complete theories with exactly one countable model (atomless Boolean algebras); $\aleph_0$ countable models (algebraically closed fields); $2^{\aleph_0}$ countable models (real closed fields); and n countable models for each $n \geq 3$ (due to Ehrenfeucht).

But the following surprising theorem is due to Vaught, 1959.

THEOREM 3. — There is no complete theory which has exactly two countable models.

4. Elementary chains.

This construction was introduced by Tarski and Vaught, 1957.

$\mathfrak{A}$ and $\mathfrak{B}$ are said to be *elementarily equivalent* if Th $(\mathfrak{A})$ = Th $(\mathfrak{B})$, that is, they are models of exactly the same sentences.

$\mathfrak{A}$ is said to be a *submodel* of $\mathfrak{B}$, $\mathfrak{A} \subset \mathfrak{B}$, if $A \subset B$ and the operations, constants, and relations of $\mathfrak{A}$ are those of $\mathfrak{B}$ restricted to A. $\mathfrak{A}$ is an *elementary submodel* of $\mathfrak{B}$, $\mathfrak{A} \prec \mathfrak{B}$, if $\mathfrak{A} \subset \mathfrak{B}$ and every sentence of Diag $(\mathfrak{A})$ is true in $\mathfrak{B}$. A simple exercice: if $\mathfrak{A} \prec \mathfrak{B}$ then $\mathfrak{A}$ and $\mathfrak{B}$ are elementarily equivalent.

Example. — Tarski, 1948 has shown that if $\mathfrak{B}$ is any real closed field and $\mathfrak{A}$ is a real closed subfield of $\mathfrak{B}$, then $\mathfrak{A} \prec \mathfrak{B}$. Similarly for algebraically closed fields. Such theories are called *model complete* (Robinson, 1963).

An *elementary chain* is a sequence of models

$$\mathfrak{A}_0, \mathfrak{A}_1, \ldots, \mathfrak{A}_\alpha, \ldots, \alpha < \gamma,$$

where γ is an ordinal, such that

$$\text{if} \quad \alpha < \beta < \gamma \quad \text{then} \quad \mathfrak{A}_\alpha \prec \mathfrak{A}_\beta .$$

The *union* of an elementary chain is the model $\mathfrak{A} = U_{\alpha<\gamma} \mathfrak{A}_\alpha$ such that $A = U_{\alpha<\gamma} A_\alpha$ and each $\mathfrak{A}_\beta$ is a submodel of $\mathfrak{A}$.

THEOREM 4 (Tarski-Vaught, 1957). — Let $\mathfrak{A}_\alpha, \alpha < \gamma$, be an elementary chain. Then each $\mathfrak{A}_\beta$ is an elementary submodel of $U_{\alpha<\gamma}\mathfrak{A}_\alpha$.

A typical application of this construction is the following Löwenheim-Skolem-Tarski type result for pairs of cardinals. For this theorem we assume that the language contains a one-placed relation symbol U. By a *model of type* $(\aleph_\alpha, \aleph_\beta)$ we mean a model $\mathfrak{A}$ such that A has cardinal $\aleph_\alpha$ and $U_{\mathfrak{A}}$ has cardinal $\aleph_\beta$.

THEOREM 5 (Vaught, 1962). — Suppose a theory T has a model of type $(\aleph_\alpha, \aleph_\beta)$ where $\aleph_\alpha > \aleph_\beta$. Then T has a model of type $(\aleph_1, \aleph_0)$.

The model $\mathfrak{A}$ of type $(\aleph_1, \aleph_0)$ is constructed as the union of an elementary chain $\mathfrak{A}_\alpha$, $\alpha < \omega_1$, of $\aleph_1$ countable models such that all the sets $U_{\mathfrak{A}_\alpha}$ are the same.

Many results in model theory depend on the Generalized Continuum Hypothesis (GCH), which states that for all infinite cardinals $\aleph_\alpha$, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$. One such result is the following.

THEOREM 6 (Chang, 1965) (GCH). — Suppose a theory T has a model of type $(\aleph_1, \aleph_0)$. Then for every $\aleph_\alpha$, T has a model of type $(\aleph_{\alpha+2}, \aleph_{\alpha+1})$.

The proof uses an elementary chain of length $\aleph_{\alpha+2}$ of models of cardinality $\aleph_{\alpha+1}$.

Example (GCH). — Let $\mathfrak{A}$ be the model

$$\mathfrak{A} = \langle R, +, ., 0, 1, <, Z \rangle.$$

where R is the set of real numbers and Z is the set of integers. $\mathfrak{A}$ is a model of type $(\aleph_1, \aleph_0)$. By Chang's theorem, Th$(\mathfrak{A})$ also has a model of type $(\aleph_2, \aleph_1)$. But Th$(\mathfrak{A})$ cannot have a model of type $(\aleph_2, \aleph_0)$.

5. Ultraproducts.

This construction was introduced by Skolem, 1934 to get a non-standard model of arithmetic and in its present general form it is due to Łós, 1955.

Let I be a non-empty set and let $\mathfrak{A}_i$, $i \in I$, be models for L. An *ultrafilter over I* is a set D of subsets of I such that D is closed under finite intersections, any superset of a member of D is in D, and for all $X \subset I$, exactly one of the sets X, $I - X$ belongs to D. A statement $P(i)$ is said to hold *almost everywhere* (D) if the set of $i \in I$ for which $P(i)$ holds is in D.

Now consider the Cartesian product $\Pi_{i\in I}A_i$. For $f, g \in \Pi_{i\in I}A_i$ we write

$$f =_D g \quad \text{iff} \quad f(i) = g(i) \text{ a. e. } (D)$$

Then $=_D$ is an equivalence relation on $\Pi_{i\in I}A_i$. Let f_D be the equivalence class of f, and $\Pi_D A_i$ the set of all equivalence classes.

The *ultraproduct* $\Pi_D\mathfrak{A}_i$ is a model with the set of elements $\Pi_D A_i$. The relation $<$ on this model is defined by

$$f_D < g_D \quad \text{iff} \quad f(i) <_{\mathfrak{A}_i} g(i) \text{ a. e. } (D).$$

The operation $+$ is defined so that

$$f_D + g_D = h_D \quad \text{iff} \quad f(i) +_{\mathfrak{A}_i} g(i) = h(i) \text{ a. e. } (D).$$

The fundamental result about ultraproducts is the following.

THEOREM 7 (Łós, 1955). — For each sentence φ, ω holds in the ultraproduct $\Pi_D \mathfrak{A}_i$ if and only if φ holds in $\mathfrak{A}_i$ almost everywhere (D).

Ultraproducts can be used to give us another proof of the Compactness Theorem. Many applications of the Compactness Theorem can be done more neatly using ultraproducts directly.

Example. — Suppose all the models $\mathfrak{A}_i$ are fields, and form the complete direct product ring $\Pi_{i\in I}\mathfrak{A}_i$. It turns out that the set of ultraproducts $\Pi_D \mathfrak{A}_i$ is exactly the same as the set of quotient fields $\Pi_{i\in I}\mathfrak{A}_i/J$ of the ring $\Pi_{i\in I}\mathfrak{A}_i$ modulo a maximal ideal J (The fields $\Pi_{i\in I}\mathfrak{A}_i/J$ were studied by Hewitt, 1948; see Gillman-Jerison, 1960).

Suppose all the models $\mathfrak{A}_i$ are the same model $\mathfrak{A}$. Then the ultraproduct $\Pi_D \mathfrak{A}$ is called an *ultrapower* of $\mathfrak{A}$. By the theorem of Łós, $\mathfrak{A}$ is elementarily equivalent to each ultrapower $\Pi_D \mathfrak{A}$.

Example (non-standard analysis, A. Robinson, 1966). — Let $\mathfrak{A}$ be the model

$$\mathfrak{A} = \langle R, +, ., 0, 1, <, \ldots \rangle$$

where R is the set of real numbers, and the three dots stand for a list of all the $2^{2^{\aleph_0}}$ operations, constants, and relations on R. Let D be an ultrafilter over the set $\omega = \{0, 1, 2, \ldots\}$ which contains no finite set. Then the ultrapower $\Pi_D \mathfrak{A}$ is a non-Archimedean real closed field; for instance, $\langle 1, 1/2, 1/3, 1/4, 1/5, \ldots \rangle_D$ is a positive infinitesimal and $\langle 1, 2, 3, \ldots \rangle_D$ is positive infinite. Using the ultrapower $\Pi_D \mathfrak{A}$, the whole subject of analysis can be based on infinitesimals in the style of Leibniz. For example, consider any real function f and real numbers c and L. Then $\lim_{x\to c} f(x) = L$ if and only if for every b in $\Pi_D A$ which is infinitely close but not equal to c, $f(b)$ is infinitely close to L.

Ultrapowers can also be used to give purely algebraic characterizations of model-theoretic notions such as elementary equivalence.

THEOREM 8 (Isomorphism theorem). — Two models $\mathfrak{A}$, $\mathfrak{B}$ are elementarily equivalent if and only if there is an ultrafilter D such that $\Pi_D \mathfrak{A}$ and $\Pi_D \mathfrak{B}$ are isomorphic.

This theorem was proved by Keisler, 1963, using the GCH, and was proved without the GCH by Shelah, 1971.

Among the important tools in model theory are the saturated models; they are used in theorems 6 and 8 above. The ultraproduct is one way of constructing such models. Let $\aleph_\alpha$ be an uncountable cardinal. $\mathfrak{A}$ is $\aleph_\alpha$*-saturated* iff for every set Φ of fewer than $\aleph_\alpha$ formulas $\varphi(x)$ in the diagram language of $\mathfrak{A}$, if for each $\varphi_1, \ldots, \varphi_n \in \Phi$ the sentence

$$\exists x \ (\varphi_1(x) \wedge \ldots \wedge \varphi_n(x))$$

is true in $\mathfrak{A}$, then the infinitely long sentence

$$\exists x \ \bigwedge_{\varphi\in\Phi} \varphi(x)$$

is true in $\mathfrak{A}$.

THEOREM 9. — Let I be a set of power $\aleph_\alpha$. There is an ultrafilter D over I such that every ultraproduct $\Pi_D \mathfrak{A}_i$ is $\aleph_{\alpha+1}$-saturated.

The above result was proved under the GCH by Keisler, 1963, and without the GCH by Kunen, 1970. $\aleph_{\alpha+1}$-saturated models were first constructed in another way by Morley-Vaught, 1962.

Example. — It turns out that a real closed field is $\aleph_\alpha$-saturated if and only if its ordering is an η_α-*set*, that is, for any two subsets X, Y of power $< \aleph_\alpha$ (perhaps empty), if $X < Y$ then there is an element z such that $X < z < Y$.

There are a number of applications of saturated models to algebra. For example, they are the main tool in the proof by Ax and Kochen, 1965 of Artin's conjecture: for each positive integer d, the following holds for all but finitely many primes p. Every polynomial in the field Q_p of p-adic numbers, with degree d, more than d^2 variables, and zero constant term, has a non-trivial zero in Q_p.

6. Indiscernibles.

Suppose we expand the language L by adding n new constant symbols $c_1, \ldots, c_n$, forming L_n. For each model $\mathfrak{A}$ for L and each n-tuple $a_1, \ldots, a_n$ of elements of $\mathfrak{A}$, we obtain a model $(\mathfrak{A}, a_1, \ldots, a_n)$ for L_n. Consider a subset X of A and a linear ordering $<$ of X, which is not necessarily one of the relations of $\mathfrak{A}$. We say that $\langle X, < \rangle$ is a set of *indiscernibles* in $\mathfrak{A}$ if for any n and any two increasing n-tuples

$$a_1 < \ldots < a_n, \qquad b_1 < \ldots < b_n$$

from $\langle X, < \rangle$, the models $(\mathfrak{A}, a_1, \ldots, a_n)$ and $(\mathfrak{A}, b_1, \ldots, b_n)$ are elementarily equivalent. The basic result below shows that there always are models with indiscernibles.

THEOREM 10 (Ehrenfeucht-Mostowski, 1956). — Let T have infinite models and let $\langle X, < \rangle$ be any linearly ordered set. Then there is a model $\mathfrak{A}$ of T such that $\langle X, < \rangle$ is a set of indiscernibles in $\mathfrak{A}$.

The construction of the model $\mathfrak{A}$ uses the partition theorem of Ramsey.

Examples. — Let $\mathfrak{A}$ be a field and $\mathfrak{B}$ be the ring of polynomials over $\mathfrak{A}$ with the set X of variables. Then for any linear ordering $<$ of X, $\langle X, < \rangle$ is a set of indiscernibles in $\mathfrak{B}$.

Let $\mathfrak{A}$ be a non-Archimedean real closed ordered field and let X be a set of positive infinite elements such that if $x < y$ in X then $x^n < y$, $n = 1, 2, \ldots$ Then X with the natural order is a set of indiscernibles in $\mathfrak{A}$.

Indiscernibles are used to prove results such as the following (Two elements $a, b \in A$ have the same *automorphism type* if there is an automorphism of A mapping a to b).

THEOREM 11 (Ehrenfeucht-Mostowski, 1956). — If T has an infinite model, then for every infinite cardinal $\aleph_\alpha$, T has a model of power $\aleph_\alpha$ with only countably many automorphism types.

The following very deep results use both the method of indiscernibles and saturated models.

A theory T is said to be $\aleph_\alpha$-*categorical* if all models of T of cardinal $\aleph_\alpha$ are isomorphic.

THEOREM 12 (Morley, 1965). — If T is $\aleph_\alpha$-categorical for some uncountable $\aleph_\alpha$, then T is $\aleph_\beta$-categorical for every uncountable $\aleph_\beta$.

Shelah, 1970, extended Theorem 12 to uncountable languages.

THEOREM 13 (Baldwin-Lachlan, 1970). — If T is $\aleph_1$-categorical, then either T is $\aleph_0$-categorical or T has exactly $\aleph_0$ models of cardinal $\aleph_0$.

We mention one theorem at the opposite extreme from the above.

THEOREM 14 (Shelah, 1970). — Suppose T has a model A such that for some formula $\varphi(x, y)$ and some infinite set $X \subset A$, the relation

$$\{ \langle a, b \rangle \in X^2 : \ \mathfrak{A} \models \varphi(a, b) \}$$

is a linear order. Then for every uncountable $\aleph_\alpha$, T has $2^{\aleph_\alpha}$ non-isomorphic models of cardinal $\aleph_\alpha$.

Example. — The theory of algebraically closed fields is $\aleph_\alpha$-categorical for every uncountable $\aleph_\alpha$ and has $\aleph_0$ countable models. The theory of abelian groups with all elements of order two is $\aleph_\alpha$-categorical for every $\aleph_\alpha$. The theory of real closed fields has $2^{\aleph_\alpha}$ models of each infinite cardinal $\aleph_\alpha$. The theory of atomless Boolean algebras is $\aleph_0$-categorical but has $2^{\aleph_\alpha}$ models of each uncountable cardinal $\aleph_\alpha$.

7. **Recent trends.**

The model theory of first order logic contains a number of substantial results, but until recently only the compactness theorem has had many applications. This situation is changing and will change more as the subject becomes more widely known. One of the bottle-necks has been that most properties arising in mathematics cannot be expressed in first order logic. For this reason there is a strong move toward model theory for more powerful logics. In the last few years there have been exciting developments in the model theory of the infinitary logic $L_{\omega_1\omega}$. This logic is like first order logic except that it allows the connectives $\bigwedge$ and $\bigvee$ to be applied to countable sets of formulas, that is, if $\varphi_0, \varphi_1, \varphi_2, \ldots$ are formulas of $L_{\omega_1\omega}$, then so are

$$\varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \ldots, \qquad \varphi_0 \vee \varphi_1 \vee \varphi_2 \vee \ldots$$

The formulas may thus be countable in length.

Examples. — The sentence

$$\forall x \quad (x = 0 \vee \quad x + x = 0 \vee \quad x + x + x = 0 \vee \ldots)$$

is true is an abelian group G if and only if G is a torsion group. The sentence

$$\forall x \quad (x < 1 \vee \quad x < 1 + 1 \vee \quad x < 1 + 1 + 1 \vee \ldots)$$

is true in an ordered field if and only if it is Archimedean.

Both the Compactness Theorem and the LST Theorem in their original form are false for $L_{\omega_1\omega}$. For the latter, note that every Archimedean ordered field has power $\leq 2^{\aleph_0}$. Nevertheless, it turns out that all of the methods from first order model theory can be used in $L_{\omega_1\omega}$. Many of the main results have been generalized to

$L_{\omega_1\omega}$, often in a more subtle form. For example, the LST Theorem takes the following form. The cardinal $\beth_\alpha$ is defined by the rule

$$\beth_0 = \aleph_0, \ \beth_{\alpha+1} = 2^{\beth_\alpha},$$
$$\beth_\alpha = \Sigma_{\beta<\alpha}\beth_\beta \text{ for limit ordinals } \alpha.$$

THEOREM 15 (Morley, 1965). — Let φ be a sentence of $L_{\omega_1\omega}$. If φ has a model of cardinal at least $\beth_{\omega_1}$, then φ has models of every infinite cardinal.

The proof is much deeper than the LST Theorem. It uses the partition calculus of Erdös and Radó, 1956, and also yields an analog of Theorem 10 on indiscernibles for $L_{\omega_1\omega}$.

Theorems 1 and 2 above were extended to $L_{\omega_1\omega}$ by Lopez-Escobar, 1965, Theorem 5 by Keisler, 1966, various forms of Theorem 12 by Choodnovsky, Keisler, and Shelah, 1969, and Theorem 14 by Shelah, 1970.

Another basic result is

THEOREM 16 (Scott, 1965). — For every countable model $\mathfrak{A}$ there is a sentence φ of $L_{\omega_1\omega}$ such that $\mathfrak{A}$ is a model of φ and every countable model of φ is isomorphic to $\mathfrak{A}$.

This result is analogous to Ulm's theorem for countable abelian torsion groups. In fact, $L_{\omega_1\omega}$ has been applied by Barwise and Eklof, 1970 to extend Ulm's theorem to arbitrary abelian torsion groups.

The model theory for $L_{\omega_1\omega}$ is greatly enriched by the use of recursion theory as a way to get a hold on infinitely long sentences (a suggestion of Kreisel). This has led to the Barwise Compactness Theorem (Barwise, 1969) which is the analog for $L_{\omega_1\omega}$ of the Compactness Theorem.

Another type of logic where model theory has had recent successes is logic with extra quantifiers, such as " there exist infinitely many " and " there exist uncountably many ". For more information see the paper [12].

A major recent trend is the impact of set theory on model theory and *vice versa.* A number of problems have been shown to be consistent or independent using Cohen's forcing, notably by Silver. Moreover, forcing itself is being used as a technique for constructing models (see A. Robinson's lecture in this Congress). Other results have been proved on the basis of strong hypotheses such as the existence of a measurable cardinal (Rowbottom and Gaifman, 1964, Silver, 1966, Kunen, 1970,) or the axiom of constructibility. For example, Jensen, 1970 has shown that if the axiom of constructibility holds then Chang's Theorem 6 above can be improved to:

If T has a model of type $(\aleph_1, \aleph_0)$ then T has a model of type $(\aleph_{\alpha+1}, \aleph_\alpha)$.

BIBLIOGRAPHY

The three new books [4], [7] and [11] taken together cover most facets of model theory and contain up to date references as of 1970. An extensive list of references to journal articles prior to 1963 can be found in [1]. We have decided that a list of books on model theory and related topics will be more useful at this time than another long list of references to the original articles in journals.

[1] Addison, Henkin and Tarski, editors. — *The Theory of Models*. Amsterdam, 1965. North Holland Publ. Co.
[2] J. L. Bell and A. B. Slomson. — *Models and Ultra products*. Amsterdam, 1969. North Holland Publ. Co.
[3] C. C. Chang and H. J. Keisler. — *Continuous Model Theory*. Princeton, 1966. Princeton Univ. Press.
[4] —. — *Model Theory*. New York, 1971. Appleton Century Crofts.
[5] P. J. Cohen. — *Set Theory and the Continuum Hypothesis*. New York, 1966. W. A. Benjamin, Inc.
[6] P. M. Cohn. — *Universal Algebra*. New York, 1965. Harper and Row.
[7] M. A. Dickmann. — *Uncountable Languages*. Amsterdam, 1971. North Holland Publ. Co.
[8] L. Gillman and M. Jerison. — *Rings of Continuous Functions*. Princeton, 1960. D. Van Nostrand Co., Inc.
[9] G. Grätzer. — *Universal Algebra*. Princeton, 1968. D. Van Nostrand Co., Inc.
[10] C. Karp. — *Languages with Expressions of Infinite Length*. Amsterdam, 1964. North Holland Publ. Co.
[11] H. J. Keisler. — *Model Theory for Infinitary Logic*. Amsterdam, 1971. North Holland Publ. Co.
[12] —. — Logic with the quantifier « There exist uncountably many ». *Annals of Math. Logic*, vol. 1 (1970), pp. 1-93.
[13] G. Kreisel and J. L. Krivine. — *Elements of Mathematical Logic*. Amsterdam, 1967. North Holland Publ. Co.
[14] R. C. Lyndon. — *Notes on Logic*. Princeton, 1966. D. Van Nostrand Co., Inc.
[15] A. Mostowski. — *Thirty Years of Foundational Studies*. Helsinki, 1965, New York, 1966. Barnes and Noble, Inc.
[16] A. Robinson. — *Introduction to Model Theory and the Metamathematics of Algebra*. Amsterdam, 1963. North Holland Publ. Co.
[17] —. — *Non-standard Analysis*. Amsterdam, 1966. North Holland Publ. Co.
[18] J. B. Rosser. — *Simplified Independence Proofs*. New York, 1969. Academic Press.
[19] J. R. Shoenfield. — *Mathematical Logic*. Reading, Mass., 1967. Addison Wesley Publishing Co.
[20] R. M. Smullyan. — *First-order Logic*. New York, 1968. Springer-Verlag.
[21] M. A. Taiclin. — *Theory of Models* (Russian). Novosibirsk, 1970.
[22] J. Van Heijenoort. — *From Frege to Gödel*. Cambridge, 1967. Harvard Univ. Press.

University of Wisconsin
Department of Mathematics,
Madison, Wisconsin 53706
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 151 à 161.

METHODS AND PROBLEMS OF COMPUTATIONAL MATHEMATICS

by G. I. MARČHUK

Computational mathematics being part of mathematics has currently at its disposal powerful techniques for solving problems of science and engineering. The range of computational methods is so wide that it is practically impossible to cover them to a full extent in one report. A series of interesting investigations by Bellman, Greyfus *et al.* devoted to dynamic programming and some related problems was discussed at the previous Congress of Mathematicians. Therefore we shall confine ourselves to some selected questions connected with the theory of approximate operations in finite, and infinite-dimensional functional spaces which the author has been concerned with. Even so, however, it is impossible to cover many interesting studies in the field because of the time limit given to the report. For the same reason the author, regretfully, had to reduce to minimum references to the original studies.

Large-scale electronic computers gave rise to algorithmic constructions and mathematical experimentation over a wide area of science and engineering. This attracted new research personnel to the problems of computational mathematics. The valuable experience we had had in solving applied problems was later used to devise effective methods and algorithms of computational mathematics.

The methods of computational mathematics are closely related to the state of computer art. New concepts and methods are formed in computational mathematics and its numerous applications influenced essentially by every new stage of computer technology.

The standard of research in computational mathematics is largely dependent on the actual connection with fundamental areas of mathematics. First of all I should like to mention functional analysis, differential equations, algebra and logic, the theory of probability, calculus of variations, etc. A mutual exchange of the ideas between different branches of mathematics has been intensified in the recent decade. This is true in the first place for computational mathematics which has used the results of fundamental mathematical areas to develop new and more sofisticated methods and to improve the old ones.

At the same time it should be emphasized that applications have an important influence on computational mathematics. Thus, for instance, mathematical simulation often stimulated a discovery of new approaches which are now a most valuable possession of computational mathematics. Such applied areas as hydrodynamics, atomic physics, mathematical economics and the control theory are most important examples.

1. The theory of approximation, stability and convergence of difference schemes.

The wide use of finite-differences method in differential equations of mathematical physics required a detailed study of those features of difference equations that affect in the first place the quality of difference schemes. Among them are above all the stability and convergence conditions.

This unfavourable feature of difference equations and the corresponding studies of John von Neumann initiated theoretical investigations in order to determine the relation between convergence and stability and to find effective stability criteria of difference schemes.

Later on several authors formulated the following fundamental theorem called the equivalence theorem. If a difference scheme approximates a linear homogeneous differential equation for a properly posed problem, then the stability of the difference scheme is a necessary and sufficient condition for its convergence. The final formulation and the proof of this theorem for an abstract evolution equation in a Banach space were given by Lax. Generalization of the equivalence theorem for non-homogeneous linear differential equation was given by Richtmyer. One can make the stability conditions of the scheme less strict provided that the initial data are suficiently smooth. This idea is implemented in the Strang equivalence theorem using the concept of weak stability.

Speaking of the effective stability conditions it is necessary to mention John von Neumann-Richtmyer's paper of 1950. They formulated a so-called local stability criterion. They introduced such new notions as a symbol of a difference scheme, a spectrum of a family of difference operators and a kernel of the spectrum of the family which made it possible to estimate norms of the powers of the step operators. These estimates were in many cases effectively used in the stability analysis.

An interesting approach to difference schemes with variable coefficients is associated with the idea of dissipativity. This idea was implemented in the studies of Kreiss. His theorems relate the order of dissipativity of the difference equations approximating systems of hyperbolic equations to the order of their accuracy. Important results have been derived by a so-called energy method which is based on the concept of strong stability. The idea of the method is to choose some norm for the vector solution. The norm of the vector solution grows from step to step not faster than $I + 0(\Delta t)$.

The energy method was first introduced by Courant, Freidrichs and Lewy and developed by other authors, in particular by Ladyzhenskaya and Lees.

Here it is necessary to mention the theory of the convergence of difference schemes developed by Samarsky who has used energy inequalities and *a priori* estimates. The theory gives necessary and sufficient stability conditions for two- and three-layer schemes formulated in a form of inequalities. The inequalities contain operator coefficients of difference schemes.

Of late the interest of mathematicians has been attracted to stable boundary-value hyperbolic problems. A certain contribution to that has been made by Kreiss. He has formulated necessary and sufficient stability conditions for some classes of problems. Ryabenky has deeply studied the theory of boundary-value problems for difference equations with constant coefficients. As before the theory of difference equations for boundary-value problems of mathematical physics is of supreme concern to mathematicians.

2. **A numerical solution of the problems of mathematical physics.**

The studies of approximation, stability and convergence have provided the necessary basis for a wide research of effective difference schemes applied to the problems of mathematical physics. The algorithms of finite difference methods combine, as a rule, the aspect of a construction of a difference equation-analogue as well as the aspect of its solution. Therefore the advance of the constructive theory of the finite difference methods depends on a mutually coordinated development of the two aspects mentioned above.

If we try to summarize the vast experience of recent years in the development of finite difference methods we can conventionally distinguish some main trends.

2.1 One of such trends is concerned with finding efficient algorithms for multi-dimentional stationary problems on mathematical physics.

As a result of the success achieved in a solution of simultaneous linear algebraic equations with Jacobi and block-tridiagonal matrices there have emerged a few excellent algorithms in which factorization of the difference operator is used. At the Institute of Applied Mathematics (AS, USSR) were proposed different variants of the direct factorization method which have been effectively applied to a solution of different classes of problems and which should be specially mentioned.

One can see that besides the precise factorization methods there is a rapid development of the approximate factorization methods where factorization of the operator is performed by means of iterations.

Early sixties were marked by a major contribution in computational mathematics associated with the names of Douglas, Peaceman and Rachford who suggested an alternating direction method. The success of the method was ensured by the use of a simple reduction of a multi-dimensional problem to a sequence of one-dimensional problems with Jacobi matrices which are convenient to handle. The theory of the alternating direction method has been developed by Douglas and Gunn, Birknoff, Wachspress, Varga and also by Kellogg, Bakhvalov, Vorobjov, Widlund *et al.*

Later Soviet mathematicians Yanenko, Diakonov, Samarsky and others developed a so-called splitting-up method. The point is that the approximation of the initial operator by each auxiliary operator is not necessary but on the whole such an approximation exists in special norms.

A series of investigations has been devoted to a choice of optimization parameters of splitting-up schemes by means of spectral and variational techniques.

2.2 The experience we have in the solution of one-dimensional problems represents a solid base when we come to the development of algorithms for the problems of mathematical physics. An important role in the development of new approaches to a solution of non-stationary two-dimensional problems belongs to the alternating direction method.

Further advancement of the methods for multi-dimensional non-stationary problems is connected with splitting-up techniques based as a rule on non-homogeneous difference approximations of the initial differential operators. The mathematical technique is related with splitting of a compound operator to simple ones. If this approach is used the given equation can be solved by means of integration of simpler equations.

In this case the intermediate schemes have to satisfy the approximation and stability conditions only as a whole which permits flexible schemes to be constructed for practically all problems of mathematical physics.

Splitting-up schemes for implicit approximations have been suggested by Yanenko, Diakonov, Samarsky *et al.* and applied in various problems. Such schemes have stimulated a more general computational approach to the problems of mathematical physics which has been called a weak approximation method.

French scientists Lions, Temam, Bensoussan, Glowinsky *et al.* have made an important contribution to the splitting-up methods and theoretically substantiated a number of new approaches. These investigations are especially important for fluid dynamics, the theory of plasticity and the control theory. The method of decomposition and decentralization formulated by these scientists should be specially mentioned. It is closely connected with the method of weak approximation.

Recently there has been found a class of splitting-up schemes equivalent in their accuracy to the Crank-Nicolson difference scheme and applied to non-stationary operators. These schemes are absolutely stable for the systems of equations with positive semi-definite operators depending explicitly on space and time coordinates. This method is easily extended to quasi-linear equations.

Lax and Wendroff have suggested a kind of a predictor-corrector scheme. This approach is used in hydrodynamics, meteorological and oceanological problems.

2.3 In the recent years there has been a rapid development of a so-called particle-in-the-cell method suggested by Harlow and applied to multi-dimensional problems of mathematical physics. It is widely used to calculate multi-dimensional hydrodynamics flows with strong deformation of the fluid, big relative displacements and colliding surfaces. We can expect that in the years to come the applicability of the method will be extended to multi-dimensional problems.

2.4 The Monte-Carlo method suggested by John von Neumann and Ulam has been developed now for more than two decades. From the very beginning it turned out that the Monte-Carlo method was effective only on very fast computers because a great number of samples is required to reduce the mean squared error of a solution.

However, in spite of the difficulties of putting this method on middle-scale computers and, maybe, due to them the theory of the method has been considerably improved which has increased its efficiency. The basic ideas intended to a considerable improvement of the method comprise the use of conditional probabilities and statistical weight coefficients which can be found when information on the solutions of conjugate equations is used, the latter being related to the essential functionals inherent in the problems.

The simplicity and universality of this method will undoubtedly make it an important tool of computational mathematics.

2.5 Lately there has been much interest in variational methods applied to problems of mathematical physics. The variational methods of Rits, Galerkin, Frefz and others have long become classical in computational mathematics.

Not long ago there emerged a new trend in variational methods, a so-called method of finite elements or functions. The main idea of it was expressed by Courant as far back as nineteen forties. The essence of this method is that one seeks an approximate solution in a form of linear combination of functions with compact support of order of the mesh width h. In other words one takes as trial functions special functions in a polynomial form identically equal to zero outside of a fixed domain having a characteristic dimension of several h's. The main problem here is the theory of approximation of the functions by a given system of finite elements.

An important contribution to the finite element method has been made by Birkhoff, Shultz, Varga *et al.* A systematic study of the theory and applications of the method has been fulfilled by Aubin, Babuška, Fix and by Strang, Bramble, Douglas and others.

Usually the main obstacle one comes across using variational methods is a choice of simple functions satisfying boundary conditions. It can be overcome by means of special variational functionals. For this purpose one employs a so-called penalty method or a weight method which reduce the initial problem to one with natural boundary conditions. The finite element method is close in its idea to the method of spline functions.

The finite element method is closely associated with the application of a variational approach to constructing finite difference equations corresponding to differential equations of mathematical physics. Lions, Cea, Aubin, Raviart and other authors have contributed to this area of research.

There is no doubt that the scope of variational methods will grow as the problems become more and more complicated. The variational approach in combination with other methods will be a powerful tool in computational mathematics.

3. Conditionally properly posed problems.

Correctness of a problem plays an important role in a numerical solution of mathematical physics equations. The concept of correctness was introduced by Hadamard at the beginning of our century. We know a variety of classical problems properly posed in the sense of Hadamard. However, with a more profound study of various problems in natural sciences and engineering it became necessary to solve so-called conditionally properly posed problems. Tykhonov has formulated the requirements which proved to be natural in a formulation of improperly posed problems in the sense of Hadamard. Tykhonov introduced a concept of regularization.

The results of the investigations of conditionally properly posed problems are presented in M. M. Lavrentiev's well-known monograph " Some improperly posed problems of mathematical physics ".

An interesting approach to the formulation of the improperly posed problems in the sense of Hadamard is based on probabilistic methods. Most complete investigations have been made by M. M. Lavrentiev and Vasiliev. Different aspects of the theory of these problems in mathematical physics are discussed by Jones, Douglas, S. Krein, Miller, Cannon and others.

Lions and Lattes have formulated a numerical method for the inverse evolution equation using a so-called quasi-inversion.

As evidenced by the tendencies of solving conditionally properly posed problems, the techniques used here is closely associated with the optimization theory of computation to be briefly reviewed in this paper.

4. Numerical methods in linear algebra.

A solution of simultaneous algebraic equations and computing of eigenvalues and eigenvectors of matrices are important problems of computational mathematics. Speaking about the numerical methods and problems in linear algebra of recent years it is necessary first of all to emphasize the growing interest in the solution of large systems of the corresponding equations, in the solution of ill-conditioned systems and in spectral problems for arbitrary matrices. Much attention has been paid to the use of *a priori* information in the process of the solution. Under the influence of computer development the old numerical methods in linear algebra have been reconsidered. The increasing use of computers has stimulated a creation of new algorithms well suited for automatic calculation.

4.1 Direct methods play an important role when simultaneous linear algebraic equations are solved or inverse matrices and determinants are found.

Direct methods have been considerably developed first by Faddeeva, Bauer, Householder, Wilkinson and then by Henrici, Forsythe, Golub, Kublanovskaya, Voevodin and others. Using some elementary transformations one can represent the initial matrix as a product of two matrices, each being easily inverted.

We used to compare computational methods according to a number of arithmetic operations and the memory requirements. Now we ought to pay attention also to their accuracy. It means that round-off error analysis has become an essential feature of the method itself.

The corresponding inverstigations were started by John von Neuman, Goldstein, Turing, Givens *et al.* A systematic study of errors was first made by Wilkinson. His results were later systematized in his excellent monograph " An algebraic eigenvalue problem " where the method of equivalent perturbations was taken as a basic mathematical technique. As a result estimates of the norms of perturbations were obtained for all fundamental transformations of linear algebra.

In parallel with the method of equivalent perturbations there was an intensive development of the statistical error theory. The results obtained by Bakhvalov, Voevodin, Kim *et al.* initiated an investigation of the real distribution of round-errors. The statistical methods are certain to play an important role in the round-off error analysis.

4.2 Iterative methods remain very important in linear algebra. An active progress of these methods has resulted in a number of powerful algorithms which are effectively used on computers.

At present there are some trends in a construction of the iterative processes and methods aimed at the minimization of the number of arithmetic operations for obtaining a solution, with the emphasis put on the use of spectral characteristics of the operators involved. A choice of iteration process parameters is part of optimization of the computational algorithm. The major difficulty here is as a rule to determine the boundaries of the spectra of the matrices.

Spectral optimization of iterative methods stimulates a formulation of a number of problems. Once again we shall discuss the two of them.

More attention has been recently attracted to the Lanszos transform of arbitrary matrices which leads to an equivalent system of equations with a symmetric matrix whose spectrum occupies two segments symmetric with respect to zero.

The second problem is a search of effective methods intended to determine the matrix eigenvalue with minimum modulus.

Let us discuss the application of variational principles to iterative methods. Such methods allow a successive minimization of some functional which attains a minimum on a desired solution. There has been much interest in such problems. Kantorovich, Lanszos, Hestens and Stiefel as well as Krasnoselsky and Krein *et al.* have stated a variational approach to iterative methods. I should like to mention the recent papers of Petryshyn, Forsythe, Daniel, Yu. Kuznetsov, Godunov and others.

When the variational approach to iterative methods is used one can select relaxation parameters on the basis of *a posteriori* information obtained at each step. This is also the case for the steepest descent method and the iterative method with minimal discrepancies. The above said is the merit of the variational approach. The rate of convergence seems to be not lower than the rate we get using Chebyshev's polynomials.

There is also probabilistic technique intended to choose optimization parameters of iterative processes. A series of interesting results has been obtained by Vorobjov.

The Young-Frankel overrelaxation method has not yet lost its importance. It has become classical and is generalized in the monographs of Wasow and Forsythe, Varga, Isaacson *et al.*

4.3 Let us consider how to solve a total eigenvalue problem for arbitrary matrices by iterations.

We shall discuss only power methods which have been advanced by Wilkinson, Bauer, Rutishauser, Collatz, Voevodin and by Frencis, Kublanovskaya, Eberlein and many others. Until recently there have been effective eigenvalue algorithms only for symmetric matrices, for instance, the Jacobi method and the method of dividing segments in two. It is hoped that the discovery of the QR-algorithm and the generalized method of rotation will allow us to deal with arbitrary matrices. As present different modifications of the QR-algorithms are developed most intensively. These are widely used in science and engineering.

5. Optimization of numerical algorithms.

An important goal of computational mathematics is to find most profitable methods for a solution of the problems, i. e. to optimize algorithms. One must study the problem of optimization under given constraints by general mathematical theorems and to estimate what is a minimal possible cost to solve a particular problem or a sequence of problems. Local optimization of one isolated part of a solution does not practically resolve the problem we are interested in. However, if one can find the best way of handling every local problem using the existing computing facilities, one is thus led to its solution. This concept of the optimization theory has been formulated by Sobolev and Babuska and it represents sufficiently well the essence of the formulated problem.

Yet in many cases it is either impossible to build an optimal algorithm or the latter turns out to be very costly. Nevertheless it appears possible to build an algorithm close an optimal one. This is the case, for example, when asymptotically optimal algorithms are constructed. It will be noted that at present the theory of asymptotic estimates is an effective tool of algorithm optimization.

The concept of ε-entropy introduced by Kolmogorov has been very useful too. A hypothesis has been proposed that the efforts spent to find a solution are essentially associated in many instances with ε-entropy of a set of elements on which the solution depends. Using the concept of ε-entropy one can estimate both upper and lower bounds of the number of operations needed for the solution of many computational problems.

Sobolev, Bakhvalov, Lebedev and others have studied a number of algorithms for the problems of mathematical physics using finite-difference methods.

A considerable contribution to the theory of computation and its optimization has been made by Babuška, Dahlquist, Henrici *et al.* Babuška, Vitašek and Prager have introduced a notion of α_κ-sequence of computational processes. This implies that if the length of a sequence of operations in the problems of mathematical analysis is increased, the accuracy of computation exponentially increases.

An idea has been expressed to introduce operations with intervals. This trend named interval arithmetic can be applied to the study of the approximation errors in mathematical analysis and to the analysis of round-off errors.

6. Trends in computational mathematics.

6.1 *The progress in computational technology* has had an important influence on many branches of computer science which show a tendency of integration. The relations between: software, the methods of computational and applied mathematics, the theory of programming and languages-become so close that the choice of a strategy for a solution of particular problems is now of paramount importance. Though optimization of individual components of computational process is as before a fundamental factor of the theory, the attention becomes more and more concentrated on optimization of the whole process. Optimization of computation is obviously one of the central goals of computational mathematics which stimulates exploration of new algorithms and new ways of their computer implementation.

6.2 The second trend is connected with a solution of classes of problems and with algorithm standardization. A large amount of computer-processed information must be systematized and put in order. The valuable experience which we have in the solution of the problems of science and engineering allows us in many cases to set as an ultimate goal a creation of universal methods suitable to handle more or less wide classes of mathematical problems of the same type. At present a care must be taken to save the efforts of the society on a creation of numerous individual algorithms for individual and rare problems. It seems that a rational strategy for a solution of various rare problems is to construct universal algorithms self-adjusting to optimal operating conditions because they use *a posteriori* information. A rational strategy for a solution of frequently repeated problems is a careful implementation of specific algorithms.

These two approaches combined will help to save social resources spent on a creation of effective software. First steps have been made in the theory of the universal algorithms which are self-adjusting to a kind of optimal operating conditions and a course of further research has been outlined.

6.3 Software is becoming a materializatioh of the society's intellect. The process of the mathematization of sciences has given rise to an active development of the methods to simulate the phenomena occurring in nature and society. High-speed, large-memory computers of new generations can store immediately available valuable information and multi-access computers allow new forms of man-machine interaction using a conversational mode of operation. Therefore standardization of solftware in general and of computational algorithms in particular is an urgent problem of scientific and technological process.

6.4 The problem of solftware has stimulated a formulation of new problems in computational mathcmatics, such as a construction of grids for complicated domains. For two-dimensional domains the above problem is close to its effective solution while for three- and multi-dimensional domains it is just being stated. This problem is closely connected with a construction of algorithms for large problems with high accuracy by difference, variational and other techniques or may be by a combination of different methods. The solution of the problems with non-linear monotonous operators is especially important. The corresponding theory is at present intensively developed.

6.5 The success achieved in analytic transformations on a computer leads practically to the solution of mathematical physics problems by the well-known technique of the continuous function analysis. As the supply of visual aids for analytic computations grows, these methods will penetrate more and more into software. The success achieved in analytic transformations on computers will give computer science new possibilities which nowadays should be taken into account.

Finally I should like to note that the further development of computational mathematics depends on the standard of research in fundamental branches of mathematics, the importance of the latter essentially growing at the age of great technological progress. Only a harmonic combination of research in all branches of mathematics will provide the necessary and favourable conditions for self-development of mathematics and its applications.

MONOGRAPHS AND REVIEW PAPERS (*)

I. Babuška and S. L. Sobolev. — The optimization of numerical methods (Russian). *Aplikace Matematiky*, 10, No. 2 (1965).

—, M. Prager and E. Vitašek. — *The numerical solution of differential equations* (Russian). « Mir », M. (1965).

(*) The reference to the original literature mentioned in the present paper, as well as other papers on the subject of the paper can be found in the bibliographies of the monographs and review papers listed here.

F. L. BAUER and C. T. FIKE. — Norms and exclusion theorems. *Numerische Math.*, 2 (1960).

N. S. BAKHVALOV, N. M. KOROBOV and N. N. CHENTSOV. — *Application of the number-theoretic nets to the problems of approximate analysis* (Russian). Trudy IV Vsesojuznogo sjezda, II, Leningrad, 1961.

G. BIRKHOFF and S. MACLANE. — *A survey of modern algebra* (revised edition). MacMillan, New York, 1953.

W. WASOW and G. FORSYTHE. — *Finite-difference methods for partial differential equations.* John Wiley and Sons, Inc., 1959.

V. V. VOEVODIN. — *Approximation and stability errors in direct methods of linear algebra* (Russian), M. (1959).

J. H. WILKINSON. — *The algebraic eigenvalue problem.* Oxford, Clarendon Press (1965).

S. K. GODUNOV and V. S. RYABENKY. — *Introduction to the theory of difference schemes* (Russian). Fizmatgiz (1962).

G. H. GOLUB and R. S. VARGA. — Chebyshev's semi-iterative methods, successive over-relaxation iterative methods and second order Richardson's iterative methods. Parts I, II. *Num. Math.*, v. 3 (1961).

A. A. DORODNITSYN. — *A method of integral relations* (Russian). Trudy IV Vsesojuznogo sjezda, II, Leningrad, 1961.

J. DOUGLAS and H. RACHFORD. — On the numerical solution of heat conduction problems in two and three space variables. *Trans. Amer. Math. Soc.* (1956).

— and J. E. GUNN. — A general formulation of alternating direction methods. Part I. Parabolic and hyperbolic problems. *Numerische Math.* (1964).

J. DOUGLAS jr. and T. DUPONT. — *Galerkin methods for parabolic equations.* Synspade (1970).

E. G. DIAKONOV. — *Some iterative methods for the systems of finite-difference equations, arising in the solution of elliptic partial differential equations* (Russian). Vychislitelnye Metody i Programmirovanie III, Izdat. MGU (1965).

ISAACSON and KELLER. — *Analysis of numerical methods.* John Wiley and Sons, Inc. (1966).

L. V. KANTOROVICH. — Functional Analysis and Applied Mathematics, *UMN*, 3, vyp. 2, 89 (1948).

— and G. P. AKILOV. — *Functional analysis in normed spaces* (Russian). Fizmatgiz (1959).

L. COLLATZ. — *Funktional analysis und Numerisch Mathematik.* Springer-Verlag (1964).

A. KOLMOGOROFF. — Uber die beste Annaherung von Funktionen einen gegebenen Funktionklassen, *Ann. of Math.*, 37 (1936).

N. M. KOROBOV. — The calculation of multiple integrals by method of optimal coefficients, *Vest. MGU*, 4, 19 (1959).

H.-O. KREISS. — On difference approximations of the dissipative type for hyperbolic differential equations, *Communs Pure and Appl. Math.*, vol. XVII, No. 3 (1964).

M. M. LAVRENTIEV. — Some improperly posed problems of mathematical physics. Springer Tracts in *Natural Phylosophy*, vol. II (1967).

O. A. LADYZHENSKAYA. — *A mixed problem for a hyperbolic equation* (Russian). Gostehizdat, M. (1953).

P. D. LAX. — Nonlinear partial differential equations and computing, *SIAM Review*, vol. II, No. I (1969).

C. LANCZOS. — *Applied analysis.* Prentice Hall, Inc., Englewood Cliffs, New York (1956).

R. LATTES et J. LIONS. — *Méthodes de quasi-réversibilité et applications.* Dunod, 1967.

J. LIONS. — *Quelques méthodes de résolution des problèmes aux limites non linéaires.* Dunod (1969).

G. I. MARCHUK and N. N. YANENKO. — *The application of the splitting-up method (fractional steps) to the problems of mathematical physics.* IFIP, New York (1965).

—. — *On the theory of splitting-up methods.* Maryland, Synspade (1970).

J. P. AUBIN. — Behaviour of the error of the approximate solutions of boundary value problems for linear elliptic operations by Galerkin's and finite difference methods, *Ann. Scula Norm.*, Pisa XXI (1967).

D. W. PEACEMAN and N. N. RACHFORD, jr. — The numerical solution of parabolic and elliptic differential equations, *J. Soc. Industr. Appl. Math.*, 3 (1955).

R. D. RICHTMYER and K. W. MORTON. — *Difference Methods for initial-value Problems* (part 1, General considerations; part 2, Applications). Interscience publishers, a division of John Wiley and Sons, New York, London, Sydney (1967).

H. RUTISHAUSER and H. R. SCHWARZ. — Handbook Series Linear Algebra. The LR transformation method for symmetric matrices, *Numerische Math.* (1963).

V. S. RYABENKY and A. F. FILIPPOV. — *On the stability of finite difference equations* (Russian), Gostehizdat (1956).

A. A. SAMARSKY. — *Lectures on the theory of finite difference schemes* (Russian), M. (1969).

S. L. SOBOLEV. — *Lectures on the theory of numerical integration formulas*. Parts I, II (Russian), Izd. NGU (1964).

G. STRANG. — The finite element method and approximation theory, *The Symposium on the Numerical Solution of Partial Differential Equations*. The Univ. of Maryland (1970).

A. N. TYKHONOV. — Regularization of improperly posed problems (Russian), *Dokl. Akad. Nauk SSSR*, 153, No. 1 (1963).

D. K. FADDEEV and V. N. FADDEEVA. — *The computational methods of linear algebra* (Russian), M.-L., Fizmatgiz (1969).

G. FORSYTHE and C. B. MÖLLER. — *Computer Solution of linear algebraic systems*, Prentice-Hall, Inc., Englewood Cliffs, New York (1967).

A. S. HOUSEHOLDER. — *The theory of matrices in numerical analysis*, Blaisdell, New York (1964).

P. HENRICI. — *Discrete variable methods in ordinary differential equations*. John Wiley and Sons, Inc. (1962).

N. N. YANENKO. — *The method of fractional steps for multi-dimensional problems of mathematical physics* (Russian), « Nauka », Novosibirsk (1967).

Computing Center
Novosibirsk 90 (U. S. S. R.)

Actes, Congrès intern. math., 1970. Tome 1, p. 163 à 171.

LES JEUX DIFFÉRENTIELS LINÉAIRES

par L. PONTRYAGIN

On considère ici des jeux différentiels linéaires dont l'exemple-type est la poursuite d'un objet contrôlable par un autre objet contrôlable.

Les jeux différentiels linéaires constituent évidemment un cas très particulier, cependant, même dans ce cas, les résultats ne sont pas triviaux, et ils sont en plus beaucoup plus efficaces que les généralisations correspondantes au cas non-linéaire.

Le problème sera posé ici pour le cas non-linéaire, tandis que les résultats seront formulés seulement pour le cas linéaire.

Position du problème.

La théorie des jeux différentiels est née comme modèle d'idéalisation mathématique de problèmes techniques. Il y a différentes possibilités d'idéalisation. Dans le choix d'un modèle il faut tendre à ce que ce dernier, d'une part, reflète les traits principaux du problème technique, et d'autre part, puisse être traité mathématiquement. Ainsi, l'exposé de la théorie ne doit pas être complètement détaché des problèmes techniques.

Pour en avoir un exemple concret, imaginons qu'un avion en poursuit un autre; le but du premier avion est d'atteindre l'autre avion ; le but du deuxième est d'échapper à la poursuite.

Chaque pilote dirige son avion, en ayant son propre but et en utilisant l'information sur la situation. L'information est composée de deux parties: premièrement, c'est la connaissance complète des possibilités techniques des deux avions; deuxièmement, ce sont les renseignements sur le comportement de son propre avion et de l'avion de l'adversaire. Les données sur le comportement des avions peuvent inclure différents éléments se rapportant à la période précédant le moment présent, mais rien ne peut être considéré comme connu en ce qui concerne le futur comportement des avions, puisqu'ils sont contrôlables, et que, à chaque instant, chacun des deux pilotes peut modifier la position des commandes, modifiant ainsi le comportement de l'avion. Dans la réalité, chaque pilote reçoit les informations sur le comportement de l'adversaire avec un certain retard, cependant il n'est pas nécessaire de tenir compte de cela dans une idéalisation ; au contraire on peut même supposer que le comportement de l'adversaire est connu avec une certaine avance et on peut construire une idéalisation mathématique sur cette base, pour démontrer ensuite que la théorie, ainsi obtenue, peut être utilisée pour la solution approximative du problème réel.

Passons à la description mathématique du processus de la poursuite. Deux objets contrôlables participent à ce processus: l'un qui poursuit et l'autre qui fuit. L'état de chaque objet à tout instant est défini par son vecteur d'état. Nous désignons par x (resp. y)

le vecteur d'état de l'objet poursuivant (resp. fuyant). Les équations d'état s'écrivent sous forme habituelle :

$$\dot{x} = f(x, u) \quad ; \quad \dot{y} = g(y, v) \tag{1}$$

où le point désigne la dérivée par rapport au temps et u et v sont des contrôles, x et y étant les vecteurs d'état, chacun d'eux se décomposant en deux parties :

$$x = (x_1, x_2) \quad ; \quad y = (y_1, y_2)$$

où x_1, et y_1 déterminent les positions géométriques des objets, et x_2 et y_2 leurs vitesses. On considère que la poursuite se termine au moment où se réalise l'égalité suivante :

$$x_1 = y_1, \tag{2}$$

c'est-à-dire au moment où les objets coïncident.

La première partie de l'information, mentionnée ci-dessus, est composée des équations (1), qui décrivent non les mouvements réels des objets, mais seulement leurs possibilités, puisque pour différents contrôles $u = u(t)$ et $v = v(t)$ on obtient des mouvements différents. Ainsi, dans le cas des avions, les équations (1) décrivent les possibilités techniques des avions.

Le processus de la poursuite peut être considéré de deux points de vue différents :

1. On peut s'identifier avec l'objet poursuivant. Dans ce cas, notre but consiste à faire aboutir la poursuite, et nous avons à notre disposition le contrôle u pour atteindre ce but. Ainsi, pour chaque instant t, nous devons construire la valeur $u(t)$ du contrôle u, en partant des équations (1) connues (la première partie de l'information) et en utilisant la deuxième partie de l'information, c'est-à-dire la connaissance des fonctions $x(s)$, $y(s)$, $v(s)$ sur l'intervalle $t - \theta \leqslant S \leqslant t$, où θ est un nombre réel choisi convenablement.

2. Nous pouvons nous identifier avec l'objet fuyant : dans ce cas, notre but est d'empêcher l'aboutissement du processus de la poursuite, et nous disposons, pour réaliser ce but du contrôle v. Donc, à chaque instant t, nous devons construire la valeur $v(t)$ du contrôle v, en partant de la connaissance des équations (première partie de l'information) et en utilisant sa deuxième partie connue sous la forme des fonctions $x(s)$, $y(s)$, $u(s)$ sur l'intervalle $t - \theta \leqslant s \leqslant t$.

C'est ce modèle du processus de la poursuite que nous considérerons ici, modèle qui inévitablement divise le problème en deux problèmes différents : le problème de la poursuite et le problème de la fuite. Ceci tient à ce que nous disposons d'informations différentes suivant que nous adoptons l'un ou l'autre point de vue.

Il existe aussi un autre modèle, dû à Isaacs, dans lequel on utilise, pour le problème de la poursuite, la même information que pour le cas de la fuite, à savoir la connaissance des valeurs $x(t)$ et $y(t)$. Dans ce modèle on suppose l'existence d'un contrôle optimal $u = u(x, y)$ de la poursuite qui est une fonction de x et de y (états des objets), ainsi que l'existence d'un contrôle optimal de la fuite $v = v(x, y)$ défini comme fonction de x et de y.

Un tel modèle rend le problème très défini du point de vue mathématique : dans ce cas le problème consiste à trouver les fonctions $u(x, y)$ et $v(x, y)$, appelées les stratégies optimales, mais cette précision justement rend la solution extrêmement difficile. De plus, en supposant l'existence de stratégies optimales, nous réduisons beaucoup la classe des problèmes considérés.

Le jeu différentiel.

Le jeu différentiel résulte, en partant du processus de la poursuite, du désir naturel de simplifier les notations, c'est-à-dire d'avoir un seul vecteur $z = (x, y)$, au lieu des deux vecteurs d'état x et y. Pour cela, on construit l'espace des variables d'état R du jeu comme somme directe des espaces des variables d'état des deux objets. Les équations (1) s'écrivent alors sous forme d'une seule équation :

$$\dot{z} = F(z, u, v) \tag{3}$$

La relation (2) définit, dans l'espace vectoriel R, une certaine variété M. Nous pouvons maintenant définir le jeu différentiel indépendamment du processus initial de la poursuite.

Un jeu différentiel est défini par la donnée de son espace des variables d'état R, l'équation (3), où $z \in R$ et F est une fonction de trois variables (u étant le contrôle de la poursuite et v le contrôle de la fuite) et dans l'espace R, un ensemble M, sur lequel s'achève le jeu.

Comme dans le cas du processus de la poursuite, nous associons au jeu différentiel deux problèmes distincts :

1. Notre but est l'achèvement du jeu, c'est-à-dire d'amener le point z dans l'ensemble M, et nous disposons, pour atteindre ce but, du contrôle de la poursuite u, et donc, à chaque instant t, nous choisissons la valeur $u(t)$ de ce contrôle, en utilisant les fonctions $z(s)$ et $v(s)$ sur l'intervalle $t - \theta \leqslant s \leqslant t$. Telles sont les règles du jeu de la poursuite.

2. Notre but est d'empêcher que le jeu ne s'achève, c'est-à-dire d'empêcher que le point z n'arrive dans l'ensemble M, et pour cela nous avons à notre disposition le contrôle v de la fuite, et donc, à chaque instant t, nous choisissons la valeur $v(t)$ de ce contrôle en utilisant les fonctions $z(s)$ et $u(s)$ sur l'intervalle $t - \theta \leqslant s \leqslant t$. Telles sont les règles du jeu de la fuite.

Jeu différentiel linéaire.

Nous considérerons que l'espace des variables d'état R du jeu linéaire est un espace vectoriel euclidien à n dimensions. L'équation du jeu a la forme suivante :

$$\dot{z} = Cz - u + v \tag{4}$$

où $z \in R$, où C est une application linéaire de R dans R et où u et v sont des vecteurs de l'espace R, qui, toutefois, ne sont pas arbitraires, mais doivent vérifier les conditions suivantes :

$$u \in P \quad ; \quad v \in Q \tag{5}$$

où P et Q sont des sous-ensembles convexes compacts de l'espace R (les dimensions des ensembles P et Q sont arbitraires). Comme fonctions du temps, les contrôles $u = u(t)$ et $v = v(t)$ sont des fonctions mesurables de t. Nous supposerons que l'ensemble M, dans lequel s'achève le jeu, est un sous-espace vectoriel de l'espace R. Il existe aussi des résultats pour le cas plus général, où M est un sous-ensemble convexe fermé quelconque de l'espace R.

Quand il sera question de ce cas plus général, nous le préciserons explicitement.

A) On désignera par $\mathscr{L}$ le supplémentaire orthogonal de M dans l'espace R et par ν (dim $\mathscr{L} = \nu$) la dimension de ce supplémentaire. La projection orthogonale de l'espace R sur $\mathscr{L}$ sera désignée par π. C étant une application linéaire de R dans R, $e^{\tau C}$, où τ est un nombre réel, est une application linéaire de R dans R, et $\pi e^{\tau C}$ est une application linéaire de R dans l'espace $\mathscr{L}$. Ces deux applications dépendent analytiquement du paramètre réel τ. Posons :

$$P_\tau = \pi e^{\tau C} P \quad ; \quad Q_\tau = \pi e^{\tau C} Q \tag{6}$$

Alors P_τ et Q_τ sont des sous-ensembles convexes compacts de l'espace $\mathscr{L}$ et dépendent continûment du paramètre réel τ.

B) *Opérations sur les convexes compacts de $\mathscr{L}$.* — Soient A et B deux sous-ensembles convexes compacts de $\mathscr{L}$, et α et β des nombres réels. Nous désignerons par :

$$\alpha A + \beta B \tag{7}$$

l'ensemble de tous les vecteurs de la forme $\alpha x + \beta y$, où $x \in A$ et $y \in B$. Il est évident que l'ensemble (7) est compact et convexe. Si l'un des deux ensembles A et B est vide, l'ensemble (7) est également vide. Il est facile de vérifier que pour α et β non-négatifs, on a la distributivité

$$(\alpha + \beta)A = \alpha A + \beta B \tag{8}$$

L'ensemble de tous les sous-ensembles compacts convexes non vides de $\mathscr{L}$ forme, d'une façon naturelle, un espace métrique complet Ω. Donc, si $X_\tau = X(\tau)$ est un sous-ensemble compact convexe de Ω, dépendant du paramètre réel τ, autrement dit, si $X(\tau)$ est une fonction du paramètre réel τ à valeurs dans Ω, on peut définir la mesurabilité de cette fonction et son intégrale de Lebesgue

$$\int_{t_1}^{t_2} X(\tau) d\tau \qquad (t_1 \leqslant t_2) \tag{9}$$

qui sera aussi un élément de l'espace Ω. Nous supposerons que, pour $t_1 = t_2$, l'ensemble (9) est composé de l'élément nul de $\mathscr{L}$.

C) Soient A et B deux sous-ensembles compacts convexes de $\mathscr{L}$. S'il existe un vecteur $x \in \mathscr{L}$ tel que :

$$x + B \subset A \tag{10}$$

nous écrirons :

$$B \overset{*}{\subset} A \tag{11}$$

L'ensemble de tous les vecteurs x qui vérifient la condition (10) sera désigné par

$$A \stackrel{*}{-} B \tag{12}$$

que nous appellerons la différence géométrique des ensembles A et B.

Il est évident que l'ensemble (12) est compact et convexe. Cet ensemble est non vide si et seulement si la condition (11) est vérifiée.

Le jeu de la poursuite.

Constituons pour le jeu (4) la différence géométrique (voir A) et C)):

$$P_\tau \stackrel{*}{-} Q_\tau \tag{13}$$

Il s'avère que cette différence est une fonction mesurable de τ, et que, par conséquent, on peut définir son intégrale de Lebesgue

$$\int_0^t (P_\tau \stackrel{*}{-} Q_\tau) d\tau \qquad 0 \leqslant t \tag{14}$$

Pour $t = 0$, cette intégrale est composée du vecteur nul. Nous désignerons par $\mathscr{I}$ l'ensemble de toutes les valeurs de t pour lesquelles (14) n'est pas vide. L'ensemble $\mathscr{I}$ est réduit à 0, ou bien est un intervalle $0 \leqslant t \leqslant t_0$, ou bien coïncide avec la demi-droite $0 \leqslant t$.

Désignons par W_t l'ensemble de tous les points $z \in R$, pour lesquels on a l'appartenance :

$$\pi e^{tC} z \in \int_0^t (P_\tau \stackrel{*}{-} Q_\tau) d\tau \tag{15}$$

et par $T(z)$, la valeur minimale du nombre t, pour laquelle on a l'appartenance (15). Il est évident que

$$W_0 = M \tag{16}$$

et que W_t est non-vide pour tout $t \in \mathscr{I}$.

On a alors le théorème suivant sur la poursuite [1].

THÉORÈME 1. — *Si, pour la valeur initiale z du jeu* (4), *le nombre $T(z\ )$ est défini, alors le jeu de poursuite ayant pour valeur initiale z_0 peut être terminé en un temps qui ne dépasse pas $T(z_0)$.*

Ce théorème n'est pas tout à fait exact. Plus précisément, en un temps t, inférieur ou égal à $T(z_0)$, le point z_0 peut être amené dans une position $z(t)$ dont la distance à M est inférieure à $c\varepsilon$, où $c > 0$ et dépend de z_0, et où $\varepsilon > 0$ est un nombre arbitrairement petit dont le choix détermine la façon dont nous menons le jeu de poursuite.

Pour donner une idée de la démonstration du théorème et de la mesure de son inexactitude, nous formulerons la propriété principale de la fonction W_t de t.

D) Soient $z_0 \in W_\tau$ et $0 < \varepsilon \leqslant \tau$. Pour chaque contrôle de la fuite $v(t)$, donnée sur le segment $0 \leqslant t \leqslant \varepsilon$, on peut trouver un contrôle de la poursuite $u(t)$, donnée sur le segment $0 \leqslant t \leqslant \varepsilon$, telle que le jeu (4) dans lequel interviennent ces contrôles $u(t)$ et $v(t)$, amène dans le temps ε le point z_0 au point $z_1 = z(\varepsilon)$ qui appartient à l'ensemble $W_{\tau-\varepsilon}$. Cette propriété des fonctions W_t s'appelle la propriété $\mathscr{P}$ (poursuite).

La propriété $\mathscr{P}$ de la fonction W_t permet de terminer le jeu en un temps ne dépassant pas $T(z_0)$, en disposant comme information, de la connaissance de $v = v(s)$ *a priori* c'est-à-dire sur le segment $t \leqslant s \leqslant t + \varepsilon$ où $\varepsilon > 0$ est arbitrairement petit. Si on ne dispose que d'une information *a posteriori*, par exemple de la connaissance de $v(s)$ sur le segment $t - 2\varepsilon \leqslant s \leqslant t - \varepsilon$, on ne peut conclure à l'arrivée sur M.

Le résultat D) peut être sensiblement amélioré [2].

E) Considérons le jeu (4) avec comme ensemble terminal M un ensemble convexe fermé quelconque dans R. Alors il existe, et on peut définir effectivement, un ensemble convexe fermé M_t, dépendant de $t (t \geqslant 0)$, vérifiant la condition $M_0 = M$ et possédant la propriété $\mathscr{P}$ (voir D)). La fonction M_t est maximale parmi les fonctions qui possèdent cette propriété.

Le résultat E) permet de démontrer un théorème analogue au théorème 1 mais plus fort que celui-ci. Si, pour un z donné ($z \in R$), il existe un τ ($\tau \geqslant 0$) tel que $z \in M_\tau$, alors nous désignerons par $T(z)$ le τ minimal pour lequel on a cette appartenance. Alors, si pour la valeur initiale z_0 le nombre $T(z_0)$ est défini, le jeu de poursuite, ayant pour valeur initiale z_0, peut être terminé dans un temps non-supérieur à $T(z_0)$.

Il convient de noter que ce résultat ne donne pas la solution complète du problème de la poursuite. En effet, si pour le z_0 donné, le $T(z_0)$ correspondant n'est pas défini, il peut tout de même arriver que le jeu de la poursuite avec la valeur initiale z_0 soit terminé dans un temps inférieur à un certain nombre. En outre, même si $T(z_0)$ est défini, ce n'est pas nécessairement la meilleure estimation du temps de terminaison.

La fonction maximale M_t a été construite par nous pour des jeux linéaires, mais le fait qu'elle soit maximale a été remarqué par N. Krassovski et A. Soubbotine. Ces mêmes auteurs ont construit une fonction maximale M_t, possédant la propriété $\mathscr{P}$ pour le jeu non-linéaire de la forme (3).

Le jeu de la fuite.

Soit $\hat{\mathscr{L}}$ un sous-espace vectoriel à deux dimensions de l'espace $\mathscr{L}$ (voir A)), pris pour le jeu (4). Par analogie avec A), nous désignerons par π l'opération de projection orthogonale de l'espace R sur $\hat{\mathscr{L}}$ et nous supposerons que

$$\hat{P}_\tau = \hat{\pi} e^{\tau C} \hat{P} \quad ; \quad \hat{Q}_\tau = \hat{\pi} e^{\tau C} Q \tag{17}$$

on a alors le théorème suivant :

THÉORÈME 2. — *Supposons que pour le jeu* (4), *il existe un sous-espace vectoriel* $\hat{\mathscr{L}}$ *a deux dimensions de l'espace* $\mathscr{L}$ (voir A)) *tel que les conditions suivantes soient réalisées :*

a) *on peut trouver un nombre réel* $\mu > 1$ *tel que pour tous les* τ *positifs suffisamment petits, on ait l'inclusion suivante* (voir (17)) :

$$\mu \hat{P}_\tau \subset \hat{Q}_\tau \quad ; \tag{18}$$

b) *il n'existe pas, dans le plan $\hat{\mathscr{L}}$, de droite fixée $\overset{*}{\mathscr{L}}$ telle que, pour tous les τ positifs suffisamment petits, on ait l'inclusion suivante :*

$$\hat{Q}_\tau \overset{*}{\subset} \overset{*}{\mathscr{L}} \tag{19}$$

Alors on peut, pour chaque valeur initiale z_0 du jeu, n'appartenant pas à M, mener le jeu de la fuite de telle façon que le point $z(t)$ n'atteigne jamais l'espace M ($0 \leqslant t < \infty$), *et que, de plus, pour la distance de $z(t)$ à M, on ait l'inégalité* (21).

F) Pour écrire l'évaluation (21), nous ferons correspondre à chaque point $z \in R$ deux nombres positifs ou nuls

$$z \to (\xi, \eta) \tag{20}$$

où ξ est la distance du point z à M et η est la distance de z à $\mathscr{L}$. Pour la valeur initiale z_0, on écrira $z_0 \to (\xi_0, \eta_0)$ et si $z(t)$ est le point variable on écrira

$$z(t) \to (\xi(t), \eta(t)).$$

Il existe alors des nombres positifs C et ε, et un entier naturel K, dépendant du jeu mais non de son déroulement, tels que

$$\xi(t) > \frac{C\xi_0^K}{(1+\eta(t))^K} \qquad \text{pour} \qquad \xi_0 \leqslant \varepsilon \tag{21}$$

Le théorème 2 découle entièrement de la proposition suivante :

G) Au jeu (4), on peut associer deux nombres positifs : θ, définissant un intervalle de temps, et ε, définissant une distance. Ensuite, à toute valeur initiale z_0, telle que $\xi_0 \leqslant \varepsilon$, et à tout contrôle $u(t)$, définie sur $0 \leqslant t \leqslant \theta$, on fait correspondre un contrôle $v(t)$ ($v(t)$ étant défini par le point z_0 et par la fonction $u(s)$, connue sur le segment $0 \leqslant s \leqslant t$). Cette correspondance est telle que, pour la solution $z(t)$ de l'équation (4) avec les contrôles indiqués $u = u(t)$ et $v = v(t)$ et avec la valeur initiale z_0, on ait les deux inégalités suivantes :

$$\xi(\theta) > \varepsilon \tag{22}$$

$$\xi(t) > \frac{C\xi_0^K}{(1+\eta(t))^K} \, 0 \leqslant t \leqslant \theta \tag{23}$$

On appelle contrôle spécial de fuite le contrôle $v(t)$.

Le processus du jeu de la fuite peut être décrit de la façon suivante :

Désignons par S l'ensemble de tous les points $z \in R$, pour lesquels $\xi \leqslant \varepsilon$, et par S' l'ensemble des points z pour lesquels $\xi = \varepsilon$. Si l'état initial z_0 du jeu appartient au cyclindre S, nous faisons immédiatement intervenir le contrôle spécial de la fuite (voir G)) pour un temps $0 \leqslant t \leqslant \theta$, à la fin duquel $z(\theta)$ se trouve en dehors du cylindre S (voir (22)) tandis que, dans le segment $0 \leqslant t \leqslant \theta$, on a l'inégalité (23).

Si, au moment initial $t = 0$, ou à un autre moment intermédiaire t, le point $z(t)$ se trouve en dehors du cylindre S, nous choisissons arbitrairement le contrôle de la fuite $v(t)$ et nous attendons le moment t_0 où le point $z(t_0)$ se trouve sur la surface S^1. En prenant le point $z(t_0)$ pour point initial dans le segment $t_0 \leqslant t \leqslant t_0 + \theta$, nous enclenchons durant ce temps le contrôle spécial de la fuite (voir (6)). Alors, en vertu de (23), dans cet intervalle de temps on a l'inégalité suivante :

$$\xi(t) > \frac{C\varepsilon^K}{(1 + \eta(t))^K} \; ; \; t_0 \leqslant t \leqslant t_0 + \theta \tag{24}$$

et, à la fin de cet intervalle du temps, le point se trouve en dehors du cylindre S et l'étude du jeu recommence. Donc, pendant toute la durée du jeu on a toujours, pour le point $z(t)$, l'une des inégalités (23), (24) ou $\xi(t) \geqslant \varepsilon$. En supposant que $\varepsilon > C\varepsilon^K$, on déduit de ces inégalités l'évaluation (21).

Si, pour la construction du contrôle spécial de fuite $v(t)$, on utilise une information *a posteriori* sur $v(t)$, c'est-à-dire si, pour calculer la valeur $v(t)$, on utilise la connaissance de $v(s)$ dans le segment $-\delta \leqslant s \leqslant t - \delta$, avec

$$0 < \delta < \frac{C_1 \xi_0^l}{(1 + \eta_0)^l} \tag{25}$$

où $C_1 > 0$ et l est un entier naturel, alors les évaluations (22) et (23) restent valables. Ainsi, on peut utiliser, dans le jeu de la fuite, l'information *a posteriori*. Initialement, le théorème 2 sur la fuite a été démontrée dans notre article [3], écrit en commun avec E. Mitchenko, où nous avons supposé les conditions *c*) et *d*) suivantes, plus fortes que *a*) et *b*) :

c) Il existe un nombre $\mu > 1$ tel que pour chaque τ suffisamment petit on ait l'inclusion (voir A)) suivante :

$$\mu P_\tau \overset{*}{\subset} Q_\tau \qquad \text{(comparer à (18))} \tag{26}$$

d) L'application $\pi e^{\tau C}$ étant linéaire et dépendant analytiquement de τ, peut être représentée par une série :

$$\pi e^{\tau C} = g_0 + \tau g_1 + \ldots + \tau g_m^m + \ldots . \tag{27}$$

La condition *d*) affirme qu'il existe un entier $m \geqslant 0$ tel que chacune des applications $g_0, g_1, \ldots, g_{m-1}$ transforme l'ensemble Q en un point et que

$$\dim g_m Q = \nu, \qquad \nu \geqslant 2 \qquad \text{(voir A))}.$$

Nous avons renforcé ultérieurement le résultat, en remplaçant la condition *d*) par la condition plus faible.

e) Pour chaque τ positif suffisamment petit, on a

$$\dim Q_\tau = \nu, \qquad \nu \geqslant 2.$$

Après avoir pris connaissance de notre article, R. Gamkrelidze a exprimé la certitude que, dans les conditions *c*) et *e*), l'espace $\mathscr{L}$ peut être remplacé par n'importe quel sous-espace à deux dimensions $\hat{\mathscr{L}}$. Ainsi, selon lui, le théorème 2 devait être juste si la condition *a*) et la condition suivante *f*) sont satisfaites : $\dim \hat{Q}_\tau = 2$ pour tout τ positif suffisamment petit.

En vérifiant notre démonstration, nous avons trouvé qu'elle reste en effet valable si les conditions *a*) et *f*) sont satisfaites et, en plus, nous avons découvert que la condition *f*) peut être, d'une façon naturelle, remplacée par *b*). Le résultat a donc pris la forme donnée ici.

Exemple.

Considérons, dans un espace euclidien E, de dimension $\nu \geqslant 2$ le mouvement des deux points x et y où x est « le poursuivant » et y l'objet qui fuit.

Le processus de la poursuite se termine quand $x = y$. Les mouvements des points x et y sont définis par les équations

$$x^{(k)} + a_1 x^{(k-1)} + \dots + a_{k-1}\dot{x} + a_k x = u \tag{28}$$

$$y^{(l)} + b_1 y^{(l-1)} + \dots + b_{l-1}\dot{y} + b_l y = v \tag{29}$$

où $x^{(i)}$ et $y^{(i)}$ sont les dérivées d'ordre i des vecteurs x et y par rapport à t, et où

$$a_i, \quad i = 1, \dots, k; \quad b_j, \quad j = 1, \dots, l \tag{30}$$

sont des applications linéaires de E dans E. Les vecteurs u et v, qui sont les vecteurs de commande, appartiennent à E et satisfont aux conditions suivantes :

$$u \in P, \quad v \in Q \tag{31}$$

où P et Q sont des sous-ensembles convexes compacts de E de dimension ν.

Nous dirons que le point y a l'avantage de manœuvrabilité par rapport au point x, si l'une des deux conditions suivantes est vérifiée :

1) $l < k$
2) pour $l = k$ il existe un nombre $\mu > 1$ tel que

$$\mu P \subset Q \tag{32}$$

On découvre que, si l'objet fuyant y a d'avantage de manœuvrabilité par rapport au poursuivant x, ce processus de la poursuite vérifie les conditions c) et d) et donc, si, au moment initial, les points x_0 et y_0 ne coïncident pas, le processus de la fuite continue indéfiniment.

Dans le cas où c'est le poursuivant x qui possède l'avantage de manœuvrabilité, nous pouvons, en appliquant le théorème, trouver dans l'espace des phases de ce jeu, un ensemble ouvert des états initiaux, en partant desquels le jeu se termine toujours.

Cet exemple a été calculé par A. Mesintzev.

BIBLIOGRAPHIE

[1] L. PONTRYAGIN. — Les jeux différentiels linéaires, *Dokl. Akad. Nauk*, 17, NG (1967).
[2] —. — Les jeux différentiels linéaires. II, *Dokl. Akad. Nauk*, 175, No. 4 (1967).
[3] — et E. MITCHENKO. — Le problème de la fuite d'un objet commandé d'un autre objet commandé, *Dokl. Akad. Nauk*, 189, No. 4 (1969).

Steklov Institute
Department of Mathematics,
Vavilova 42, Moscow V 333
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 173 à 189.

SOME PROBLEMS IN HARMONIC ANALYSIS SUGGESTED BY SYMMETRIC SPACES AND SEMI-SIMPLE GROUPS

by E. M. STEIN

CONTENTS

Our purpose is to survey some recent contributions and also to suggest several avenues of further development in the area of analysis indicated by the title of this talk.

1. Introduction: euclidean background.

We begin by saying a few words about the classical case corresponding to $\mathbb{R}^1$. In order to facilitate the presentation that follows we single out three main concerns of that theory as points of reference. These are

A. The Fourier transform

B. The Hilbert transform, $\frac{1}{\pi}\int_{-\infty}^{\infty}\frac{f(x-y)}{y}\,dy$

C. Harmonic and holomorphic functions in the upper half-plane,

$$\mathbb{R}^2_+ = \{ (x, y), y > 0, x \in \mathbb{R}^1 \}.$$

By B we mean of course the whole apparatus that goes with the Hilbert transform, including maximal functions, operators of fractional integration (Riesz potentials), etc., and by C such things as Fatou's theorem, Poisson integrals, Hardy spaces, etc.

Now the upper half-plane is the arena of action of the group $SL(2, \mathbb{R})$ of fractional linear transformations; it is the symmetric space of that group. In this setup the harmonic analysis is taking place, in effect, on the space $\mathbb{R}^1$ which is the *boundary* of the symmetric space [1].

There are two points of view we may take about extending these theories, and in particular A, B and C, in the context of symmetric spaces and semi-simple groups. The first point of view, and the one I have already suggested, is to start with a semi-simple group and its corresponding symmetric space (of non-compact type), and consider a " boundary ". One then performs the harmonic analysis on the boundary, relating it of course to the objects on the group or symmetric space, such as harmonic or holomorphic functions on the symmetric space, or the theory of unitary representations of the group, etc. The first point of view will be taken up in Parts I and II below.

The second point of view is that of considering the (semi-simple) group itself as the primary object of the analysis what we have in mind will be described later, but the best known example that one may cite is that of the " Plancherel formula " for the group [2]. We shall be dealing with other problems, however.

A few more words about the Euclidean background may be in order. Much of what is indicated by our points of reference A, B, and C can be extended to the context of Euclidean $\mathbb{R}^n$. We shall here comment only on the singular integral operators generalizing B [3]. Our concern is then with operators of the form

$$f \to Tf = \int_{\mathbb{R}^n} K(y) f(x-y) dy,$$

where K is a suitable singular kernel. Under appropriate conditions of existence these operators can also be realized as multiplier operators, namely $(Tf)\hat{}(x) = m(x)\hat{f}(x)$, where $\hat{}$ denotes the Fourier transform, and m is in effect the Fourier transform of the kernel K. In the well-known and important case studied by Mihlin and Calderón and Zygmund $K(x)$ is, besides some regularity, homogeneous of degree $-n$, and has mean value zero on the unit sphere. The multiplier m is then homogeneous of degree 0. The Mihlin-Calderón-Zygmund theory and its variants take care of one important class of singularities of the kernel, but there are many other types of singularities and the study of their corresponding operators represents serious difficulties which are still unsurmounted. I cite an example which is both fundamental for the Euclidean theory and has some bearing on our later discussion.

PROBLEM 1 [4]. — *Consider the case of T when the multiplier m is the characteristic*

---

(1) For the theory in the closely related and analogous setting where the unit disc replaces the upper half-plane, see ZYGMUND [36].

(2) See GELFAND and NEUMARK [7], and HARISH-CHANDRA [10], [11].

(3) See e. g. STEIN [29], and the references given there.

(4) For some recent progress in the direction of the solution of this problem, see FEFFERMAN [4]. (Added in proof). A counterxample for $p \neq 2$ has been found by FEFFERMAN.

function of the unit ball in $\mathbb{R}^n$. *It is known that* T *is not bounded on* $L^p(\mathbb{R}^n)$, *when* $1 \leq p \leq 2n/(n+1)$, *or* $2n/(n-1) \leq p \leq \infty$. *Is it bounded when*

$$2n/(n+1) < p < 2n/(n-1)\,?$$

PART I. — ANALYSIS ON THE BOUNDARY

2. Examples of boundaries.

We shall come more quickly to the main points if instead of giving a systematic discussion of the class of spaces X which arise as " boundaries " of non-compact semi-simple groups or symmetric spaces, we list some typical examples (5) (6).

One type of boundary (that could properly be called the *maximal distinguished boundary*) arises from an Iwasawa decomposition of G as KAN. Then the boundary in question of the symmetric space has two essentially equivalent realizations; either in its non-compact form, when it is isomorphic to the nilpotent group N, or in its compact form as K/M; M is the centralizer of A in K. One example of this is

$$G = SU(n-1), \tag{2.1}$$

G/K is the complex n-ball, K/M is its boundary $2n-1$ sphere. Here X is isomorphic with N, and is defined below; it is the genuine boundary of the realization of G/K as a Siegal domain of type II, equivalent to the complex ball via a Cayley transform (7).

X is $\{ (z, \omega), z \in \mathbb{C}^{n-1}, \omega \in \mathbb{R}^1 \}$, with the multiplication law

$$(z_1, \omega_1) \circ (z_2, \omega_2) = (z_1 + z_2, \omega_1 + \omega_2 - 2\,\mathrm{Im}\, z_1 . \bar{z}_2).$$

Another example of a maximal distinguished boundary is

$$G = SL(n, \mathbb{R}), \tag{2.2}$$

and X is isomorphic with $N = n \times n$ strictly upper triangular matrices of G.

Notice that when $n = 3$ in (2.2) we get a boundary which is isomorphic with the one that arises in (2.1) for $n = 2$. The problems that will arise however will be quite different since in the context of (2.1) we are dealing with a rank one situation, and in (2.2) we are in the higher rank case.

Other examples, which do not arise from the Iwasawa decomposition, are:

$$G = Sp(n, \mathbb{R}), \tag{2.3}$$

G/K is the Siegel upper half-space $= \{ x + iy$, x, y real symmetric $n \times n$ matrices,

(5) See however the general theory of SATAKE [24], FURSTENBERG [5] and C. C. MOORE [21].

(6) We shall consider primarily the realizations of the boundaries in their non-compact form, as nilpotent groups.

(7) For the realization of bounded Cartan domains as Siegel domains of type II, see PJATECKIĬ-SAPIRO [22].

and y is pos. def.$\}$. Here X = set of real sym. $n \times n$ matrices, with the additive structure.

$$G = SL(2n, \mathbb{R}), \tag{2.4}$$

but if portioned into $n \times n$ blocks, then the appropriate boundary is isomorphic with $\left\{ \begin{matrix} I_n & x \\ 0 & I_n \end{matrix} \right\}$ as x ranges over $M_n(\mathbb{R}) = n \times n$ real matrices. Thus X can be taken to be $M_n(\mathbb{R})$, with its additive structure

Notice that X, in both (2.3) and (2.4), is a Euclidean space (of dimensions n^2 and $\frac{n(n+1)}{2}$ respectively); but the problems of interest in these examples will not be the Euclidean ones alluded to in section 1.

3. Singular integrals on nilpotent groups.

In generalizing the Euclidean theory to the nilpotent groups which arise as boundaries two fundamental notions need to be introduced: that of *dilations* (8), and that of a *norm function* (9). The first concept generalizes the standard dilations in $\mathbb{R}$ given by scalar multiplication, i. e. $x \to \delta x$, $\delta > 0$, $x \in \mathbb{R}^n$, and is prompted by the observation that broadly speaking, much of the usual harmonic analysis on $\mathbb{R}^n$ is not only translation invariant, but also dilation invariant. The precise definition of dilations is as follows. We assume that with our group X (which is nilpotent and simply connected) we are given a one-parameter group of automorphisms of X, namely $\{\alpha_\delta\}_{0<\delta<\infty}$, so that $\alpha_{\delta_1} \circ \alpha_{\delta_2} = \alpha_{\delta_1 \delta_2}$, α_1 = identity, which is continuous in δ and also contractive. The idea we want is that $\lim\limits_{\delta \to 0} \alpha_\delta(K)$ reduces to the group identity, for any compact set K. A more useful, and somewhat stronger assumption, and the one we shall adopt here, is that when we consider its effect on the Lie algebra of X, namely α_δ^*, then $\alpha_\delta^* = \delta^A$, where A is diagonable with all positive eigenvalues.

Given such a one-parameter group of dilations we introduce a norm function $x \to |x|$ on X as follows. We have $|x| = |x^{-1}|$, also:

$$|x| \geq 0 \tag{3.1}$$

$$|x| \quad \text{is } C^\infty \text{ on the set where} \quad |x| > 0 \tag{3.2}$$

the measure

$$\frac{dx}{|x|} \tag{3.3}$$

is invariant under dilations; here dx is Haar measure on X.

For the purposes of Part I we add the important assumption:

$$|x| = 0, \tag{3.4}$$

if and only if x is the group identity.

---

(8) See Stein [27].

(9) See Knapp and Stein [16].

This is equivalent with the statement that the sets $\{ |x| \leq C \}$ are bounded. We shall see that whether we impose (3.4) or not makes a crucial difference in the theory.

We cite two quick examples. First in $\mathbb{R}^n$ $\alpha_\delta(x) = \delta . x$, and $|x| = \|x\|^n$, where $\| . \|$ is the usual Euclidean norm. Secondly for the boundary X corresponding to the unit ball cited in (2.1), we may take $\alpha_\delta(x) = (\delta z, \delta^2 \omega)$ if $x = (z, \omega)$, and

$$|x| = (|z|^4 + \omega^2)^{n/2}.$$

Armed with the above notions, we come now to some of the results that can be proved. First, there is an elegant analogue of the Hardy-Littlewood maximal theorem. Let K be any bounded subset with non-empty interior on which the dilations α_δ are contractive in the sense that $\alpha_\delta(K) \subset K$, if $\delta \leq 1$; e. g. $K = \{ x, |x| \leq 1 \}$. Write $K_\delta = \alpha_\delta(K)$, and let

$$(Mf)(x) = \sup_{\delta > 0} \frac{1}{m(K_\delta)} \int_{K_\delta} |f(xy)| \, dy \tag{3.5}$$

where $dy = dm$ denotes Haar measure. Then M satisfies all the usual properties of the maximal function. As a consequence whenever f is integrable

$$\lim_{\delta \to 0} \frac{1}{m(K_\delta)} \int_{K_\delta} |f(xy) - f(x)| \, dy = 0, \tag{3.6}$$

for a. e. $x \in X$. We shall come to the applications of the maximal function and (3.6) momentarily.

We discuss next a basic class of singular integrals, written in the form

$$\int_X f(x \cdot y) \frac{\Omega(y)}{|y|^{1-s}} dy \tag{3.7}$$

where the function Ω is homogeneous under α_δ of degree 0, that is $\Omega(\alpha_\delta(x)) = \Omega(x)$, and Ω is suitably smooth away from the group identity. While the integrals have an interest for all complex values of s, and can indeed be studied as meromorphic functions of s, the range when Re $(s) = 0$ is the most critical, and we shall thus impose that restriction for the rest of this section.

Assuming then that Re $(s) = 0$, and f is bounded and sufficiently smooth, then the integral (3.7) can be defined in several ways. First if the mean-value of Ω vanishes, i. e.

$$\int_{a_1 \leq |x| \leq a_2} \Omega(x) dx = 0,$$

then as a principal-value integral

$$\lim_{\varepsilon \to 0} \int_{|y| \geq \varepsilon} f(x \cdot y) \frac{\Omega(y)}{|y|^{1-s}} dy; \tag{3.7'}$$

or more generally, if the mean-value of Ω vanishes or if $s \neq 1$, then the integral exists as

$$\lim_{\substack{s' \to s \\ \mathrm{Re}(s') > 0}} \int f(x \cdot y) \frac{\Omega(y)}{|y|^{1-s'}} dy \ ([10]). \tag{3.7''}$$

([10]) If $s = 1$ and the mean-value of Ω is nonzero, then the integral cannot be defined without a non-trivial normalizing factor; such a factor has the effect of making it a constant multiple of $f(x)$.

The above limits exist for every x and also in the $L^2(X)$ norm. If we denote the limiting operator by $f \to T(f)$, then the first result is its extensibility to a bounded operator on $L^2(X)$,

$$\| T(f) \|_2 \leq A \| f \|_2. \tag{3.8}$$

Unfortunately this fundamental result cannot be proved by following the standard arguments of the Euclidean case of $\mathbb{R}^n$, because what would amount to a calculation in terms of the Fourier transform (in the sense of the unitary representations of the group X) seems to lead to unmanageable computations. The one attack which has succeeded in proving (3.8) was suggested by a method originally applicable only in $\mathbb{R}^n$. It turns out that even in the general case T can be written, in effect, as an infinite sum of uniformly bounded operators

$$T = \sum_{j=-\infty}^{\infty} T_j, \qquad \| T_j \| \leq A, \tag{3.9}$$

where the T_j are almost orthogonal in the sense

$$\| T_j^* T_k \| \leq a(|j-k|), \qquad \| T_j T_k^* \| \leq a(|j-k|) \tag{3.10}$$

with a sequence $\{ a(k) \}$ which decreases sufficiently rapidly. The two conditions (3.9) and (3.10) suffice to prove the boundedness of T ([11]).

Once the L^2 result (3.8) has been obtained then by using the facts about the maximal function (3.5), and following the broad lines laid down by Calderón and Zygmund for the case of $\mathbb{R}^n$, one can also obtain the L^p theory, and the L^1 results, namely that the operators in question are of weak type (1,1) ([12]).

Some rather immediate generalizations of the above are possible. First, the specific form of the kernel $\dfrac{\Omega(x)}{|x|^{1-s}}$ allows a variety of modifications in form. Secondly, and more interesting, is the fact that the same theory can be carried out in a setting which replaces the existence of dilations by appropriate substitute conditions on the open sets $K_\delta = \{ x : |x| < \delta \}$. This generalization is used if one wants to find the analogues of the above maximal function and singular integrals on the compact version of X, which is of course related to X via a Cayley transform.

4. Some applications.

We shall now discuss several applications of the theory sketched above.

1. One can construct the *intertwining operators* for the principal series of representations by means of the operator (3.7). Let $G = KAN$ as before, then the representations induced by irreducible representations of the subgroup MAN are the principal series. Thus there is natural action of G on the boundary X (where X is isomorphic with N), which action generalizes the usual action of $SL(2, \mathbb{R})$ in $\mathbb{R}^1$ given

([11]) See Knapp and Stein [16]. Earlier ideas of this kind are due to M. Cotlar.

([12]) This is due to Rivière [23], Koranyi and Vagi [18], Coifman and de Guzman [3].

by fractional linear transformations ([13]), and in terms of which the principal series can be defined. Now the action of the elements of M on X are particularly simple, and these transformations have Jacobian determinant equal to one. This allows us to define the Jacobian determinant corresponding to each element of the Weyl group of G. The square roots of the reciprocals of these Jacobian determinants each provide us with an example of a norm function. It is to be emphasized that each satisfies the properties (3.1), (3.2) and (3.3) for appropriate " dilations " coming from the subgroup A, but in general not the crucial compactness property (3.4). However, in the case of *rank one* (when $\dim A = 1$), the non-trivial element of the Weyl group gives us a norm function (satisfying also (3.4)), and the dilations are provided by the conjugations of X given by A. All the intertwining operators are then of the form (3.7), after suitable normalization. This construction provides the basic information as to irreducibility and analytic continuation (that is existence and unitarity of the complementary series). The general case, when G has higher rank, can also be treated to some extent, since the intertwining operators can then be written as products of rank-one intertwining operators ([14]).

2. A special case of the intertwining operators, which arise for a particular representation of the group $SU(n, 1)$ (discussed with its boundary in (2.1)) is the *Cauchy integral* for the complex ball. In the unbounded realization of the ball, if one takes the Cauchy-Szego kernel which represents H^2, then as boundary integrals one is lead the singular integrals (3.7) with $\dfrac{\Omega(x)}{|x|} = \text{constant} \times (|z|^2 + i\omega)^{-n}$, and

$$|x| = (|z|^4 + \omega^2)^{n/2},$$

where $(z, \omega) \in \mathbb{C}^{n-1} \times \mathbb{R}^1$, and $\alpha_\delta(z, \omega) = (\delta z, \delta^2 \omega)$ ([15]).

3. In this application the space $X = \mathbb{R}^n$, but the dilations are not the usual ones. These are now given by $\alpha_\delta(x) = (\delta^{a_1} x_1, \delta^{a_2} x_2, \ldots, \delta^{a_n} x_n)$, with $x = (x_1, \ldots, x_n)$, where $a_i > 0$. We can put

$$|x| = \inf\{\lambda > 0, \sum_{i=1}^{n} x_i^2/\lambda^{2a_i} \leq 1\}^{\Sigma a_i}.$$

Then the theory described above reduces essentially to the Euclidean theory of singular integrals with separate homogeneity due to Jones, Fabes and Rivière, Lizorkin and Kree ([16]). Notice that this has many points in common with example 2 just cited, in that the degree of singularity of the kernels depends on the different directions of approach to the group identity. The present application differs from the preceding, however, in that the convolution is commutative.

([13]) This comes about by identifying (modulo sets of measure zero) G/MAN with θN, where θ is the Cartan involution, and then identifying X with θN.

([14]) For details concerning the above application to intertwining operators, see Knapp and Stein [16]. Some earlier works in this subject may be found in Kunze and Stein [20], and Schiffman [25]. See also the recent paper of Helgason in *Advances in Mathematics*, vol. 5, 1970, 1-154.

([15]) See Gindikin [9] and Koranyi and Vagi [18].

([16]) See e. g., Kree [19].

Examples 2 and 3 suggest the following problem which, as should be understood, we state only rather vaguely.

PROBLEM 2. — *Construct appropriate algebras of singular integrals (or more generally pseudo-differential operators), together with their symbolic calculus, which algebras are to incorporate such examples as* 2 *and* 3 *as their building blocks.*

It is strongly indicated that such algebras should have applications to various non-elliptic problems, in particular in complex analysis, such as behavior near a pseudo-convex boundary and properties of solutions of $\bar{\partial}$ problems.

4. As a final application, in this case of the maximal function (3.5) we mention some results dealing with harmonic functions on the symmetric space G/K and centering about *Fatou's theorem* and *Poisson integrals.* In the case of bounded functions, the generalization of the boundary behavior guaranteed by the classical Fatou theorem turns out to be a direct consequence of two facts: *a)* Furstenberg's representation of bounded harmonic functions as Poisson integrals, and *b)* the maximal function, and in particular (3.6) ([17]).

However, in the case of Poisson integrals in general (e. g. of L^p functions), much remains to be done. The problems involving Poisson integrals will be discussed more fully when we treat the higher rank case below.

PART II. — ANALYSIS ON THE BOUNDARY; HIGHER RANK CASE

We shall discuss now the situation when the assumption (3.4) concerning the norm function is not satisfied, that is when the sets $\{ x : |x| \leq c \}$ are no longer bounded. Very often in this case the group of automorphisms of X which preserve the measure $\frac{dx}{|x|}$ is larger than a one-parameter group, and so in considering the appropriate dilations it is not entirely natural to limit oneself to a fixed one-parameter group of dilations as we did in Part I. It is for this reason that we refer to the situation when (3.4) is not satisfied as the *higher rank case.*

The rank-one case treated above provides us—at least on the formal level—with an idea of the kind of problems that may be of interest in the general case. However, those results have only a limited applicability in the present context; one instance of this is the decomposition of intertwining operators for the principal series as products of rank-one intertwining operators, already mentioned. In general, however, new and different methods surely need to be developed here.

We shall organize our presentation by discussing several different but related problems which reflect the fragmentary state of our knowledge at this stage.

([17]) HELGASON and KORANYI [12]. This has been superseded by a later results of KORANYI and KNAPP and WILLIAMSON. See [17].

5. **The Siegel upper half-space.**

We are dealing with the example cited in (2.3). X is the space of $n \times n$ real symmetric matrices under addition, which is the Bergman-Shilov boundary of the Siegel domain $= \{ x + iy;\ x, y$ real $n \times n$ symmetric, y pos. def. $\}$. The action of $Sp(n, \mathbb{R})$ imposes the following structure on X. The dilations are provided by the mappings: $x \to ax^ta$, where $a \in GL(n, \mathbb{R})$, and for norm function we take $|x| = |\det(x)|^{\frac{n+1}{2}}$.

Let us first look at the analogues of the integrals (3.7) with the kernels $\dfrac{\Omega(x)}{|x|^{1-s}}$, where Ω is homogeneous in the sense that $\Omega(ax^ta) = \Omega(x)$, $a \in GL(n, \mathbb{R})$. These integrals have a long history, going back to Siegel, Bochner, and others. We indicate an interesting example arising from the Cauchy kernel. Consider the H^2 space of holomorphic functions $f(x + iy)$ on the Siegel upper half-space, those which satisfy

$$\sup_{y>0} \int_X |f(x+iy)|^2 dx < \infty.$$

Such functions have boundary values, namely $\lim_{y \to 0} f(x + iy) = f(x)$ exists in the $L^2(X)$ norm. Their integral representation in terms of their boundary values is then [18]

$$f(x+iy) = c \int_X \left(\det(t+iy)\right)^{\frac{-n-1}{2}} f(x-t)\,dt \tag{5.1}$$

where c is an appropriate constant.

The boundary value functions form a closed subspace of $L^2(X)$, and the orthogonal projection on this subspace is formally given by an operator of the form (3.7), where now $\dfrac{\Omega(x)}{|x|} = c\left(\det(x)\right)^{\frac{-n-1}{2}}$. Rigorously the operator is given as the limit as $y \to 0$ in (5.1), and more particularly as

$$\lim_{\substack{\varepsilon \to 0 \\ \varepsilon > 0}} c \int_X \left(\det(t + i\varepsilon I)\right)^{\frac{-n-1}{2}} f(x-t)\,dt. \tag{5.2}$$

This operator then is clearly a natural generalization of the Hilbert transform to the present context. A host of questions arise for it, but only a few have an answer at present. We indicate one such unsolved problem:

PROBLEM 3. — *The operator* (5.2) *is a projection on* $L^2(X)$. *Is it bounded on any other* $L^p(X)$ *space*?

The close relation of this problem with problem 1 (in section 1) can be aeen as follows. The operator (5.2) is a multiplier operator corresponding to the characteristic function of the cone of positive definite real $n \times n$ matrices. When $n = 2$ this cone is equivalent with a circular cone in $\mathbb{R}^3$, and the intersection of that cone with an appropriate plane is a disc in $\mathbb{R}^2$. Thus by a theorem of de Leeuw, a positive resolution of problem 3 for any p, when $n = 2$, implies the same for problem 1 when $n = 2$.

([18]) See BOCHNER [1].

Part of the difficulty in dealing with integrals such as (5.2) lies in the fact that the singularities of the kernel, that is where $|x| = 0$, are a whole variety and not merely a point. However, one is not always stimied by this obstacle. An example of this is the Poisson integral, closely related to (5.2); it is given by

$$\int_X P_y(t) f(x-t)\,dt \tag{5.3}$$

where

$$P_y(x) = \frac{c\,(\det(2y))^{\frac{n+1}{2}}}{|\det(x+iy)|^{n+1}},$$

and $f \in L^p(X)$.

It can be shown that as $y \to 0$ " regularly ", then the integral (5.3) converges to f almost everywhere, even for $f \in L^1(X)$ ([19]). This result is rather delicate because as $y \to 0$, the singularities of the kernel $P_y(x)$ again appear on the variety $|x| = 0$. It shows us that the hope of carrying out a theory for integrals of the type (5.2) may not be entirely forlorn.

Our discussion for the Siegel upper half-space may be generalized as follows. We consider any bounded symmetric domain of Cartan and realize it as a tube domain when this is possible, or in general as a Siegel domain of type II ([20]). The Cauchy kernel has also been determined ([21]), and we can of course pose the analogue of problem 3 (For the complex ball the answer is in the affirmative for $1 < p < \infty$, by the discussion of section 4). Finally there is an analogue of the Poisson kernel, and the result sketched above is known to hold in that generality ([19]).

6. **Poisson integrals.**

We have already alluded to Poisson integrals at several occasions, and we shall now discuss them in their generality. Briefly the setting is as follows. For any symmetric space G/K, the class of harmonic functions are those annihilated by all G-invariant differential operators which annihilate constants. Equivalently, these functions can be characterized by the mean-value property. Now every harmonic function which is appropriately bounded at ∞ can be represented as a Poisson integral, which is in effect a convolution on the group X isomorphic to N. By the mean-value property the Poisson kernel P can be described as follows. We have already pointed out the existence of a natural correspondence between X and the compact homogeneous space K/M, if one leaves out an appropriate set of measure zero ([22]). If we transplant Haar measure of K/M to X we get a measure of the form $P(x)dx$, where dx is Haar measure on X.

Now the subgroup A acts on X by automorphisms $x \to axa^{-1}$, $a \in A$. Let α_δ be a one-parameter subgroup of these automorphisms which are dilations in sense defined

([19]) STEIN and N. J. WEISS [33].
([20]) See footnote ([7]).
([21]) See GINDIKIN [9].
([22]) See footnote ([13]).

in section 3. It is then easy to see that for any $f \in L^p(X)$, $1 \leq p < \infty$, the Poisson integral

$$\int_X P(y) f(x \cdot \alpha_\delta(y)) dy \tag{6.1}$$

converges to f in the $L^p(X)$ norm, as $\delta \to 0$.

The main real-variable problem can then be stated as follows.

PROBLEM 4. — *Does the integral* (6.1) *converge almost everywhere, as* $\delta \to 0$, *for any* $f \in L^p(X)$, $1 \leq p$?

One gets an idea of the resistive nature of the problem by observing the increase in difficulty met in passing from the classical case of the upper half-plane, to the case of the product of half-planes contained in the theorem of Marcinkiewicz and Zygmund (23).

The farthest advance of the problem at present is the solution of a closely related variant for the symmetric spaces which are bounded domains, already alluded to in section 5. That variant differs from the present one in that it refers to a different boundary of the symmetric space in question, one that can be viewed as a quotient space of the maximal distinguished boundary occurring in problem 4 (24).

There is a reason why problem 4 in its general setting seems more complicated than the analogue already obtained for the case of bounded domains. To over-simplify matters a little, it is as follows: the locus of singularities in the latter problem (e. g. $\{ \det(x) = 0 \}$) is generated by straight lines issuing from the origin. Along these lines the theory for $\mathbb{R}^1$ is applicable and then the result follows by a rather delicate calculation which is akin to " integrating " over appropriate lines. In the general case, however, straight lines would have to be replaced by other curves; these curves are the orbits of points under one-parameter groups of dilations. The above raises a simply-stated (and possibly fundamental) problem which we shall discuss only in the context of $\mathbb{R}^n$. Let $\gamma(t)$ be the curve $\gamma(t) = \operatorname{sign}(t)(A_1 |t|^{a_1}, A_2 |t|^{a_2}, \ldots, A_n |t|^{a_n})$ where $A_1, \ldots, A_n$ are real, and $a_i > 0$. Consider the analogue of the Hilbert transform

$$(Tf)(x) = \int_{-\infty}^{\infty} f(x + \gamma(t)) \frac{dt}{t} \tag{6.2}$$

(Notice that if $a_1 = a_2 \ldots = a_n$, then this reduces essentially to the classical Hilbert transform along the direction defined by $(A_1, A_2, \ldots, A_n)$). Consider also the associated maximal operator

$$(Mf)(x) = \sup_{h>0} \frac{1}{h} \int_0^h | f(x + \gamma(t)) | \, dt \tag{6.3}$$

PROBLEM 5. — *Is there an* $L^p(\mathbb{R}^n)$ *theory for* T *and* M?

An analogous result for nilpotent groups (in particular for M) could be applied to the solution of problem 4.

---

(23) See ZYGMUND [36], Chapter 17.

(24) This incidentally raises the question of giving an intrinsic characterization of the functions which arise as Poisson integrals for the other boundaries.

There is one hopeful indication that may be mentioned concerning problem 5. A calculation carried out by Wainger and myself (see [31]) shows that the operators (6.2) when suitably defined is bounded on $L^2(\mathbb{R}^n)$, (and the bound does not depend on $A_1, A_2, \ldots, A_n$).

7. The matrix space $M_n(\mathbb{R})$.

We shall now consider the example (2.4), with $X = M_n(\mathbb{R})$ the $n \times n$ real matrices, and $G = SL(2n, \mathbb{R})$. Here we take as dilations the mappings $x \to axb^{-1}$, with $a, b \in GL(n, \mathbb{R})$, and as norm function $|\det(x)|^n$.

This example has obviously some resemblance to that of the Siegel upper half-space in section 5, but it differs from it in that the space $M_n(\mathbb{R})$ has not only the obvious additive structure (its group structure), but upon removal of a set of measure zero what remains also has a multiplicative structure ($GL(n, \mathbb{R})$). The situation has an analogy with that of a field (e. g. $\mathbb{R}^1$) where one of the concerns is with the interplay of an additive and a multiplicative harmonic analysis. The additive harmonic analysis here is that given by

$$(7.1) \qquad \mathscr{F}(f) = \int_{M_n(\mathbb{R})} e^{2\pi i tr(x^t y)} f(y)dy,$$

while the multiplicative analysis (the analogue of the Mellin transform) is given by the unitary (infinite-dimensional) representations of $GL(n, \mathbb{R})$. This interplay is at the bottom of the results detailed below (See also section 8).

The most direct analogue of the integral (3.7) arises if $\Omega \equiv 1$. We consider therefore

$$(7.2) \qquad I_s(f) = \int_{M_n(\mathbb{R})} f(x-y) \frac{dy}{|y|^{1-s}}$$

The L^2 theory of this integral is contained in the following statement ([25]). Suppose f is C^∞ and has bounded support. (7.2) initially defined as an absolutely convergent integral when $\mathrm{Re}(s) > 1 - \frac{1}{n}$ has a meromorphic continuation into the whole complex plane, and when $\mathrm{Re}(s) = 0$ the operator $f \to I_s(f)$ is unitary modulo a multiplicative constant. More precisely, with

$$\gamma_*(s) = \prod_{j=1}^{n} \alpha(ns - j + 1), \qquad \alpha(s) = \pi^{1/2-s}\Gamma\left(\frac{s}{2}\right)/\Gamma\left(\frac{1-s}{2}\right),$$

we have that when $\mathrm{Re}(s) = 0$, I_s is a multiplier operator with multiplier $\gamma_*(s)|x|^{-s}$.

The above also has the following consequences:

(*a*) The facts just stated can be reinterpreted by saying that the Fourier transform of the distribution $|x|^{-1+s}$ is $\gamma_*(s)|x|^{-s}$, where both distributions are defined by analytic continuation. This functional equation is closely related to the functional equations of generalizations of the zeta function, and is therefore of interest in several number-theoretic questions (see also the generalizations in (8.3) below).

([25]) See the references cited in footnote ([29]).

(*b*) The operators (7.2) also serve as intertwining operators, but not for the principal series. They arise typically in the " degenerate series ", in this case for the group $SL(2n, \mathbb{R})$.

(*c*) If we write $A(s) = \gamma_*^{-1}(s)I_s$, and $B(s)$ as the multiplication operator by $|x|^{-s}$, then as we have seen $A(s)B(s)$ is unitary when $\text{Re}(s) = 0$. In addition $A(s)B(s)$ has an analytic continuation as bounded operators (on $L^2(M_n(\mathbb{R}))$, in the strip $0 \leq \text{Re}(s) < 1/2n$. This fact is important in constructing certain uniformly bounded and unitary (complementary series) representations of the group $SL(2n, \mathbb{R})$.

There are many variants and generalizations of the above that can be suggested; we shall discuss briefly one typical of those we have in mind. The underlying space X will be $\mathbb{R}^n$ and we will pick a fixed non-degenerate quadratic form Q on it, which for simplicity we normalize as $Q(x) = x_1^2 + x_2^2 \ldots + x_k^2 - x_{k+1}^2 \ldots - x_n^2$. We introduce the norm function $|x| = |Q(x)|^{n/2}$. The analogue of the integral (7.2) is the integral

$$I_s(f) = \int_{\mathbb{R}^n} f(x-y)\,|Q(y)|^{-\frac{n}{2}(1-s)}dy \tag{7.3}$$

It has well-known analytic continuations, going back to M. Riesz and Gelfand and Graev ([26]). We let $B(s)$ denote the operator of multiplication by $|x|^{-s} = |Q(x)|^{-ns/2}$.

PROBLEM 6. — *Are the $I_sB(s)$ bounded operators on $L^2(X)$ in some strip of the form* $0 < \text{Re}(s) < c$? ([27]).

An interesting approach to this problem might be to study the decomposition of the action of $0(n, Q)$ on $L^2(\mathbb{R}^n)$, since after all, the operators $I_sB(s)$ commute with this action ([28]).

PART III. — ANALYSIS ON THE GROUP

8. Euclidean Fourier transform.

The interplay of the additive and multiplicative harmonic analysis on $M_n(\mathbb{R})$, mentioned in the previous section, will now be outlined. We take the additive Fourier transform given by (7.1). A simple change of variables leads to a slight modification of itself, which we shall call $\mathscr{F}^*$ where now

$$\mathscr{F}^*(f) = e * f, \tag{8.1}$$

with the convolution taken on the group $GL(n, \mathbb{R})$, and

$$e(x) = e^{2\pi i tr(x-1)}\,|x|^{-n/2}.$$

([26]) See GELFAND *et al.* [8].

([27]) When Q is definite, the answer is yes, with $c = 1/2$. The cases $n = 1$ and 2 are in KUNZE and STEIN [20]; their method essentially applies to all n, but in the definite case only. When $n = 4$, $k = 2$, we are back to $M_2(\mathbb{R})$, so $c = 1/4$.

([28]) Part of the decomposition of the action of $0(n, Q)$ on $L^2(\mathbb{R}^n)$ is in the book of VILENKIN [34].

The properties of $\mathscr{F}^*$ are then twofold: $\mathscr{F}^*$ is unitary on $L^2(GL(n, \mathbb{R}))$, and secondly $\mathscr{F}^*$ commutes with both left and right group multiplication, i. e. with the action $f(x) \to f(a^{-1}x)$, $f(x) \to f(xb)$, $a, b \in GL(n, \mathbb{R})$. (The original $\mathscr{F}$ had this commutation property only when both a and b were orthogonal). $\mathscr{F}^*$ is therefore a *central* operator on $L^2(GL(n, \mathbb{R}))$. From this it follows by a general form of Schur's lemma that whenever $x \to \rho(x)$ is an irreducible unitary representation of $GL(n, \mathbb{R})$ we may expect that

$$\rho(\mathscr{F}^*(f)) = \gamma(\rho)\rho(f) \tag{8.2}$$

whenever f and $\mathscr{F}^*(f)$ are in $L^1(GL(n, \mathbb{R})) \cap L^2(GL(n, \mathbb{R}))$. Here $\gamma(\rho)$ is a constant factor which depends only on the representation ρ.

This identity is formally equivalent with the statement

$$\mathscr{F}\left(\frac{\rho(x)}{|x|^{1-s}}\right) = \gamma_s(\rho)\rho({}^tx^{-1})\,|x|^{-s} \tag{8.3}$$

where the factor $\gamma_s(\rho)$ can be immediately read off from the factor $\gamma(\rho)$.

When ρ is the trivial representation, then $\gamma_s(\rho)$ reduces to the factor $\gamma_*(s)$ of the previous section. The other cases where the factor $\gamma_s(\rho)$, (and thus $\gamma(\rho)$) has been computed explicitly are those for the representations ρ which arise in the decomposition of $L^2(GL(n, \mathbb{R}))$, (i. e. those which occur in the " Plancherel formula " for the group). In this case, because of the unitary character of $\mathscr{F}^*$, all the factors $\gamma(\rho)$ have absolute value one.

It is particularly simple to describe these factors in the analogous case corresponding to $M_n(\mathbb{C})$. In that case if the representation is induced from the character of the triangular subgroup which has value

$$|\delta_1|^{it_1}\left(\frac{\delta_1}{|\delta_1|}\right)^{m_1} \cdots |\delta_n|^{it_n}\left(\frac{\delta_n}{|\delta_n|}\right)^{m_n}$$

for a triangular matrix with eigenvalues $(\delta_1, \ldots, \delta_n)$, then

$$\gamma(\rho) = \prod_{j=1}^{n} \left\{ i^{|m_j|}\pi^{it_j}\Gamma\left(\frac{|m_j| + 1 + it_j}{2}\right) \Big/ \Gamma\left(\frac{|m_j| + 1 - it_j}{2}\right) \right\}$$

The formulae in the case $M_n(\mathbb{R})$ have a similar appearance but are more complicated because there are now $[n/2] + 1$ different series of representations which occur in the L^2 reduction of $GL(n, \mathbb{R})$ ([29]).

The mapping $f \to \rho(f)$ may be viewed as the natural generalization of the Mellin transform (to which it reduces when $n = 1$). The explicit determination of the factors $\gamma(\rho)$ which occur in (8.2) gives the desired multiplicative analysis of the additive Fourier transform in $M_n(\mathbb{R})$. This " Mellin transform " analysis of $\mathscr{F}$ is the main tool in the proof of several results of the previous section, in particular those stated in paragraph (*c*).

([29]) The results sketched above, and those in section 7, were first obtained in the complex case (corresponding to $M_n(\mathbb{C})$); see STEIN [26]. In the real case they were obtained by GELBART [6], but in the meanwhile several of these problems had been dealt with from a different point of view by GODEMENT (unpublished), and JACQUET and LANGLANDS [14]. These authors have also obtained extensions to the p-adic analogue, when $n = 2$.

A related question arises by analogy with the ordinary Fourier transform on $\mathbb{R}^n$. The fact that the Fourier transform commutes with rotations leads to a well-known decomposition of $L^2(\mathbb{R}^n)$, compatible with the Fourier transform. The various invariant subspaces are defined in terms of spherical harmonics, and the restriction of the Fourier transform to each can be described in terms of appropriate Bessel functions ([30]). The theory of higher Bessel functions, in the setting of matrix spaces, has been started by Bochner ([31]), but much still remains to be done. This discussion is the background for the following problem.

PROBLEM 7. — *Describe the action of the Fourier transform* $\mathscr{F}$ *on* $L^2(M_n(\mathbb{R}))$ *when restricted to the subspaces invariant under the action* $f(x) \to f(a^{-1}xb)$, $a, b \in O(n)$, *in terms of appropriate generalizations of spherical harmonics and Bessel functions.*

9. **Other problems on the group manifold.**

The last general question we shall deal with is the following. Is it possible to develop a systematic generalization of some of the objects dealt with in Parts I and II, such as Hilbert transforms, boundedness of various convolution operators, multipliers, etc. but on the semi-simple group itself, and not on one of its boundaries.

For compact groups, the answer is surely yes ([32]). However, for non-compact groups, the situation seems to be far from clear. Part of the difficulty of the problem there, and also its interest I believe, is that unlike the classical case the group Fourier transform of an L^p function, $1 \leq p < 2$, is actually analytic in some of its parameters. It is thus more like the classical Laplace transform than the classical Fourier transform. The analyticity of the Fourier transform is intimately connected with the possibility of analytic continuation of the representations of the non-compact semi-simple groups, but even this subject is far from understood ([33]).

To get a better inkling of the nature of these questions, we pose the simplest convolution problems. Suppose we know the L^p classes of two functions f and g, what is the class of $f * g$? There is a very general answer, valid for any locally compact unimodular group, and it is given by Young's inequality and its variants. Young's inequality is

$$\| f * g \|_r \leq \| f \|_p \| g \|_q, \qquad \text{where} \qquad \frac{1}{r} = \frac{1}{p} + \frac{1}{q} - 1.$$

The variants of Young's inequality (which include the theorem of fractional integration for $\mathbb{R}^n$ of Hardy, Littlewood and Sobolev) arise when we replace these norms by " weak-type " norms. For $\mathbb{R}^n$ these inequalities are in the nature of best possible; for semi-simple groups this is far from the case. In fact the evidence already at hand, and described below, suggests the following L^2 convolution problem for semi-simple groups.

([30]) See e. g. STEIN and WEISS [32], Chapter IV.

([31]) See BOCHNER [2] and HERZ [13].

([32]) See STEIN [28], where part of this has been carried out; see also COIFMAN and DE GUZMAN [3] and N. J. WEISS [35].

([33]) See KUNZE and STEIN [20], and the survey article, STEIN [30].

PROBLEM 8. — *Suppose G is semi-simple and has finite center. Prove that*

$$\| f * g \|_2 \leq A_p \| f \|_p \| g \|_2, \quad \text{if} \quad 1 \leq p < 2.$$

This problem involves only the relative sizes of $|f|$ and $|g|$, and thus, one would think, should be resolvable without any detailed study of the group Fourier transform of f or of analytic continuation of representations. Paradoxically however, that approach is the only one that has had any substantial success so far. The answer to problem 7 is known to be affirmative in the following cases ([33]).

(i) $G = SL(2, \mathbb{R})$
(ii) G is any complex classical group, i. e. $SL(n, \mathbb{C})$, $SO(n, \mathbb{C})$, or $Sp(n, \mathbb{C})$
(iii) G is any semi-simple group, but the function f is assumed to be bi-invariant, i. e. $f(k_1 x k_2) = f(x)$, when $k_1, k_2 \in K$, and K is a maximal compact subgroup of G.

REFERENCES

[1] S. BOCHNER. — Group invariance and Cauchy's formula in several variables, *Ann. of Math.*, 45 (1944), pp. 686-701.

[2] —. — Bessel functions and modular relations of higher type and hyperbolic differential equations, *Com. Sem. Math. Lund* (1952), pp. 12-20.

[3] R. COIFMAN and M. DE GUZMÀN. — Singular integrals and multipliers on homogeneous spaces, to appear.

[4] C. FEFFERMAN. — Inequalities for strongly singular convolution operators, *Acta Math.*, 124 (1970), pp. 9-36.

[5] H. FURSTENBERG. — A Poisson formula for semi-simple Lie groups, *Ann. of Math.*, 77 (1963), pp. 335-386.

[6] S. GELBART. — Fourier analysis on $GL(n, \mathbb{R})$, *Proc. Nat. Acad. Sci.*, 65 (1970), pp. 14-18.

[7] I. M. GELFAND and M. NEUMARK. — *Unitäre Darstellungen der Klassischen Gruppen*, Berlin, 1957.

[8] I. M. GELFAND *et al.* — *Generalized functions*, vol. 1, New York, 1964.

[9] S. G. GINDIKIN. — Analysis in homogeneous domains, *Uspekhi Mat. Nauk*, 19 (1964), pp. 3-92.

[10] HARISH-CHANDRA. — The Plancherel formula for complex semi-simple groups, *Trans. Amer. Math. Soc.*, 76 (1954), pp. 485-528.

[11] —. — Harmonic analysis on semi-simple Lie groups, *Bull. Amer. Math. Soc.*, 76 (1970), pp. 529-551.

[12] S. HELGASON and A. KORANYI. — A Fatou-type theorem for harmonic functions on symmetric spaces, *Bull. Amer. Math. Soc.*, 74 (1968), pp. 258-263.

[13] C. HERZ. — Bessel functions of matrix argument, *Annals of Math.*, 61 (1955), pp. 474-523.

[14] H. JACQUET and R. LANGLANDS. — Automorphic forms on $GL(2)$, *Lecture notes*, No. 114, Springer-Verlag.

[15] A. W. KNAPP. — Fatou's theorem for symmetric spaces I, *Ann. of Math.*, 88 (1968), pp. 106-127.

[16] — and E. M. STEIN. — Singular integrals and the principal series, *Proc. Nat. Acad. Sci.*, 63 (1969), pp. 281-284 ; II, *ibid.*, 66 (1970), pp. 13-17 ; also « Existence of Complementary Series » in *Problems in Analysis: Symposium in Honor of Salomon Bochner*, Proceedings to appear in 1971.

[17] — and R. E. WILLIAMSON. — Poisson integrals and semi-simple groups, to appear in *J. d'Analyse Math.*

[18] A. Koranyi and S. Vagi. — Intégrales singulières sur certains espaces homogènes, *C. R. Acad. Sci. Paris*, 268 (1969), pp. 765-768.
[19] P. Kree. — Sur les multiplicateurs dans FL_p, *Ann. Inst. Fourier*, 16 (1966), pp. 31-89.
[20] R. A. Kunze and E. M. Stein. — Uniformly bounded representations, *Amer. J. of Math.*, 82 (1960), p. 162 ; II, *ibid.*, 83 (1961), pp. 723-786 ; III, *ibid.*, 89 (1967), pp. 385-442.
[21] C. C. Moore. — Compactifications of symmetric spaces, I, *Amer. J. of Math.*, 86 (1964), pp. 201-218 ; II, *ibid.*, pp. 358-378.
[22] I. I. Pjateckii-Shapiro. — *Geometry of classical domains and automorphic functions*, Fizmatgiz (1961) (Russian).
[23] N. Rivière. — On singular integrals, *Bull. Amer. Math. Soc.*, 75 (1969), pp. 843-847.
[24] I. Satake. — On representations and compactifications of Symmetric Riemannian spaces, *Ann. of Math.*, 71 (1960), pp. 77-110.
[25] G. Schiffman. — Intégrales d'entrelacement, *C. R. Acad. Sci.* Paris, 266 (1968), pp. 47-49, pp. 859-861 ; also Thèse Paris (1969).
[26] E. M. Stein. — Analysis in matrix spaces and some new representations of $SL(N, \mathbb{C})$, *Annals of Math.*, 86 (1967), pp. 461-490.
[27] —. — *The analogues of Fatou's theorem and estimates for maximal functions* (C. I. M. E., 3° Ciclo, Urbino, 1967), Cremonese, Roma (1968), pp. 291-307.
[28] —. — Topics in harmonic analysis related to the Littlewood-Paley theory, *Annals of Math.*, study No. 63, Princeton, 1970.
[29] —. — *Singular integrals and differentiability properties of functions*, Princeton, 1970.
[30] —. — Analytic continuation of group representations, *Advances in Math.*, 4 (1970), pp. 172-207.
[31] — and S. Wainger. — The estimation of an integral arising in multiplier transformations, *Studia Math.*, 35 (1969), pp. 101-104.
[32] — and G. Weiss. — *Introduction to Fourier Analysis on Euclidean Spaces*, 1971
[33] — and N. J. Weiss. — On the convergence of Poisson integrals, *Trans. Amer. Math. Soc.*, 140 (1969), pp. 35-54.
[34] N. A. Vilenkin. — Special functions and the theory of group representations, *Amer. Math. Soc. Transl.*, Providence, 1968.
[35] N. J. Weiss. — Article in preparation.
[36] A. Zygmund. — *Trigonometric series*, Cambridge, 1959.

Department of Mathematics
Princeton University
Fine Hall
Princeton, N. J. 08540
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 191 à 199.

ALGEBRAIC K-THEORY

by RICHARD G. SWAN

I will give here a brief account of the history of algebraic K-theory and some of its main ideas and problems. Some of the work being done in this field at the present time will then be discussed in more detail.

1. Origin and basic results.

Although some early work of J. H. C. Whitehead [41] [42] and G. Higman [19] was later recognized as properly belonging to algebraic K-theory, the subject really began with Grothendieck's work on the Riemann-Roch theorem [9]. In this work, Grothendieck introduced the functor K, now known as K_0. For the case of rings, this functor may be described as follows. If R is a ring with unit, $K_0(R)$ is the abelian group with one generator $[P]$ for each finitely generated projective R-module P, and a relation $[P] = [P'] + [P'']$ for each short exact sequence $O \to P' \to P \to P'' \to 0$. The definition obviously extends to other categories, eg. sheaves, vector bundles, etc. Aside from its use in the Riemann-Roch theorem, this functor has found a number of applications to topology and algebra. For example, Wall [39] showed that if, X is a connected space dominated by a finite CW complex, there is a well defined obstruction $w \in K_0(Z\pi_1(X))$ such that X has the homotopy type of a finite complex if and only if $w = 0$. This result was then used by Siebenmann [31] to give a similar obstruction to the possibility of adding a boundry to an open manifold. This result, together with a calculation of $K_0(Z\pi)$ for a free abelian group π, was then used to prove the important Splitting theorem for manifolds [32]. A more algebraic application may be found in [36]. If G is the cyclic permutation group acting on 47 indeterminates x_i, then the fixed field of $Q(x_1, \ldots, x_{47})$ under G is not a pure transcendental extension of Q.

Probably the best known application of Grothendieck's functor K is the topological K-theory of Atiyah and Hirzebruch [3]. These authors consider a topological space X and define $K^0(X)$ by using vector bundles on X in place of the projective modules considered above. By applying this functor to suspensions of X, they define $K^n(X)$ for $n \leqslant 0$. Bott periodicity shows that $K^n(X) \approx K^{n+8}(X)$ and this is used to define $K^n(X)$ for all $n \in Z$. The resulting functors K^n constitute a cohomology theory, i. e. they satisfy the exactness, excision, and homotopy axioms of [10]. The resulting topological K-theory has found many important applications, for example in Adams' solution of the vector field problem for spheres [1]. A good exposition of this theory may be found in [2].

The next big step in algebraic K-theory was taken by Bass [4]. He tried to find algebraic analogues of the topological functors K^n. By imitating the construction of bundles over a suspension using clutching functions, he found a good definition for the functor $K_1(R)$. This is generated by symbols $[P, \alpha]$ where P is a finitely generated projective R-module and α is an automorphism of P. The relations are $[P, \alpha\beta] = [P, \alpha] + [P, \beta]$ and $[P, \alpha] = [P', \alpha'] + [P'', \alpha'']$ if $O \to P' \xrightarrow{i} P \xrightarrow{j} P'' \to 0$ is exact and $\alpha i = i\alpha', j\alpha = \alpha'' j$. Thie group turns out to be the same as one introduced by J. H. C. Whitehead [41] [42], $K_1(R) = GL(R)/E(R)$ where $E(R) = [GL(R), GL(R)]$ is the subgroup of $GL(R)$ generated by elementary matrices $e_{ij}(r) = 1 + re_{ij}$. Whitehead's theory of simple homotopy types shows that the group $K_1(Z\pi)$ has important topological applications. An example of this is the well known s-cobordism theorem [22].

Bass also succeeded in proving a partial analogue of the exactness and excision properties.

THEOREM 1 (Bass). — *If I is a 2-sided ideal of R, there is an exact sequence*

$$K_1(R, I) \to K_1(R) \to K_1(R/I) \to K_0(R, I) \to K_0(R) \to K_0(R/I).$$

The group $K_0(R, I)$ depends only on I considered as a ring without unit.

The second statement expresses the excision property. For the definition of the relative groups $K_i(R, I)$ and the proof, see [6].

There are two other, essentially equivalent, formulations of this result which avoid the use of the relative groups.

THEOREM 2 (Milnor [26]). — *Let*

$$\begin{array}{ccc} A & \to & A_1 \\ \downarrow & & \downarrow{\scriptstyle f_1} \\ A_2 & \underset{f_2}{\to} & A' \end{array}$$

be a cartesian diagram of ring homomorphisms such that f_1 or f_2 is onto. Then there is an exact Mayer-Vietoris sequence

$$K_1(A) \to K_1(A_1) \oplus K_1(A_2) \to K_1(A') \to K_0(A) \to K_0(A_1) \oplus K_0(A_2) \to K_0(A').$$

The other formulation, due to Gersten, requires a preliminary definition. If R is a ring without unit, we can adjoin a unit formally to R getting a ring R^+ with unit and a split exact sequence $O \to R \to R^+ \leftrightarrows Z \to 0$. If F is a functor from rings with unit to abelian groups, we extend the definition of F by setting

$$F(R) = \ker [F(R^+) \to F(Z)].$$

This is consistent provided that F preserves finite products [35], in particular for K_0 and K_1. Theorem 2 continues to hold with this extended definition.

THEOREM 3 (Gersten [13]). — *If $O \to A \to B \to C \to 0$ is an exact sequence of rings, there is an exact sequence $K_1A \to K_1B \to K_1C \to K_0A \to K_0B \to K_0C$.*

The hypothesis means that A is a 2-sided ideal of B and $C = B/A$. Therefore A has no unit if $C \neq 0$ (in general).

In addition to the above exact sequences, there is also an exact sequence associated with a localization [6]. This is rather technical and we will not consider it here, but will only mention one of its most important consequences. The following theorem is due to Bass, Farrell and Hsiang [6] [12] and gives a more precise version of an earlier result of Bass, Heller and Swan [7].

THEOREM 4. — *There is a split exact sequence*

$$O \to K_1R \to K_1R[t] \oplus K_1R[t^{-1}] \to K_1R[t, t^{-1}] \to K_0R \to 0$$

Also we have $K_1R[t] = K_1R \oplus \mathrm{Nil}\ R$ *where* $\mathrm{Nil}\ R = 0$ *if* R *is regular.*

It follows that $K_1R[t, t^{-1}] = K_1R \oplus K_0R \oplus \mathrm{Nil}\ R \oplus \mathrm{Nil}\ R$.

The group Nil R is defined in a manner similar to K_0R using pairs (P, ν) where ν is a nilpotent endomorphism of P. Details may be found in [6]. This group also has an interesting topological application [11].

2. Problems.

One of the most important problems in algebraic K-theory is simply to compute the groups K_iR for various rings R. Group rings $Z\pi$ are particularly important in view of the topological applications. Considerable work has been done on various special cases. Most of the results can be found in [6] [8] [25]. Recently Kervaire and Murthy [23] computed $K_0(Z\pi)$ for π cyclic of prime power order. The computation makes use of classfield theory.

Another important problem is that of finding analogues of algebraic K-theory corresponding to the various classical groups. For $K_1R = GL(R)/E(R)$, the group $GL(R)$ is replaced by orthogonal, symplectic, and unitary groups. For K_0 we consider projective modules with quadratic, symplectic, and Hermitian forms. There is considerable topological interest in this since Wall's surgery obstruction groups are K-functors of this type [40]. Work on this problem has been done by Wall and his students, Bass [5], Milnor [27], Shaneson [30] and M. Stein [34].

A third major problem is that of defining functors $K_n(R)$ for all $n \in Z$. This problem is immediately suggested by the analogy with topological K-theory. A great deal of work is being done on this problem at the present time. I will discuss here some of the results which have been obtained.

It is natural to ask that the functors K_n satisfy the analogues of Theorems 2 and 3, i. e. that the exact sequences extend indefinitely in both directions. We would also like the analogue of Theorem 4 to hold with K_1, K_0 replaced by K_n, K_{n-1}. For $n \leqslant 0$ this determines K_n uniquely. If we have K_n, $K_{n-1}R$ must be the cokernel of the map $K_nR[t] \oplus K_nR[t^{-1}] \to K_nR[t, t^{-1}]$. This definition of K_n for $n < 0$ is due to Bass [6] who shows that it satisfies all the above requirements. Also $K_nR = 0$ for $n < 0$ if R is regular. Details may be found in [6].

For $n \geqslant 2$, we are not so fortunate. A number of definitions for K_nR have been proposed but no analogue of Theorem 2 has been found. This is explained by the following result.

THEOREM 5. — *There is no functor* K_2 *from rings to abelian groups such that for each cartesian diagram*

$$\begin{array}{ccc} A & \to & A_1 \\ \downarrow & & \downarrow f \\ A_2 & \to & A' \end{array}$$

with f a split epimorphism, there is an exact sequence

$$K_2A_1 \oplus K_2A_2 \to K_2A' \to K_1A \to K_1A_1 \oplus K_1A_2$$

We will now consider some of the definitions which have been proposed for K_nR, $n \geqslant 2$.

3. Milnor's K_2.

A very reasonable candidate for K_2R was defined by Milnor [26]. The elementary matrices $e_{ij}(r)$ satisfy certain relations which were found by Steinberg. Milnor considers the group $St(R)$ with generators $x_{ij}(r)$ satisfying the Steinberg relations

$$x_{ij}(r+s) = x_{ij}(r)x_{ij}(s), \ [x_{ij}(r), x_{kl}(s)] = 1$$

if $i \neq 1$, $j \neq k$, and $[x_{ij}(r), x_{jk}(s)] = x_{ik}(rs)$ if $i \neq k$. Define $\varphi : St(R) \to GL(R)$ by $\varphi(x_{ij}(r)) = e_{ij}(r)$. Milnor defines $K_2R = \ker \varphi = \text{center } (St(R))$.

THEOREM 6 (Milnor [26]). — *If*

$$\begin{array}{ccc} A & \to & A_1 \\ \downarrow & & \downarrow f_1 \\ A_2 & \underset{f_2}{\to} & A' \end{array}$$

is a cartesian diagram of ring homomorphisms and both f_1 and f_2 are onto, there is an exact sequence

$$K_2A \to K_2A_1 \oplus K_2A_2 \to K_2A' \to K_1A \to K_1A_1 \oplus K_1A_2 \to K_1A' \to \ldots \to K_0A'.$$

This is quite a reasonable approximation to Theorem 2 and about the best one can expect in view of Theorem 5. There is no obvious analogue of Theorem 3 but the sequence of Theorem 1 extends to

$$K_2(R, I) \to K_2R \to K_2(R/I) \to K_1(R, I) \to K_1R \to K_1(R/I) \to \ldots \to K_0(R/I).$$

Excision fails for $K_1(R, I)$ by Theorem 5.

It is not known whether the analogue of Theorem 4 holds for K_2 but J. Wagoner [38] has recently shown that $K_2(R[t, t^{-1}]) = K_2R \oplus K_1R \oplus$? (1). The last summand is still unknown. It is also not known whether $K_2R[t] = K_2R$ for R regular.

The group K_2R is extremely difficult to compute in general. Recently, H. Matsumoto succeeded in computing K_2F for any field F using a very ingenious construction. This leads to some interesting results on algebraic number fields [31].

One further difficulty with K_2 is that there is no obvious definition in terms of categories similar to that of K_0 and K_1. In § 7 we will discuss one possible solution to this problem.

4. Theory of Gersten and Swan.

For convenience, we will work here with rings without unit. If R is a free ring, Gersten [14] and Stallings [33] have shown that $K_0R = K_1R = 0$. This suggests

(1) This result was also obtained independently by KAROUBI [43].

the requirement $K_nR = 0$ for free R. This resembles the effacability axiom of homological algebra [18] and suggests defining K_n by taking the derived functors of $GL(-)$. Since this is nonabelian, we have to use simplicial methods. A resolution of GL is a functor G_* from rings to simplicial groups together with an augmentation $\varepsilon\colon G_0 \to GL$ such that $\varepsilon\partial_0 = \varepsilon\partial_1$. We want to choose some such resolution and define $K_nR = \pi_{n-2}(G_*(R))$, for $n \geqslant 3$. We define K_1 and K_2 by the exact sequence $0 \to K_2R \to \pi_0 G_*(R) \to GL(R) \to K_1R \to 0$. In [35], I used the theory of acyclic models to find such a resolution. The requirement that $K_nR = 0$ for a free ring R is equivalent to the requirement that G_* be aspherical on models, the models being the free rings. Among all such resolutions, there is a universal one G_* such that if H_* is any resolution which is aspherical on models, there is a map $G_* \to H_*$ unique up to homotopy. Using this G_* we get a series of functors which I will denote by K_n^S. A different approach was investigated by Gersten [15]. He considers the forgetful functor U: Rings $\to$ Sets and its coadjoint $F(S)$ = free ring on S. The composition $T = FU$ is a cotriple on the category of rings which can be used to construct a simplicial ring $T_*(R)$. Gersten uses the resolution $GL(T_*(R)) \to GL(R)$ to define his K functors which I will denote by K_n^G. Gersten's resolution is aspherical on models so there is a map $K_n^S \to K_n^G$. I have recently shown that this is an isomorphism and will therefore use the notation K_n^{GS} for these functors. It is known that $K_1^{GS} = K_1$ and that there is an epimorphism $K_2 \to K_2^{GS}$. This will be an isomorphism if and only if $K_2R = 0$ for free rings R but this has not yet been proved.

The sequence of Theorem 1 is easily extended by converting $G_*(R) \to G_*(R/I)$ into a fibration but it is not known whether there is an exact Mayer-Vietoris sequence for the K_n^{GS} under any reasonable hypothesis, eg. that of Theorem 6. It is also not known whether any of the statements of Theorem 4 hold for the K_n^{GS}. The problem of computing K_n^{GS}, even for a field, seems to be extremely difficult. It is also not known how to extend the definition to categories.

5. Theory of Karoubi-Villamayor.

In [28], Nobile and Villamayor gave another definition of K_n, essentially by defining the " suspension (2) " of a ring. Independently, Karoubi [20] gave a definition of K_n for categories. The two points of view were combined in [21]. The construction of these functors was rather complicated. Recently, Gersten gave a simpler definition using simplicial methods [16]. I will follow Gersten in denoting these functors by $\kappa_n(R)$. The theory has the disadvantage that $\kappa_1(R) \neq K_1(R)$. In fact,

$$\kappa_1(R) \approx GL(R)/U(R)$$

where $U(R)$ is the subgroup generated by all unipotent elements. However, except for this, the theory has many very nice properties. The functors κ_n can be characterized by axioms similar to those of homology theory [16] [21]. To state these, we need some preliminary definitions. We again use the category of rings without unit. A ring homomorphism $f\colon R \to R'$ will be said to have the covering homotopy property if every $X(t) \in GLR'[t]$ with $X(0) = 1$ can be lifted to $GLR[t]$. We say that f is a fibration is $R[x_1,\ldots,x_m, y_1,\ldots,y_n, y_1^{-1},\ldots,y_n^{-1}] \to R'[x_1,\ldots,y_1,\ldots,y_1^{-1},\ldots]$ has the

(2) Karoubi points out that the term " loop space " would be more appropriate.

covering homotopy property for all m, n. (This is somewhat stronger than the property used in [16] [21]). We also say that two ring homomorphisms $f, g: R \to R'$ are homotopic ($f \simeq g$) if there is a ring homomorphism $h: R \to R'[t]$ such that $\partial_0 h = f$, $\partial_1 h = g$, where $\partial_i: R'[t] \to R'$ is given by $\partial_i(p(t)) = p(i)$, $i = 0, 1$.

The functors κ_n are characterized by the following axioms [16] [21].

(1) For each exact sequence $O \to A \to B \to C \to 0$ of ring homomorphisms with f a fibration, there is a natural exact sequence

$$\ldots \to \kappa_n A \to \kappa_n B \to \kappa_n C \to \kappa_{n-1} A \to \ldots \to \kappa_1 B \to \kappa_1 C \to K_0 A \to K_0 B \to K_0 C$$

(2) If $f \simeq g: R \to R'$, then $\kappa_n(f) = \kappa_n(g): \kappa_n R \to \kappa_n R'$.

Axiom 2 is equivalent to the statement that $\kappa_n R[t] = \kappa_n R$. The functors κ_n can be computed as follows [16]. Let $ER = tR[t] = \ker \partial_0 : R[t] \to R$. Then $\partial_1 : ER \to R$ is a fibration. Let $\Omega R = t(t-1)R[t]$ be its kernel. Then Axiom 2 shows that $\kappa_n ER = 0$ so Axiom 1 gives $\kappa_{n+1} R = \kappa_n \Omega R$ for $n \geqslant 1$ and $\kappa_1 R = \ker [K_0 \Omega R \to K_0 ER]$.

To compare κ_n with K_n^{GS} we make one more definition. If F is a functor from rings to abelian groups, we define $\bar{F}(R)$ to be the co-equalizer of $F(\partial_0)$, $F(\partial_1): F(R[t]) \rightrightarrows FR$. This $\bar{F}$ satisfies Axiom 2 and $F \to \bar{F}$ is universal for maps of F into a functor satisfying Axiom 2. Gersten's simplicial definition and the universal property of K_n^S give us a map $K_n^{GS} \to \kappa_n$ and therefore $\bar{K}_n^{GS} \to \kappa_n$. It is not known whether this is an isomorphism for all n, but this is so for $n = 1$. Using a result of Gersten [15], it is easy to see that $\bar{K}_2(R) = \bar{K}_2^{GS}(R) = \kappa_2(R)$ if Nil $R = 0$, eg. if R is regular.

It is not known whether the analogue of Theorem 4 holds for the functors κ_n, but Gersten [17] has shown that this is so when Nil $R = 0$, i. e. $\kappa_n R[t, t^{-1}] = \kappa_n R \oplus \kappa_{n-1} R$ in this case (3). In general, if we define $\kappa_0 = K_0$, then $\kappa_n R[t, t^{-1}] = \kappa_n R \oplus \kappa_0 \Omega^n R$, so Theorem 4 will hold if and only if $\kappa_0 \Omega R = \kappa_1 R$. This is equivalent to the statement that, in the exact sequence of Axiom 1, we can replace K_0 by κ_0. If so, this can be extended to all $n \leqslant 0$ using the functors $\kappa_n = K_n$, $n \leqslant 0$, all of which satisfy Axiom 2.

So far, little progress has been made in computing $\kappa_n R$ for $n \geqslant 2$. Even for the case where R is a field, it is not known whether $\kappa_2 R = K_2 R$. It is quite possible, however, that $\kappa_n R$ will turn out to be easier to compute than K_n. Perhaps a simpler proof of Matsumoto's theorem could be found in this way. Karoubi's definition can be used to define κ_n for categories but this is quite complicated compared to the definitions of K_0 and K_1.

6. Theory of Quillen.

A very interesting topological definition of $K_n R$ was recently proposed by Quillen [29]. I would like to thank Quillen for sending me a detailed account of his work. All rings here will be assumed to have a unit. The definition was suggested by the relation between the homology of the group $GL(R)$ and the functors $K_1(R)$, $K_2(R)$. In fact, $K_1 R = H_1(GL(R))$ and $K_2 R = H_2(E(R))$. Quillen takes the classifying space $BGL(R)$ and attaches 2-cells to kill the subgroup $E(R)$ of $\pi_1 BGL(R) = GL(R)$. This introduces new cycles in dimension 2 but these can all be killed by attaching 3-cells. The result is a space B_R with some very remarkable properties.

(3) This result was also obtained independently by KAROUBI [43].

THEOREM 7 (Quillen). — *B_R is a homotopy associative, homotopy commutative H-space. The map $BGL(R) \to B_R$ gives an isomorphism of homology.*

Clearly B_R can be regarded as the best H-space approximation to $BGL(R)$. Quillen also considers a functor $R\ (X)$ which is defined as K_0 of the category of finitely generated projective R-modules with $\pi_1(X)$-action. He shows that the functor $[X, B_R]$ is, in a reasonable sense, the best approximation to R_R by a representable functor. This justifies his definition of $K_n R$ as $\pi_n(B_R)$. We denote these functors here by K_n^Q. Quillen also notes that $K_1^Q = K_1$ and $K_2^Q = K_2$ (Milnor's K_2). This gives further justification for his definition.

Using his calculation of the cohomology of finite linear groups, Quillen can actually compute all of the $K_n^Q(R)$ for the case where R is a finite field.

THEOREM 8 (Quillen). — *For $i > 0$, $K_{2i}^Q(F_q) = 0$ and $K_{2i-1}^Q(F_q) = \otimes\, {}^i\mu_{q^i-1}$, where μ_m is the group of m — th roots of unity in the algebraic closure of F_q.*

To compute $K_n^Q(R)$ for other rings R, the first step would be to calculate $H_*(GL(R))$. For example, it is reasonable to conjecture that $K_n(\underline{Z})$ is a torsion group for all n. This is equivalent to the conjecture that $H_*(GL(Z), Q)$ is trivial. In fact, Mumford and Milnor have conjectured that $H_*(GL_n(\underline{Z}), \underline{Q})$ is trivial for each n. If P_n is the space of positive definite quadratic forms in n variables and $X_n = P_n/GL_n(\underline{Z})$, the above conjecture is equivalent to the conjecture that X_n is acyclic over $\underline{Q}$. Now X_2 is actually contractible and the same seems to be true for X_3 although the proof involves a long calculation which I have not checked. Perhaps X_n is contractible for all n. A result of Magnus [24] shows that $GL_n(\underline{Z})$ is a direct limit of subgroups related to GL_2 and GL_3. It should be possible to use this to reduce the general case to that where $n = 2$ and 3. It would also be interesting to extend the results of Magnus to other rings. Possibly this could be used to prove a stability theorem for K_n^Q analogous to that of Bass for K_1 [6].

It is natural to ask whether $K_n^Q \approx K_n^{GS}$. This would imply that for a free ring R (with unit) we would have $K_n^Q(R) \approx K_n^Q(\underline{Z})$ or, equivalently, that $H_n(GL(R)) \approx H_n(GL(\underline{Z}))$. A proof of this would probably be one of the main steps in showing that $K_n^Q \approx K_n^{GS}$.

One can produce an exact sequence for K_n^Q similar to that of Theorem 1 by converting $B_R \to B_{R/I}$ into a fibration. I do not know whether the analogue of Theorem 4 holds for K_n^Q.

7. Extension to categories.

The groups $K_n^Q(R)$ depend only on the group $GL(R)$. This property is regarded as a disadvantage by Karoubi and Villamayor [21] who would like $K_n(R)$ to reflect properties of the ring R and not just those of $GL(R)$. However, this property suggests a simple way to extend the definition of K_n^Q to categories. If F is a functor from groups to groups, we would like to define $K_F(\mathscr{A})$ for a category $\mathscr{A}$ by taking some sort of direct limit of the groups F (Aut $(\mathscr{A})$) for $A \in \mathscr{A}$. The functor K_1 was treated in this way by Bass in [6]. I will give here one easy way of doing this which is suggested by the definition of K_1.

If E is a short exact sequence $O \to A' \xrightarrow{i} A \xrightarrow{j} A'' \to 0$, we define Aut (E) to be the subgroup of Aut (A') $\times$ Aut (A) $\times$ Aut (A'') consisting of those $(\alpha', \alpha, \alpha'')$ with $\alpha i = i\alpha'$, $j\alpha = \alpha'' j$.

Let F be a functor from groups to groups. We define $K_F(\mathscr{A})$ to be the abelian group with generators $[A, u]$ for $A \in \mathscr{A}$, $u \in F(\mathrm{Aut}(A))$ and with the relations.

(1) $[A, uv] = [A, u] + [A, v]$.

(2) If E, as above, is a short exact sequence and $w \in F(\mathrm{Aut}(E))$ has images $u' \in F(\mathrm{Aut}(A'))$, $u \in F(\mathrm{Aut}(A))$, $u'' \in F(\mathrm{Aut}(A''))$, then $[A, u] = [A', u'] + [A'', u'']$.

For example, if $F(G) = G$ or $G/[G, G]$, then $K_F(\mathscr{A}) = K_1(\mathscr{A})$. If F is a constant functor with value $F(G) = \pi$ for all G, then $K_F(\mathscr{A}) = K_0(\mathscr{A}) \oplus \pi/[\pi, \pi]$.

To get $K_n(\mathscr{A})$, we define F_n by taking BG, killing $[G, G] \subset \pi_1 BG$ by Quillen's method, getting a space BG^+, and setting $F_n(G) = \pi_n BG^+$. We then let $K_n(\mathscr{A}) = K_{F_n}(\mathscr{A})$ (The group Aut (A) should be replaced by $\varinjlim$ Aut (A^n) here).

Now, if $\mathscr{A} = \mathscr{P}_R$ is the category of finitely generated projective R-modules, it is not hard to show that $K_F(\mathscr{P}_R) = F(GL(R))$ provided that F has certain properties. These properties are exactly those which Quillen proves in his work on K_n^Q. Therefore we see that $K_n(\mathscr{P}_R) = K_n^Q(R)$. This gives some justification for our definition. In particular, since $K_2^Q = K_2$, this method gives a reasonable extension of Milnor's K_2 to categories.

If we use only split exact sequences, it should not be too hard to express $K_F(\mathscr{A})$ as a filtered direct limit as in [6]. In this way we could presumably obtain a space B_{A} with $K_n(\mathscr{A}) = \pi_n(B_{\mathrm{A}})$.

A more general form of the above construction is obtained by replacing F (Aut (A)) by K (End A) where K is a functor from rings to groups. In this way, any K-theory could be extended to categories.

REFERENCES

[1] J. F. Adams. — Vector fields on spheres, *Ann. of Math.*, 75 (1962), pp. 603-632.

[2] M. F. Atiyah. — *K-theory*, Benjamin, New York (1967).

[3] — and F. Hirzebruch. — Vector bundles and homogeneous spaces, *Proc. of Symp. in Pure Math., Amer. Math. Soc.*, 3 (1961), pp. 7-38.

[4] H. Bass. — K-theory and stable algebra, *Publ. Math. I. H. E. S.*, 22 (1964), pp. 5-60.

[5] —. — *Topics in algebraic K-theory*, Tata Inst., Bombay (1966).

[6] —. — *Algebraic K-theory*, Benjamin, New York (1968).

[7] —, A. Heller and R. G. Swan. — The Whitehead group of a polynomial extension, *Publ. Math. I. H. E. S.*, 22 (1964), pp. 61-79.

[8] —, J. Milnor and J.-P. Serre. — Solution of the congruence subgroup problem for SL_n, $n \geq 3$ and Sp_{2n}, $n \geq 2$, *Publ. Math. I. H. E. S.*, 33 (1968), pp. 59-137.

[9] A. Borel et J.-P. Serre. — Le théorème de Riemann-Roch (d'après A. Grothendieck), *Bull. Soc. Math., France*, 86 (1958), pp. 97-136.

[10] S. Eilenberg and N. E. Steenrod. — *Foundations of Algebraic Topology*, Princeton (1952).

[11] T. Farrell. — The obstruction to fibering a manifold over a circle, *Bull. Amer. Math. Soc.*, 73 (1967), pp. 737-740.

[12] — and W. C. Hsiang. — A formula for $K_1 R_\alpha[T]$ *Proc. of Symp. in Pure Math., Amer. Math. Soc.*, 17 (1970), pp. 192-218.

[13] S. Gersten. — Thesis, Cambridge (1964).

[14] —. — Whitehead groups of free associative algebras, *Bull. Amer. Math. Soc.*, 71 (1965), pp. 157-159.

[15] —. — On the functor K_2, *I*, to appear.
[16] —. — On Mayer-Vietoris functors and algebraic K-theory, to appear.
[17] —. — On the K-theory of Laurent polynomials, to appear.
[18] A. GROTHENDIECK. — Sur quelques points d'algèbre homologique, *Tohoku Math. J.*, 9 (1957), pp. 119-221.
[19] G. HIGMAN. — The units of group rings, *Proc. London Math. Soc.*, 46 (1940), pp. 231-248.
[20] M. KAROUBI. — Foncteurs dérivés et K-théorie, *C. R. Acad. Sci. Paris*, 267 (1968), pp. 328-331 et 345-348.
[21] — et O. VILLAMAYOR. — K-théorie algébrique et K-théorie topologique, *C. R. Acad. Sci. Paris*, 269 (1969), pp. 416-419.
[22] M. KERVAIRE. — Le théorème de Barden-Mazur-Stallings, *Comm. Math. Helv.*, 40 (1965), pp. 31-42.
[23] — and M. P. MURTHY. — To appear.
[24] W. MAGNUS. — Über *n*-dimensionale Gittertransformationen, *Acta Math.*, 64 (1935), pp. 355-367.
[25] J. MILNOR. — Whitehead torsion, *Bull. Amer. Math. Soc.*, 72 (1966), pp. 358-426.
[26] —. — *Notes on algebraic K-theory*, mimeographed, M. I. T. (1969).
[27] —. — Algebraic K-theory and quadratic forms, to appear.
[28] A. NOBILE et O. VILLAMAYOR. — Sur la K-théorie algébrique, *Ann. Sci. Ec. Norm. Sup.*, 1 (1968), pp. 581-616.
[29] D. QUILLEN. — The K-theory associated to a finite field, to appear.
[30] J. SHANESON. — Wall's surgery obstruction groups for *Z*, *G*, *Bull. Amer. Math. Soc.*, 74 (1968), pp. 467-471.
[31] L. SIEBENMANN. — Thesis, Princeton (1965).
[32] — and D. SULLIVAN. — To appear.
[33] J. STALLINGS. — Whitehead torsion of free products, *Ann. of Math.*, 82 (1965), pp. 354-363.
[34] M. STEIN. — Thesis, Columbia (1970).
[35] R. G. SWAN. — Non-abelian homological algebra and K-theory, *Proc. of Symp. in Pure Math., Amer. Math. Soc.*, 17 (1970), pp. 88-123.
[36] —. — Invariant rational functions and a problem of Steenrod, *Invent. Math.*, 7 (1969), pp. 148-158.
[37] J. TATE. — Symbols in arithmetic, *this volume*.
[38] J. WAGONER. — On the structure of K_2 of the Laurent series ring, to appear.
[39] C. T. C. WALL. — Finiteness conditions for *CW* complexes, *Ann. of Math.*, 81 (1965), pp. 56-69.
[40] —. — *Surgery on compact manifolds*, mimeographed notes, Liverpool (1968).
[41] J. H. C. WHITEHEAD. — Simplicial spaces, nuclei and *m*-groups, *Proc. London Math. Soc.*, 45 (1939), pp. 243-327.
[42] —. — Simple homotopy types, *Amer. J. Math.*, 72 (1950), pp. 1-57.
[43] M. KAROUBI. — La périodicité de Bott en *K*-théorie générale, *C. R. Acad. Sci. Paris*, 270 (1970), pp. 1305-1307.

Department of Mathematics,
University of Chicago
Chicago, Illinois 60637
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 201 à 211.

SYMBOLS IN ARITHMETIC

by JOHN TATE

§ 1. Symbols and K_2.

Let F be a commutative field, $F^{\cdot}$ its multiplicative group, and let C be a commutative group. A *symbol on F with values in C* is a function

$$(\,,\,): F^{\cdot} \times F^{\cdot} \to C$$

satisfying the two identities

$$(1) \qquad (aa', b) = (a, b)(a', b) \quad \text{and} \quad (a, bb') = (a, b)(a, b')$$

$$(2) \qquad (a, 1 - a) = 1.$$

Replacing a by a^{-1} in (2) and then using (1) and (2) gives

$$(3) \qquad (a, -a) = 1, \quad \text{and hence} \quad (a, a) = (a, -1).$$

Replacing a by ab in (3) and expanding using (1) and (3) gives then

$$(4) \qquad (a, b) = (b, a)^{-1}.$$

EXAMPLE 1. — Suppose v is a discrete valuation of F, with residue field k_v. Then

$$(5) \qquad (a, b)_v = \text{residue class of } (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}}$$

is a symbol on F with values in $k_v^{\cdot}$, called the *tame symbol at v*; Cf. e. g. [12, Ch. III, no. 4].

Let F_s denote a separable algebraic closure of F, and let $G_F = \mathrm{Gal}\,(F_s/F)$. If X is a topological G_F-module we shall write $H^r(F, X)$ for the r-th cohomology group of the complex $C^*(G_F, X)$ of continuous standard cochains on G_F with values in X. When X is discrete, these groups are the usual Galois cohomology groups; cf. e. g. [13].

EXAMPLE 2. — Let m be a natural number not divisible by the characteristic of F, and let μ_m be the group of m-th roots of unity in F_s. The exact sequence

$$(6) \qquad 0 \to \mu_m \to F_s^{\cdot} \xrightarrow{m} F_s^{\cdot} \to 0$$

gives rise to a homomorphism

$$(7) \qquad \delta_m : F^{\cdot} \to H^1(F, \mu_m),$$

Putting

$$(8) \qquad (a, b)_m = \delta_m a \,.\, \delta_m b,$$

we obtain a symbol on F with values in $H^2(F, \mu_m \otimes \mu_m)$ which was discussed briefly in [16]. Its main property is this

$$\{ a, b \} \in (K_2F)^m \Leftrightarrow (a, b)_m = 1 \Leftrightarrow b \in N_{E_a/F}E_a^{\cdot}, \tag{9}$$

where E_a is the F-algebra $F[X]/(X^m - a)$, and the notations $\{\ ,\ \}$ and K_2 are as explained below.

When $\mu_m \subset F$ we have

$$H^2(F, \mu_m \otimes \mu_m) = H^2(F, \mu_m) \otimes \mu_m = (\mathrm{Br}\ F)_m \otimes \mu_m,$$

where $(\mathrm{Br}\ F)_m$ is the group of elements of order dividing m in the Brauer group of F. In this case the symbol $(a, b)_m$ is well known; cf. e. g. [11, Ch. XIV].

Example 3. — The formula

$$(a, b)_{\mathrm{diff}} = \frac{da}{a} \wedge \frac{db}{b}$$

defines a symbol on F with values in the group $\Omega^2_{F/\mathbb{Z}}$.

Steinberg [15] showed that for $n \geq 3$, the group $H_2(SL_n(F), \mathbb{Z})$ was generated by the values $\{ a, b \}_n$ of a certain canonical symbol on F with values in that group, except if F has 2, 3 or 4 elements, in which case the same result holds for $n \geq 5$. Matsumoto [7], showed that Steinberg's symbols $\{\ ,\ \}_n$ are universal. It follows that the group $K_2F = H_2(SL_\infty(F), \mathbb{Z})$ discussed by Swan at this Congress is the target group of a universal symbol $\{\ ,\ \}$; for each abelian group C, the map $f \mapsto f(\{\ ,\ \})$ is a bijection between Hom (K_2F, C) and the group of symbols on F with values in C. In other words, K_2F is presented as an abelian group by the generators $\{ a, b \}$, for a and b in F, and the relations $\{ 1 \}$ and $\{ 2 \}$ obtained by replacing parentheses by curly brackets in (1) and (2) above. This is the " computation " of K_2F referred to yesterday by Swan.

The notions of *dimension* of a vector space and *determinant* of a linear transformation give rise to isomorphisms

$$K_0F \approx \mathbb{Z} \qquad \text{and} \qquad K_1F \approx F^{\cdot}.$$

Milnor [8], [9] interprets $\{ a, b \}$ as the product of a and b under a " multiplication "

$$K_1F \times K_1F \to K_2F.$$

In general one might ask whether the K-theories discussed by Swan are furnished with products

$$K_iR \times K_jR \to K_{i+j}(R \underset{\mathbb{Z}}{\otimes} R')$$

which for a commutative ring R lead to a graded ring structure on $K_*R \doteq \Sigma_n K_n R$ via the homomorphism $R \otimes R \to R$.

Suppose E/F is a field extension of finite degree. Then there is [8] a transfer homomorphism

$$\mathrm{Tr}_{E/F} : K_2E \to K_2F, \tag{10}$$

whose importance was first emphasized by Bass, such that

$$\mathrm{Tr}_{E/F} \{ a, b \}_E = \{ a, N_{E/F}b \}_F \qquad \text{for} \qquad a \in F^{\cdot},\ b \in E^{\cdot}.$$

In general, if $R \subset R'$ are commutative rings such that R' is a projective R module of finite rank, one would expect a K_*R-linear map $\mathrm{Tr}\colon K_*R' \to K_*R$.

Suppose F is the fraction field of a Dedekind ring R. The maximal ideals of R correspond to certain discrete valuations v of F; for each such v, let $\lambda_{v,\text{tame}}\colon K_2F \to k_v^{\cdot}$ be the homomorphism corresponding to the tame symbol (5) at v, and let

$$\lambda_R : K_2F \to \coprod_v k_v^{\cdot} \tag{11}$$

be the homomorphism whose components are the $\lambda_{v,\text{tame}}$. (We can write direct sum $\coprod_v$ instead of product, because for each fixed pair of elements a, b in $F^{\cdot}$ we have $(a, b)_v = 1$ for almost all v). Bass [1] has shown that the cokernel of λ_R is canonically isomorphic to SK_1R, and that if the set of maximal ideals of R is countable then the kernel of λ_R is the image of K_2R, and even of $H_2(SL_nR, \mathbb{Z})$ for $n \geq 3$.

§ 2. Results of C. Moore.

Suppose now that F is a global arithmetic field, i. e. a number field of finite degree, or a function field in one variable over a finite constant field k. For each place v of F, let F_v denote the completion of F at v, and let μ_v denote the group of roots of unity in F_v. For v non-complex, the group μ_v is of finite order $m_v = |\mu_v|$ and the Hilbert *m_v-norm residue symbol* $\left(\dfrac{a, b}{v}\right) = (a, b)_{m_v}$ is a symbol on F with values in $\mu_v = (\mathrm{Br}\, F_v)_m \otimes \mu_v$ (cf. Example 2 above). Calvin Moore [10] has shown that this symbol is a universal for *continuous* symbols on F_v with values in locally compact abelian groups (see also his talk at this Congress). Thus μ_v should be viewed as a *topological* K_2 of the locally compact field F_v.

Lichtenbaum has raised the question whether μ_v is the ordinary non-topological $K_2F'_v$ where F'_v is the field of algebraic numbers in F_v. This is true at least for $F_v = \mathbb{R}$.

For each place v let

$$\lambda_v \colon K_2F_v \to \mu_v \tag{12}$$

be the homomorphism corresponding to the symbol $\left(\dfrac{a, b}{v}\right)$. For non-archimedean v we have

$$\lambda_{v,\text{tame}} = \text{residue of } \lambda_v^{g_v}, \tag{13}$$

where g_v is the power of the residue characteristic p_v dividing m_v. Note that $g_v = 1$ for all v in the function field case, and for almost all v in the number field case (e. g. those v such that $p_v - 1 > [F_v : \mathbb{Q}_{p_v}]$). The kernel of λ_v is divisible. It is uniquely divisible if $F = \mathbb{R}$ or $\mathbb{Q}_2$; I wonder whether it is always so.

The maps λ_v give a homomorphism

$$K_2F \xrightarrow{\lambda} \coprod_{v\,\text{non-complex}} \mu_v . \tag{14}$$

Calvin Moore *(loc. cit.)* has shown that the cokernel of λ is the group μ_F of roots of unity in F. The reciprocity law

$$\prod_v \left(\frac{a,\, b}{v}\right)^{m_v/m} = \prod_v \left(\frac{a,\, b}{v}\right)_m = 1$$

for $a, b \in F$ and $m = |\,\mu_F\,|$ gives a map of coker λ onto μ_F. The new thing is that this map is injective, and it is really new; in classical class field theory, one never considered simultaneously norm residue symbols whose orders m_v vary with v!

§ 3. **Finiteness of** Ker λ.

The main subject of this talk is the study of Ker λ which has taken place over the past two years. If Ker $\lambda = 0$, then there are no " exotic " symbols on F, every global symbol is expressible in terms of the local ones $\left(\frac{a,\, b}{v}\right)$. On the other hand, if Ker λ is large, then there are many exotic symbols. In this section we discuss work which has limited the size of Ker λ.

Two years ago, Bass and I showed that Ker λ is finitely generated and is finite and prime to the characteristic in the function field case, by the following method. For each finite set of places S, let $U_S \subset F^{\cdot}$ be the group of S-units and let $K_2^S F$ be the subgroup of $K_2 F$ generated by the elements $\{ a, b \}$ for $a, b \in U_S$. If a_i are generators for U_S, then $\{ a_i, a_j \}$ generate $K_2^S F$. Hence the groups $K_2^S F$ are finitely generated. Bass and I proved that if S is a sufficiently large initial segment of the places, relative to an ordering by increasing norms, then the sequence

$$0 \to K_2^S F \hookrightarrow K_2 F \xrightarrow{\lambda_{R_S}} \coprod_{v \notin S} k_v^{\cdot} \to 0 \tag{15}$$

is exact, where R_S is the ring of S-integers in F. The exactness of (15) follows by induction over the set of places from the exactness of the sequences

$$0 \to K_2^{S'} F \to K_2^{S''} F \xrightarrow{\lambda_{v,\mathrm{tame}}} k_v^{\cdot} \to 0 \tag{16}$$

where S' and $S'' = S \cup \{ v \}$ are successive initial segments containing S. It is proving the exactness of (16) that is difficult, or at least tedious.

For the rational field $F = \mathbb{Q}$ the exactness of (16) follows easily from the Euclidean algorithm. The argument is essentially that used by Gauss in his first proof of the quadratic reciprocity law in the Disquisitiones, by an induction over the primes. Gauss was in fact classifying symbols on $\mathbb{Q}$ with values in a group of order 2. His methods give the isomorphism

$$K_2\mathbb{Q} \approx (\pm\, 1) \times \coprod_p \mathbb{F}_p^{\cdot}, \tag{17}$$

the direct sum taken over all odd primes p, and $\mathbb{F}_p$ denoting the prime field with p elements; cf. [8, § 11] for details.

Since Ker λ is contained in Ker λ_{R_S}, it follows from (15) that Ker λ is finitely generated. In the function field case one can show that Ker λ is divisible by the characteristic p of F and is therefore finite and prime to p. By (14) it is enough to prove this divisibility by p for K_2F itself, and this holds for any field E of characteristic $p > 0$ such that $[E: E^p] = p$. Indeed, let $a, b \in E^{\cdot}$. Let $\alpha, \beta \in E' = E^{1/p}$ such that $\alpha^p = a$ and $\beta^p = b$. Then

$$\{ a, b \} = \{ a, N_{E'/E}\beta \} = \mathrm{Tr}_{E'/E} \{ a, \beta \} = \mathrm{Tr}_{E'/E} \{ \alpha, \beta \}^p.$$

Hence $K_2E = (K_2E)^p$.

In the number field case, the result of Bass mentioned at the end of § 1, for R the ring of integers in F, gave another proof of the finite generation of Ker λ and showed that Ker λ is finite if $H_2(SL_nR, \mathbb{R}) = 0$ for some n. This vanishing of H_2 for n sufficiently large and therewith the finiteness of Ker λ has recently been proved by H. Garland [4], using results from differential geometry and analysis on symmetric spaces.

§ 4. The structure of Ker λ.

By the method of Bass-Tate discussed above, one can effectively construct generators for Ker λ, but the set of defining relations is infinite. Roughly speaking, there is one relation, induced by $\{ a, 1 - a \} = 1$, for each element $a \in F$, and the method does not give a procedure for deciding which finite subsets of these relations suffice to define Ker λ. Thus, by taking the generators and some set A of relations one obtains a group X_A of which Ker λ is a quotient, and if A is large, there is a good chance that $X_A =$ Ker λ, although the precedure gives no way to prove this, unless $X_A = 0$.

Indeed for some F one can show Ker $\lambda = 0$ by this method. This is true, for example, for imaginary quadratic fields F of small discriminant d; certainly for $|d| \leq 11$, and almost certainly for $|d| \leq 23$ (there is a theoretical bound on the norm of primes to be considered which increases like $|d|^{3/2}$ and consequently the amount of computation required to achieve absolute certainty increases rapidly with $|d|$).

After the imaginary quadratic fields, our next experiment was with the five function fields F of genus 1 over the field with 2 elements (for genus 0 one has Ker $\lambda = 0$; cf. [9]). For these fields we have $h = 1, 2, 3, 4$ and 5, where h is the number of divisor classes of degree 0. After many mistakes and considerable effort we found groups X_A of orders $h' = 5, 7, 9, 11$ and 13, respectively, for these fields. If α and α' are the characteristic roots of the Frobenius endomorphism π, then

$$h = (1 - \alpha)(1 - \overline{\alpha}) \qquad \text{and} \qquad \alpha\overline{\alpha} = 2,$$

hence

$$h' = 3 + 2h = (1 - 2\alpha)(1 - 2\overline{\alpha}). \tag{18}$$

A theoretical explanation for this experimental result is as follows.

Suppose F is a function field whose constant field k has q elements. Let $\overline{k}$ be an algebraic closure of k, let $F_\infty = F\overline{k}$, let $G = \mathrm{Gal}\,(F_\infty/F)$, and let $\mu = (\overline{k})^{\cdot}$ be the group of roots of unity in F_∞. Let D and C be the groups of divisors and divisor classes of F_∞. Tensoring the exact sequence

$$0 \to \mu \to F_\infty^{\cdot} \to D \to C \to 0 \tag{19}$$

with μ gives an exact sequence

$$0 \to \mathrm{Tor}\,(\mu, C) \to \mu \otimes F_\infty^{\cdot} \to \mu \otimes D \to \mu \to 0 \tag{20}$$

Taking invariants under G we obtain

$$(21)\qquad 0 \to \operatorname{Tor}(\mu, C)^G \to (\mu \otimes F_\infty^{\cdot})^G \xrightarrow{\lambda'} (\mu \otimes D)^G,$$

still exact. Now consider the homomorphism

$$(22)\qquad \mu \otimes F_\infty^{\cdot} \to K_2 F_\infty$$

for which $\zeta \otimes f \mapsto \{\zeta, f\}$, and the homomorphism

$$(23)\qquad K_2 F \to (K_2 F_\infty)^G$$

induced by the inclusion $F \subset F_\infty$. Suppose (22) and (23) are isomorphisms. Then

$$(24)\qquad K_2 F \approx (\mu \otimes F_\infty^{\cdot})^G$$

On the other hand, it is easy to see that

$$(25)\qquad \coprod_v \mu_v \approx (\mu \otimes D)^G$$

and that the map λ' in (21) becomes identified with λ via the isomorphisms (24) and (25). Hence we would have

$$(26)\qquad \operatorname{Ker} \lambda \approx (\operatorname{Tor}(\mu, C))^G$$

This last group is the kernel of $1 - \sigma$ acting on $\operatorname{Tor}(\mu, C)$, where $\sigma \in G$ is the Frobenius automorphism, and this kernel is non-canonically isomorphic to the kernel of $1 - q\sigma$ acting on C, or, what is the same, the kernel of $1 - q\pi$ acting on the Jacobian variety of F_∞, where π is the Frobenius endomorphism. The order of this kernel is

$$(27)\qquad \deg(1 - q\pi) = \prod_{i=1}^{2g}(1 - q\alpha_i) = (q - 1)(q^2 - 1)\zeta_F(-1),$$

where the α_i are the characteristic roots of π and where ζ_F is the zeta function of F. Since $|\operatorname{Coker} \lambda| = q - 1$ (by Moore) this would give the formula

$$(28)\qquad \frac{|\operatorname{Ker} \lambda|}{|\operatorname{Coker} \lambda|} = (q^2 - 1)\zeta_F(-1).$$

THEOREM 1. — *For a function field F the maps* (22) *and* (23) *are bijective, and consequently we have isomorphisms* (24) *and* (26), *and formula* (28) *holds.*

At the time of the Congress in Nice, only the 2-primary part of this theorem was proved, via methods of Birch [2]. Shortly afterwards, the theorem was proved in general, using the cohomological methods described in § 5 below, which were inspired by a suggestion of Lichtenbaum.

When Theorem 1 was first conjectured two years earlier, it was natural to seek an analog for number fields. A formula like (28) could not make much sense in general, because the zeta function of a number field F has a zero of order r_2 at $s = -1$, where r_2 is the number of complex places of F. But Birch suggested that some such formula might very well hold in the totally real case ($r_2 = 0$), and he and Atkin quickly produced numerical evidence to the effect that, for real quadratic F of discriminant $d < 50$, a prime like 5 or 7 occuring in the numerator of $\zeta_F(-1)$ always divides the order of X_A.

Using the Atlas computer, Atkin was able to take very large sets A of relations, so this evidence was quite convincing. Further experimentation suggested that the conjecture should be

$$(29) \qquad | \operatorname{Ker} \lambda_R | = \pm w_F^{(2)} \zeta_F(-1),$$

where R is the ring of integers of the totally real field F and where $w_F^{(2)}$ is a certain integer, the simplest description of which was recently suggested by Lichtenbaum, namely, for $r > 0$, $w_F^{(r)}$ denotes the largest integer m such that Gal $(\overline{F}/F)$ acts trivially on the r-fold tensor product $\mu_m \otimes \ldots \otimes \mu_m$, where μ_m is the group of m-th roots of unity in an algebraic closure $\overline{F}$ of F. In the function field case we have $w^{(r)} = q^r - 1$. Since λ_R is surjective, formulas (28) and (29) are two special cases of one formula.

Formula (29) predicts various non-trivial divisibility properties of $\zeta_F(-1)$ which have been proven by various people. An especially good example is due to Serre [14 (3.7)] (our $w^{(2)}$ is Serre's w).

For a given number field F, one can show that, for prime numbers l outside a certain finite set Σ_F, the order of Ker $\lambda/(l \operatorname{Ker} \lambda)$ divides the order of $(C_l \otimes \mu_l)^{G_l}$, where C_l is the ideal class group of $F(\mu_l)$ and $G_l = \operatorname{Gal}(F(\mu_l)/F)$. Using methods of Leopoldt-Kubota [6] and Iwasawa, Brumer showed that if F is totally real and abelian over $\mathbb{Q}$ and l outside another finite set Σ'_F, then $(C_l \otimes \mu_l)^{G_l} = 0$ if l does not divide $\zeta_F(-1)$. This gave added evidence for (29), and it also proved the finiteness of Ker λ for totally real abelian fields before Garland proved the finiteness for all number fields.

More recently, John Coates has produced evidence for a number field analog of (26) in certain cases. Here one must treat the l-primary part of Ker λ separately for each prime l, and one replaces F_∞ by $F(\mu)$ where μ is the group of l^n-th roots of unity, all n. Coates' work shows there are some close relations between conjectures about Ker λ and conjectures in Iwasawa's theory of the $\mathbb{Z}_l$-extension $F_\infty/F(\mu_l)$ (cf. Iwasawa's talk at this Congress).

§ 5. **Symbols in Galois cohomology.**

Let m be a natural number not divisible by the characteristic of F, and let

$$(30) \qquad h_m : K_2 F \to H^2(F, \mu_m \otimes \mu_m)$$

be the homomorphism corresponding to the symbol $(a, b)_m$ discussed in example 2 of § 1 above.

THEOREM 2. — *The map h_m is surjective, and its kernel is $(K_2F)^m$, i. e., h_m induces an isomorphism*

$$(31) \qquad K_2F/(K_2F)^m \approx H^2(F, \mu_m \otimes \mu_m)$$

A series of reduction steps reduces the proof of this theorem to the case in which m is a prime and $\mu_m \subset F$. In that case the surjectivity is well known. For injectivity one starts from the fact (9) that an element of the form $\{ a, b \}$ is in $(K_2F)^m$ if and only if it is in Ker h_m. To treat an arbitrary element $\Pi_i \{ a_i, b_i \}$, one uses the following two lemmas, which are true at least for arithmetic fields containing μ_m, m a prime.

LEMMA 1. — *Given elements $a_1, b_1, a_2, b_2, a_3, b_3 \in F^{\cdot}$, there exist elements c_1, c_2, c_3 and d in $F^{\cdot}$ such that $(a_i, b_i)_m = (c_i, d)_m$ for $i = 1, 2, 3$.*

This just means that any three elements of order m in the Brauer group of F have a common cyclic splitting field $F(d^{1/m})$ of degree m.

LEMMA 2. — *Given a, b, c, d in $F^{\cdot}$ such that $(a, b)_m = (c, d)_m$, there exist x, y in $F^{\cdot}$ such that*

$$(a, b)_m = (x, b)_m = (x, y)_m = (c, y)_m = (c, d)_m \tag{32}$$

To prove Lemma 2 one selects y such that for each place v an x_v exists such that (32) holds locally; then a standard lemma on norm residue symbols guarantees the existence of an x globally.

I do not know whether these lemmas, and consequently Theorem 2, hold for all fields, or for a wide class of fields, or only for very special fields. The situation for $m = 2$ seems a bit special. For $m = 2$, Lemma 2 holds for all fields, even with $y = d$, and Milnor [9] has interpreted $K_2F/(K_2F)^2$ in terms of the Witt ring for all fields F.

It can be shown that the map

$$H^2(F, \mu_m \otimes \mu_m) \to \coprod_v H^2(F_v, \mu_m \otimes \mu_m) \tag{33}$$

is injective if m is not divisible by 8, and in any case has kernel of order 1 or 2. Thus the common kernel of the h_m, which by Theorem 2 is the group $\bigcap_m (K_2F)^m$ of elements divisible by m in K_2F for all m, is of index 1 or 2 in Ker λ. For this reason I thought until recently that Galois cohomology could not help in the attempt to show Ker λ very non-trivial and to determine its structure. I could not have been more wrong; one has only to make a symbol with values in

$$H^2(F, \varprojlim_m (\mu_m \otimes \mu_m)) \quad \text{instead of in} \quad \varprojlim_m H^2(F, \mu_m \otimes \mu_m)$$

in order to get a cohomological symbol which promises to be universal!

It is better for this to fix a prime l different from the characteristic of F and to restrict m to be a power of l. Let

$$T = \varprojlim_n (\mu_{l^n}) \tag{34}$$

be the free $\mathbb{Z}_l$-module of rank one on which Galois acts according to its action on the l^n-th roots of unity. For each integer $r > 0$, let

$$0 \to T^{(r)} \to V^{(r)} \to W^{(r)} \to 0 \tag{35}$$

denote the exact sequence obtained by tensoring the exact sequence

$$0 \to \mathbb{Z}_l \to \mathbb{Q}_l \to \mathbb{Q}_l/\mathbb{Z}_l \to 0$$

r times over $\mathbb{Z}_l$ with T.

Recently S. Lichtenbaum suggested that the l-primary part of K_2F should be isomorphic to $H^1(F, W^{(2)})$ if $r_2 = 0$, and to a quotient of $H^1(F, W^{(2)})$ if $r_2 > 0$. Considering Lichtenbaum's idea together with the connecting homomorphisms

$$H^q(F, W^{(r)}) \to H^{q+1}(F, T^{(r)}) \tag{36}$$

associated with the sequence (35) suggests that there is a symbol with values in

$$H^2(F, T^{(2)}) = H^2(F, \varprojlim_n (\mu_{l^n} \otimes \mu_{l^n})) \tag{37}$$

analogous to the m-symbol (8). Such a symbol is easy to make; one simply replaces the δ_m in definition (8) by the analogous homomorphism $F^\cdot \to H^1(F, T)$. To show that the resulting pairing is a symbol one proves that a and $1 - a$ are paired to an element in the divisible part of $H^2(F, T^{(2)})$, and uses

PROPOSITION. — *The divisible part of $H^q(F, T^{(r)})$ is 0 for all q and r.*

Since $H^q(F, V^{(r)})$ is uniquely divisible and $H^q(F, W^{(r)})$ is a torsion group we get

COROLLARY. — *The homomorphism* (36) *induces an isomorphism*

$$H^q(F, W^{(r)})/H^q(F, W^{(r)})_{\mathrm{div}} \xrightarrow{\sim} H^{q+1}(F, T^{(r)})_{\mathrm{tors}} \tag{38}$$

Here X_{div} (resp. X_{tors}) denotes the largest divisible (resp. torsion) subgroup of the abelian group X.

Let

$$h : K_2F \to H^2(F, T^{(2)})$$

denote the homomorphism corresponding to the symbol just discussed. If $\mu_l \subset F$, there is an exact commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker} \alpha \arrow[r] \arrow[d] & \mu_l \otimes F^\cdot \arrow[r, "\alpha"] \arrow[d, "\wr"] & (K_2F)_l \arrow[d, "h"] & \\ 0 \arrow[r] & H^1(F, T^{(2)})/lH^1(F, T^{(2)}) \arrow[r] & H^1(F, \mu_l \otimes \mu_l) \arrow[r] & (H^2(F, T^{(2)}))_l \arrow[r] & 0 \end{tikzcd} \tag{39}$$

in which the bottom row comes from the exact sequence

$$0 \to T^{(2)} \xrightarrow{l} T^{(2)} \to \mu_l \otimes \mu_l \to 0. \tag{40}$$

The symbol X_l denotes the kernel of the map $X \xrightarrow{l} X$. The homomorphism α is characterized by $\alpha(\zeta \otimes a) = \{ \zeta, a \}$ for $\zeta \in \mu_l$ and $a \in F^\cdot$. The middle vertical isomorphism is that obtained by tensoring (7) with μ_l (with $m = l$).

Suppose now that we do not known that Ker λ is finite, but only that it is finitely generated, say of rank ρ (so $\rho = 0 \Leftrightarrow$ Ker λ finite).

LEMMA 3. — *If $\mu_l \subset F$, then $|\operatorname{Ker} \alpha| / |\operatorname{Coker} \alpha| = l^{1+r_2+\rho}$.*

This is proved by considering the composed map $\lambda\alpha$, and using the following

COROLLARY OF THEOREM 2. — *The map λ induces an injection*

$$K_2F/(K_2F)^l \to \coprod_v \mu_v/\mu_v^l .$$

Combining Lemma 3 with diagram (39) gives

THEOREM 3. — *Suppose $\mu_l \subset F$. Then $(H^1(F, T^{(2)}) : lH^1(F, T^{(2)})) \geq l^{1+r_2}$, and equality holds if and only if* Ker λ *is finite, α is surjective, and h is injective on the l-primary part of K_2F.*

By the Corollary of the Proposition, we have

(41) $$H^1(F, T^{(2)})_{\text{tors}} \approx H^0(F, W^{(2)}),$$

a cyclic group of order l^n for some $n \geq 1$. Hence Theorem 3 suggests the

MAIN CONJECTURE (1) — *The rank of the $\mathbb{Z}_l$-module $H^1(F, T^{(2)})$ is r_2, or, equivalently, the divisible part of $H^1(F, W^{(2)})$ is isomorphic to $(\mathbb{Q}_l/\mathbb{Z}_l)^{r_2}$.*

Let $F_\infty = \bigcup_n F(\mu_{l^n})$ and let $G = \mathrm{Gal}\,(F_\infty/F)$. Let M be the maximal abelian pro-l extension of F_∞ which is unramified outside places dividing l, and let $X = \mathrm{Gal}\,(M/F_\infty)$. Then the Main conjecture translates into $\mathrm{Hom}_G\,(X, T^{(2)}) \approx \mathbb{Z}_l^{r_2}$, i. e. into a statement about the G-module X. This module has been intensively studied by Iwasawa [5] in the number field case. In the function field case, the module is described by the action of the Frobenius endomorphism on the Jacobian, and results of A. Weil show $\mathrm{Hom}_G\,(X, T^{(2)}) = 0$, hence

THEOREM 4. — *The Main conjecture is true for function fields.*

A proof of the Main conjecture for number fields would give (via Theorem 3) a new proof of the finiteness of Ker λ, completely different from Garland's. In fact, a proof of the Main conjecture would justify the ideas of Lichtenbaum which inspired it and would reduce all questions about K_2F to questions about Galois cohomology, in view of

THEOREM 5. — *If the Main conjecture is true for the field $F(\mu_l)$, then h induces an isomorphism*

(42) $$K_2F(l) \xrightarrow{\sim} H^2(F, T^{(2)})_{\text{tors}} \approx H^1(F, W^{(2)})/H^1(F, W^{(2)})_{\text{div}}$$

where $K_2F(l)$ denotes the l-primary part of K_2F.

In the function field case these cohomology groups are readily computed and one easily derives Theorem 1 from Theorems 4 and 5.

In the number field case such definitive results await a proof of the Main conjecture; nevertheless Theorem 5 seems to be an excellent guide as to what to expect, and it should at least suggest partial and special results which can be proven.

For $l = 2$ there is one general result which is slightly weaker than the Main conjecture but still can be used to prove the existence of plenty of exotic symbols, i. e. to show that Ker $\lambda/(\text{Ker }\lambda)^2$ can be very large. This is the fact that the map α in diagram (39) is surjective for $l = 2$. Indeed, methods suggested by Birch [2] lead to a proof of the following algebraic theorem which applies in particular to arithmetic fields.

---

(1) (Note added during the correction of proofs). It seems that this « Main Conjecture » has now been proved for number fields as well as function fields (cf. H. BASS, K_2 des Corps globaux (d'après TATE, GARLAND,...), *Séminaire Bourbaki*, No. 394, June, 1971). The proof uses Garland's finiteness theorem [4] (hence the remark in the text following Theorem 4 is a bit ridiculous), as well as Matsumoto's theorem [7], Moore's result on Coker λ [10], and a fundamental result of Iwasawa.

THEOREM 6. — *Suppose F is any field of characteristic $\neq 2$ for which Lemma* 1 *holds for $m = 2$. Then every element of order* 2 *in K_2F is of the form* $\{ -1, a \}$.

I do not know whether the hypothesis about Lemma 1 is essential, nor do I have any idea how to prove a corresponding statement for $l \neq 2$.

Let me finish by emphasizing one question to which we have not even a conjectural answer at present, namely, what should be the analog of (29) in case $r_2 \neq 0$, e. g. for an imaginary quadratic field F? Lichtenbaum suggests that the right hand side should involve some $r_2 \times r_2$ determinant multiplied by the value at $s = -1$ of $(s+1)^{-r_2}\zeta_F(s)$, but which determinant? Is there a bilinear form on $H^2(F, T^{(2)})$?

REFERENCES

[1] H. BASS. — K_2 of global fields, *Lecture at A. M. S. meeting in Cambridge*, Mass. October 1969 (Tape recording and supplementary manual available at American Mathematical Society, Providence, Rhode Island).

[2] B. J. BIRCH. — K_2 of global fields, *Proc. Sympos. Pure Math.*, vol. 20, *Amer. Math. Soc.*, Providence, Rhode Island, 1970.

[3] CASSELS-FRÖHLICH. — *Algebraic Number Theory*, Academic Press, New York, 1967.

[4] H. GARLAND. — A finiteness theorem for K_2 of a number field (to appear in *Annals of Math.*).

[5] K. IWASAWA. — (His talk at Nice, in this volume).

[6] T. KUBOTA and H. W. LEOPOLDT. — Eine p-adische Theorie der Zetawerte, *Jour. f. reine. angew. Math.*, vol. 214-215 (1964), pp. 328-339.

[7] H. MATSUMOTO. — Sur les sous-groupes arithmétiques des groupes semi-simples déployés, *Ann. Sci. École Norm. Sup.* (4), 2 (1969), pp. 1-62.

[8] J. MILNOR. — Notes on algebraic K-theory (to appear in *Annals of Math. Studies*).

[9] —. — Algebraic K-theory and quadratic forms, *Inventiones math.*, 9 (1970), pp. 318-344.

[10] C. C. MOORE. — Group extensions of p-adic and adelic linear groups, *Inst. Hautes Études Sci. Publ. Math.*, No. 35 (1968), pp. 157-221.

[11] J.-P. SERRE. — *Corps locaux*, Hermann, Paris, 1962.

[12] —. — *Groupes algébriques et corps de classes*, Hermann, Paris (1959).

[13] —. — *Cohomologie Galoisienne*, troisième édition, Springer, *Lecture notes*, vol. 5 (1965).

[14] —. — Cohomologie des groupes discrets (to appear in *Annals of Math. Studies*).

[15] R. STEINBERG. — *Générateurs, relations et revêtements de groupes algébriques*, Coll. Théorie des Groupes (Bruxelles, 1962), Librairie Universitaire, Louvain et Gauthier-Villars, Paris (1962), pp. 113-127.

[16] J. TATE. — K_2 of global fields, *Lecture at A. M. S. meeting at Cambridge*, Mass., October 1969 (Tape recording and supplementary manual available at American Mathematical Society, Providence, Rhode Island).

Harvard University
Department of Mathematics,
2, Divinity Avenue
Cambridge, Mass. 02138
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 213 à 219.

GEOMETRIC TOPOLOGY: MANIFOLDS AND STRUCTURES

by C. T. C. WALL

The term " geometric topology " has gradually been gaining currency in the last few years: you may wonder what the subject is all about. The object of this talk is to explain just that: to introduce the concepts involved and the main problems, and to discuss some of the most important results that have been obtained up to now.

The most basic concept in geometry is that of euclidean space, and the main branches of geometry involve the study of the various structures which it carries: linear, algebraic, differentiable, topological, etc. Many types of structure are defined by pseudogroups.

A *pseudogroup* Φ on E is a category whose objects are the open subsets of E, and whose morphisms must be continuous, invertible in Φ, and locally defined. Thus if $G\Phi$ is the set of all germs (at all points) of morphisms of Φ, and $\phi : U \to V$ is a homeomorphism whose germ at each point of U belongs to $G\Phi$, then $\phi \in \Phi$.

Φ is transitive if for all $x, y \in E$ there is a germ in $G\Phi$ with source x and target y.

The most important examples of pseudogroups are:

C^r : ϕ and ϕ^{-1} must be of class C^r. As special cases we have C^0 (the largest pseudogroup), C^∞ and C^ω, where C^ω denotes real analytic. In the complex case we have the pseudogroup C^Ω of complex analytic maps.

Lip, maps satisfying a local Lipschitz condition.

Maps preserving Lebesgue measure, or just orientation.

Nash, ϕ (and ϕ^{-1}) is an algebraic map, which is also C^ω.

Affine maps, or piecewise affine (usually called piecewise linear, or *PL*) maps: here the pieces come from a locally finite partition of U into polyhedra.

Trivial, identity maps only (the smallest pseudogroup) or translations (the smallest transitive one).

For any (closed) subgroup G of $GL(E)$, consider C^r (for some $r \geqslant 1$) maps whose derivative at each point is in G; interesting cases are the symplectic and orthogonal groups, orthogonal similitudes (giving conformal structure), maps preserving a subspace (giving foliations) or—in the case E is Hilbert space—invertible maps of the form I plus a compact operator, giving Fredholm structures.

Foliations lead to a wide variety of pseudogroups. Suppose E, F are Euclidean spaces, Φ a pseudogroup on $E \times F$ and Ψ a pseudogroup on F. Then $\mathscr{F}(\Phi, \Psi)$ is the pseudogroup on $E \times F$ of maps whose germs ϕ belong to a commutative diagram

$$\begin{array}{ccccc} E \times F & \supset & U & \xrightarrow{\phi} & E \times F \\ \downarrow p & & \downarrow & & \downarrow p \\ F & \supset & p(U) & \xrightarrow{\psi} & F \end{array}$$

with $\phi \in \Phi$, $\psi \in \Psi$. One can further specify a pseudogroup X on E, and require the restriction of ϕ to each leaflet $U \cap (E \times x)$ to belong to X.

We now come to manifolds. Let M be a topological space, E a euclidean space. A *chart* on M with model E is a pair (U, ϕ) where U is open in M, $\phi: U \to E$ an embedding with $\phi(U)$ open. An *atlas* is a collection $\{(U_\alpha, \phi_\alpha)\}$ of charts with $\cup U_\alpha = M$: if M has such an atlas, it is called a manifold modelled on E. Usually one requires also that M is Hausdorff and paracompact. If two charts (U_α, ϕ_α) and (U_β, ϕ_β) overlap, we have a coordinate transformation

$$g_{\alpha\beta}: \phi_\alpha(U_\alpha \cap U_\beta) \xrightarrow{\phi_\alpha^{-1}} U_\alpha \cap U_\beta \xrightarrow{\phi_\beta} \phi_\beta(U_\alpha \cap U_\beta).$$

If Φ is a pseudogroup on E, an atlas $\{(U_\alpha, \phi_\alpha)\}$ on M is a Φ-*atlas* if each coordinate transformation $g_{\alpha\beta}$ is in Φ. Two Φ-atlases A, A' are *compatible* if $A \cup A'$ is a Φ-atlas. The union of all Φ-atlases compatible with a given one, A, is still a Φ-atlas: clearly a maximal one. A maximal Φ-atlas on M is called a Φ-*structure*: thus each Φ-atlas defines a unique Φ-structure.

For examples, we have smooth (C^∞) structure, real or complex analytic structure, orientation, flat structure (take Φ = affine maps), PL-structure, immersion in E (take Φ = identity maps), and foliations of various kinds.

Having defined structures on manifolds, we must say what we mean by structures on morphisms (i. e. maps) of manifolds. The corresponding notion (less standard) is as follows. Given pseudogroups Φ on E, Ψ on F a *morphism* $\Omega: \Phi \to \Psi$ is a locally defined family of continuous maps from open sets in E to open sets in F, which is closed under composition on the right with maps in Φ and on the left with maps in Ψ: thus $\Psi \circ \Omega \circ \Phi \subset \Omega$. This notion seems more fundamental than that of pseudogroup; note also that in nearly all examples above of pseudogroups we first chose an Ω with $\Omega \circ \Omega \subset \Omega$ and then considered the invertible morphisms of Ω.

Examples are easy to supply, for example C^r (non-invertible) maps define a morphism $C^s \to C^t$ whenever $r \leqslant s, t \leqslant \omega$. So do C^r-immersions (note that embeddings are not locally defined), or more generally maps whose jacobians everywhere have rank $\geqslant k$. Another good example is provided by piecewise smooth maps : $PL \to C^\infty$; here again we can restrict to immersions with jacobian of maximal rank everywhere it is defined.

If M has a Φ-structure, N a Ψ-structure, $f: M \to N$ is a continuous map and $\Omega: \Phi \to \Psi$, then we call f an Ω-*morphism* if for all charts (U, ϕ) of M, (V, ψ) of N with $f(U) \subset V$, the composite $\psi \circ f \circ \phi^{-1}: \phi(U) \to \psi(V)$ belongs to Ω. Again, it suffices to check this for each chart of a (non-maximal) Φ-atlas of M.

Not all structures are defined by atlases. For example, we may be given a Ψ-manifold F, and a morphism $\Omega: \Phi \to \Psi$; then an Ω-map $M \to F$ can be regarded as constituting a certain type of structure on the Φ-manifold M. Write $\mathscr{S}(M)$ for the set of such maps: in many cases this will be endowed with a natural topology, e. g. C^r (uniform convergence on compact sets: not the fine topology here).

More generally we may have a Φ-*bundle* B with fibre F: by definition this assigns functorially to each $\phi: U \to U'$ in Φ a map $B(\phi): U \times F \to U' \times F$ over ϕ. Using these to glue over charts defines a bundle $B(M)$ over any Φ-manifold M. Now a structure will be defined as a section of $B(M)$, satisfying local conditions which can be specified by assigning a Φ-*sheaf* $\mathscr{S}$ of sections of B. Here for each open U in E, $\mathscr{S}(U)$ is a collection of maps $U \to F$; $\mathscr{S}$ is locally defined, i. e. is a sheaf; and for $\phi \in \Phi$, $B(\phi)$ transforms the sections $U \to U \times F$ which are graphs of members of $\mathscr{S}(U)$ into graphs of members of $\mathscr{S}(U')$.

Note. — It is simpler axiomatically to define $\mathscr{S}$ and omit B, but this takes us too far away from the geometry. One should consider a Φ-bundle or Φ-sheaf as a bundle or sheaf over E, endowed with the Grothendieck topology induced by Φ.

The most obvious example of Φ-bundle is the tangent bundle. This also has analogues in the topological and PL cases which originated with Milnor's work on microbundles. We also have the associated bundles of tensors (with, perhaps, symmetry conditions) in the traditional sense of differential geometry, the tangent bundles of higher order, and the bundle of connections: note particularly the classical cases of the Riemann bundle, and the bundle of (tangent) p-forms. Another example is the bundle normal to the foliation, if Φ defines a foliation. Also for each of the vector bundles above we have the associated projective bundle and frame bundle, and more generally, Grassmann and Stiefel bundles.

The possible sheaves $\mathscr{S}$ have a wide variety. In each case we may consider all continuous, or (perhaps) all differentiable (of some class C^r) sections—holomorphic in the complex case: examples are Riemann metrics, tangent 1-forms and connections. More generally, we could restrict the local maps $U \to F$ to lie in some suitable preassigned class Ω. E. g. for vector bundles in the differentiable case, we can consider smooth sections transverse to the zero section. Indeed, some of the most fruitful illustrations come by imposing such conditions on derivatives: assuming sufficient differentiability, given a Φ-bundle B there is an extended bundle E^rB of r-jets of sections of B. Now for any sub-Φ-bundle E^r_0B of E^rB, we can consider those sections of B whose r-jets are sections of E^r_0B (equivalently, those sections of E^r_0B which come from B: the *integrable* ones in the usual terminology). As one concrete geometrical illustration, we can take B the Riemann bundle, $r = 1$ and consider metrics with everywhere positive (or everywhere negative) sectional curvatures.

I now consider the problem of existence and classification of structures of a given type on a given manifold: this is of course a global problem since Euclidean space possesses structures of all types. More generally, I am interested in when the existence of one type of structure implies the existence of another. For classification one needs a notion of equivalence: a general definition which seems to cover all cases of interest in geometric topology (though not in differential geometry) is this:

Two structures α, β of a given type on M are *concordant* if there is a structure γ of this type on $M \times I$ inducing α on $M \times 0$ and β on $M \times 1$.

Of course, this needs to be made explicit in each case, but it is usually obvious how to interpret the definition. A stronger relation is *isotopy*: here one demands a level-preserving homeomorphism F of $M \times I$ — i. e. $F(m, t) = (f_t(m), t)$ — with $f_0 =$ identity and $f_1^*\alpha = \beta$. Frequantly, F and F^{-1} are also supposed differentiable. In many cases (e. g. smooth or PL structures on topological manifolds of dimension $\geqslant 6$) concordance and isotopy are equivalent: but this is always a tricky technical question. The most interesting problem of this type, where a structure is a diffeomorphism of the smooth manifold M onto a fixed manifold M_0, has been studied by Cerf and Wagoner.

Now suppose we are comparing structures of two different types, say Φ and Φ'. We will suppose that a Φ-structure implies a Φ'-structure—this holds trivially, for example, if we have two pseudogroups $\Phi \subset \Phi'$, or we are considering appropriately restricted sections of two bundles B, B' with a morphism $B \to B'$. The simplest sort of result is that for any M (perhaps satisfying some side conditions), each Φ'-structure is induced by a Φ-structure, unique up to concordance. Some results of this kind, where $\Phi \subset \Phi'$ are pseudogroups, are

Whitney, 1936: for $1 \leqslant r \leqslant s \leqslant \omega$, comparing C^s and C^r,

Nash, 1952: the same, with C^s replaced by Nash,

Moise, 1952; Bing, 1959: comparing PL and C^0 in dimension 3;

the result is also known, due to work of many authors, comparing topological, differentiable and trivial structures in the infinite dimensional case (here, a trivial structure is an open immersion in Hilbert space). For references see, for example, the talks of Anderson and Kuiper at this congress.

When the above simple result does not apply, one looks for a theorem of the following kind, which I will describe as an *obstruction theory*: it reduces the problem to one in homotopy theory, concerning only continuous maps. Such a theorem specifies first a space X and a functor providing for each Φ-structure on M a continuous map $M \to X$, determined up to homotopy (typically, a structure of class C^1 on M^m gives, via the tangent bundle—which has structure group $GL_m \simeq O_m$—a classifying map $M \to BO_m$). Similarly for Φ' we have an X'. There should also be a map $X \to X'$, which we may suppose a fibration, such that for any Φ-structure on M and the induced Φ'-structure, the diagram

$$\begin{tikzcd} & X \arrow[d] \\ M \arrow[ur] \arrow[r] & X' \end{tikzcd}$$

commutes up to a (preferred) homotopy. The theorem will then say that (subject perhaps to some side conditions on M), given M with Φ'-structure, the equivalence classes of Φ-structures on M which induce it (or something equivalent—but usually we can hit the structure on the nose) correspond bijectively to homotopy classes of lifts $M \to X$ of the given map $M \to X'$.

Such a theorem has some applications by its very nature—for example, take M contractible. But for effective work, information on the spaces X and X' is essential, and to obtain such information is often a central problem in geometric topology. Some such theorems are as follows:

Smoothing theory (due to the work of many people) gives an obstruction theory to imposing C^r structures ($r \geqslant 1$) on PL-manifolds. This is technically difficult since $C^r \not\subset PL$: instead one needs the result of Whitehead, 1940. The corresponding spaces here are usually denoted by $BO \to BPL$; the former has been familiar for many years, some striking results on the latter were obtained by Sullivan, 1970. Next we have the results of Kirby and Siebenmann, 1969 on imposing PL structures on topological manifolds of dimension $\geqslant 5$. Here the only obstruction to existence of a PL-structure on M is a cohomology class in $H^4(M; \mathbb{Z}_2)$. See also Eells' talk at this congress for an account of Fredholm structures.

Recent results of Haefliger, 1970 (see also below) have provided obstruction theories for existence of foliations and of complex analytic structures: indeed I think that a result is obtained for any pseudogroup Φ. A side condition is needed: that M is open (i. e. has no compact unbounded component). Nothing is known about the obstruction groups except the results of Bott which he discussed yesterday.

For structures of the second type, most known results are subsumed in the following theorem of M. L. Gromov, 1969. Take $\Phi = C^\infty$, let B be a differentiable Φ-bundle, E^rB the bundle of r-jets of sections of B (as above) and E_0^rB an *open* subbundle of E^rB. Let $\mathscr{S}(M)$ be the space of sections of $B(M)$ whose r-jets map into $E_0^rB(M)$; $T(M)$ the space of sections of $E_0^rB(M)$—thus taking r-jets defines a map j^r: $\mathscr{S}(M) \to T(M)$. Give $T(M)$ the compact-open topology, and topologise $\mathscr{S}(M)$ as a subspace of it.

THEOREM — *If M is open, j^r: $\mathscr{S}(M) \to T(M)$ is a weak homotopy equivalence.*

The proof is an improvement of that of the Smale-Hirsch, 1959 classification of immersions, and is not unduly difficult.

Many examples of applications were mentioned in the talk of Gromov at the congress. The immersion case is when $B(M)$ is a trivial bundle $M \times F$; a point of $E^1B(M)$ can be identified with a linear map of a tangent space of M to one of F, so a section of $E^1B(M)$ can be identified as a map of tangent bundles $TM \to TF$, and we let $E_0^1B(M)$ be the injective linear maps. Results corresponding to this case can now also be formulated in the PL and topological cases, and proved in the same manner—the difficult step was an isotopy extension theorem. See Haefliger and Poenaru, 1966 and Lees, 1969.

Other suitable $E_0^1B(M)$, for the same B, are maps of rank $\geqslant k$ (some fixed k)—previously treated by Sidnie Feit, 1968—and maps whose projection on the normal bundle of a prescribed foliation of F is surjective—this case was discovered independently by Phillips.

It is clearly of great interest to determine in particular cases whether or not the result is valid also for closed manifolds. For immersions $M \to F$ this is well-known to be the case provided $\dim M < \dim F$. Mrs Feit's result allows M closed if $k < \dim F$. A recent result of Feldman allows M to be a circle, considering curves immersed in the Riemannian manifold F with everywhere nonzero geodesic curvature, provided $\dim F \geqslant 3$. The underlying condition seems to be that F has at least one dimension " to spare ". Note that no advantage is gained by removing a point from M, applying the result, and attempting to reinsert the point: consider submersions $M \to \mathbb{R}$.

The classification of immersions can be made the basis of a proof of many of the theorems cited above. Put rather too crudely, the idea is this: if $\dim M = \dim V$, we have an immersion $M \to V$, and V carries a Φ-structure, then one is induced on M by using the immersion to pull charts on V back to M. There are two ways to make this the basis of a proof. One is to take $V = E$ and work by induction on coordinate charts of M. This method, which needs a special argument if M is closed, was explained in Lashof's talk at the congress. The other is to use the theorem in the case $\dim M < \dim V$, which leads (rather easily) to obtaining a Φ-structure on $M \times \mathbb{R}^q$ for some q, and then use a stability theorem of the type: a Φ-structure on $M \times \mathbb{R}$ is concordant to the product of a Φ-structure on M and the natural one on $\mathbb{R}$. The product theorem for comparison of C^r and PL structures is due to Cairns, 1961 and Hirsch, 1961; in the topological case it is due to Kirby and Siebenmann, 1969.

A subtler use of Gromov's result to obtain structure theorems was made by Haefliger, 1970. His idea is to contemplate bundles over any space X with fibre E with (roughly) a Φ-structure on each fibre and a " foliation " transverse to the fibres. By a general argument (Ed. Brown's representability theorem), he obtains a classifying space for such structures on X. If now X is a manifold modelled on E, and the bundle is equivalent to the tangent bundle of X, the theorem implies the existence of a section transverse to the foliation. The local projections of the section on the fibres now induce a Φ-structure on M.

I will conclude with an example which does not quite fit into the above framework. Instead of beginning with a topological space which is locally euclidean, start with a space which is only prescribed up to homotopy type. To substitute for the local condition, I insist that a strong form of the Poincaré duality theorem holds. The most interesting question here is whether the prescribed homotopy type contains a manifold. The simplest result concerns the relative case when we have a pair (Y, X) satisfying Lefschetz duality. Suppose also that X, Y are connected and that the inclusion map $X \to Y$ induces an isomorphism of fundamental groups. Then, in dimensions $\geqslant 6$, there is an obstruction theory for existence of a corresponding manifold.

As with Gromov's theorem one can define (semi-simplicially) spaces $\mathscr{S}(Y)$ and $T(Y)$ and generalise this theory to obtain a homotopy equivalence $\mathscr{S}(Y) \to T(Y)$. If the corresponding map is considered now in the case when Y satisfies Poincaré (not Lefschetz) duality, it turns out that the homotopy type of the mapping fibre $\mathscr{L}(Y)$ depends only on $\pi_1(Y)$ and on dim Y (mod 4)—provided this dimension $\geqslant 5$. Although explicit calculation is difficult, the spaces $\mathscr{L}(Y)$ are gradually being determined, and I have learnt several new results at this congress. For details of what is known, see my forthcoming book, Wall, 1970.

REFERENCES

R. H. Bing. — An alternative proof that 3-manifolds can be triangulated, *Ann. of Math.*, vol. 69 (1959), pp. 37-65.

S. S. Cairns. — The manifold smoothing problem, *Bull. Amer. Math. Soc.*, vol. 67 (1961), pp. 237-238.

S. D. Feit. — k-mersions of manifolds, *Bull. Amer. Math. Soc.*, vol. 74 (1968), pp. 294-297 (see also *Acta Math.*, 1969).

M. L. Gromov. — Stable maps of foliations in manifolds (in Russian), *Izv. Akad. Nauk SSSR*, vol. 33 (1969), pp. 707-734.

A. Haefliger. — Feuilletages sur les variétés ouvertes, *Topology*, vol. 9 (1970), pp. 183-194.

— et V. Poenaru. — La classification des immersions combinatoires, *Publ. Math. I. H. E. S.*, vol. 23 (1966), pp. 75-91.

M. W. Hirsch. — Immersions of manifolds, *Trans. Amer. Math. Soc.*, vol. 93 (1959), pp. 242-276.

—. — On combinatorial submanifolds of differentiable manifolds, *Comm. Math. Helv.*, vol. 36 (1961), pp. 103-111.

R. C. Kirby and L. C. Siebenmann. — On the triangulation of manifolds and the Hauptvermutung, *Bull. Amer. Math. Soc.*, vol. 75 (1969), pp. 742-749.

J. Lees. — Immersions and surgeries of topological manifolds, *Bull. Amer. Math. Soc.*, vol. 75 (1969), pp. 529-534.

E. E. Moise. — Affine structures in 3-manifolds. V. The triangulation theorem and Hauptvermutung, *Ann. of Math.*, vol. 56 (1952), pp. 96-114.
J. Nash. — Real algebraic manifolds, *Ann. of Math.*, vol. 56 (1952), pp. 405-421.
S. Smale. — The classification of immersions of spheres in Euclidean spaces, *Ann. of Math.*, vol. 69 (1959), pp. 327-344.
D. Sullivan. — Geometric topology, Part I. Localization, Periodicity and Galois Symmetry, *Notes*, *M. I. T.* (1970).
C. T. C. Wall. — *Surgery on Compact Manifolds*, Academic Press (1970).
J. H. C. Whitehead. — On C^1-complexes, *Ann. of Math.*, vol. 41 (1940), pp. 809-824.
H. Whitney. — Differentiable manifolds, *Ann. of Math.*, vol. 37 (1936), pp. 645-680.

Department of Pure Mathematics,
University of Liverpool,
L69 3BX.
England.

A

LOGIQUE MATHÉMATIQUE

Actes, Congrès intern. math., 1970. Tome 1, p. 223 à 227.

LA THÉORIE DES ÉNUMÉRATIONS

par Yu. L. ERŠOV

Avant de passer aux définitions précises, je donnerai la liste de quelques travaux qui étaient à la base de la création de la théorie générale des énumérations et des problèmes considérés dans cet exposé :

1. Études des suites calculables des ensembles récursivement énumérables (Rice, Lachlan, Ouspenski et d'autres).
2. Étude de la notion de créativité et de *m*-universalité pour des ensembles et suites (Myhill et d'autres).
3. Étude des fonctions partielles récursives de Gödel (Rogers).
4. Étude des modèles et des algèbres énumérés (Fröhlich et Shepherdson, Malcev, Rabin et d'autres).
5. Étude des fonctionnelles calculables de types supérieurs (Kleene, Kreisel et d'autres).

Les premiers travaux de systématisation des notions principales de la théorie des énumérations ont été faits par A. I. Malcev [2], [3]. En particulier, c'est lui qui a introduit la notion importante d'un ensemble complet. Cette notion a permis, d'une façon naturelle, d'établir le lien entre les remarquables théorèmes de Myhill et Rogers.

Ma communication n'est pas un exposé de tous les résultats obtenus dans la théorie des énumérations. Mon but est de formuler une série de notions principales de cette théorie et d'exposer quelques nouveaux théorèmes, qu'on peut diviser en les trois groupes suivants :

La première partie contient les théorèmes structuraux sur des ensembles complètement énumérés, la deuxième représente la formulation, en termes d'énumération, de la théorie de créativité-*m*-universalité, théorie qui a un caractère achevé et qui embrasse une large classe de cas inconnus jusqu'à présent, même dans le cas traditionnel, des suites calculables des ensembles récursivement énumérables. La troisième partie est consacrée à la théorie de la construction énumérative de la classe des fonctionnelles calculables de tous les types finis. La construction proposée se distingue parmi d'autres par le plus grand naturel de ses définitions et par l'absence totale de conditions limitatives (monotonie, continuité, etc.).

J'espère que la liste de théorèmes donnée ci-dessous montrera la fécondité des points de vue de la théorie générale des énumérations.

Passons aux définitions précises.

Soient N l'ensemble de tous les nombres naturels, S un ensemble non-vide, fini ou dénombrable. On appelle *énumération de l'ensemble* toute application ν de l'ensemble N sur $S(\nu : N \to S)$. *On appelle ensemble énuméré* γ le couple (S, ν) ; où ν est une énumération de l'ensemble S. On appelle *morphisme* d'un ensemble énuméré $\gamma_0 = (S_0, \nu_0)$

dans l'ensemble $\gamma_1 = (S_1, \nu_1)$ une application $\mu: S_0 \to S_1$ telle, qu'il existe une fonction générale récursive (f. g. r.) g pour laquelle $\mu\nu_0 = \nu_1 g(\mu: \gamma_0 \to \gamma_1)$.

Nous désignons par Mor(γ_0, γ_1) l'ensemble de tous les morphismes de γ_0 dans γ_1. La classe de tous les ensembles énumérés avec des morphismes définis plus haut forme la catégorie $\mathfrak{N}$, catégorie des ensembles énumérés. La catégorie $\mathfrak{N}$ possède des sommes et des produits finis $(+, \times)$. Par N sera désigné l'ensemble énuméré (N, id) où N est l'objet initial de la catégorie.

I. Ensembles complètement énumérés.

Définition. — Soit γ un ensemble énuméré. On appelle *sous-objet* de γ tout couple (γ_0, μ) où $\mu: \gamma_0 \to \gamma$ est un morphisme univoque.

On appelle *e-sous-objet* un sous-objet (γ_0, μ) pour lequel les conditions suivantes se vérifient:

a) l'ensemble $\nu^{-1}\mu(S_0)$ est récursivement énumérable;
b) il existe une fonction partielle récursive (f. p. r.) g telle que $x \in \nu^{-1}\mu$ entraîne que $g(x)$ est définie et $\mu g x = \nu x$.

Remarque. — La notion de *e*-sous-objet représente une généralisation naturelle de la notion d'ensemble récursivement énumérable.

L'ensemble γ est appellé *complet*, si pour chaque *e*-sous-objet (γ_0, μ) de chaque ensemble énuméré γ_1 et pour chaque morphisme $\mu_0: \gamma_0 \to \gamma$ il existe un morphisme $\mu_1: \gamma_1 \to \gamma$ tel que le diagramme

$$\begin{array}{ccc} \gamma_0 & \xrightarrow{\mu} & \gamma_1 \\ & {\scriptstyle\mu_0}\searrow \quad \swarrow{\scriptstyle\mu_1} & \\ & \gamma & \end{array}$$

est commutatif; c'est-à-dire $\mu_0 = \mu_1\mu$.

Cette propriété de l'ensemble énuméré γ a une ressemblance avec l'injectivité. Notons que la catégorie $\mathfrak{N}$ ne possède pas d'objets injectifs non-triviaux.

Exemples. — 1. Si U^2 est une fonction de Gödel (de Kleene) universelle partielle récursive, on peut la considérer comme une certaine énumération κ de la classe Y_p de fonctions partielles récursives à un argument. L'ensemble énuméré $\boldsymbol{K} = (Y_p, \kappa)$ correspondant est complètement énuméré.

2. Soit P_n la classe de tous les sous-ensembles récursivement énumérables de N. L'application $d: Y_p \to P_n$ est définie de la façon suivante: $d\varphi$ est le domaine de définition de φ, d est une application surjective. L'application $\pi = d\kappa: N \to P_n$ est une énumération (de Post) de la classe P_n. L'ensemble énuméré $\boldsymbol{\Pi} = (P_n, \pi)$ est complètement énuméré.

Soient $\gamma = (S, \nu)$ un ensemble énuméré, $\mu: S \to S_0$ une application surjective quelconque. On appelle *ensemble-quotient* de γ l'ensemble énuméré $\gamma_0 = (S_0, \mu\nu)$ $(\gamma_0 = \gamma/\mu)$. Par exemple: $\boldsymbol{\Pi}$ est un ensemble-quotient de $\boldsymbol{K}$.

Il est évident qu'un ensemble-quotient d'un ensemble complètement énuméré est aussi complètement énuméré.

On découvre que *tout ensemble complètement énuméré est équivalent à un ensemble-quotient de* $\boldsymbol{K}$.

Notons que $\boldsymbol{\Pi}$ ne possède pas cette propriété.

THÉORÈME DE COMPLÉTION. — *Tout ensemble énuméré* γ *peut être plongé en tant que e-sous-objet dans un certain ensemble complètement énuméré.*

On peut même démontrer qu'il existe une complétion « minimale ». En effet, la complétion se fait fonctoriellement : si $\mathfrak{N}_\pi$ est une sous-catégorie complète de $\mathfrak{N}$ ayant pour objets des ensembles complètement énumérés, on peut formuler alors le théorème suivant :

THÉORÈME DE PLONGEMENT. — *Il existe un foncteur* $F_\pi : \mathfrak{N} \to \mathfrak{N}_\pi$ *et une application naturelle* $\eta : Id \to F_\pi$ *tels que pour chaque ensemble énuméré* γ, (γ, η) *est un e-sous-objet de l'ensemble complètement énuméré* $F_\pi(\gamma)$.

II. Créativité et *m*-universalité.

Soit Λ un ensemble quelconque non-vide. On appelle Λ-*suite* (des sous-ensembles de l'ensemble de nombres naturels) l'application $\boldsymbol{A} : \Lambda \to P(N)$ de l'ensemble Λ dans l'ensemble de tous les sous-ensembles de N. Désignons-la par $\boldsymbol{A} = \{ A_\lambda \}_{\lambda \in \Lambda}$ où $A_\lambda = \boldsymbol{A}(\lambda)$. A chaque Λ-suite $\boldsymbol{A}$ s'associe une énumération $\nu_{\boldsymbol{A}}$ d'un sous-ensemble $S \subset P(\Lambda)$, $\nu_{\boldsymbol{A}}(n) = \{ \lambda \mid n \in A_\lambda \}$. Nous désignons par $\hat{\boldsymbol{A}}$ l'ensemble énuméré correspondant. Inversement, pour chaque ensemble énuméré $\gamma = (S, \nu)$ où $S \subseteq P(\Lambda)$, on peut construire une Λ-suite $\{ A_\lambda \}_{\lambda \in \Lambda}$; ainsi $A_\lambda = \{ n \mid \lambda \in \nu(n) \}$. Nous désignons cette Λ-suite par $\hat{\gamma}$.

On a $\hat{\hat{\boldsymbol{A}}} = \boldsymbol{A}$, $\hat{\hat{\gamma}} = \gamma$.

Soient $\boldsymbol{A}$ et $\boldsymbol{B}$ deux Λ-suites. On dit que $\boldsymbol{A}$ *se réduit-m* à $\boldsymbol{B}(\boldsymbol{A} \leqslant {}_m\boldsymbol{B})$ s'il existe une fonction générale récursive f telle que

$$\forall x \in N \ \ \forall \lambda \in \Lambda(x \in A_\lambda \Leftrightarrow f(x) \in B_\lambda)$$

Soient $\boldsymbol{A}$ une Λ-suite, g une fonction partiellement récursive, alors $g^{-1}(\boldsymbol{A})$ est une Λ-suite $\{ g^{-1}(A_\lambda) \}_{\lambda \in \Lambda}$.

Nous appellerons la classe Q des Λ-suites *fermée* si $(\boldsymbol{A} \in Q \,\&\, (g$ est une fonction partielle récursive$)) \Rightarrow g^{-1}(\boldsymbol{A}) \in Q$.

La classe Q s'appelle Y-*classe* si Q est fermée et contient une suite m-universelle, c'est-à-dire $\exists \boldsymbol{A} \in Q \forall \boldsymbol{B} \in Q(\boldsymbol{B} \leqslant {}_m\boldsymbol{A})$.

Soient Q une Y-classe, $\boldsymbol{A}$ une suite m-universelle dans Q. On appelle *énumération canonique* de Q l'énumération $\nu : N \to Q$ qui se définit par $\nu n = \kappa_n^{-1}(\boldsymbol{A})$.

La Λ-suite $\boldsymbol{A}$ s'appelle *coproductive* pour une Y-classe Q, s'il existe une fonction générale récursive h telle que pour chaque $x \in N$

$$h(x) \in \bigcup_{\Lambda_0 \subseteq \Lambda} \Big[\bigcap_{\lambda \in \Lambda_0} (A_\lambda \cap \nu(x)_\lambda) \setminus \bigcup_{\lambda \in \Lambda \setminus \Lambda_0} (A_\lambda \cup \nu(x_\lambda)) \Big] = \bigcap_{\lambda \in \Lambda} (A_\lambda \nabla \nu(x_\lambda))$$

où

$$A \nabla B = [A \cap B] \cup [(N \setminus A) \cap (N \setminus B)]$$

et ν est une énumération canonique de Q.

THÉORÈME. — *Soient Q une Y-classe, $\nu : N \to Q$ une énumération canonique. Pour chaque Λ-suite A les propriétés suivantes sont équivalentes:*

1. *A est m-universelle pour Q, c'est-à-dire $\forall \boldsymbol{B} \in Q(\boldsymbol{B} \leqslant {}_m A)$.*
2. *A est coproductive pour Q.*
3. *Il existe une fonction générale récursive h telle, que pour chaque $x \in N$*

$$\nu_A(h(x)) = \nu_{\widehat{\nu(x)}}(h(x))$$

Une suite coproductive pour Q dans Q s'appelle une *suite créative.*

COROLLAIRE. — *Une Λ-suite $A \in Q$ est m-universelle pour Q si et seulement si A est créative.*

Il existe un lien étroit entre les Y-classes et les ensembles complètement énumérables. Ce lien permet d'établir le fait suivant: *deux Λ-suites créatives quelconques d'une Y-classe sont récursivement isomorphes.*

Considérons séparément le cas de $\Lambda = N$ et des classes comportant exclusivement des suites calculables, c'est-à-dire les suites $\{ A_n \}_{n \in N}$ pour lesquelles l'ensemble $\{ \langle x, y \rangle \mid y \in A_x \}$ est récursivement énumérable. La classe Q_0 de toutes ces suites possède une énumération de Gödel (calculable) $\bar{\kappa}$. Soit $Q \subseteq Q_0$. On dit que la suite A est coproductive pour Q par rapport à $\bar{\kappa}$ s'il existe une fonction partiellement récursive h telle que si $\bar{\kappa}(x) \in Q$, alors $h(x)$ est définie et

$$h(x) \in \cap \, (A_n \nabla \bar{\kappa}(x)_n).$$

Toutes les Y-classes $Q \subseteq Q_0$ ne possèdent pas nécessairement une suite créative par rapport à $\bar{\kappa}$. Cependant on peut donner la description complète de toutes ces Y-classes. Pour cela, rappelons la définition d'une classe standard $K \subseteq P_n$ d'ensembles récursivement énumérables (Lachlan [4]): une classe $K \subseteq P_n$ s'appelle standard, s'il existe une fonction générale récursive h, telle que $\forall x \in N . \pi_{h(x)} \in K$, et si $\pi_x \in K$, alors $\pi_{h(x)} = \pi_x$. Si K est une classe d'ensembles récursivement énumérables, alors on désignera par K' la classe de toutes les suites calculables des ensembles appartenant à K, c'est-à-dire

$$\{ A_n \}_{n \in N} \in K' \Leftrightarrow \{ A_n \}_{n \in N} \in Q_0 \qquad \text{et} \qquad \forall n \in N (A_n \in K)$$

THÉORÈME. — *Une classe Q de suites calculables est une Y-classe et elle contient une suite créative (par rapport à $\bar{\kappa}$) si et seulement s'il existe une classe standard K, contenant un ensemble vide tel que*

$$Q = \hat{K}' = \{ \hat{A} \mid A \in K' \}$$

III. Familles calculables de morphismes.

Soient γ_0 et γ_1 des ensembles énumérés quelconques, $S \subseteq \operatorname{Mor}(\gamma_0, \gamma_1)$ un ensemble de morphismes de γ_0 dans γ_1. L'énumération $\nu : N \to S$ s'appelle *calculable* si l'application $\langle x, s_0 \rangle \to \nu(x)(s_0)$ de l'ensemble $N \times S_0$ dans S_1 est un morphisme de $N \times \gamma_0$ dans γ_1. *Le problème P pour le couple* (γ_0, γ_1) consiste à trouver une énumération ν_0 calculable de l'ensemble $\operatorname{Mor}(\gamma_0, \gamma_1)$ telle que pour chaque autre énumération calculable $\nu : N \to S \subseteq \operatorname{Mor}(\gamma_0, \gamma_1)$, le plongement de S dans $\operatorname{Mor}(\gamma_0, \gamma_1)$, soit un morphisme de (S, ν) dans $(\operatorname{Mor}(\gamma_0, \gamma_1), \nu_0)$.

Si le problème P est décidable pour le couple (γ_0, γ_1), l'ensemble énuméré $(\operatorname{Mor}(\gamma_0, \gamma_1), \nu_0)$, où ν_0 est la numération recherchée, est désigné par ***Mor*** (γ_0, γ_1).

THÉORÈME. — *Pour le couple* (γ_0, γ_1), *le problème P est décidable si et seulement si le foncteur* $\gamma \rightsquigarrow \boldsymbol{Mor}\,(\gamma_0 \times \gamma, \gamma_1)$ *de* $\mathfrak{N}$ *dans S et est représentable; en cas de décidabilité, l'ensemble énuméré* $\boldsymbol{Mor}\,(\gamma_0, \gamma_1)$ *est justement la solution du problème de représentation de ce foncteur.* Les équivalences suivantes ont lieu (en cas de décidabilité du problème P pour des couples convenables):

$$\boldsymbol{Mor}\,(\gamma_0 \times \gamma_1, \gamma_2) \approx \boldsymbol{Mor}\,(\gamma_0, \boldsymbol{Mor}\,(\gamma_1, \gamma_2))$$
$$\boldsymbol{Mor}\,(\gamma_0 + \gamma_1, \gamma_2) \approx \boldsymbol{Mor}\,(\gamma_0, \gamma_2) \times \boldsymbol{Mor}\,(\gamma_1, \gamma_2)$$

EXEMPLES. — 1. Pour le couple (N, N), le problème P est indécidable.

2. Si $\mathbf{1}$ est un ensemble énuméré à un seul élément, alors pour chaque γ ont lieu les équivalences suivantes: $\boldsymbol{Mor}\,(\gamma, \mathbf{1}) \approx \mathbf{1}$, $\boldsymbol{Mor}\,(\mathbf{1}, \gamma) \approx \gamma$.

L'auteur a trouvé des conditions suffisantes assez larges de décidabilité du problème P dans la classe d'énumérations calculables des ensembles récursivement énumérables, mais la formulation de ces conditions est trop complexe pour qu'on puisse la donner ici. Cependant, comme corollaire, nous pouvons indiquer ici l'existence d'une suite d'ensembles énumérés, qui peut être assez naturellement interprétée comme une famille de fonctionnelles partielles calculables de tous les types finis. Ces ensembles énumérés sont indexés par des types correspondants (0 est un type, si σ et τ sont des types, alors $(\sigma \to \tau)$ est un type).

$$F_0 = N, \ldots, F_{(\sigma \to \tau)} = \boldsymbol{Mor}\,(F_\sigma, F_\pi(F_\tau))$$

A noter que $F_{(0 \to 0)} \approx K$ est la classe de toutes les fonctions partiellement récursives (avec l'énumération de Gödel). Les fonctionnelles définies de cette manière possèdent des propriétés intéressantes (continuité, monotonie, théorèmes de récursion, fermeture par rapport au point minimal fixe, bar-récursions, etc.).

BIBLIOGRAPHIE

[1] Yu. L. ERŠOV. — La Théorie des Énumérations, *I. N. G. U.*, 1 (1969), p. 176.

[2] A. I. MALCEV. — Algèbres constructives, *Ouspekhi mat. Naouk*, 16, No. 3 (1961), pp. 3-60.

[3] A. I. MALCEV. — Ensembles complètement énumérés, *Algèbre et Logique*, 2, No. 2 (1963), pp. 4-29.

[4] A. H. LACHLAN, Standard classes of recursively enumerable sets, *Zeit. Math. Log. Gr. Math.*, 10 (1964), pp. 23-42.

Institut des Mathématiques
Section Sibérienne
de l'Académie des Sciences
de l'U. R. S. S.
Novossibirsk 90, U. R. S. S.

Actes, Congrès intern. math., 1970. Tome 1, p. 229 à 233.

ORDINALS AND FUNCTIONALS IN PROOF THEORY

by Solomon FEFERMAN

I shall present some recent results on various familiar *classes* $\mathscr{K}$ *of total functionals of finite type over the natural numbers* N. The methods of proof extend the two principal techniques of proof theory, viz. Gentzen's *normalization (cut-elimination)* and Gödel's *functional interpretation.* Thus, though the paper is not a survey, it gives a good idea of current work [1]. The principal novelty is the systematic use of *non-constructive* operations, at least as an auxiliary, in particular of functionals connected with *numerical and function quantification.*

Part I. — For F of type 2, the *class of functions of type* 1 *generated by* $\mathscr{K}$, F is described as a *hierarchy* in F (indexed by *ordinals*).

Part II. — From I we get explicit information about *existential theorems* of *subsystems of formalized analysis* and, generally, *reductions* of these systems to more familiar ones.

I. 1. **Functionals: notions and notation.**

As usual, the *type symbols* (t. s.) are 0 and $(\sigma \to \rho)$ if σ, ρ are t. s.; $n+1 =_{\mathrm{def}} (n \to 0)$. A *finite type* (f. t.) *structure* $\mathfrak{M}$ over N is of the form

$$\mathfrak{M} = (\langle M_\tau \rangle_\tau, \langle \mathrm{App}_\tau \rangle_{\tau \neq 0}, 0,')$$

where $M_0 = N$,$'$ is successor, and for $\tau = (\sigma \to \rho)$, $\mathrm{App}_\tau\colon M_\tau \times M_\sigma \to M_\rho$. $f, g, h, \ldots, F, G, H, \ldots$ range over arbitrary M_τ; $x, y, z, \ldots$ range over N. fg is written for $\mathrm{App}_\tau(f, g)$ and $fg_1 \ldots g_n$ for $(\ldots(fg_1)\ldots)g_n$. In the *maximal* $\mathfrak{M}$, $M_{(\sigma\to\rho)}$ consists of all function(al)s $f\colon M_\sigma \to M_\rho$ and fg is the *application* $f(g)$. For simplicity, throughout Part I all notions and results are formulated for the maximal $\mathfrak{M}$; they generalize directly to any structure satisfying suitable closure conditions.

For each class $\mathscr{K}$ of functionals, Gen $(\mathscr{K})$ is the class of objects *generated by explicit definition from* $\mathscr{K}$. That is, let Tm $(\mathscr{K})$ be the class of *formal terms of* f. t. built up from *variables* of each type and *constants* $\bar{F}$ of type τ for each F in $(\mathscr{K} \cup \{0\}) \cap M_\tau$, by the formation rules:

(*a*) *if t is of type* 0 *then t' is also of type* 0,
(*b*) *if t, s are of type $(\sigma \to \rho)$, σ resp. then ts is of type ρ,*
(*c*) *if φ is a variable of type σ and t is of type ρ then $\lambda\varphi\cdot t$ is of type $(\sigma \to \rho)$.*

[1] Cf. [5] for a rather comprehensive up-to-date survey of proof theory, including an extensive bibliography.

Each term t of type τ *defines* $t^{(\mathcal{K})}[\vec{f}]$ in M_τ under an assignment $\vec{f}$ to its free variables, where λ is interpreted as the *abstraction* operator; thus for closed $t = \lambda\varphi \cdot t_1$, $t^{(\mathcal{K})}f = t_1^{(\mathcal{K})}[f]$. $\mathrm{Gen}_\tau(\mathcal{K})$ consists of all $t^{(\mathcal{K})}$ for closed t of type τ in $\mathrm{Tm}(\mathcal{K})$; $\mathrm{Gen}(\mathcal{K}) = \cup_\tau \mathrm{Gen}_\tau(\mathcal{K})$.

I.2. Classes of functionals studied.

(*i*) The *primitive recursion functionals* $R = R_\tau$, given by

$$Rfg0 = f, \quad Rfgx' = gx(Rfgx),$$

in each type τ making this coherent.

(*ii*) $\mathcal{R} = \{R_\tau\}_\tau$ and $\mathcal{PR} = \mathrm{Gen}(\mathcal{R})$.

(*iii*) *The predicative primitive recursion functionals* $R^\vee = R_\tau^\vee$, given by

$$R^\vee fg0h = fh, \quad R^\vee fgx'h = gx(R^\vee fgxh)h$$

in each type τ where fh *is of type* 0.

(*iv*) $\mathcal{R}^\vee = \{R_\tau^\vee\}_\tau$ and $\mathcal{PR}^\vee = \mathrm{Gen}(\mathcal{R}^\vee)$.

(*v*) The *numerical quantification functional* E of type 2:

$$Ef = 0 \quad \text{if} \quad \exists x(fx = 0), \quad \text{and} \quad = 1 \quad \text{otherwise.}$$

(*vi*) The *unbounded minimum operator* μ of type 2:

$$\mu f = (\text{the least } x \text{ with } fx = 0 \text{ if } Ef = 0), \quad \text{and} \quad = 0 \quad \text{otherwise.}$$

μ, rather than E, is needed for Part II. This work is extended to functionals for *function quantification* and corresponding *selection operators*.

I.3. Infinite terms.

These are used for stating the first main results, though the applications require only special cases which can be stated for familiar hierarchies. It is technically useful to distinguish formally *sequences* of type τ from functionals of type $(0 \to \tau)$; the *t. s.* are now extended to include τ^0 whenever τ is a t. s. Let $\mathcal{F}$ be *any collection of type* 2 *functionals*; for each $F \in \mathcal{F}$, $\bar{F}$ is taken as a constant of type $(0^0 \to 0)$ in $Tm^\infty(\mathcal{F})$. The formation rules for $\mathrm{Tm}^\infty(\mathcal{F})$ are just like those of 1.1(*a*)-(*c*) and, in addition:

(*b'*) *if* t, s *are terms of type* τ^0, 0 *resp. then* ts *is of type* τ,

(*d*) *if* t_n *is a sequence of terms of type* τ *then* $\langle t_n \rangle_n$ *is a term of type* τ^0.

For $t = \langle t_n \rangle_n$ closed, $t^{(\mathcal{F})} = \lambda n \cdot t_n^{(\mathcal{F})}$. Each $t \in \mathrm{Tm}^\infty(\mathcal{F})$ can be regarded as a *coded well-founded tree in* N, with a natural ordinal length $|t|$, where

$$|\langle t_n \rangle_n| = \sup_n (|t_n| + 1).$$

Also, it makes sense to say that t is recursive, etc.

The *reducibility relation* $\dashv$ is the least relation satisfying:

A. $(\lambda\varphi \cdot t)s \dashv \mathrm{Subst}(s/\varphi)t$,

B. $\langle t_n \rangle_n \bar{k} \dashv t_k$,

C. $\langle t_n \rangle_n rs \dashv \langle t_n s \rangle r$, and which is transitive and preserves the operations of term formation. Let $\mathrm{Irr}_\tau^\infty(\mathscr{F})$ be the set of *irreducible* t in $\mathrm{Tm}^\infty(\mathscr{F})$ of type τ; these are also said to be *normal form* (*n. f.*). The new conditions on types ensure that *every* t *in* $\mathrm{Irr}_0^\infty(\mathscr{F})$ *is built entirely from members of* $\mathrm{Irr}_0^\infty(\mathscr{F})$, since then t is either of the form (*i*) $\overline{0}$, (*ii*) a variable, (*iii*) t_0', (*iv*) $\langle t_n \rangle_n s$ where s is not a numeral, or (*v*) $\overline{F}(\langle t_n \rangle_n)$ for some $F \in \mathscr{F}$.

I.4. Hierarchies.

These are associated to $\mathrm{Tm}^\infty(\mathscr{F})$. For any ordinal α, let

$\mathscr{H}_\alpha^{\mathscr{F}}$ = *the collection of all* $(\lambda x \cdot t)^{(\mathscr{F})}$ *where* $\lambda x \cdot t$ *is closed*, $t \in \mathrm{Irr}_0^\infty(\mathscr{F})$, $|t| < \alpha$ *and* t *is recursive* (²).

Besides directly employing type 2 functionals, this scheme is notation-free, in contrast with the usual recursion-theoretic analogues of classical (Borel, etc.) hierarchies where an operation of type $(1 \to 1)$ is iterated along special systems of ordinal notations, taking " effective joins " at limits; cf. [6]. In particular, the familiar hyperarithmetic hierarchy is got by iterating a " jump operator " (related to E). For recursive limit ordinals α (writing $\mathscr{H}_\alpha^F = \mathscr{H}_\alpha^{\{F\}}$):

$\mathscr{H}_\alpha^\mu = \mathscr{H}_\alpha^E$ = *the class of functions recursive in the hyperarithmetic hierarchy by stage* α.

For $\alpha = \omega$ these are just the *arithmetical functions.*

I.5. Theorem.

For any class $\mathscr{F}$ *of type* 2 *functionals containing* μ *we have:*

(*i*) $\mathrm{Gen}_1(\mathscr{R}^\vee \cup \mathscr{F}) = \mathscr{H}_\omega^{\mathscr{F}}$, *and*

(*ii*) $\mathrm{Gen}_1(\mathscr{R} \cup \mathscr{F}) = \mathscr{H}_{\varepsilon_0}^{\mathscr{F}}$.

The proof of $\supseteq$ in (*i*) is straightforward. In (*ii*), $\supseteq$ uses the fact that $(R^\prec) \in \mathscr{P}\mathscr{R}$ for each initial segment $\prec$ of the natural well-ordering in N of type ε_0, where the $R^\prec$ are the functionals for transfinite recursion on $\prec$.

The proof of $\subseteq$ in (*ii*) follows Tait's description in [7] of $\mathrm{Gen}_1(\mathscr{R})$ in terms of a subrecursive hierarchy up to ε_0. He extended Gentzen's cut-elimination method to infinite terms; this simply relativizes to any $\mathscr{F}$, as follows (still with effective steps). For each r in $\mathrm{Tm}(\mathscr{R} \cup \mathscr{F})$ there is an r^+ in $\mathrm{Tm}^\infty(\mathscr{F})$ with $|r^+| < \omega \cdot 2$, defining the same functional; $(\bar{R})^+ = \lambda\varphi \cdot \lambda\psi \cdot \langle t_n \rangle_n$ where $t_0 = \varphi$, $t_{n+1} = \psi \bar{n} t_n$. Now for $r \in \mathrm{Tm}^\infty(\mathscr{F})$ let $|r| < \alpha$, with $2^\alpha = \alpha$ (i. e. $\alpha = \omega$ or α is an ε_β). Then there is r^* in n. f. such that $r \dashv r^*$ and $|r^*| < \alpha$. To prove $\subseteq$ in (*i*) note that the $R^\vee$ can be explicitly defined in terms of $+$, . and μ; we can then restrict attention to r in $\mathrm{Tm}^\infty(\mathscr{F})$ with $|r| < \omega$.

II.1. Non-constructive functional interpretations.

Let $T = T_{\mathscr{R},\mu}$ be a formally intuitionistic theory with variables in all f. t., but with quantifiers in type 0 only; in addition to the standard axioms for 0, $'$ and induction,

---

(²) Recursiveness is only appropriate for the hierarchies in this paper; in general this requirement is to be widened.

one has for each member of Gen $(\mathscr{R}, \mu)$ an axiom expressing its definition. These imply

$$\exists x(\varphi x = 0) \leftrightarrow \varphi(\mu\varphi) = 0, \qquad \forall x(\varphi x \neq 0) \leftrightarrow \varphi(\mu\varphi) \neq 0,$$

hence also $\exists x(\varphi x = 0) \vee \sim \exists x(\varphi x = 0)$. Every *arithmetical formula* A is equivalent in T to a *quantifier-free* (*q. f.*) P. Let T^+ be the extension of T with quantifiers in all types and the following schemata for all q. f. P:

$$(M) \qquad \sim \forall\psi \sim P(\psi) \rightarrow \exists\psi P(\psi),$$

$$(AC) \qquad \forall\varphi\ \exists\psi P(\varphi, \psi) \rightarrow \exists\psi\ \forall\varphi P(\varphi, \psi\varphi).$$

Using recursion, this *axiom of choice* implies the *axiom of dependent choices* (*DC*) for such P. The classical 2nd-order system $S = (\Sigma_1^1 - DC)$ is a fragment of T^+ when the primitives of S are $\sim, \wedge, \forall$ and $\exists$ is replaced by $\sim \forall \sim$.

Föllowing Godel [3], with each formula A of T^+ is associated a formula $\exists\varphi\ \forall\psi P_A(\varphi, \psi)$ with P_A q. f. such that: *if* $T^+ \vdash A$ *then* $T \vdash P_A(t, \psi)$ *for some term* t *of* T. By (*ii*) of the above theorem and the model for T in Gen $(\mathscr{R}, \mu)$ we get:

COROLLARY (Friedman [2]). — *If* $(\Sigma_1^1 - DC) \vdash \exists\varphi A(\varphi)$ *with* $\exists\varphi A(\varphi)$ *closed, A arithmetical, then $A(f)$ holds for some* $f \in \mathscr{H}^\mu_{\varepsilon_0}$.

Applying the theorem to $\mathscr{F} = \{ \mu, F \}$ with F a functional for function quantification (explicitly yielding an associated selection operator) we also get the similar result for $(\Sigma_2^1 - DC)$ in [2]. It is likely that this can be extended to the further results stated there for $(\Sigma_n^1 - DC)$, $n > 3$.

II.2. **Reductions of subsystems of analysis.**

By formalizing the argument just sketched we get new proofs of refinements obtained by Friedman in [2]; for example, $(\Sigma_1^1 - DC)$ is proof-theoretically reducible to the system $S^* = (\Pi_0^1 - CA)_{<\varepsilon_0}$ expressing the existence of the hyperarithmetic hierarchy up to α for each $\alpha < \varepsilon_0$. One new point is involved. In the model for T above we had in mind the maximal type structure, which cannot be dealt with in S^*. Instead, one uses a " term model " $\mathfrak{M}$ in which the M_τ consist of the closed t in $\mathrm{Irr}_\tau(\mu)$. For M_0 to be N, each such t of type 0 must be a numeral. This does not hold for the $\dashv$ relation given by I.3(*A-C*), but is ensured when we add:

$$D. \qquad \bar{\mu}(\langle \bar{k}_n \rangle_n) \dashv \overline{\mu(\lambda n \cdot k_n)}.$$

This introduces no new " cuts ", so again every r with $|r| < \varepsilon_0$ reduces to r^* in n. f. (in the new sense) with $|r^*| < \varepsilon_0$. The association is no longer recursive, but it does not lead outside of $\mathscr{H}^\mu_{\varepsilon_0}$. Similarly one gets the reduction of [2] for $(\Sigma_2^1 - DC)$ to a system $(\Pi_1^1 - CA)_{<\varepsilon_0}$.

Remark on alternative proofs. — Those in [2] involve an ingenious use of non-standard models whose existence follows from a proof-theoretical result concerning ε_0 (due to Kreisel). (By [4] non-standard, and not ω-models, have to be used, even for the corollary, since the minimum ω-model of $(\Sigma_1^1 - DC)$ consists of all the hyperarithmetic functions). The proofs sketched here extend current general methods in a straightforward way.

II.3. **Relations to predicativity and mathematical practice.**

The results also eliminate the use of *prima-facie* impredicative definitions, such as for $\mathscr{R}$, in favor of predicative ones. When extended to $\mathscr{R}^{\prec}$ for predicative well-orderings $\prec$, they lead to more elegant reformulations of the systems studied in [1], suppressing all quantifiers in types > 0.

As pointed out in [4], substantial portions of analysis have been developed predicatively; but they happen to require only closure under arithmetical definability. This is explained by (*i*) of the theorem (I.5), in the sense that this part of mathematics can easily be seen to require only the closure conditions of Gen ($\mathscr{R}^{\vee}$, μ). More generally, it is fair to say that in terms of the notions studied here we can make clear what more we know when we have proved a theorem of analysis by restricted means than when we merely know that it is true.

BIBLIOGRAPHY

[1] S. Feferman. — Systems of predicative analysis, *J. Symbolic Logic*, v. 29 (1964), pp. 1-30.

[2] H. Friedman. — Iterated inductive definitions and Σ_2^1-AC, pp. 435-442 in *Intuitionism and proof theory* (ed., Myhill, Kino, Vesley), Amsterdam (1970).

[3] K. Godel. — Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes, *Dialectica*, v. 12 (1958), pp. 280-287.

[4] G. Kreisel. — The axiom of choice and the class of hyperarithmetic functions, *Indag. Math.*, v. 24 (1962), pp. 307-319.

[5] —. — A survey of proof theory, *J. Symbolic Logic*, v. 33 (1968), pp. 321-388.

[6] J. Shoenfield. — A hierarchy based on a type 2 object, *Trans. Amer. Math. Soc.*, v. 134 (1968), pp. 103-108.

[7] W. W. Tait. — Infinitely long terms of transfinite type, pp. 176-184 in *Formal Systems and Recursive Functions* (ed. Crossley), Amsterdam (1965).

Math. Dept.
Stanford University
Stanford Calif. 94305
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 235 à 238.

DIOPHANTINE REPRESENTATION OF RECURSIVELY ENUMERABLE PREDICATES

by YU. V. MATIJASEVIČ

The tenth problem on David Hilbert's famous list (cf. [1]) is formulated as follows:

10. *Entscheidung der Lösbarkeit einer diophantischen Gleichung.*

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt; man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

A diophantine equation is an equation of the form

$$P(x_1, \ldots, x_n) = 0$$

where P is a polynomial (all polynomials considered here are polynomials with integer coefficients).

It is well-known (cf. [2] or [3]) that an algorithm for determining the solvability in integers would yield an algorithm for determining the solvability in positive integers and conversely. Hence we will limit our discussion to questions of solvability in positive integers. Lower-case Latin letters will always be variables whose range is the positive integers.

A relation $\mathscr{R}(x_1, \ldots, x_n)$ among natural numbers is called *diophantine* if there is a polynomial P such that

$$\mathscr{R}(x_1, \ldots, x_n) \Leftrightarrow \exists y_1 \ldots y_k[P(x_1, \ldots, x_n, y_1, \ldots, y_k) = 0].$$

MAIN THEOREM. — *Every recursively enumerable predicate is diophantine.*

COROLLARY. — *Hilbert's tenth problem is unsolvable.*

The first major contribution to the proof of the Main Theorem was made by Martin Davis. He has shown in [4] that *every recursively enumerable predicate $\mathscr{R}(x_1, \ldots, x_n)$ can be represented in the form*

$$\mathscr{R}(x_1, \ldots, x_n) \Leftrightarrow \exists w \forall z_{\leqslant w} \exists y_1 \ldots y_k[P(x_1, \ldots, x_n, y_1, \ldots, y_k, w, z) = 0]$$

where P is a polynomial.

Taking advantage of this representation Martin Davis, Hilary Putnam and Julia Robinson proved in [5] that *every recursively enumerable predicate $\mathscr{R}(x_1, \ldots, x_n)$ can be represented in the form*

$$\mathscr{R}(x_1, \ldots, x_n) \Leftrightarrow \exists y_1 \ldots y_k[P(x_1, \ldots, x_n, y_1, \ldots, y_k) = Q(x_1, \ldots, x_n, y_1, \ldots, y_k)] \quad (1)$$

where P and Q are functions built from variables and particular positive integers by addition, multiplication and exponentiation.

To prove the Main Theorem it is sufficient to show that the relation given by

$$z = x^y \tag{2}$$

is diophantine. For then we can eliminate exponentiation from (1) in the usual way and thus obtain a diophantine representation of $\mathscr{R}$.

The question of whether the relation (2) is diophantine was studied by Julia Robinson in [6]. Among other theorems she proved the following one:

If there exists a diophantine relation $\mathscr{D}(u, v)$ such that

$$\forall uv[\mathscr{D}(u, v) \Rightarrow v \leqslant u^u] \tag{3}$$

and

$$\forall k \exists uv[\mathscr{D}(u, v) \,\&\, u^k < v] \tag{4}$$

then the relation (2) *is diophantine.*

A relation $\mathscr{D}(u, v)$ is said *to be a relation of exponential growth* if it meets conditions (3) and (4).

The first example of a diophantine relation of exponential growth appears in [7]. This work completes the proof of the Main Theorem. Here we exibit this relation and outline the proof.

Let φ_n be defined by

$$\varphi_0 = 0, \qquad \varphi_1 = 1, \qquad \varphi_{k+1} = \varphi_k + \varphi_{k-1}$$

(φ_n is the famous Fibonacci series). The relation given by

$$v = \varphi_{2u} \tag{5}$$

is an example of a diophantine relation of exponential growth.

It can be easily proved that for every u

$$2^{u-1} \leqslant \varphi_{2u} < 3^u.$$

This implies that relation (5) is a relation of exponential growth.

It is proved in [7] that $v = \varphi_{2u}$ *if and only if there are positive integers l, z, g, h, m, x, y such that*

$$\begin{array}{rr} u \leqslant v, & l \mid m - 2, \\ l > v, & 2h + g \mid m - 3, \\ l^2 - lz - z^2 = 1, & x^2 - mxy - y^2 = 1, \\ g^2 - gh - h^2 = 1, & l \mid x - u, \\ l^2 \mid g, & 2h + g \mid x - v. \end{array} \tag{6}$$

It is easy to see that the relations $a \leqslant b$, $a > b$, $a \mid b$ are diophantine and hence can be eliminated from (6). A system of diophantine equations can easily be transformed into a single equation (cf. [2] or [3]). Hence the relation (5) is diophantine.

To prove that conditions (6) are necessary and sufficient we consider the sequences $\psi_{m,n}$ defined for every $m \geqslant 2$ by

$$\psi_{m,0} = 0, \qquad \psi_{m,1} = 1, \qquad \psi_{m,k+1} = m\psi_{m,k} - \psi_{m,k-1}.$$

It can be easily proved by induction that

$$\begin{aligned} \psi_{m,n} &\equiv n \pmod{m-2}, \\ \psi_{m,n} &\equiv \varphi_{2n} \pmod{m-3}. \end{aligned}$$

Hence if $d \mid m - 3$, then

$$\operatorname{Rem}(\psi_{m,n}, d) = \operatorname{Rem}(\varphi_{2n}, d)$$

(Rem (a, b) denotes the remainder obtained upon dividing a by b).

We study the sequence

$$\operatorname{Rem}(\varphi_0, d), \qquad \operatorname{Rem}(\varphi_2, d), \ldots, \operatorname{Rem}(\varphi_{2n}, d), \ldots \tag{7}$$

where $d = \varphi_{2k} + \varphi_{2(k+1)}$ for some k. It can be proved that sequence (7) is periodic, the length of the period is equal to $2k + 1$, and the period consists of the following numbers:

$$\varphi_0, \varphi_2, \ldots, \varphi_{2k} = d - \varphi_{2(k+1)}, \varphi_{2(k+1)} = d - \varphi_{2k}, \ldots, d - \varphi_4, d - \varphi_2.$$

We also use the following properties of numbers φ_n and $\psi_{m,n}$:

$$\begin{gathered} x^2 - xy - y^2 = 1 \Leftrightarrow \exists i[x = \varphi_{2i+1} \;\&\; y = \varphi_{2i}], \\ m \geqslant 2 \Rightarrow [[x^2 - mxy + y^2 = 1 \;\&\; x \geqslant y] \Leftrightarrow \exists i[x = \psi_{m,i+1} \;\&\; y = \psi_{m,i}]], \\ \varphi_s^2 \mid \varphi_t \Rightarrow \varphi_s \mid t, \\ s\varphi_s \mid t \Rightarrow \varphi_s^2 \mid \varphi_t. \end{gathered}$$

It is not very difficult to prove these properties by induction and course-of-values induction.

Having proved the above mentioned properties of numbers φ_n and $\psi_{m,n}$ we can easily complete the proof of the necessity and sufficiency of the conditions (6).

Combining our Main Theorem with an earlier result of Hilary Putnam [8], we can obtain the following theorem:

Every recursively enumerable set S of positive integers can be represented in the form

$$a \in S \Leftrightarrow \exists y_1 \ldots y_n[a = P(y_1, \ldots, y_n)] \tag{8}$$

where P is a polynomial.

For example, the set of all prime numbers coincides with the set of all positive values of some polynomial with integer coefficients!

If S in (8) is any recursively enumerable, but not recursive set of positive integers, then there is no algorithm for determining for given a whether the equation

$$P(y_1, \ldots, y_n) = a$$

has a solution. This result is stronger than the unsolvability of Hilbert's tenth problem.

Using Gödel numbering of recursively enumerable sets we can construct a polynomial $M(y_1, \ldots, y_k, g)$ such that every recursively enumerable set S of positive integers can be represented in the form

$$a \in S \Leftrightarrow \exists y_1 \ldots y_k [a = M(y_1, \ldots, y_k, g_S)]$$

where g_S is any Gödel number of S.

The constructions known today yield such universal polynomials with some 200 variables. For the set of all primes we can construct a polynomial with about 25 variables. Of course, these constructions are not the best ones and we can hope they will be essentialy improved in the future.

REFERENCES

[1] D. Hilbert. — Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris, 1900. *Nachr. K. Ges. Wiss. Göttingen, Math.-Phys. Kl.* (1900), pp. 253-297.

[2] А. И. Мальцев. — Алгоритмы и рекурсивные функции. Москва, (1965).

[3] M. Davis. — *Computability and Unsolvability* (New York, 1958).

[4] M. Davis. — Arithmetical problems and recursively enumerable predicates, *J. Symb. Logic*, 18 (1953), pp. 33-41.

[5] M. Davis, H. Putnam and J. Robinson. — The decision problem for exponential diophantine equations, *Ann. of Math.*, 74, n° 3 (1961), pp. 425-436.

[6] J. Robinson. — Existential definability in arithmetic, *Trans. Amer. Math. Soc.*, 72 (1952), pp. 437-449.

[7] Ю. В. Матиясевич. — Диофантовость перечислимых множеств. Доклады АН СССР, 191, N° 2 (1970), pp. 279-282.

[8] H. Putnam. — An unsolvable problem in number theory, *J. Symb. Logic*, 25, n° 3 (1960), pp. 220-232.

Steklov Mathematical Institute
of Academy of Sciences of USSR
Leningrad (U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 239 à 244.

DECIDABILITY AND DEFINABILITY IN SECOND-ORDER THEORIES

by MICHAEL O. RABIN

The purpose of this note is to collect and present from a unified point of view certain results concerning second-order logic which were obtained in recent years [5, 6, 7]. In addition, several open problems and directions for further research are indicated.

It is well known that a second-order language with variables for binary relations, where the relation variables have the *standard* interpretation, is strong enough to express all statements of arithmetic as well as many set-theoretical facts. Thus there is no hope for positive decidability results for the theory of any (infinite) structure in such a language.

Here we deal with $S2S$-the monadic second-order theory of the structure of two successor functions (the full binary tree). We are able to not only solve the decision problem for this theory, but also to completely characterize the relations definable in it. Because the theory in question is taken with the standard interpretation for the set variables, the result turns out to be very powerful and many other decision problems are directly reducible to it. The solution of the decision problem of $S2S$ involves development of a theory of automata on infinite trees. The basic concepts and results of this theory are also outlined here.

1. Terminology and main result.

We employ the usual set theoretic notations concerning mappings, sequences, etc. In particular, every ordinal $\alpha = \{ \beta \mid \beta < \alpha \}$ is the set of all smaller ordinals. Integers will be denoted by k, l, m, n. The set $\{ 0, 1, \ldots, \}$ of all integers is denoted by ω. For a set A and an ordinal α, $A^\alpha = \{ x \mid x : \alpha \to A \}$ is the set of α-termed sequences on A. An n-termed sequence $x \in A^n$ is written as $(x(0), \ldots, x(n-1))$. The *length* of x is $l(x) = n$. A sequence (a) of length 1 will also be written as a. The (unique) sequence of length 0 is denoted by Λ. For a set A denote by $A^* = \bigcup_{n<\omega} A^n$, the set of all finite sequences (*words*) on A. For words $x, y \in A^*$ let $xy \in A^*$ stand for the result of concatenating x with y. Thus $x = x(0)x(1) \ldots x(n-1)$. For $a \in A$ we define the *successor function* $r_a : A^* \to A^*$ by $r_a(x) = xa$, $x \in A^*$. On A^* define a partial-ordering $x \leqq y$ (x is an *initial* of y) by $\exists z[xz = y]$.

For $n \leqq \omega$ the *n-ary tree* T_n is defined by $T_n = n^*$. Each $x \in T_n$ is called a *node* of T_n; $r_i(x)$, $i < n$, is the i-th *successor* of x; $\Lambda \in T_n$ is the *root* of the tree. A subset $\phi \neq \pi \subseteq T_n$ is called a *path* if: 1) $y \leq x \in \pi$ implies $y \in \pi$; 2) for $x \in \pi$ there exists exactly one $i < n$ such $r_i(x) \in \pi$. On T_n, $n \leqq \omega$ we define the lexicographic (total) ordering $x \preccurlyeq y$ by $x \leqq y \vee \exists z \exists k \exists m[zk \leqq x \wedge zm \leqq y \wedge k < m]$.

Corresponding to a given structure $A = \langle H, f_1, \ldots, R_1, \ldots, \rangle$, or a class $\mathscr{K}$ of structures similar to A, we introduce the following (monadic) second-order language L_2. It has the usual logical connectives and quantifiers, equality, the member ship symbol $\in$, symbols $f_1, \ldots, R_1, \ldots$, to denote the corresponding functions and relations of A. The variables of L_2 are $x, y, z, \ldots$, which range over elements of the domain H, $\alpha, \beta, \gamma, \ldots$, which range over *all* finite subsets of H, and variables $A, B, C, \ldots$, which range over *all* subsets of H. Quantification is permitted over all three types of variables.

The notion of satisfaction of a formula F of L_2 in A is defined in the usual way and is denoted by $A \models F$. The *theory* of A in L_2 is defined by $\mathrm{Th}_2(A) = \{\sigma \mid \sigma$ *sentence* of L_2, $A \models \sigma\}$. $\mathrm{Th}_2(A)$ is called the *(monadic) second-order theory of* A. If $\mathscr{K}$ is a class of similar structures then we define $\mathrm{Th}_2(\mathscr{K}) = \bigcap_{A \in \mathscr{K}} \mathrm{Th}_2(A)$.

With the above notations, define, for $n \leq \omega$, the *structure of n successor functions*, $\mathscr{N}_n = \langle T_n, r_i, \leqq, \preccurlyeq \rangle_{i<n}$, and the second-order theory of n successor functions $SnS = \mathrm{Th}_2(\mathscr{N}_n)$. The main result is the following

THEOREM 1. — The (monadic) second-order theory of two successor functions ($S2S$) is,decidable.

An immediate corollary is that SnS, $n \leqq \omega$, is decidable.

2. Automata on T_2.

We shall write $T_2 = T$. In the following Σ denotes a finite set called the alphabet.

DEFINITION 1. — A Σ-(valued) *tree* is a pair $t = (v, T)$ where $v: T \to \Sigma$. The set of all Σ-trees will be denoted by V_Σ.

DEFINITION 2. — A *finite automaton* (f. a.) over Σ-trees (Σ-automaton) is a system $\mathfrak{A} = \langle S, M, s_0, \Omega \rangle$ where S is a finite set of *states*, M is a function $M: \Sigma \times S \to P(S \times S)$, the (non-deterministic) *table of moves* ($P(A)$ denotes the set of all subsets of A), $s_0 \in S$ is the *initial state*, and $\Omega = ((L_i, U_i))_{i<k}$ is a finite sequence of pairs of subsets of S.

A *run* of $\mathfrak{A}$ on $t = (v, T)$ is a mapping $r: T \to S$ such that $(r(x0), r(x1)) \in M(r(x), v(x))$, for all $x \in T$. The set of all runs will be denoted by $\mathrm{Rn}(\mathfrak{A}, t)$.

For a mapping $\varphi: A \to S$ define $\mathrm{In}(\varphi) = \{s \mid \omega \leqq c(\varphi^{-1}(s))\}$ where $c(H)$ denotes the cardinality of the set H. With Ω as above, we say that φ is of *type* Ω ($\varphi \in [\Omega]$), if for some $i < k$, $\mathrm{In}(\varphi) \cap L_i = \emptyset$ and $\mathrm{In}(\varphi) \cap U_i \neq \emptyset$.

DEFINITION 2. — The automaton $\mathfrak{A}$ *accepts* the Σ-tree t if for some run $r \in \mathrm{Rn}(\mathfrak{A}, t)$: (*i*) $r(\Lambda) = s_0$, (*ii*) for every path $\pi \subset T$, $r \mid \pi \in [\Omega]$.

The set of all Σ-trees accepted by $\mathfrak{A}$ is denoted by $T(\mathfrak{A})$ and called the set *defined by* $\mathfrak{A}$. A set $H \subseteq V_\Sigma$ is called *(automaton) definable* if for some Σ-automaton $\mathfrak{A}$, $H = T(\mathfrak{A})$.

Let Σ_1 be an alphabet and $p : \Sigma \to \Sigma_1$. For a Σ-tree $t = (v, T)$ define the *projection* $p(t) = (pv, T) \in V_{\Sigma_1}$.

THEOREM 2. — If $A, B \subseteq V_\Sigma$ are automaton definable then so are (*i*) the union $A \cup B$; (*ii*) the complement $V_\Sigma - A$; (*iii*) the projection $p(A)$.

Of the above statements, (*i*) is trivial, (*ii*) is a deep result requiring a difficult proof, and (*iii*) follows at once from the fact that our automata are non-deterministic.

THEOREM 3. — There exists an algorithm for deciding for every given automaton $\mathfrak{A}$ whether $T(\mathfrak{A}) = \varnothing$. If $\mathfrak{A}$ has n states and $c(\Sigma) = m$, then the algorithm requires about $m4^{mn}$ steps.

DEFINITION 3. — The automaton $\mathfrak{A}$ is called *special* if $k = 1$ and $L_0 = \varnothing$. A set $H \subseteq V_\Sigma$ is *weakly definable* if it is definable by a special automaton.

Weakly definable sets satisfy (*i*) and (*iii*) but not necessarily (*ii*) of Theorem 2.

3. Second-order definability.

A relation $R \subseteq P(T)^n$ is *definable* in $S2S$ if for some formula $F(A_1, \ldots, A_n)$ of $L_2 : R = \{ (A_1, \ldots, A_n) \mid \mathcal{N}_2 \models F(A_1, \ldots, A_n) \}$. The relation R is *weakly definable* if the above holds with a formula F which contains no arbitrary set quantifiers (but may contain finite-set quantifiers).

Let now $\Sigma(n) = \{ 0, 1 \}^n$, $n < \omega$. With $A = (A_1, \ldots, A_n) \in P(T)^n$, we associate the $\Sigma(n)$-tree $\tau(A) = (v, T)$ where $v(x) = (\chi_{A_1}(x), \ldots, \chi_{A_n}(x))$, $x \in T$ (χ_H is the characteristic function of H).

THEOREM 4. A relation $R \subseteq P(T)^n$ is definable in $S2S$ if and only if $\tau(R) \subseteq V_{\Sigma(n)}$ is automaton definable. R is weakly definable if and only if $\tau(R)$ and $V_{\Sigma(n)} - \tau(R)$ are definable by special automata.

The proof of Theorem 4 is effective in the sense that from a formula $F(A_1, \ldots, A_n)$ an automaton $\mathfrak{A}_F$ defining $\tau(R)$ can be effectively (even primitive-recursively) constructed. Combined with Theorem 3, this immediately implies Theorem 1.

4. Applications.

We shall illustrate some of the many possible applications of the above results.

Let $\mathscr{K}_{\leq}^{\omega}$ denote the class of all countable totally ordered sets, let $\mathscr{K}_f$ denote the class of all unary algebras $\langle A, f \rangle$ where $f : A \to A$, and let $\mathscr{K}_f^{\omega}$ be the class of all countable unary algebras.

THEOREM 5. — $\mathrm{Th}_2(\mathscr{K}_{\leq}^{\omega})$ is decidable.

Proof. — For every countable $\langle \overline{A}, \trianglelefteq \rangle$ there exists a subset $A \subseteq T$ such that $\langle \overline{A}, \preccurlyeq \rangle \simeq \langle \overline{A}, \trianglelefteq \rangle$. Rewrite every sentence σ of the monadic second-order language of ordering by replacing $\leqq$ by $\preccurlyeq$ and relativizing all individual and set variables to a set variable A. For the resulting formula $\sigma(A)$ we have $\mathscr{N}_2 \models \forall A\sigma(A)$ iff $\sigma \in \mathrm{Th}_2(K^{\omega}_{\leq})$.

THEOREM 6. — $\mathrm{Th}_2(\mathscr{K}_f)$ is decidable.

This proved by first showing that $\mathrm{Th}_2(\mathscr{K}^{\omega}_f)$ is decidable by direct interpretation in $S2S$, and then using an unpublished result of J. J. Le Tourneau to the effect that $\mathrm{Th}_2(\mathscr{K}_f) = \mathrm{Th}_2(\mathscr{K}^{\omega}_f)$.

The set of all paths of T can be naturally identified with Cantor's discontinuum $CD = \{0, 1\}^{\omega}$. The closed subsets of CD are then obtained as the sets $\{\pi \mid \pi \subset A\}$, $A \subseteq T$. This yields

THEOREM 7. — The first-order theory of the lattice of all closed subsets of CD is decidable. Similarly for the real line.

The last results answered in the affirmative a long standing question of Grzegorczyk [2].

CD is the Stone-space of the free denumerable Boolean algebras $\mathfrak{B}_{\omega}$. The ideals $I \subseteq \mathfrak{B}_{\omega}$ stand in a natural one-to-one correspondence with the open subsets of CD. This implies

THEOREM 8. — Let $\mathscr{K}^{\omega}_B$ be the class of countable Boolean algebras, and let L_I be the appropriate monadic second-order language with the set variables restricted to range over ideals. The theory of $\mathscr{K}^{\omega}_B$ in L_I is decidable.

COROLLARY. — Let $\mathscr{K}_{BI}$ be the class of all Boolean algebras

$$\mathfrak{B} = \langle B, \cup, \cap, ', I_1, I_2, \ldots, \rangle$$

where the I_n, $n < \omega$, are distinguished ideals. The first-order theory of $\mathscr{K}_{BI}$ is decidable.

It is well known that various non-classical logical calculi such as fragments and extensions of the intuitionistic calculus, modal and tense logics, etc., have Kripke style interpretations by valued trees. Combining this with Theorem 1, D. Gabbay was able to derive a large number of decidability results for these calculi [1].

5. Regular trees.

A Σ-tree (v, T) is called *regular* if $v^{-1}(\sigma) \subseteq \{0, 1\}^*$ is a regular set for every $\sigma \in \Sigma$. Here " regular " means definable by an ordinary sequential automaton (see [4]).

THEOREM 9. — If $T(\mathfrak{A}) \neq \varnothing$ then there exists a regular tree $t \in T(\mathfrak{A})$.

COROLLARY. — If $F(A)$ is a formula of $S2S$ such that $\mathscr{N}_2 \models \exists AF(A)$, then there exists a regular set $A \subseteq \{0, 1\}^*$ such that $\mathscr{N}_2 \models F(A)$.

COROLLARY. — The regular sets form a basis for quantification in $S2S$.

Combined with the proof of Theorem 5, Theorem 9 also yields.

THEOREM 10. — If σ is not valid in $\mathscr{K}^{\omega}_{\leq}$ then there exists a regular set $A \subseteq \{0, 1\}^*$ such that $\langle A, \preccurlyeq \rangle \models \sim \sigma$.

Another application of Theorem 9 is to give (see [7]) a very simple solution to Church's solvability problem which was originally solved by L. Landweber in his thesis [3].

6. Open problems.

1. Find a simpler proof for Theorem 2 (*ii*), possibly avoiding the transfinite induction used in [2].

2. Find additional applications of Theorem 1. For example, can it be used to derive the well known result concerning the decidability of the theory of commutative groups.

3. Is it solvable to determine for a given tree automaton $\mathfrak{A}$ whether there exists a special automaton $\mathfrak{B}$ such that $T(\mathfrak{A}) = T(\mathfrak{B})$. Relatedly, is it decidable to determine for a given formula $F(A)$ of $S2S$ whether the corresponding relation is weakly definable. A positive answer to this new type of decidability-definability question, will shed light on the corresponding problem for the many theories interpratable in $S2S$.

4. *Uniformization.* Is it true that for every formula $F(A, \boldsymbol{B})$ such that

$$\mathscr{N}_2 \models \forall A \exists \boldsymbol{B}\, F(A, \boldsymbol{B})$$

there exists a formula $G(A, \boldsymbol{B})$ satisfying $\mathscr{N}_2 \models \forall A \exists\, !\, \boldsymbol{B} G(A, \boldsymbol{B})$ and

$$\mathscr{N}_2 \mid \forall A \forall \boldsymbol{B}[G(A, \boldsymbol{B}) \rightarrow F(A, \boldsymbol{B})].$$

An affirmative answer may be of help in Problem 1.

5. In general, study the question of tree-automaton transformations and possible generalizations of Church's solvability problem for tree automata.

BIBLIOGRAPHY

[1] D. M. GABBAY. — *Decidability results in non-classical logics I*, O. N. R. Technical Report 29 (Jerusalem, 1969), pp. 42.

[2] A, GRZEGORCZYK. — Undecidability of some topological theories, *Fund. Math.*, 38 (1951), pp. 137-152.

[3] L. H. LANDWEBER. — Finite state games. A solvability algorithm for restricted second-order arithmetic, *Notices Amer. Math. Soc.*, 14 (1967), pp. 129-130.

[4] M. O. RABIN. — Mathematical theory of automata, *Proc. Sympos. App. Math.*, vol. 19, *Amer. Math. Soc.*, Providence, R. I. (1968), pp. 153-175.

[5] —. — Decidability of second-order theories and automata on infinite trees, *Trans. Amer. Math. Soc.*, 141 (1969), pp. 1-35.
[6] —. — *Weakly definable relations and special automata, Mathematical Logic and Foundations of Set Theory* (Y. Bar Hillel, editor), North Holland Pub. Co. (1970), pp. 1-23.
[7] —. — *Automata on infinite trees and the synthesis problem*, O. N. R. Technical Report 37 (Jerusalem, 1970), pp. 24.

Hebrew University,
Department of Mathematics,
Jérusalem (Israël)
and IBM T. J. Watson
Research Center
P. O. Box 218
Yorktown Heights,
New York 10598
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 245 à 250.

FORCING IN MODEL THEORY (1)

by ABRAHAM ROBINSON

1. Introduction.

The forcing concept of Paul J. Cohen has had an immense effect on the development of Axiomatic Set Theory but it also possesses an obvious general significance. It therefore was to be expected that it would have an impact also on general Model Theory. In the present talk, I shall show that this expectation is indeed justified and that the forcing notion provides us with a new tool in Model Theory, which leads to a better understanding of concepts that have by now become classical in this area and to their further development.

The work on which this talk is based [1, 3, 4] was begun in the summer of 1969. While I am confident that it will have further consequences, enough results have become available to make a presentation on the subject appropriate.

Experimentation shows that there are several ways in which the forcing concept can be formalized within Model Theory. Here we shall explicate this notion as an analogue of the satisfaction relation (in fact, strictly, as a generalization of it), i. e., in the first place as a binary metamathematical relation which may hold between a structure and a sentence in the Lower Predicate Calculus [4]. Only the connectives $\neg$, $\vee$, $\wedge$ and only the existential quantifier will be regarded as basic (2).

2. Foundations.

We start with a specified class Σ of (first order) structures. The following rules provide a definition of the binary relation $M \Vdash X$ (*M forces X*) for structures $M \in \Sigma$ and for sentences X which are defined in M, i. e. whose extralogical constants have interpretations in M.

2.1. For atomic X, $M \Vdash$ iff $M \models X$ (M satisfies X); for $X = Y \wedge Z$, $M \Vdash X$ iff $M \Vdash Y$ and $M \Vdash Z$; for $X = Y \vee Z$, $M \Vdash X$ iff $M \Vdash Y$ or $M \Vdash Z$; for $X = (\exists y)Q(y)$, $M \Vdash X$ iff $M \Vdash Q(a)$ for some a; and for $X = \neg Y$, $M \Vdash X$ iff M' does not force Y for any $M' \in \Sigma, M' \supset M$.

The following lemma is basic. It shows that the forcing relation persists under extension of its first argument.

(1) The research on which this paper is based was supported in part by the National Science Foundation Grant No. GP-18728.

(2) The approach described here differs in some points from that adopted in ref. [4].

2.2. If $M, M' \in \Sigma$, $M' \supset M$, and $M \Vdash X$ then $M' \Vdash X$.

A structure $M \in \Sigma$ is called Σ-generic (briefly, generic) if for any X defined in M, $M \Vdash X$ iff $M \Vdash X$. The class of generic structures is denoted by G_Σ. Then

2.3. If $M, M' \in G_\Sigma$ and $M \subset M'$ then $M \prec M'$, i. e., M' is an elementary extension of M.

2.4. If $\{ M_\nu \}$ is a monotonic set of elements of G_Σ and $M = U_\nu M_\nu$ belongs to Σ then $M \in G_\Sigma$.

From now on we assume

2.5. Σ is inductive, i. e. it is closed under unions of monotonic sets of its elements. By 2.4, G_Σ is then also inductive. Then

2.6. Every element of Σ is contained in some element of G_Σ.

2.7. If $M \in G_\Sigma$, $M' \in \Sigma$, $M \subset M'$ and X is an existential or, more generally, an $\forall\exists$ sentence, which is defined in M then $M' \models X$ entails $M \models X$.

3. Universal classes.

Let U be a set of universal sentences which is closed under deduction (A sentence is *universal* if it belongs to the smallest class containing all atomic sentences or their negations and closed under conjunction, disjunction, and universal, i. e. $\neg(\exists)\neg$, quantification. U is closed under deduction if every universal X defined in U and deducible from it belongs to U). We take Σ to be the class of all models of U. Such a Σ is called a *universal class*. For example, if K is a (nonempty and consistent: n. e. a. c.) set of sentences then U may be the set of universal sentences defined in K and deducible from it, and we then write $U = K_\forall$.

3.1. Let K and K' be two n. e. a. c. sets of sentences. Then K' is model-consistent relative to K (every model of K can be embedded in a model of K') iff $K'_\forall \subset K_\forall$. And K and K' are mutually model-consistent iff $K'_\forall = K_\forall$.

U is called *irreducible* iff for any two universal sentences X_1 and X_2, $X_1 \vee X_2 \in U$ entails $X_1 \in U$ or $X_2 \in U$. A set of sentences K has the *joint embedding property* if any two models M_1 and M_2 of K can be injected into a model M of K consistently with the interpretation of the constants of K in M_1 and M_2.

3.2. K has the joint embedding property iff $K_\forall$ is irreducible.

4. Forcing in universal classes.

A universal class Σ is inductive. Accordingly, the results of section 2 above apply to it.

The following *reduction lemma* is fundamental in provinding a link between forcing and the classical concepts of model theory. The *existential degree* of a well-formed formula (w. f. f.) $Q(x_1, \ldots, x_n)$ is defined as the number of its existential quantifiers which are not in the scope of a negation.

4.1. For given U and corresponding Σ, let $Q(x_1, \ldots, x_n)$ be a w. f. f. of existential degree in which is defined in (the vocabulary of) U. Then there exists a set S_Q of sets of w. f. f., $\{Q_\nu(x_1, \ldots, x_n, y_1, \ldots, y_m)\}$ which are defined in U such that for any $a_1, \ldots, a_n$ denoting elements of an $M \in \Sigma$, $M \Vdash Q(a_1, \ldots, a_n)$ iff there exist elements of M, denoted by $b_1, \ldots, b_m$, such that for at least one $\{Q_\nu(x_1, \ldots, x_n, y_1, \ldots, y_m)\} \in S_Q$, the sentences $Q_\nu(a_1, \ldots, a_n, b_1, \ldots, b_m)$ all hold in M.

Let $|U|$ be the cardinal of U. Since the cardinality of the set of predicates definable in U is $\max(|U|, \omega)$, 4.1 leads to the following result, which may be regarded as a kind of compactness theorem or Löwenheim-Skolem theorem.

4.2. If $M \Vdash X$ then there exists an $M' \subset M$, $M \in \Sigma$, such that $M' \Vdash X$, where $|M'| \leq \max(|U|, \omega)$.

Similarly

4.3. If $M \in \Sigma$ there exists an $M \in G_\Sigma$, $M' \supset M$ such that $|M'| \leq \max(|U|, |M|, \omega)$.

The reduction lemma also enables us to axiomatize the class G_Σ in an infinitary language $L_{\beta,\omega}$ where $\beta = (2^{\max(|K|,\omega)})^+$. Other applications of 4.1 will be given later.

5. The forcing operator.

Given K, nonempty and consistent (n. e. a. c.), let $U = K_\forall$, and consider the class of generic structures G_Σ in the corresponding Σ. Let K^F be the set of sentences in the vocabulary of K which hold in all generic structures of Σ. K^F is called the *forcing companion* of K. We call $K \to K^F$ the *forcing operator*. Its basic properties are given by 5.1 and 5.2.

5.1. $K^F = (K_\forall)^F$; $(K^F)_\forall = K_\forall$; $K^{FF} = K^F$.

5.2. For any n. e. a. c. sets K_1 and K_2, $K_1^F = K_2^F$ if and only if $K_{1\forall} = K_{2\forall}$.

Also

5.3. K^F is complete if and only if K has the joint embedding property (compare 3.2).

The forcing operator will now be related to the classical theory of model-completeness. To lead up to this, we first state the following result which is a consequence of 4.1.

5.4. Let M, $M' \in \Sigma$, $M' \in G_\Sigma$, and $M \prec M'$. Then $M' \in G_\Sigma$.

We now know (2.6, 2.3, and 5.4) that $G = G_\Sigma$, as a subclass of Σ, possesses the following properties

5.5. (*i*) Any $M \in \Sigma$ is contained in some $M' \in G$; (*ii*) if M, $M' \in G$, $M \subset M'$, then $M \prec M'$; (*iii*) if $M \in \Sigma$, $M' \in G$ and $M \prec M'$ then $M \in G$.

The properties 5.5 determine the class G uniquely. That is

5.6. For a given universal class Σ, let $G = G_1$ and $G = G_2$ be subclasses of Σ which satisfy 5.5. Then $G_1 = G_2$.

For the proof, let $M \in G_1$. Using 5.5 (*i*) we construct a chain

$$M = M_0 \subset M_1 \subset M_2 \subset M_3 \subset \ldots$$

such that $M_{2j} \in G_1$, $M_{2j+1} \in G_2$, $j = 0, 1, 2, \ldots$ Then $M_0 \prec M_2 \prec M_4 \quad \ldots$ and $M_1 \prec M_3 \prec M_5 \prec \ldots$ by 5.5 (*ii*), and so, for $M' = \cup M_{2j} = \cup M_{2j+1}$, $M \prec M'$ and $M_1 \prec M$. Hence $M \prec M_1$ and so $M \in G_2$, by 5.5 (*iii*). Thus $G_1 \subset G_2$ and, similarly, $G_2 \subset G_1$, $G_1 = G_2$.

This shows, without the use of forcing, that there is at most one G as described by 5.5. We know from the results stated previously that there is at least one such G.

Recall that a n. e. a. c. set of sentences K is called model-complete if for any two models M, M' of K, $M \subset M'$ entails $M \prec M'$. A set K^* is called a *model companion* of a n. e. a. c. set K, if K^* has the same vocabulary as K, is mutually model-consistent with K, and is model-complete. This is a generalization, due to Eli Bers, of the notion of *model completion* (K^* is a model completion of K if, in addition to the conditions just stated, $K^* \supset K$ and K^* is also model-complete *relative to* K, i. e. $K^* \cup D$ is complete for the diagram D of any model M of K). It is known that for a given K there is, up to logical equivalence, at most one model companion (and, hence, at most one model completion) K^*, and this is also an immediate consequence of the results given below.

Suppose that K possesses a model companion K^*. Let Σ be the universal class of models of $U = K_\forall$. Then the class of models of K^*, G, is a subclass of Σ since $K^*_\forall = K_\forall$ (see 3.1). Also, G satisfies 5.5 (In particular G satisfies 5.5 (*ii*) since K^* is model-complete). Hence $G = G_\Sigma$ and

5.7. Suppose K has a model companion, K^*. Then K^F is the deductive closure of K^* (and, hence, is the largest model companion of K).

Thus, the notion of forcing companion is a generalization of the notion of model companion.

6. Subclasses of Σ.

For given U and Σ, we introduce three more subclasses of Σ, which are related to G_Σ. Let $M \in \Sigma$ and let X be a sentence such that the relations and functions of X occur in M (and U), but not necessarily its constants. *M forces X weakly*, $M \Vdash^* X$ if no $M' \in \Sigma$, $M' \supset M$, forces X. Then $M \Vdash^* X$ iff X holds in all generic structures $M' \supset M$ in which it is defined.

$M \in \Sigma$ is called *pregeneric* if for any sentence X which is defined in M, either $M \Vdash^* X$ or $M \Vdash^* \neg X$. The class of pregeneric structures will be denoted by P_Σ.

6.1. Suppose that $M \in P_\Sigma$, M_1, $M_2 \in G_\Sigma$, $M \subset M_1$, $M \subset M_2$, and let X be a sentence which is defined in M. Then X either holds in both M_1 and M_2 or in neither one of these structures.

6.2. Let Σ be the class of models of $U = K_\forall$ where K is n. e. a. c. Suppose that the class of models of K (which, in any case, is a subclass of Σ) is a subclass of P_Σ and includes G_Σ. Suppose that G_Σ is the class of models of a set K^*. Then K^* is a model completion of K.

Let Σ be a universal class which is given by a set U, as before. $M \in \Sigma$ is *existentially complete* (within Σ) if for every existential sentence X which is defined in M and for every extension M' of M in Σ, $M' \Vdash X$ entails $M \Vdash X$. The class of existentially complete elements of Σ will be denoted by E_Σ.

A structure $M \in \Sigma$ is *existentially universal* (in Σ) if it satisfies the following condition. Let $\{ Q_\nu(x_1, \ldots, x_n, y_1, \ldots, y_m) \}$ be a set of existential predicates formulated in the vocabulary of U, $n \geq 0$, $m \geq 0$. Suppose that for some $b_1, \ldots, b_m$ (denoting elements) of M there exists an $M' \in \Sigma$, $M' \supset M$ such that for certain $a'_1, \ldots, a'_n$ of M' all $Q_\nu(a'_1, \ldots, a'_n, b_1, \ldots, b_m)$ hold in M'. Then there exist $a_1, \ldots, a_n$ in M such that all $Q_\nu(a_1, \ldots, a_n, b_1, \ldots, b_m)$ hold in M. The class of existentially universal structures in Σ will be denoted by A_Σ.

For a given M, the number of distinct sets $\{ Q_\nu(x_1, \ldots, x_n, b_1, \ldots, b_m) \}$ is at most $2^{\max(|U|, |M|, \omega)}$. This enables us to show, by a procedure of successive extension (compare the proof of 2.6 above which is given in ref. 4) that every $M \in \Sigma$ can be embedded in an $M' \in A_\Sigma$. Moreover, if $U = K_\forall$, M' may be chosen as the union of a monotonic set of models of K.

The four subclasses of Σ that we have introduced are related by

6.3. $$P_\Sigma \supset E_\Sigma \supset G_\Sigma \supset A_\Sigma$$

Of the inclusion relations contained in 6.3, the first and last are consequences of the reduction lemma 4.1, while $E_\Sigma \supset G_\Sigma$ is contained in 2.7. Suitable examples (section 8, below) show that any two of the four classes may be distinct. We have, as a consequence of 5.3 and 6.3,

6.4. If $U = K_\forall$ where K possesses the joint embedding property then any two existentially universal structures in Σ are elementarily equivalent in the vocabulary of K.

7. Finite forcing; forcing of infinite sentences.

In Paul Cohen's original method, the forcing objects or *conditions* are finite sets of basic sentences (atomic sentences or their negations) of Set Theory. An analogous approach may be adopted for general Model Theory [1, 3]. This leads to a concept of finite forcing (or *fforcing*) and to corresponding finitely generic structures. The resulting theory is in some ways quite similar and in others radically different from the theory of (infinite) forcing described in the preceding sections. A major difference is that it is no longer true that every structure (in the class under consideration) can be embedded in a finitely generic structure. Nevertheless, we can still define a fforcing operator $K \to K^f$ such that if K possesses a model companion K^* then K^f is its deductive closure and, hence, is itself a model companion of K. The situation can also be looked at from the point of view of Boolean valued Logic.

In another direction, a forcing theory in which the forced sentences are elements of an infinitary language, has been developed by Carol W. Coven (unpublished).

8. Examples and applications.

(*i*) Suppose K is a set of axioms for commutative field theory. Then K^F is the theory of algebraically closed fields (" the " model completion of K) and so is K^f. The class G_Σ coincides with E_Σ and is the class of all algebraically closed fields. All fields are contained in P_Σ and so are all integral domains. A_Σ consists of all fields that are of infinite degree of transcendence over their prime fields (universal domains).

(*ii*) Let K be a set of axioms for the theory of groups. In this case E_Σ is the class of so called *algebraically closed* (or, *existentially closed*, see ref. 2) groups and A_Σ is a subclass of E_Σ all of whose elements are elementarily equivalent (in the language of group theory). Using forcing, A. Macintyre showed recently that the elements of E_Σ are not all elementarily equivalent. It is known [2] that K does not possess a model companion. This implies that neither E_Σ nor G_Σ are arithmetical classes (varieties).

(*iii*) Let K be the set of all sentences formulated in terms of equality, addition, and multiplication, and true for the system of natural numbers. Then K is complete and, hence, possesses the joint embedding property. It follows that K^F also is complete, although it can be proved that $K^F \neq K$ (This contrasts with $K^f = K$ for the fforcing operator in this case). Hence $N \notin G_\Sigma$, although $N \in E_\Sigma$. It can be shown that K does not possess a model companion, so K^F cannot be model-complete. It can also be shown that K^F is not recursively enumerable. However, it contains many theorems of elementary Arithmetic. Thus, K^F and the associated classes G_Σ and A_Σ are appealing, if somewhat enigmatic, mathematical objects.

REFERENCES

[1] J. Barwise and A. Robinson. — Completing theories by forcing, *Annals of Mathematical Logic*, vol. 2 (1970), pp. 119-142.

[2] P. Eklof and G. Sabbagh. — Model-completions and modules, Yale University, February 1970 (mimeographed), to be published in the *Annals of Mathematical Logic*.

[3] A. Robinson. — Forcing in model theory, Yale University, October 1969 (mimeographed), to be published in the *Proceeding of the Colloquium on Model Theory*, Rome, November 1969.

[4] —. — Infinite forcing in model theory, Yale University, July 1970 (mimeographed), to be published in the *Proceedings of the Second Scandinavian Symposium in Logic*, Oslo, June 1970.

Yale University
Department of Mathematics,
New Haven
Connecticut 06520
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 251 à 254.

RECURSION IN OBJECTS OF FINITE TYPE

by Gerald E. SACKS

My hope here in Nice is to draw attention to the work of S. C. Kleene [7] on recursion in objects of finite type. In pursuit of that hope I will touch lightly on some related developments in generalized recursion theory. My Nicene creed is: Kleene's notion of recursive object of finite type and Gödel's notion of constructible set are of similar, but not of the same, substance. An Athanasian might see them as the same after reading Shoenfield [20] on hierarchies, but the Arian view is more balanced in the light of Moschovakis [11, 12] on hyperprojective sets.

I owe much to R. Gandy, T. Grilliot, and P. Hinman, who patiently explained to me the concept of recursion in objects of finite type, and to G. Kreisel [8], who taught me that such things as " concepts " exist in the context of recursion theory.

An object of type 0 is a natural number. An *object of type* $n > 0$ is a total function whose arguments and values are of type $< n$. $U, V, \ldots$ denote objects of finite type. Kleene [7] introduced a transitive relation $U \leq V$ (to be read U is *recursive in* V). If U and V are objects of type 1, then $\leq$ coincides with Turing reducibility. For each finite type, 0 ambiguously denotes the function of that type which is everywhere equal to 0. If $U \leq 0$, then U is said to be recursive. If $U \leq V$ and $V \leq U$, then $U \equiv V$ (to be read U and V have the same *degree*). $X, Y, \ldots$ denote members of 2^ω called reals, and $F, G, H, \ldots$ denote total functions from the reals into the reals.

For each $n > 0$, $\underline{{}^nE}$ is the characteristic function of equality for objects of type $< n$. Thus ${}^2E(X, Y) = 0$ if $X = Y$, and $= 1$ otherwise. ${}^2E$ has the same degree as the Turing jump operator. A result of great internal beauty obtained by Kleene [7] is: the objects of type ≤ 2 recursive in ${}^2E$ are just the hyperarithmetic ones. $\underline{S_k U}$, the *k-section* of U, is the set of all objects of type k recursive in U. Kleene [7] asked: do there exist F's such that (1) S_1F consists of the arithmetic reals?, (2) S_1F consists of the Δ^1_2 reals? Recently Grilliot [5] answered (1) negatively by showing: if S_1F is closed under the Turing jump, then ${}^2E \leq F$. (2) is answered affirmatively below.

Platek [13] calls a transitive set A *admissible* if A is closed under finitary set operations and all instances of the Σ_1 reflection and Δ_0 comprehension axiom schemas are true in A. A function f from A into A is called A-recursive if the graph of f is a Σ_1 subset of A. For every F it is possible to construe S_1F as a countable transitive set $\underline{AS_1F}$ by exploiting the standard encoding of hereditarily countable sets by reals. An immediate consequence of Shoenfield [20], Hinman [6], and Grilliot [5] is: AS_1F is admissible if and only if ${}^2E \leq F$. It follows from Gandy's work [3] on selection operators that if ${}^2E \leq F$, then AS_1F satisfies the Σ_1 dependent choice axiom schema.

Theorem 1 [17]. — (*i*) and (*ii*) are equivalent.

(*i*) A is a countable admissible set that satisfies the Σ_1 dependent choice axiom schema, and every member of A is countable in A.

(*ii*) There exists an F of type 2 such that ${}^2E \leq F$ and $A = AS_1F$.

For each ordinal α let L_α be the set of all constructible sets of constructible order $<\alpha$. Kripke [10] and Platek [13] call α an *admissible ordinal* if L_α satisfies the Σ_1 replacement axiom schema. A function is α-recursive if its graph is a Σ_1 subset of L_α. A set is α-recursively enumerable if it is the range of an α-recursive function. If α is admissible, then by Gödel there is an α-recursive well-ordering of all the computations needed to compute all the α-recursive functions. It follows that a great deal of classical recursion theory can be generalized from ω to α. For example, it can be shown that the Friedberg-Muchnik solution of Post's problem holds for every admissible α. The recursive functions of ordinals were first defined by Takeuti [22]. One of his early results restated in current terms says that every cardinal is an admissible ordinal. His proof is an application of *Gödel's Skolem-Lowenheim principle for L:* Σ_1 subsystems of L are isomorphic to initial segments of L. Gödel's principle (with L replaced by L_α) is central to current work on admissible ordinals; it plays an unexpected part in the solution of Post's problem [19]. I say " unexpected " because the use of model-theoretic ideas in recursion theory was at one time a surprise to me. On the other hand Kreisel's approach [8, 9] to generalized recursion theory was based from the beginning on the model-theoretic notion of *implicit invariant definability.* Later Barwise showed by means of a compactness argument: if A is a countable admissible set, then the implicitly invariantly definable functions from A into A are equivalent to the A-recursive functions (The equivalence fails for most uncountable A's). I would like to recommend the joint paper [1] of Barwise, Gandy, and Moschovakis as a starting point for any one curious about the great variety of ideas now current in generalized recursion theory.

COROLLARY 2. — If α is a countable admissible ordinal, then there exists an F of type 2 such that $L_\alpha \cap 2^\omega = S_1F$, and such that for every G of type 2 and of lower degree than F, $L_\alpha \cap 2^\omega \neq S_1G$.

COROLLARY 3. — If $n > 0$, then there exists an F of type 2 such that the reals recursive in F are just the Δ_n^1 reals.

THEOREM 4. — If U is of type n and ${}^nE \leq U$, then $S_1U = S_1F$ for some F of type 2.

The above four results are proved with the aid of Gödel's Skolem-Lowenheim principle for L, Cohen's forcing method, and Grilliot's hierarchies based on objects of finite type [4]. The next theorem combines forcing with the Friedberg-Muchnik priority method. Platek [13] calls X F-recursive in Y if $X \# F, Y$. Two reals have the same *F-degree* if each is F-recursive in the other. Hinman calls a real *F-recursively enumerable* if it is the range of a partial function of type 1 recursive in F. A well-known result of Spector [21] can be extended to show: if ${}^2E \leq F$, then all non-F-recursive, F-recursively enumerable reals have the same F-degree. I say *X is Σ_1 in Y over $\overline{AS_1F}$* if X is a Σ_1 subset of $AS_1F(Y)$, where $AS_1F(Y)$ is the result of adjoining Y to $\overline{AS_1F}$ and closing under Δ_0 comprehension.

THEOREM 5. — If ${}^2E \leq F$, then there exist two F-recursively enumerable reals such that neither is Δ_1 in the other over AS_1F.

Kleene [7] showed that the ${}^2E$-recursively enumerable reals were just the Π_1^1 reals. Theorem 5 for $F = {}^2E$ was proved in [15].

The *superjump* is a fundamental object of type 3 introduced by Gandy [3]; it lifts F to F^1. Let $\{ e \}^F(X)$ denote the value (possibly undefined) of the e-th partial function of type 2 recursive in F for real argument X. The value of $F^1(e, X)$ is 0 if $\{ e \}^F(X)$ is defined and 1 otherwise. ${}^2E^1$ is the hyperjump and has the same degree as E_1, an object of type 2 associated with the Souslin operation and introduced by Tugué [23]. Gandy [3] showed: if $F \leq G$, then $F^1 \leq G^1$. Hinman has asked: is there a condition on G that implies the existence of an F such that $F^1 \equiv G$? Hinman's question was inspired by Friedberg's classic result [2]: if $JO \leq X$, then there exists a Y such that $JY \equiv X$, where 0 is the empty set and J is the Turing jump.

THEOREM 6 [18]. — Assume the continuum hypothesis. Then there exists an H such that $(G)(EF)[H \leq G \rightarrow F^1 \equiv G]$.

The F's of Theorems 1 through 5 are constructed in countably many steps, but the F of Theorem 6 is constructed in uncountably many steps. If the continuum hypothesis is dropped, then Theorem 6 can be approximated in the sense of Theorem 7. The continuum hypothesis is needed to make the approximations cohere with one another.

THEOREM 7. — If S_1G is closed under hyperjump, then there exists an F such that $S_1F^1 = S_1G$.

The next theorem is intended to suggest that the Tugué hierarchy for S_1E_1 is similar to the Shoenfield hierarchy for S_1F^1 whenever ${}^2E \leq F$; it was proved in [16] for the case of $F = {}^2E$.

THEOREM 8. — If ${}^2E \leq F$, then the F-degrees of S_1F^1 have a minimal, but no least, upper bound.

Most of the results of this paper have the following form: a structure B associated with some generalization of recursion theory is given; then an object U of type n is constructed such that the members of B coincide with the objects of type $< n$ that are recursive in U. Since Kleene's definition of relative recursiveness is inductive, it follows that B can be defined by an induction based on U. If enough results of the above form can be found, it may be possible (as Kreisel has suggested) to prove theorems about structures occurring in generalizations of recursion theory by thinking of them as having been built up by inductive definitions based on objects of finite (or higher) type. Among the means to that end would be various sharpenings of Theorem 4. The superjump ${}^3S$ is an object of type 3 of lower degree than ${}^3E$, but an application of Corollary 2 above to Platek [14] provides an F of type 2 such that $S_1{}^3S = S_1F$. So it seems likely that the hypothesis " ${}^nE \leq U$ " of Theorem 4 can be replaced by something of wider scope. Theorem 4 can be extended from 1-sections to k-sections as follows. For each n there is a V of type n such that for all U of type n: if $V \leq U$ and $k < n$, then $S_kU = S_kW$ for some W of type $k + 1$. It is possible that ${}^nE$ may suffice for V, but at the moment I need a V whose degree appears to be higher than ${}^nE$ save when $k = 1$ (Added in proof: if Gödel's axiom of constructibility holds, then $V = {}^nE$.)

BIBLIOGRAPHY

[1] J. Barwise, R. Gandy and Y. Moschovakis. — The next admissible set, *Jour. Symb. Log.*, to appear.
[2] R. Friedberg. — A cirterion for completeness of degrees of unsolvability, *Jour. Symb. Log.*, 22 (1957), pp. 159-160.
[3] R. Gandy. — *General recursive functionals of finite type and hierarchies of functions*, University of Clermont-Ferrand (1962).
[4] T. Grilliot. — Hierarchies based on objects of finite type, *Jour. Symb. Log.*, 34 (1969), pp. 177-182.
[5] —. — On effectively discontinuous type 2 objects, *Jour. Symb. Log.*, to appear.
[6] P. Hinman. — Ad astra per aspera: hierarchy schemata in recursive function theory, Ph. D. Thesis, Berkeley (1966).
[7] S. C. Kleene. — Recursive functionals and quantifiers of finite type, *Trans. Amer. Math. Soc.*, 91 (1959), pp. 1-52; 108 (1963), pp. 106-142.
[8] G. Kreisel. — Model theoretic invariants: applications to recursive and hyperarithmetic operations, *The Theory of Models*, North Holland (1965), pp. 190-205.
[9] — and G. E. Sacks. — Metarecursive sets, *Jour. Symb. Log.*, 30 (1965), pp. 318-338.
[10] S. Kriple. — Transfinite recursions on admissible ordinals, *Jour. Symb. Log. (Abstracts)*, 29 (1964), pp. 161-162.
[11] Y. Moschovakis. — Hyperanalytic predicates, *Trans. Amer. Math. Soc.*, 129 (1967), pp. 249-282.
[12] —. — Abstract first order computability, *Trans. Amer. Math. Soc.*, 138 (1969), pp. 427-504.
[13] R. Platek. — Foundations of recursion theory, Ph. D. Thesis, Stanford (1966).
[14] —. — A countable hierarchy for the superjump, *Proceedings of the* 1969 *Manchester conference*, to appear.
[15] G. E. Sacks. — On the reducibility of Π_1^1 sets, *Advances in Math.*, to appear.
[16] —. — Countable admissible ordinals and hyperdegrees, to appear.
[17] —. — The 1-section of a type n object, to appear.
[18] —. — Inverting the superjump, to appear.
[19] —. — and S. Simpson. — The α-finite injury method, to appear.
[20] J. Shoenfield. — A hierarchy based on a type 2 object, *Trans. Amer. Math. Soc.*, 134 (1968), pp. 103-108.
[21] C. Spector. — Recursive well-orderings, *Jour. Symb. Log.*, 20 (1955), pp. 151-163.
[22] G. Takeuti. — On the recursive functions of ordinals, *Jour. Math. Soc. Japan*, 12 (1960), pp. 119-128.
[23] T. Tugué. — Predicates recursive in a type 2 object and Kleene hierarchies, *Comment. Math. Univ. St. Paul* (Tokyo), 8 (1960), pp. 97-117.

P-P69
Department of Mathematics,
MIT
Cambridge, Mass 02139
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 255 à 260.

THE THEORY OF SEMISETS

by Petr VOPĚNKA

The theory of semisets has arisen by exploring the consistency results of K. Gödel and P. Cohen. In the theory of semisets, the usually studied universum of the set theory is enlarged by adding new objects called semisets.

The theory of sets is a particular case of the theory of semisets. Adding suitable suplementary axioms to the axioms of the theory of semisets we can obtain other particular cases differing considerably from the theory of sets. Many of them, however, have the property that the formulas concerning only sets which are provable in them are provable also in the theory of sets and *vice versa.*

The theory of semisets and the theory of sets are mutually relatively consistent.

The theory of semisets can be used for proving consistency of many statements with the axioms of the set theory. All relative consistency proofs are done exclusively by interpreting theories in other theories and the existence of a countable model is not assumed.

The theory of semisets will be described in detail in the monography $[V+H]$.

In the present lecture, we will often prefer brief formulations to full generality.

1.1. By the theory of sets TS we understand the axiomatic Gödel-Bernays theory $[G]$ with the axiom groups A, B, C and the weak axiom of regularity

$$(D') \qquad \mathscr{M}(\mathscr{U}r) \ \& \ (\forall x \neq 0)(\exists y \in x)[y \cap x \subseteq \mathscr{U}r]$$

where

$$\mathscr{U}r = \{ x; x = \{ x \} \}$$

(Note that according to Gödel we use the lower case Roman letters as variables for sets).

1.2. A class M is said to be a model class, $\mathscr{M}cl(M)$, if we have simultaneously

$$(1) \qquad \mathrm{Comp}(M) \qquad (\text{i. e. } (\forall x \in M)[x \subseteq M])$$

$$(2) \qquad (\forall x, y \in M)[\mathscr{F}_i(x, y) \in M] \qquad i = 1, \ldots, 8$$

where $\mathscr{F}_1, \ldots, \mathscr{F}_8$ are the Gödel operations

$$(3) \qquad (\forall x \subseteq M)(\exists y \in M)[x \subseteq y]$$

1.3. We have $\mathscr{M}cl(V)$, $\mathscr{M}cl(L)$, where V is the universal class and L is the class of all constructible sets in the sense of Gödel.

1.4. Let M be a class variable. In an arbitrary formula of TS, interpret the fundamental notions of TS as follows:

$$\mathscr{M}^M(X) \equiv X \in M$$
$$Cls^M(X) \equiv X \subseteq M \;\&\; (\forall y \in M)[X \cap y \in M]$$
$$X \in^M Y \equiv \mathscr{M}^M(X) \;\&\; Cls^M(Y) \;\&\; X \in Y$$

Then, in TS, the interpretations of all the axioms of TS are provable from the assumption $\mathscr{M}cl(M)$.

This interpretation is called the model determined by M.

1.5. $Cstr(x)$ designates the least model class containing x. It is easy to prove that such a class exists.

Let us remark that $L = Cstr(0)$.

1.6. We denote by AC the axiom of choice for sets, i. e. for instance the statement " every set can be well-ordered ".

1.7. Balcar-Vopěnka. Let $\mathscr{M}cl(M)$, $\mathscr{M}cl(M_1)$, $\mathscr{M}cl(M_2)$ and suppose $M \subseteq M_1$, $M \subseteq M_2, M \cap \mathscr{U}r = M_1 \cap \mathscr{U}r = M_2 \cap \mathscr{U}r, \mathscr{P}(M) \cap M_1 = \mathscr{P}(M) \cap M_2$. If AC holds in the model determined by M_1 then $M_1 = M_2$.

The statement 1.7 indicates that it may be useful to investigate axiomatically the situation in the first power of an arbitrary model class. The required axiomatics is given by the theory of semisets.

2.1. The theory of semisets is obtained from TS by leaving off the axioms $C2$, $C3$ and $C4$ and adding the axioms

$$C2' \quad (\forall R)[[(\forall x, y)[x, y \in \mathscr{D}(R) \;\&\; x \neq y \rightarrow R''\{x\} \neq R''\{y\}] \;\&\; (\forall x)(\exists z)[R''\{x\} \subseteq z] \rightarrow [(\exists a)[\mathscr{D}(R) \subseteq a] \equiv (\exists b)[\mathscr{W}(R) \subseteq b]]]$$

$$Bi' \qquad (\forall x, y) \quad \mathscr{M}(\mathscr{F}_i(x, y)), \qquad i = 2,\ldots, 8$$

where $\mathscr{F}_2, \ldots, \mathscr{F}_8$ are the Gödel operations.

Remark. — The Gödel axioms $C2$, $C3$ are provable in TSS. Further, it is possible to show that, for every restricted set formula, the comprehension axiom is provable in TSS.

2.2. In TSS, a subclass of a set need not be a set. Thus, we define semisets by

$$Sm(X) \equiv (\exists a)[X \subseteq a]$$

2.3. TS is equivalent to the theory $TSS + (\forall x)[Sm(X) \rightarrow \mathscr{M}(X)]$.

2.4. We define real classes by

$$\text{Real}(X) \equiv (\forall y) \;\; \mathscr{M}(y \cap X)$$

It is easy to see that every set is a real class.

2.5. In an arbitrary formula of TS interpret the fundamental notions as follows:

$$\mathcal{M}^*(X) \equiv \mathcal{M}(X)$$
$$Cls^*(X) \equiv \mathrm{Real}(X)$$
$$X \in^* Y \equiv \mathcal{M}^*(X) \;\&\; Cls^*(Y) \;\&\; X \in Y$$

Then, in TSS, the interpretations of all the axioms of TS are provable. This interpretation is called the real model.

COROLLARY. — Con $(TS) \Leftrightarrow$ Con (TSS).

3.1. A semiset X is said to be dependent on Z if it is a set image of Z:

$$\mathrm{Dep}(X, Z) \equiv (\exists r)[X = r''Z]$$

3.2. A class Z is said to be a support (Supp (Z)) if

$$Z \neq 0 \;\&\; (\forall X, Y)[\mathrm{Dep}(X, Z) \;\&\; \mathrm{Dep}(Y, Z) \rightarrow \mathrm{Dep}(X - Y, Z)]$$

A class Z is called a total support (T Supp (Z)) if

$$(\forall X)[Sm(X) \rightarrow \mathrm{Dep}(XZ)]$$

3.3. Let Z be a class variable. In an arbitrary formula of TSS interpret the fundamental notions of TSS as follows

$$\mathcal{M}_Z(X) \equiv \mathcal{M}(X)$$
$$Cls_Z(X) \equiv (\forall y)[\mathrm{Dep}(X \cap y, Z)]$$
$$X \in_Z Y \equiv \mathcal{M}_Z(X) \;\&\; Cls_Z(Y) \;\&\; X \in Y$$

Then, in TSS, the interpretations of all the axioms of TSS are provable from the assumption Supp (Z).

This interpretation is called the support model determined by Z. Obviously, in this model, Z is a total support.

3.4. Let B be a real set-complete Boolean algebra (possibly a proper class). An ultrafilter Z on B is said to be set-complete, if $(\forall x \subseteq Z)[\Lambda x \in Z]$

Denote the formula " B is a real set-complete Boolean algebra, Z is a set-complete ultrafilter on B " by $\mathscr{V}(B, Z)$.

3.5. Let $\mathscr{V}(b, Z)$. If b is atomless then Z is a semiset which is not a set.

3.6. $$\mathscr{V}(B, Z) \rightarrow \mathrm{Supp}(Z)$$

3.7. Balcar. Let Supp (Z_1), $Sm(Z_1)$. Then there exist b and Z such that $\mathscr{V}(b, Z)$ and that

$$(\forall X)[\mathrm{Dep}(X, Z_1) \equiv \mathrm{Dep}(X, Z)]$$

3.8. In the following, $\varphi(x)$ is a set formula with one free variable, such that in TS the statement

$$(\forall x)[\varphi(x) \rightarrow x \text{ is a complete Boolean algebra})$$

is provable.

3.9. *Metatheorem on consistency.*

$$\mathrm{Con}\,(TS + AC + (\exists b)\varphi(b)) \Leftrightarrow \mathrm{Con}\,(TSS + AC + (\exists b, Z)[\varphi(b) \;\&\; \mathscr{V}(b, Z)])$$

4.1. Let M, P be class variables. In an arbitrary formula of TSS interpret the fundamental notions of TSS as follows:

$$\begin{aligned} &\mathscr{M}^{MP}(X) \equiv \mathscr{M}^{M}(X) \\ &Cls^{MP}(X) \equiv X \subseteq M \;\&\; Cls^{P}(X) \\ &X \in^{MP} Y \equiv \mathscr{M}^{MP}(X) \;\&\; Cls^{MP}(Y) \;\&\; X \in Y \end{aligned}$$

Then, in TS, the interpretations of all the axioms of TSS are provable from the assumptions $\mathscr{M}cl(M)$, $\mathscr{M}cl(P)$, $M \subseteq P$, $M \cap \mathscr{U}r = P \cap \mathscr{U}r$. This interpretation is called the model determined by M, P.

4.2. If, moreover, the class form of the axiom of choice holds in the model determined by P then the axiom

$$(\exists B)(\exists Z)[\mathscr{V}(B, Z) \;\&\; T\;\mathrm{Supp}\,(Z)]$$

holds in the model determined by M, P.

This statement indicates that the theory of semisets TSS satisfies the demands which have given the impulses to introduce it.

4.3. *Metatheorem on extending the theory of semisets to the theory of sets.*

Let T be the theory

$$TSS + (\exists b, Z)[\mathscr{V}(b, Z) \;\&\; \varphi(b) \;\&\; T\;\mathrm{Supp}\,(Z)]$$

Then $\mathrm{Con}\,(T) \Leftrightarrow \mathrm{Con}\,(TS + (\exists M)[\mathscr{M}cl(M) \;\&\; T^{MV}])$.

This metatheorem enables us to consider, under mentioned assumptions, the semisets as sets in a larger universe. By means of this metatheorem, we can establish the consistency proofs obtained by the Cohen's method for the theory of sets with the axiom of choice as well as for the theory with the negation of the axiom of choice. The point is always in transfering the problem into a problem concerning set Boolean algebras.

My student J. Mlček has found conditions under which in the previous theorem the set Boolean algebras may be replaced by algebras which are proper classes.

The theory of semisets TSS, if necessary with additional axioms, has also other applications than proving consistency of various statements with the theory of sets.

5. *Metatheorem on equiprovability.*

Let ψ be a closed formula concerning sets only. Then ψ is provable in

$$TS + AC + (\exists b)\varphi(b)$$

if and only if it is provable in

$$TSS + AC + (\exists b, Z)[\mathscr{V}(b, Z) \;\&\; \varphi(b) \;\&\; T\;\mathrm{Supp}\,(Z)]$$

By this metatheorem it follows that it is possible to prove statements on sets using the assumption of the existence of a set-complete ultrafilter on various complete Boolean algebras. This is analogous to proving statements on real numbers by means of complex numbers.

Let us introduce some results obtained using this metatheorem.

6.1. We say that a relation $\sim$ is a similarity relation, if

(1) $\langle x_1, \ldots, x_n \rangle \sim \langle x_1, \ldots, x_n \rangle$

(2) $\langle x_1, \ldots, x_n \rangle \sim \langle y_1, \ldots, y_m \rangle \rightarrow n = m$

(3) $\langle x_1, \ldots, x_n \rangle \sim \langle y_1, \ldots, y_n \rangle \rightarrow [(x_i \in x_j \equiv y_i \in y_j) \; \& \; (x_i = x_j \equiv y_i = y_j)]$

We say that sets a and b are locally similar $a \overset{\text{loc}}{\sim} b$ if the following holds:

If $x_1, \ldots, x_n \in a$, $y_1, \ldots, y_n \in b$, $\langle x_1, \ldots, x_n \rangle \sim \langle y_1, \ldots, y_n \rangle$ then

(1) $(\forall x_{n+1} \in a)(\exists y_{n+1} \in b)[\langle x_1, \ldots, x_{n+1} \rangle \sim \langle y_1, \ldots, y_{n+1} \rangle]$

(2) $(\forall y_{n+1} \in b)(\exists x_{n+1} \in a)[\langle x_1, \ldots, x_{n+1} \rangle \sim \langle y_1, \ldots, y_{n+1} \rangle]$

6.3. Let ψ be an arbitrary closed formula of TS. Then in the theory $TS + AC$ the following is provable:

If Comp(a), Comp(b), $a \overset{\text{loc}}{\sim} b$ then $\psi^{Cstr(a)} \equiv \psi^{Cstr(b)}$.

6.4. (In $TS + AC$). Let Comp(a), $a \overset{\text{loc}}{\sim} a$ and suppose

$$(\forall x_1, \ldots, x_n \in a)(\forall y_1, \ldots, y_n \in a)[\langle x_1, \ldots, x_n \rangle \sim \langle y_1, \ldots, y_n \rangle \\ \rightarrow (\exists x_{n+1} \in a)(\exists y_{n+1} \in a)[x_{n+1} \neq y_{n+1} \; \& \; \langle x_1, \ldots, x_{n+1} \rangle \sim \langle y_1, \ldots, y_{n+1} \rangle]]$$

Then AC does not hold in the model determined by $Cstr(a)$.

This theorem gives a new method of constructing models (interpretations) of the set theory without AC. If, e. g., a is an atomless Boolean algebra without non-identical automorphism, represented by subsets of $\mathscr{U}r$, then AC does not hold in $Cstr(a)$. On the other hand, every model of the Fraenkel-Mostowski type containing a contains all sets.

7.1. (In $TS + AC$). Let s be an uncountable set of a regular cardinality. Denote by $b(s)$ the Boolean algebra of all subsets of s modulo subsets of smaller cardinality. Let $\alpha(s)$ be the Stone space of $b(s)$. Obviously, $\alpha(s)$ is a compact totally disconnected Hausdorff space.

7.2. (In $TS + V = L$). The Boolean algebra of regular open subsets of $\alpha(s)$ (which is the completion of $b(s)$) is isomorphic to the algebra of regular open subsets of a metric space.

7.3. (In $TS + V = L$). The space $\alpha(s)$ is a union of a monotone system of $\aleph_1$ nowhere-dense subsets $\{ F_\alpha, \alpha \in \omega_1 \}$ (In fact, any regular $\aleph_p$ with $\aleph_0 < \aleph_p \leq |s|^+$).

These theorems may be reformulated as follows:

7.2′ (In $TS + V = L$). There exists a system $\{ P_n, n \in \omega_0 \}$ such that (1) for every n, $P_n \subseteq \mathscr{P}(s)$; (2) for every $x \in P_n$, $|x| = |s|$; (3) for distinct $x, y \in P_n$ is $|x \cap y| < |s|$; (4) whenever $y \subseteq s$ and $|y| = |s|$, there is an $n \in \omega_0$ and $x \in P_n$ with $|x - y| < s|$.

7.3′. A filter F on s is uniform if all its members have the cardinality of s. A filter F on s is nowhere-dense if

$$(\forall x)[x \subseteq s \ \& \ |x| = |s| \rightarrow (\exists y \in F)(|x - y| = |s|)]$$

In $TS + V = L$ the following theorem holds:

For every regular $\aleph_p, \aleph_0 < \aleph_p \leq |s|^+$ there exists a monotone system $\{ F_\alpha, a \in \omega_p \}$ of uniform nowhere-dense filters such that every uniform ultrafilter is an extension of some of them.

REFERENCES

[C] P. J. COHEN. — The independence of the continuum hypothesis I, *Proc. Nat. Acad. Sci.* (U. S. A.), 50 (1963), pp. 1143-1148 ; II, *Proc. Nat. Acad. Sci.* (U. S. A.), 51 (1964), pp. 105-110.

[G] K. GÖDEL. — *The consistency of the axiom of choice, etc.* Princeton University Press (1940).

[V+B] P. VOPĚNKA and B. BALCAR. — On complete models of the set theory, *Bull. Acad. Polon. Sci.*, 15 (1967), pp. 839-841.

[V+H] — and P. HÁJEK. — *The theory of semisets*, North Holland Publ. Comp. and Academia Prague (to appear).

[S+V] P. ŠTĚPA'NEK and P. VOPĚNKA. — Decomposition of metric spaces into nowhere dense sets, *Commentationes Mathematicae Universitatis Carolinae*, 8, 3 (1967).

Universita Karlova
Sokolovska 83
Praha-Karlin
(Tchécoslovaquie)

B

ALGÈBRE

Actes, Congrès intern. math., 1970. Tome 1, p. 263 à 267.

B_1 - ALGÈBRE GÉNÉRALE

IDENTITÉS DANS LES GROUPES

par S. I. ADJAN

§ 1. Problème de Burnside.

En 1902, Burnside [1] a formulé le problème suivant :

« Tout groupe avec un nombre fini de générateurs et dans lequel est vérifiée la relation identique :

$$x^n = 1 \tag{1}$$

serait-il fini ? »

Depuis cette date, ce problème a attiré l'attention de nombreux algébristes du monde entier. Ces groupes ont été nommés groupes burnsidiens d'exposant n. La réponse affirmative au problème de Burnside a été donnée pour $n = 3$ par Burnside lui-même [1], pour $n = 4$ par I. N. Sanov en 1940 [2] et pour $n = 6$ par Marshall Hall en 1957 [3]. Des modifications intéressantes du problème de Burnside ont été proposées pour les groupes, ainsi que pour d'autres systèmes algébriques. Des résultats intéressants obtenus sur ces voies ont été exposés au cours des congrès mathématiques précédents par A. I. Kostrikin à Stockholm [4] et E. S. Golod à Moscou [5]. Dans le présent exposé seront donnés des résultats se rapportant au problème de Burnside lui-même, ainsi que d'autres résultats concernant les groupes avec des relations identiques du type (1). Tous ces résultats ont comme trait commun l'unité de leur méthode de démonstration.

En 1959, P. S. Novikov [6] a annoncé que pour tout $n \geqslant 72$, le groupe libre burnsidien d'exposant n et ayant m (> 1) générateurs est infini. Il a indiqué, en même temps, l'idée de la démonstration de ce résultat. Toutefois, les tentatives de donner corps à cette idée se sont heurtées à une série de difficultés. Ces difficultés ont été progressivement surmontées dans le travail effectué en commun par P. S. Novikov et l'auteur durant la période de 1960 à 1967. Le résultat de ce travail a été la solution du problème de Burnside pour des exposants impairs suffisamment grands, solution qui a été publiée en 1968 [7]. Il a fallu renoncer au cas des exposants pairs et élever considérablement la borne pour l'exposant n, mais, en revanche, il n'a plus été nécessaire d'utiliser la méthode de V. A. Tartakovsky [8].

Dans l'article [7] on construit, pour chaque $m > 1$ et tout nombre impair $n \geqslant 4381$, un groupe périodique $\Gamma(m, n)$ avec m générateurs et la relation identique (1). Pour construire ce groupe, on introduit une certaine classification de mots périodiques constitués par des signes pris dans l'alphabet du groupe :

$$a_1, a_2, \ldots, a_m, a_1^{-1}, a_2^{-1}, \ldots, a_m^{-1}, \tag{2}$$

et on construit une théorie des transformations de mots, correspondant à l'identité (1) pour n impair.

Récemment, on a réussi à simplifier considérablement cette théorie et à abaisser la borne pour n jusqu'à 697. En outre, tous les autres résultats obtenus, en partant de cette théorie, pour les groupes burnsidiens libres, dans les travaux [9] et [10] — qui seront traités au § 2 — sont valables pour les exposants impairs $n \geqslant 697$.

La théorie des transformations de mots, élaborée dans [7], contient un grand nombre de notions interdépendantes qui se définissent par induction simultanée suivant le paramètre naturel α, ainsi que de nombreuses propriétés de ces notions, qui se démontrent aussi par induction simultanée suivant α. N'ayant pas la possibilité de donner, dans ce court exposé, une définition exacte même des notions principales de [7], nous nous bornons à indiquer quelques particularités de cette théorie qui ont une formulation suffisamment simple.

Supposons choisi un entier impair $n \geqslant 697$. Considérons les mots réduits en l'alphabet (2). Nous désignons par $\partial(x)$ la longueur d'un mot X et par $X \doteq Y$ l'égalité graphique des mots X et Y. Par induction simultanée suivant le paramètre naturel α, on définit les principales notions suivantes de la théorie considérée dans [7] :

1) Classe des mots Π_α. Dans le cas de $\alpha = 0$, c'est l'ensemble de tous les mots réduits.

2) Noyau de rang α d'un mot X ($X \in \Pi_\alpha$). Si $\alpha = 0$, c'est une occurrence quelconque d'une lettre dans le mot X. Si $\alpha > 0$, tout noyau de rang α de $X \in \Pi_\alpha$ est une occurrence d'un mot élémentaire de rang α (voir 6) dans le mot X.

3) La relation $X \overset{\alpha}{\sim} Y$, qui est symétrique, réflexive et transitive, est définie pour les mots X, $Y \in \Pi_\alpha$ et elle s'appelle l'équivalence de rang α. Pour $\alpha = 0$, cette relation coïncide avec l'égalité graphique.

4) Si X, $Y \in \Pi_\alpha$ et si, pour certains X_1 et Y_1 (X_1, $Y_1 \in \Pi_\alpha$), sont vérifiées les relations $X \overset{\alpha}{\sim} X_1$, $Y \overset{\alpha}{\sim} Y_1$, $X_1 \doteq X_2 T$, $y_1 \doteq T^{-1} Y_2$ et $X_2 Y_2 \in \Pi_\alpha$, alors nous écrivons $X_2 Y_2 = [X, Y]_\alpha$. L'opération $Z = [X, Y]_\alpha$ est définie pour tous X, $Y \in \Pi_\alpha$. Elle est univoque à l'équivalence de rang α près, et associative.

5) La fonction $W = f_\alpha(V, Y)$, pour tout couple de mots X, Y où $X \overset{\alpha}{\sim} Y$, donne une application bijective de l'ensemble de tous les noyaux V de rang α du mot X sur l'ensemble de tous les noyaux W de rang α du mot V. Si $W = f(V, Y)$, alors $V = f(W, X)$. Cette fonction conserve la disposition mutuelle des noyaux de rang α.

6) A la base de la classification des mots considérée se trouve la notion de mot élémentaire de rang $\alpha + 1$, qui représente une généralisation de la notion de mot périodique. En particulier, un mot périodique $A^t A_1$, avec la période minimale A, est appelé mot élémentaire de rang 1, si le mot A^3 ne contient aucune occurrence d'un mot $B^r B_1$, où $\partial(B^r B_1) > 8\partial(B)$. Le mot $X \doteq A^t A_1$ s'appelle mot périodique de rang $\alpha + 1$ si A_1 est un commencement du mot A, $\partial(X) \geqslant 18\partial(A)$, $X \in \Pi_\alpha$ et si l'on peut indiquer un noyau $V = P * E * Q$ de rang α du mot $A^t A_1$, tel que $\partial(P) \geqslant 8\partial(A)$ et $\partial(Q) \geqslant 8\partial(A)$. Ces noyaux V de rang α du mot X s'appellent des noyaux de base de X. On dit que deux noyaux de base V_1 et V_2 sont en correspondance de phase, si V_2 peut être obtenu par le déplacement de V_1 d'un nombre entier de périodes A. Si $Y \in \Pi_\alpha$ et $Y \overset{\alpha}{\sim} X$, où X est un mot périodique de rang $\alpha + 1$, alors Y s'appelle un mot entier de rang $\alpha + 1$. Généralement, les mots entiers du rang $\alpha + 1$ ne sont pas périodiques. Toutefois, si l'on utilise la fonction $f_\alpha(V, Y)$, on peut étendre à Y la correspondance de phase des noyaux de base de rang α qui a été définie pour X. De cette façon, on obtient pour les mots de rang $\alpha + 1$, ainsi que pour des mots « suffisamment longs » entrant dans les mots entiers (mots semi-entiers), certaines propriétés des mots périodiques de rang $\alpha + 1$. Ainsi apparaît la notion de nombre de parties d'un mot semi-entier de

rang $\alpha + 1$, qui représente un analogue du nombre des périodes d'un mot périodique. Les mots périodiques (entiers ou semi-entiers) de rang $\alpha + 1$ s'appellent mots élémentaires de rang $\alpha + 1$ s'ils ne contiennent pas de mots semi-entiers « suffisamment longs » (contenant un nombre suffisamment grand de parties) « d'autre nature ».

7) On appelle rotation simple de rang $\alpha + 1$ une transformation du type

$$PB^tB_1Q \to P(B^{-1})^{n-t-1}B_2^{-1}Q, \tag{3}$$

où B^tB_1 est un mot élémentaire de rang $\alpha + 1$ avec la période B, $B \equiv B_1B_2$, $PB^tB_1Q \in \Pi_\alpha$, $P(B^{-1})^{n-t-1}B_2^{-1}Q \in \Pi_\alpha$ et où chacun des mots B^tB_1 et $(B^{-1})^{n-t-1}B_2^{-1}$ contient un nombre suffisamment grand de parties $B(B^{-1})$. On appelle rotation de rang $\alpha + 1$ toute transformation $X \to Y$, où $X, Y \in \Pi_\alpha$ et pour une certaine rotation simple (3) $X \overset{\alpha}{\sim} PB^tB_1Q$, $Y \overset{\alpha}{\sim} P(B^{-1})^{n-t-1}B_2^{-1}Q$. Parmi les rotations de rang $\alpha + 1$, on distingue les rotations dites « réelles » de rang $\alpha + 1$.

Deux mots $X, Y \in \Pi_\alpha$ s'appellent équivalents de rang $\alpha + 1$ ($X \overset{\alpha+1}{\sim} Y$) si ou bien $X \overset{\alpha}{\sim} Y$, ou bien on peut indiquer une suite de rotations réelles du rang $\alpha + 1$ qui transforme X en Y.

On définit ensuite la notion de noyau de rang $\alpha + 1$, qui est toujours une occurrence d'un mot élémentaire contenant au minimum 9 parties. On désigne par $\Pi_{\alpha+1}$ l'ensemble des mots $X \in \Pi_\alpha$ dont chaque noyau contient au plus $n - 50$ parties.

Ainsi, d'après la définition des classes Π_α, nous avons

$$\Pi_0 \supset \Pi_1 \supset \Pi_2 \supset \ldots \Pi_i \supset \Pi_{i+1} \ldots$$

Soit $\mathscr{A} = \bigcap_{i=0}^{\infty} \Pi_i$. Nous appelons deux mots $X, Y \in \mathscr{A}$ équivalents ($X \sim Y$) si $X \overset{\alpha}{\sim} Y$, où $\alpha = \max(\partial(x), \partial(y))$. Soit $\mathscr{L}$ l'ensemble de toutes les classes d'équivalence de $\mathscr{A}$ défini par la relation $X \sim Y$. Sur l'ensemble $\mathscr{L}$, on définit l'opération

$$u \circ v = \{ [x, y]_\alpha \} \tag{4}$$

où $X \in u$, $Y \in v$, $\alpha = \max(\partial(x), \partial(y))$ et $\{ Z \}$ est la classe des mots équivalents au mot Z. On peut démontrer que l'ensemble $\mathscr{L}$ avec l'opération $u \circ v$ est un groupe. Ce groupe est précisément ce $\Gamma(m, n)$ que nous avons cherché. Il est engendré par les générateurs $\{ a_1 \}, \{ a_2 \}, \ldots, \{ a_m \}$.

§ 2. **Les groupes burnsidiens libres d'exposant impair.**

Soit $B(m, n)$ un groupe défini par des générateurs (2) et par l'identité générique (1), où n est un nombre impair $\geqslant 697$, et $m > 1$. Il est facile de démontrer que la correspondance

$$a_i \to \{ a_i \} \tag{5}$$

donne une application isomorphe du groupe $B(m, n)$ sur le groupe $\Gamma(m, n)$. En utilisant une telle représentation d'un groupe burnsidien libre $B(m, n)$, on peut étudier différentes propriétés de celui-ci.

Étant donné que toutes les classes de mots et les relations entre les mots définies dans [7] sont récursives, nous obtenons la solution du problème d'identité dans le groupe $B(m, n)$ [9]. Dans [9] il est également démontré que l'identité (1) est équivalente au système infini des relations de définition $A^n = 1$, où A^n parcourt l'ensemble de tous les mots élémentaires de rang α avec la période A, pour tous les $\alpha > 0$, mais cette identité ne peut être remplacée par aucun nombre fini de relations de définition.

A l'aide de la représentation (5) du groupe $B(m, n)$, il est démontré dans [10] que, si $AB = BC$ et $A \neq 1$ dans $B(m, n)$, on peut trouver un mot E tel que $E = B$ dans $B(m, n)$ et $\partial(E) \leqslant \pi_1(n, \partial(AC))$, où $\pi_1(n, j)$ est une fonction récursive, ce qui nous donne un algorithme pour la solution du problème de conjugaison dans les groupes $B(m, n)$. De là, résulte aussi que le normalisateur de tout élément (non neutre) du groupe $B(m, n)$ est fini.

Récemment, l'auteur a démontré une proposition plus forte. Si $AB = BA$ dans $B(m, n)$, on peut indiquer un C tel que pour certains t et r, $A = C^t$ et $B = C^r$ dans $B(m, n)$. De là découle que le normalisateur de tout élément (non neutre) du groupe $B(m, n)$ est un groupe cyclique d'ordre n. Le groupe $B(m, n)$ fournit donc un exemple d'un groupe infini non-abélien, où tout sous-groupe abélien est fini et cyclique.

Si l'on se limite à la considération des mots élémentaires dont la première et la dernière lettre sont a, on peut, en modifiant en conséquence la théorie des transformations de mots exposée dans [7], démontrer que les mots bab^{-1}, b^2ab^{-2} et b^4ab^{-4} engendrent, dans $B(2, n)$, un sous-groupe isomorphe au groupe $B(3, n)$. Ceci est une solution négative du problème 17 de l'article [12]. On en déduit facilement que le groupe $B(m, n)$ ne vérifie pas la condition minimale pour les sous-groupes.

On peut aussi démontrer que pour $m \geqslant n - 1$, les conditions minimale et maximale relatives aux sous-groupes normaux ne sont pas vérifiées dans le groupe $B(m, n)$. Pour cela, il faut étendre la théorie exposée en [7] à une classe de transformations plus large que les transformations (3). Pour n impair composé, $n = kl$, où $k \geqslant 697$ et $l > 1$, cette proposition est facile à démontrer pour $m > 1$. Toutefois, pour n et $m < n - 1$ premiers, la question reste ouverte. Il paraît vraisemblable que tout sous-groupe de $B(m, p)$ pour les nombres premiers $p > 697$, engendré par k générateurs ($k \leqslant 2$), est isomorphe à $B(1, p)$ ou à $B(2, p)$, et pour $k \geqslant p - 1$ il peut n'être isomorphe à aucun groupe $B(l, p)$.

§ 3. Systèmes irréductibles infinis d'identités dans les groupes.

Un système d'identités dans les groupes s'appelle irréductible si aucune de ces relations ne peut être déduite des autres relations.

Dans [14], il est démontré que pour $n = 4381$, l'ensemble de toutes les relations

$$(x^{rn}y^{rn}x^{-rn}y^{-rn})^n = 1 \tag{6}$$

où r parcourt tous les nombres premiers, est irréductible. Ceci se démontre en construisant, dans [14], pour chaque ensemble P de nombres premiers, un groupe $\Gamma(2, P)$ avec 2 générateurs, dans lequel l'identité (6) se vérifie si et seulement si $r \in P$. Pour cela, on définit la notion de mot « marqué » élémentaire de rang α, qui dépend de l'ensemble P, et on admet les rotations (3) uniquement pour les mots élémentaires « marqués » B^tB_1. Ensuite, en partant de la théorie des transformations de mots obtenue, on construit le groupe cherché $\Gamma(2, P)$, par une construction analogue à celle du groupe $\Gamma(2, n)$ dans [7].

Si une certaine identité se déduit du système d'identités (6), on ne peut utiliser, dans sa déduction, qu'un nombre fini d'identités de ce système. C'est pourquoi chaque sous-ensemble infini du système d'identités (6) n'est équivalent à aucun système fini. Ceci constitue une solution effective du problème connu de la base finie pour une variété de groupes ([12], p. 39). Une solution non effective de ce problème a été trouvée récemment, mais avant l'auteur, par A. Yu. Olchansky [15]. Il a démontré que l'ensemble des variétés de groupes résolubles de classe 5, qui ont l'exposant $8pq$, où p et q sont des nombres impairs arbitraires premiers entre eux, a la puissance du continu. Étant donné que l'ensemble de tous les systèmes finis d'identités de groupes est dénombrable, il s'ensuit qu'il existe des variétés de groupes de cette classe, qui ne sont pas définies par un système fini d'identités. D'autre part, de l'irréductibilité du système (6) découle l'existence d'un ensemble continu de différentes variétés de groupes correspondant aux sous-ensembles du système d'identités (6).

Soit S un ensemble énumérable et indécidable de nombres premiers. Par $\Gamma(S)$, nous désignons le groupe défini par 2 générateurs et par toutes les identités (6) pour $r \in S$ et $n = 4381$. Il est évident que toute relation du groupe $\Gamma(S)$ est une identité. Du fait que le système (6) est irréductible découle qu'une des relations (6) est vérifiée si et seulement si $r \in S$. Étant donné l'indécidabilité de l'ensemble S, on en déduit que dans $\Gamma(S)$ le problème d'identité est indécidable. Il est à noter que cela donne le premier exemple d'un groupe pour lequel le problème d'identité est indécidable et qui soit défini par des identités. Il serait sans doute intéressant de savoir s'il existe de tels exemples de groupes, définis par des ensembles d'identités finis ou, tout au moins, décidables.

BIBLIOGRAPHIE

[1] W. BURNSIDE. — *Quart. J. of Pure and Appl. Math.*, 33 (1902), pp. 230-238.

[2] И. Н. САНОВ. — Ученые записки Ленингр. ун-та, сер. матем., 10 (1940), pp. 166-170.

[3] M. HALL. Jr. — *Proc. Nat. Acad. Sci. USA*, 43 (1957) pp. 751-753.

[4] А. И. КОСТРИКИН — *Proc. Internat. Congress Math. Stockholm* (1962).

[5] Е. С. ГОЛОД. — *Proc. internat. Congress Math. Moscow* (1966). Изд-во « Мир ». Москва (1968).

[6] П. С. НОВИКОВ. — Доклады АН СССР, 127 (1959), pp. 749-752.

[7] —, С. И. АДЯН. — Известия АН СССР, сер. матем., 32, №s 1, 2, 3 (1968).

[8] В. А. ТАРТАКОВСКИЙ. — Изв. АН СССР, сер. матем., 13, № 6 (1949).

[9] П. С. НОВИКОВ, С. И. АДЯН. — Известия АН СССР, сер. матем., 32, № 4 (1968).

[10] —, —. — Известия АН СССР, сер. матем., 32, № 5 (1968).

[11] С. Е. АРШОН. — Матем. сборн., 2 (44), № 4 (1937).

[12] H. NEUMANN. — *Varieties of Groups* (1967), Springer-Verlag.

[13] С. И. АДЯН — Доклады АН СССР, 190, № 3 (1970).

[14] —. — Известия АН СССР, сер. матем., 34, № 4 (1970).

[15] А. Ю. ОЛЬШАНСКИЙ. — Известия АН СССР, сер. матем., 34, № 2 (1970).

Steklov Mathematical Institute
Department of Mathematics,
Vavilova street 42,
Moscow V 333
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 269 à 272.

SOME RESULTS ON RINGS WITH POLYNOMIAL IDENTITIES

by S. A. AMITSUR

A complete survey of recent results in this area should at least cover the following topics: 1) Group rings with polynomial identities. 2) Identities in rings with involutions. 3) Prime rings with generalized $p.i.$ 4) Rings of polynomial and rational functions. 5) Tensor products. 6) Embedding in matrix rings. 7) Prime ideals and localizations, etc.

No attempt will be made to cover all topics, but some references will be given.

Let R be an algebra over a commutative ring Ω with a unit; R is said to satisfy a $p.i$ $p[x] = \Sigma\alpha_{(i)}x_{i_1} \dots x_{i_2} = 0$ if $p[r_1, \dots] = 0$ for all substitution $x_i = r_i \in R$, and for simplicity we assume that some coefficient of a monomial of highest degree $\alpha_{(i)} = 1$.

1. **Tensor products.**

An old problem was: Does the matrix ring $M_n(R)$ satisfy a $p.i$ if R satisfies, and more generally if R and S satisfy $p.i$, does $R \bigotimes_{\Omega} S$ satisfy a polynomial identity. The first part was solved rather simply in the affirmative by C. Procesi, L. Small [13] and consequently it follows that the endomorphism ring $\mathrm{Hom}_R(V, V)$ satisfies an identity if V is a finitely generated R-module and R satisfies a $p.i.$ The second problem remains open in the general form though one can reduce the problem to nil rings. Liron-Vafne [5] have shown that by defining equivalence of two ring: $A \equiv B$ if they satisfy the same identities, then if also $C \equiv D$ then $A \otimes C = B \otimes D$. This in particular shows the invariance of the identities under scalar extension in the known cases.

2. **Embedding in matrix rings** (over commutative ring).

For simplicity assume henceforth that $\Omega = F$ is an infinite field. One of the earlier results was that semi-prime rings with a $p.i$ of degree d can be embedded in $M_n(K)$ for some commutative ring K, $n \leq \frac{d}{2}$. An extension of this result that, a $p.i$ is necessary and sufficient for a ring K to be embedable in a matrix ring over a commutative ring, was shown not to be valid by (Drazin and P. M. Cohn) and the problem remained whether the condition is that the ring shall satisfy exactly the identities of $M_n(F)$. This also is now known to be wrong. The first example was given in [2] by Amitsur, and a second example given by Small [11] will appear soon. Small's examples shows that one can have a finitely generated algebra with a nilpotent Jacobson's radical with the same identities as $M_n(F)$ and which cannot be embedded in matrices of finite order over any commutative ring.

These examples raise the problem: what characterizes subrings of matrix rings. If we try to attack the problem of finding all commutative rings K for which we have an embedding $R \hookrightarrow M_n(K)$, one gets readily to the following simple observation: for fixed $n \geq 1$, for every ring R there exists a commutative ring $S = S(R\,; n)$ and a homomorphism $\rho : R \to M_n(S)$ such that for every homomorphism $\sigma : R \to M_n(K)$ for any commutative ring K, there exists a unique (!) homomorphism η: $S \to K$ such that the following diagram is commutative:

$$\begin{tikzcd} R \arrow[r, "\rho"] \arrow[dr, "\sigma"'] & M_n(S) \arrow[d, "M_n(\eta)"] \\ & M_n(K) \end{tikzcd}$$

The ring S is uniquely determined up to isomorphism and so is ρ. With the aid of the ring S one can show that if R is a finitely generated and $P_1 \subseteq P_2 \subseteq \ldots \subseteq P_r \subseteq \ldots$ is a sequence of ideals such that each R/P_i can be embedded in some $M_n(K_i)$, then the sequence must be finite, which is a form of a Hilbert basis theorem in the commutative case.

A non trivial property of $\rho : R \to M_n(S)$ is that $\rho(R)S = M_n(S)$ if and only if all irreducible representations of R are of dimension $\geq n$. In view of the properties of S, and the fact that ρ is mono for azumaya-algebras R —, it follows that, S is a generic splitting ring of R. Note, that even for the simple case $R = M_n(F)$, $S \neq F$(!).

This is the place to mention an interesting result of M. Artin [4], that an algebra R with a unit is an azumaya algebra if and only if R satisfies all identities of $M_n(F)$ and its irreducible representations are all of the same dimension n.

3. Prime ideals.

Rings with $p.i$ are a natural generalization of commutative rings, and one would expect to be able to extend our knowledge of the latter to rings with $p.i.$ This in fact was the leading thought in developing the theory of rings with $p.i.$ First steps in this direction have been done, like existence of rings of quotients, and the non commutative Hilbert Nullstellersats. A great push toward this goal has been given recently by a series of works of C. Procesi. The extensions to the non-commutative case are far from being trivial and usually hold in a restricted form.

Let K be commutative, $R = K[a_i, \ldots, a_m]$ be a finitely generated prime ring with a $p.i$ of degree $d = 2n$, then R satisfies the ascending (descending) chain condition on prime ideals if K does. R is a Jacobson ring (a Hilbert algebra) if K is such. If K has finite rank then R has also finite rank. If $K = F$ is a field and C is the center of the ring of quotients of R, then rank $R \leq$ tr. deg $C/F \leq (m-1)n^2 + 1$, and the maximum of tr. deg C/F is obtained for the ring of m generic matrices.

All these results, and more which were not mentioned are well known theorems for commutative domains (the case $d = 2n = 2$), which indicate that commutative theory can be pushed into rings with $p.i.$ But beware of the pitfalls, like the structure of the nil radicals of $p.i$ rings, and localization at primes. A prime ring R has a classical ring of quotient $Q(R)$, and if P is a prime ideal, then $Q_p = \{ a^{-1}b \mid a \text{ regular mod } P \}$ is a well defined subring of R only if R/P and R have the same identities (Small [12]). This reveals that only these prime ideals are " good " for the non-commutative case and those for which R/P has lower identities introduce distortion in the theory.

More examples to support our arguments that rings with $p.i$ are the next step after commutative rings can be found in the papers of C. Procesi. Special interest lies in the ring of generic matrices.

4. **The ring of generic matrices** is the algebra $F[X] = F[X_1, \ldots, X_m]$ generated by m generic matrices $X_i = (\xi^i_{\lambda\mu})$, $\lambda, \mu = 1, 2, \ldots, m$; with $\{ \xi^i_{\lambda\mu} \}$, mn^2 commutative indeterminates. This ring should be the replacement of the ring of commutative polynomials in m variables and in fact $F[X]$ is isomorphic with the ring of polynomial functions in m variables with values in $M_n(F)$, or in any central simple algebra of dimension n^2 over a center containing F for that matter. Some interesting properties of this ring proved by Procesi [8] are: $F[X]$ is a domain (Amitsur) with an Ore ring of quotient $F(X)$ which is central simple division algebra of dimension n^2 and which is isomorphic to the ring of all rational functions in m-variables over $M_n(F)$. The tr. deg. of its center C over F is $(m-1)n^2 + 1$ (obtained independently by Kyrilov). The field of all rational functions $F(\xi)$ is the $\{ \xi^i_{\lambda\mu} \}$ is a splitting field, and

$$F[X]F(\xi) = M_n(F(\xi));$$

furthermore the center C has an algebraic extension $C(u)$ which is a pure transcendental extension of F, and $C(u)$ is a normal extension of C and its Galois group in the full symmetric group on n-elements. Procesi gives also the cross product form of the class of $F(X)$. Again some properties of $F[X_1, \ldots, X_m]$ are extensions of the properties of the ring $F[t_1, \ldots, t_m]$ in m-commutative polynomials—but some do not ! Hilbert Hullstellersatz does hold, but $F[X]$ is not Noetherian, and even it does not satisfy chain conditions on two sided ideals, but it does satisfy chain conditions for ideals P such that $F[X]/P$ can be embedded in $M_n(K)$ for some commutative ring K.

REFERENCES

[1] S. A. Amitsur. — Identities in rings with involutions, *Israël Jour. Math.*, vol. 7 (1969), pp. 63-68.
[2] —. — A non commutative Hilbert basis theorem and subrings of matrices, *Trans. Amer. Math. Soc.*, vol. 149 (1970), pp. 133-142.
[3] —. — Embedding in matrix ring, *Pacific Journal* (to be published).
[4] M. Artin. — On Azumaya-algebras and finite dimensional representations, *Jour. of Alg.*, vol. 11 (1969), pp. 532-563.
[5] V. Liron and S. Vafne. — To be published in *Israël Journ.* (1970).
[6] W. Martindale. — III. Prime rings satisfying a generalized polynomial identity, *Journ. of Alg.*, vol. 12 (1969), pp. 576-586.
[7] D. S. Passman. — Linear identities in group rings (Preprint).
[8] C. Procesi. — Non-commutative affine rings, *Atti. Della. Accad. Naz. dei Lincei.*, vol. 8, ser. 8 (1967), pp. 239-255.

[9] —. — Non commutative Jacobson rings, *Annoli della Scuola Normale Superiore di Piza*, vol. 21 (1967), pp. 381-390.
[10] —. — Sulle identita delle algebre semplici, *Rendi de Cir. Mat. di Palermo*, vol. 17, ser. 2 (1968), pp. 13-17.
[11] L. W. SMALL. — An example in PI-rings (Preprint).
[12] —. — Local ring of quotients (Preprint).
[13] C. PROCESI and L. SMALL. — *Math. Zeit*, 106 (1968), pp. 178-180.

Department of Mathematics,
Hebrew University
Jerusalem (Israël)

Actes, Congrès intern. math., 1970. Tome 1, p. 273 à 278.

FREE IDEAL RINGS AND FREE PRODUCTS OF RINGS

by P. M. COHN

My aim in this talk is to describe a class of rings and give some reasons for considering this class. All rings will be associative, with a unit-element.

1. In any ring R, consider the relation

$$x.y = x_1y_1 + \ldots + x_ny_n = 0. \tag{1}$$

We say that (1) is *trivial* if for each $i = 1, \ldots, n$, $x_i = 0$ or $y_i = 0$. Every ring $\neq \{0\}$ has non-trivial relations, so we define: (1) is *trivializable* if there exists $A \in GL_n(R)$ such that $xA.A^{-1}y$ is trivial. It is easy to give examples of rings with non-trivializable relations (e. g. $2.x - x.2 = 0$ in $Z[x]$), but not every ring has them, so the following definition makes sense.

DEFINITION. — An *n-fir* is a ring in which every relation with at most n terms is trivializable.

Thus 1-firs are just integral domains (not necessarily commutative), 2-firs (formerly called " weak Bezout rings ") are integral domains R such that $aR + bR$ is principal whenever $aR \cap bR \neq 0$, and for higher n we get smaller classes, until we get to rings that are n-firs for all n, the *semifirs*. In the commutative case, 2-firs are already semifirs (the familiar Bezout rings) but in general all these classes are distinct [9]. A characterization of n-firs is given in

THEOREM 1. — *A ring R is an n-fir if and only if every right ideal on at most n generators is free as right R-module, of unique rank.*

In particular, a semifir is a ring in which every finitely generated right ideal is free, of unique rank. The same holds with " left " for " right ".

All this suggests that we look at a still smaller class: we define a *right fir* (= free ideal ring) as a ring in which every right ideal is free, of unique rank. This notion is no longer left-right symmetric [18, 8], so we must define left firs separately. By a *fir* we understand a left and right fir.

A commutative fir is just a principal ideal domain, and firs may be looked upon as a natural generalization. Of course every principal ideal domain, commutative or not, is a fir, but the class of firs is much wider than that: it includes all free algebras (on any free generating set) and group algebras of free groups, over any field [6, 7]. Other examples of firs will be given later.

2. Commutative principal ideal domains are unique factorization domains, and this notion has been extended to the non-commutative case, first for the ring of linear differential operators [15, 16] and later for any principal ideal domains [1]. The general definition is as follows. By an *atom* we mean a non-unit which is not a product of non-units; a ring is *atomic* if every element not zero or a unit is a product of atoms. Two elements $a, b \in R$ are *similar* if $R/aR \cong R/bR$. For non-zero-divisors a, b this notion is left-right symmetric [11, 5]; in a commutative integral domain similar elements are associated.

Now a *unique factorization domain* (*UFD* for short) is defined to be an atomic integral domain such that if

$$c = a_1 \dots a_r = b_1 \dots b_s$$

are two atomic factorizations of a given element, then $r = s$ and there is a permutation $i \mapsto i'$ such that a_i is similar to $b_{i'}$. This reduces to the customary notion of *UFD* in the commutative case. The results quoted may now be generalized as follows [5]:

THEOREM 2. — *Every atomic 2-fir is a UFD.*

To apply this result to firs one first shows that every right fir satisfies the ascending chain condition on principal right ideals, briefly, right ACC_1 [7]. Since every integral domain with left and right ACC_1 is atomic, we see that every fir is a *UFD*.

The unique factorization property can be generalized to matrix rings over firs; this is best stated in terms of categories.

Given a finitely presented module M over a fir R,

$$0 \to R^r \to R^s \to M \to 0,$$

we define the *characteristic* of M as $\chi(M) = s - r$. Over a principal ideal domain every module has non-negative characteristic (this is no longer true for firs) and the torsion modules are characterized by $\chi(M) = 0$. Guided by this analogy we define a *torsion module* over a fir as a module M such that (i) $\chi(M) = 0$ and (ii) $\chi(M') \geq 0$ for all submodules M' of M.

THEOREM 3. — *For any fir R the category $\mathcal{T}_R$ of all right torsion modules over R and all homomorphisms between them is an abelian category in which all objects have finite length.*

Now the unique factorization property for firs is just the Jordan Hölder theorem for cyclic torsion modules. Similarly the general Jordan Hölder theorem in $\mathcal{T}_R$ leads to a unique factorization property for matrix rings over firs [8].

3. In the late 1940's, in a paper which has become a classic, Higman, Neumann and Neumann [12] made some very interesting applications of the free product construction for groups. Any ring theorist would naturally wonder whether the same could be done for rings.

For any two rings R_1, R_2 with a common subring K we can form the free composition P in the class of rings [4] (i. e. the coproduct, also definable as a pushout). This is the free product in case the canonical maps $R_i \to P$ are injective and their images intersect precisely in K. In contrast to the group case, the free product of rings need not exist, even in the case of two factors (e. g. suppose that some element of K is invertible in R_1 and a zero-divisor in R_2). The examples suggest that flatness conditions might ensure the existence of free products, and indeed one has [4]

THEOREM 4. — *A family* (R_λ) *of rings with a common subring* K *has a free product over* K *provided that each* R_λ *is faithfully flat, as right* K*-module.*

Thus the free product over a field (not necessarily commutative) always exists, in fact the analogy with the group case is closest for fields. Of course the free product of fields is never itself a field but one is naturally led to the following

EMBEDDING PROBLEM. — *Embed the free product of fields in a field.*

It is this problem that I want to discuss. First let me persuade you that this problem is interesting, by listing three applications that would follow from its solution. Let us assume that we have a construction that embeds the free product $*K_\lambda$ in a field $\circ K_\lambda$, in a reasonably tidy fashion. Then we can imitate the Higman-Neumann-Neumann technique to prove

A. *Given a field* K *with a central subfield* C, *we can embed* K *in a field* L *with centre* C *such that two elements of* L *are conjugate (by an inner automorphism) if and only if they have the same minimal equation over* C.

The following answers a rather natural question which apparently has not been raised before (in the skew case):

B. *For any two fields of the same characteristic, there is a field containing both.*

Finally we can solve a problem of Galois theory. Recall that a field extension L/K is said to be *Galois* if for each $x \in L$, $x \notin K$, there is an automorphism of L fixing K but moving x.

C. *Every field extension* K/k *is contained in a Galois extension.*
Here is a 3-line proof: Take a family of copies K_i of K indexed by $\mathbf{Z}$ and form their field product over k. The automorphism which consists in increasing all suffixes by 1 has k as a fixed field.

4. To justify what has been said I now want to present a solution of the embedding problem which I completed this summer (1970). It provides a raison d'être for firs (for those who need one) as well as some results on the embedding of rings in fields, of quite general validity.

Let $P = *K_\lambda$ be the free product. It is not hard to show that this is an integral domain [4]. The standard method for embedding an integral domain in a field, due to Ore, requires the common multiple condition, and this does not hold here except in one very special case [4]. Now P has an important property (which in fact was responsible for the introduction of firs [6, 7]):

THEOREM 5. — *Any free product of fields (over a common subfield) is a fir.*

So the embedding problem will be solved if we show how to embed a fir in a field.

5. Let us go back to Ore's method. It consists in adjoining solutions of equations

$$ax + b = 0, \qquad \text{where} \qquad a \neq 0. \tag{2}$$

We generalize this by replacing a by a matrix and x, b by columns. This step is suggested by the Schützenberger-Nivat criteria for rationality of power series [17]. Thus we adjoin solutions of the matrix equation

$$Ax + b = 0. \tag{3}$$

The main difficulty is to know what conditions to impose on A. To get an embedding, A must be a non-zero-divisor in R, but in general that is not enough. For a moment let us drop the requirement that we have an embedding, then in (2) we can take a in any multiplicatively closed set, and it is not hard to formulate conditions for the solutions of (3) to form a ring. Essentially the class of matrices to be inverted must be *closed under extensions* [10].

Given any set Σ of matrices over R, let us write R_Σ for the ring obtained by formally adjoining matrix inverses of all the matrices in Σ. We have a homomorphism

$$\lambda : R \to R_\Sigma$$

which may be described as the *universal Σ-inverting homomorphism.* Our object is to find a class Σ such that (i) λ is injective and (ii) R_Σ is a field. If λ is to be injective, Σ must not contain any zero-divisors, but this condition is not enough. Let us define a matrix A over R to be *full* if it is square, say $n \times n$, and has no factorization $A = PQ$, where P is $n \times r$, Q is $r \times n$ and $r < n$. Clearly any matrix over R whose image under a homomorphism into a field is invertible must be full. So the most we can hope to invert are the full matrices, and to obtain the best results we shall assume that R can be embedded in a ring in which every full matrix over R can be inverted. With another mild condition, to exclude pathologies, we can now state the main result [10]:

THEOREM 6. — *Let R be a non-zero ring in which the class Φ of full matrices is closed under extensions. If the universal Φ-inverting mapping $R \to R_\Phi$ is an embedding, then R_Φ is a field.*

6. It only remains to find a class of rings satisfying the conditions of Th. 6. As it happens, the results proved about firs are just sufficient: a full matrix over a fir corresponds to a torsion module and this class is certainly closed under extensions. We also know that every full matrix over a fir is either a unit or a product of atoms. So to apply Th. 6 to firs we need only show that finite sets of full atoms in R_n can be inverted.

This requires a study of conditions under which we can formally adjoin an inverse to a ring without causing collapse. The problem is so general that one needs a hint on what sort of condition to look for. Fortunately the theory of torsion modules provides such a hint: if p is an atom in a fir R, then End (R/pR) is a field. This is essentially Schur's lemma for torsion modules, and it still holds if p is a full atom in a total matrix ring over a fir. What we need is

THEOREM 7. — *Let R be a ring and S any subset of R such that*

(i) *each element of* S *is a non-zero-divisor in* R,
(ii) End (R/pR) *is a field for each* $p \in S$,
(iii) Hom $(R/pR, R/qR) = 0$ *for* $p, q \in S$ *if* $p \neq q$;

then the universal S-inverting homomorphism $R \to R_S$ *is injective.*

This is proved by analysing the relations in a tensor product [10], and it leads to a proof that every fir can be embedded in a field. This completes the solution of the embedding problem.

7. There are some interesting corollaries. Thus Th. 7 yields fairly easily

THEOREM 8. — *If* R *is an atomic 2-fir, then the semigroup of non-zero elements of* R *is embeddable in a group.*

This result is of some interest because it is very easy to construct atomic 2-firs that are not embeddable in a field [9], so one has another solution of Malcev's problem in addition to the three found in 1966 [2, 3, 13]. This example makes the difference between embeddability in a group and in a field rather clear: embeddability in a group requires 2-term conditions, whereas embeddability in a field requires n-term conditions, for every n.

Th. 8 should be compared with Klein's result [14]. In a semifir the non-zero elements can be embedded in a group. This suggests a common generalization, obtained by dropping the word " atomic " in Th. 8. Similarly one would expect that every semifir is embeddable in a field.

REFERENCES

[1] K. ASANO. — Nichtkommutative Hauptidealringe, *A. S. I.*, No. 696 (Paris, 1938).
[2] L. A. BOKUT. — On Malcev's problem, *Sibir. Zh. Mat.*, 10 (1969), pp. 965-1005.
[3] A. J. BOWTELL. — On a question of Malcev, *J. Algebra*, 6 (1967), pp. 126-139.
[4] P. M. COHN. — On the free product of associative rings I, II, *Math. Zeits*, 71 (1959), pp. 380-398; 73 (1960), pp. 433-456.
[5] —. — Noncommutative unique factorization domains, *Trans. Amer. Math. Soc.*, 109 (1963), pp. 313-331.
[6] —. — Rings with a weak algorithm, *Trans. Amer. Math. Soc.*, 109 (1963), pp. 332-356.
[7] —. — Free ideal rings, *J. Algebra*, 1 (1964), pp. 47-69.
[8] —. — Torsion modules over free ideal rings, *Proc. London Math. Soc.* (3), 17 (1967), pp. 577-599.
[9] —. — Dependence in rings II, *Trans. Amer. Math. Soc.*, 135 (1969), pp. 267-279.
[10] —. — The embedding of firs in skew fields, to appear.
[11] H. FITTING. — Über den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie, *Math. Ann.*, 112 (1936), pp. 572-582.
[12] G. HIGMAN, B. H. NEUMANN and H. NEUMANN. — Embedding theorems for groups, *J. London Math. Soc.*, 24 (1949), pp. 247-254.
[13] A. A. KLEIN. — Rings nonembeddable in fields with multiplicative semigroups embeddable in groups, *J. Algebra*, 6 (1967), pp. 101-125.
[14] —. — Necessary conditions for embedding rings into fields, *Trans. Amer. Math. Soc.*, 137 (1969), pp. 141-151.

[15] E. Landau. — Ein Satz über die Zerlegung homogener linearer Differentialausdrücke in irreduzible Faktoren, *J. reine angew. Math.*, 124 (1902), pp. 115-120.
[16] A. Loewy. — Über reduzible homogene Differentialausdrücke, *Math. Ann.*, 56 (1903), pp. 549-584.
[17] M. Nivat. — Séries rationnelles et algébriques en variables non commutatives, Cours D. E. A. (unpublished).
[18] L. A. Skornyakov. — On Cohn rings (Russian), *Algebra i Logika*, 4, No. 3 (1965), pp. 5-30.

Department of Mathematics,
Bedford College,
Regent's Park,
London, N. W. 1.
(Grande-Bretagne)

Actes, Congrès intern. math., 1970. Tome 1, p. 279 à 283.

JORDAN ALGEBRAS AND DIFFERENTIAL GEOMETRY

by MAX KOECHER

1. Basic notions.

Let $\mathfrak{A}$ be a finite dimensional Jordan algebra over the field K of characteristic $\neq 2$. Using the left multiplication L given by $L(a)b = ab$ we define the so-called *quadratic representation* P by $P(a) = 2L^2(a) - L(a^2)$. Then for $a, b \in \mathfrak{A}$ the *fundamental formula* $P(P(a)b) = P(a)P(b)P(a)$ holds. Suppose that the Jordan algebra $\mathfrak{A}$ contains a unit element e. An element $a \in \mathfrak{A}$ is called *invertible* if the linear transformation $P(a)$ is bijective. In this case the *inverse* of a is given by $a^{-1} = [P(a)]^{-1}a$ and $[P(a)]^{-1} = P(a^{-1})$ holds. The set of invertible elements of $\mathfrak{A}$ is denoted by Inv $\mathfrak{A}$.

For a given $f \in \mathfrak{A}$ we define a new product on the vector space of $\mathfrak{A}$ by

$$a \perp b = a(bf) + b(af) - (ab)f.$$

The vector space of $\mathfrak{A}$ together with this product is called the *mutant* $\mathfrak{A}_f$ of $\mathfrak{A}$ with respect to f. Each mutant $\mathfrak{A}_f$ is a Jordan algebra and its quadratic representation is given by $P_f(a) = P(a)P(f)$. The algebra $\mathfrak{A}_f$ has a unit element iff $f \in \operatorname{Inv} \mathfrak{A}$, in this case the unit element of $\mathfrak{A}_f$ is given by f^{-1}. Clearly, $f \in \operatorname{Inv} \mathfrak{A}$ implies $\operatorname{Inv} \mathfrak{A}_f = \operatorname{Inv} \mathfrak{A}$.

2. The structure group.

The group Aut $\mathfrak{A}$ of automorphisms of $\mathfrak{A}$ is a linear algebraic group. Furthermore, let $\Gamma(\mathfrak{A})$ be the set of bijective linear transformations W of $\mathfrak{A}$ for which there exists a bijective linear transformation W^* of $\mathfrak{A}$ such that $P(Wu) = WP(u)W^*$ for all $u \in \mathfrak{A}$. Then $\Gamma(\mathfrak{A})$ is a linear algebraic group, the so-called *structure group* of $\mathfrak{A}$. The fundamental formula shows $P(a) \in \Gamma(\mathfrak{A})$ whenever $a \in \operatorname{Inv} \mathfrak{A}$.

The set Inv $\mathfrak{A}$ carries the structure of a *reflection space* in the sense of O. Loos [6]: Defining $x.y = P(x)y^{-1}$ for $x, y \in \operatorname{Inv} \mathfrak{A}$ the fundamental formula yields (i) $x.x = x$, (ii) $x.(x.y) = y$, (iii) $x.(y.z) = (x.y).(x.z)$. This product does not change if one passes from $\mathfrak{A}$ to a mutant $\mathfrak{A}_f$ where $f \in \operatorname{Inv} \mathfrak{A}$. From the definition it follows that the structure group $\Gamma(\mathfrak{A})$ becomes a subgroup of the automorphisms of the reflection space.

3. Components of Inv $\mathfrak{A}$.

Let $\mathfrak{A}$ be a Jordan algebra with unit element e over the field $\mathbb{R}$ of real numbers. Hence the vector space $\mathfrak{A}$ carries the natural topology and Inv $\mathfrak{A}$ is open. Suppose that the *trace form* τ given by $\tau(u, v) = \text{trace } L(uv)$ is non degenerate. Then the (not necessarily positive definite) line element $ds^2 = \tau(\dot{x}, P(x^{-1})\dot{x})dt^2$ where $x = x(t)$ is a curve in Inv $\mathfrak{A}$ is invariant under the maps $x \to Wx$, $W \in \Gamma(\mathfrak{A})$, and $x \to x^{-1}$. In order to discuss the induced pseudo-riemannian structure let C be a component of Inv $\mathfrak{A}$. Then there exists $f \in C$ such that $f^2 = e$. Writing Comp $\mathfrak{A}$ for the component of Inv $\mathfrak{A}$ containing e we obtain $C = \text{Comp } \mathfrak{A}_f$ whenever $f \in C$, $f^2 = e$. Since $\mathfrak{A}_f$ is again a Jordan algebra (with unit element f) it suffices to consider Comp $\mathfrak{A}$. From [1], XI, Satz 2.4, we obtain.

THEOREM 1. — *Let $\mathfrak{A}$ be a Jordan algebra over $\mathbb{R}$ such that its trace form is non degenerate. Then* Comp $\mathfrak{A}$ *is a homogeneous symmetric space.*

4. Formally real Jordan algebras.

A Jordan algebra $\mathfrak{A}$ over $\mathbb{R}$ is called *formally real* if $a^2 + b^2 = 0$ for $a, b \in \mathfrak{A}$ implies $a = b = 0$. $\mathfrak{A}$ is formally real iff its trace form τ is positive definite. Hence Comp $\mathfrak{A}$ is riemannian whenever $\mathfrak{A}$ is formally real. Using the (algebraic) exponential one has

THEOREM 2. — *Let $\mathfrak{A}$ be a formally real Jordan algebra. Then*

$$\text{Comp } \mathfrak{A} = \exp \mathfrak{A} = \{ x^2 ; x \in \text{Inv } \mathfrak{A} \}$$

and the map $x \to \exp x$ *is bijective.*

Let $D \neq \emptyset$ be an open convex cone in a real vector space $\mathfrak{B}$. We call D *homogeneous* if the group Aut D of all bijective linear transformations W of $\mathfrak{B}$ satisfying $WD = D$ acts transitively on D. For a positive definite bilinear form σ of $\mathfrak{B}$ we define the *dual cone* $D^\sigma = \{ x ; x \in \mathfrak{B}, \sigma(x, y) > 0 \text{ for } 0 \neq y \in \bar{D} \}$. D is called self dual if there exists a positive definite σ such that $D^\sigma = D$.

THEOREM 3. — (i) *Let D be a homogeneous convex self dual cone in a real vector space $\mathfrak{B}$. Then there exists a formally real Jordan algebra $\mathfrak{A}$ in $\mathfrak{B}$ such that* $D = \text{Comp } \mathfrak{A}$.

(ii) *Let $\mathfrak{A}$ be a formally real Jordan algebra. Then* Comp $\mathfrak{A}$ *is a homogeneous convex cone that is self dual with respect to the trace form of $\mathfrak{A}$.*

5. The primitive idempotents in a formally real Jordan algebra.

Let $\mathfrak{A}$ be a simple formally real Jordan algebra and let Idem $\mathfrak{A}$ be the set of idempotents $\neq 0$ of $\mathfrak{A}$. An idempotent c is called *primitive* if there is no representation $c = c_1 + c_2$ where $c_1, c_2 \in \text{Idem } \mathfrak{A}$. Using the trace form τ of $\mathfrak{A}$ we obtain a metric ρ on the set $\text{Idem}_1 \mathfrak{A}$ of primitive idempotents of $\mathfrak{A}$ by defining $\rho(c, d) = 1 - \tau(cd)$.

THEOREM 4 (U. Hirzebruch [3]). — (i) *The pair* $I = (\text{Idem}_1 \mathfrak{A}, \rho)$ *is a connected compact metric space.*

(ii) *The group* Aut $\mathfrak{A}$ *acts doubly transitively as a group of isometries on I.*

(iii) *Each isometry of I extends to an automorphism of the Jordan algebra $\mathfrak{A}$.*

(iv) $\mathrm{Idem}_1\, \mathfrak{A}$ *as a submanifold of the* τ*-sphere is a two point homogeneous symmetric space and hence of rank* 1.

Using the classification of H. C. Wang [8], Hirzebruch obtains

THEOREM 5. — *Let* $\mathfrak{X}$ *be a connected double homogeneous compact metric space. Then there exists a simple formally real Jordan algebra* $\mathfrak{A}$ *such that* $\mathfrak{X}$ *is homeomorphic to* $\mathrm{Idem}_1\, \mathfrak{A}$.

It would be of interest to prove this theorem without Wang's classification.

6. **Helwig's construction.**

Let J be an automorphism of the formally real Jordan algebra $\mathfrak{A}$ such that $J^2 = \mathrm{id}$. We assume that the trace from τ is non degenerate. Let $\mathrm{Inv}\,(\mathfrak{A}, J)$ be the set of all invertible elements q of $\mathfrak{A}$ such that $q^{-1} = Jq$. One can easily show that

$$\mathrm{Inv}\,(\mathfrak{A}^q, J_q) = \mathrm{Inv}\,(\mathfrak{A}, J)$$

holds for all $q \in \mathrm{Inv}\,(\mathfrak{A}, J)$ where $\mathfrak{A}^q$ is the mutant of $\mathfrak{A}$ with respect to q^{-1}, and $J_q = P(q)J$ an automorphism of $\mathfrak{A}_q$. Thus, as in 3, it suffices to study the component M of $\mathrm{Inv}\,(\mathfrak{A}, J)$ containing the unit element e of $\mathfrak{A}$. M is a regular analytic submanifold of Comp $\mathfrak{A}$. With the " metric " inherited from Comp $\mathfrak{A}$, M is pseudo-riemannian and symmetric. The following results are due to K. H. Helwig [2].

THEOREM 6. — *M is a totally geodesic submanifold of* Comp $\mathfrak{A}$. *In case the pair* $(\mathfrak{A}, J)$ *is simple* (i. e. $\mathfrak{A}$ *contains no proper J-invariant ideal*), *M is an Einstein space iff $\mathfrak{A}$ is central simple.*

The geodesic symmetry around a point q of M is given by J_q. The group $\Gamma(M)$ generated by $P(q)$, $q \in M$, is a transitive group of isometries of M. Neglecting a few exceptions, $\Gamma(M)$ is effective on M if $(\mathfrak{A}, J)$ is simple, and $\Gamma(M)$ is a semi simple Lie group if $\mathfrak{A}$ is central simple. Using the classification of riemannian symmetric spaces one can prove the following.

THEOREM 7. — *Let N be an irreducible riemannian symmetric space of non compact type. Suppose that N is classical or of type E* IV *or the non compact dual of the projective Cayley plane. Then there is a formally real Jordan algebra $\mathfrak{A}$ and an automorphism J of $\mathfrak{A}$ such that M is homothetic to N or to $\mathbb{R}^+ \times N$.*

Now we assume $\mathfrak{A}$ to be simple and $\mu\colon (a, b) \to \tau(a, Jb)$ to be positive definite. Then M is compact. Replacing the pseudo-riemannian structure of M given above by its negative, M is a riemannian submanifold of the $(n-1)$-sphere S consisting of all $a \in \mathfrak{A}$ such that $\mu(a, a) = n = \dim \mathfrak{A}$.

THEOREM 8. — (i) *If the* 1*-eigenspace $\mathfrak{A}_+$ of J is a simple algebra then the inclusion $M \subset S$ is an equivariant* (*w.r.t.* $\Gamma(M)$) *and minimum* (*w.r.t. mean curvature*) *imbedding. If $\mathfrak{A}_+$ is not simple then there is a minimum and equivariant imbedding of M into a $(n-2)$-sphere.*

(ii) *The cut locus of a point p of M consists of all q in M for which $p + q$ is not invertible.*

(iii) *Every maximal torus of M through p contains exactly one antipodal point of p.*

COROLLARY 1. — *The isotropy group of p is transitive on the antipodal set of p.*

COROLLARY 2 (Principle of duality). — *Distinct points of M have distinct antipodal sets.*

7. **Jordan triple systems.**

We consider a finite dimensional vector space $\mathfrak{B}$ over the field K of characteristic $\neq 2, 3$ to gether with a trilinear map $(a, b, c) \to \{ a, b, c \}$ of $\mathfrak{B} \times \mathfrak{B} \times \mathfrak{B}$ into $\mathfrak{B}$. As an abbreviation define the linear transformation $a \square b$ of $\mathfrak{B}$ by $(a \square b)c = \{ a, b, c \}$ and the *trace form* σ of $\mathfrak{B}$ by $\sigma(a, b) = \text{trace}\,(a \square b + b \square a)$. Suppose that σ is non degenerate. Then by T^* we denote the adjoint of the linear transformation T of $\mathfrak{B}$ *w.r.t.σ*. Furthermore let $\mathfrak{T}$ be the space spanned by $a \square b$ for all $a, b \in \mathfrak{B}$. We call $\mathfrak{B}$ a *Jordan triple system* (and the map $(a, b) \to a \square b$ a *pairing*) if in addition $(a \square b)c = (c \square b)a$, $[T, a \square b] = Ta \square b - a \square T^*b$, $(a \square b)^* = b \square a$ holds for $a, b, c \in \mathfrak{B}$ and $T \in \mathfrak{T}$. In particular $\mathfrak{T}$ becomes a Lie algebra of linear transformations of $\mathfrak{B}$. Denote by Γ the set of bijective linear transformations W of $\mathfrak{B}$ such that $W(a \square b)W^{-1} = Wa \square W^{*-1}b$ holds for all $a, b \in \mathfrak{B}$. Then Γ is a linear algebraic group. The connection between Jordan triple systems and Jordan algebras is given by

MEYBERG'S THEOREM [7]. — *Let $\mathfrak{B}$ be a Jordan triple system and let $d \in \mathfrak{B}$. Then $\mathfrak{B}$ together with the product $(u, v) \to \{ u, d, v \}$ becomes a Jordan algebra denoted by $\mathfrak{B}_d$.*

Conversely, a Jordan algebra $\mathfrak{A}$ induces a Jordan triple system in the same vector space by setting $\{ a, b, c \} = P(a, c)b$.

The following results are taken from [5]. Let $\square : \mathfrak{B} \times \mathfrak{B} \to \text{End}\,\mathfrak{B}$ be a pairing. In the vector space $\mathfrak{K} = \mathfrak{T} \oplus \mathfrak{B} \oplus \mathfrak{B}$ an anti-commutative algebra is given by the commutator product for the elements of $\mathfrak{T}$, by zero for two elements in the second or the third component, and by $(T, a) \to Ta$, $(T, b) \to -T^*b$, $(a, b) \to a \square b$, where $T \in \mathfrak{T}$, a in the second and b in the third component.

THEOREM 9. — *$\mathfrak{K}$ is a Lie algebra having a non degenerate Killing form.*

Using various examples of pairings one verifies that Lie algebras of type A, B, C, D, E_6 and E_7 can be obtained by this construction. According to K. Meyberg [7] no Lie algebra of type G_2, F_4 and E_8 occurs.

Let x be a generic element of $\mathfrak{B}$ and define birational mappings t_a and s_b by $t_a(x) = x + a$, $s_b(x) = (I + \frac{1}{2}x \square b)^{-1}x$ for $a, b \in \mathfrak{B}$. We denote by Ξ the group of birational mappings generated by $W \in \Gamma$, $t_a(a \in \mathfrak{B})$ and $s_b(b \in \mathfrak{B})$.

THEOREM 10. — (i) *Each element of Ξ can be written as $W \circ t_a \circ s_b \circ t_c$ where $W \in \Gamma$ and $a, b, c \in \mathfrak{B}$.*

(ii) *Ξ is (in an explicit manner) isomorphic to a Zariski open subgroup of* Aut $\mathfrak{K}$.

For pairings that are induced by formally real Jordan algebras the group Ξ is in fact isomorphic to Aut $\mathfrak{K}$.

8. **Bounded symmetric domains.**

Let $\mathfrak{B}_0$ be a real vector space and let $\square : \mathfrak{B}_0 \times \mathfrak{B}_0 \to \operatorname{End} \mathfrak{B}_0$ be a pairing. Suppose that the pairing is *formally real*, i. e. its trace form σ_0 is positive definite. The pairing extends to a pairing of the complexification $\mathfrak{B}$ of $\mathfrak{B}_0$ with trace form σ. For $u \in \mathfrak{B}$ we denote by $\bar{u}$ the complex conjugate. Then $(u, v) \to \sigma(u, \bar{v})$ becomes a hermitian positive definite form on $\mathfrak{B}$. For a linear transformation T of $\mathfrak{B}$ that is self-adjoint with respect to this hermitian form we write $T > 0$ whenever $\sigma(Tu, \bar{u}) > 0$ for $0 \neq u \in \mathfrak{B}$. Using the identification of a generic element x of $\mathfrak{B}$ and a " variable " $z \in \mathfrak{B}$ the group Ξ becomes a group of bimeromorphic mappings.

THEOREM 11. — (i) *The set* $Z = \{ z : z \in \mathfrak{B}, 2I - z \,\square\, \bar{z} > 0 \}$ *is a bounded symmetric domain and it is convex.*

(ii) *The group Bih Z of all biholomorphic automorphisms of Z coincides with the subgroup of* $f \in \Xi$ *such that* $f^{-1}(z) = -f(-z)$.

(iii) *The elements f of* Bih Z *are exactly the mappings* $U \circ t_a \circ B_a \circ s_{\bar{a}}$ *where* $a \in Z$, *U in the isotropy group of o and where* B_a *is some (explicitly known) linear transformation uniquely determined by a.*

Without classification one obtains

THEOREM 12. — *Let D be a bounded symmetric domain in some complex vector space* $\mathfrak{B}$. *Then there exists a real form* $\mathfrak{B}_0$ *of* $\mathfrak{B}$ *and a formally real pairing* $\square$ *of* $\mathfrak{B}_0$ *such that D is biholomorphically equivalent to* $\{ z : z \in \mathfrak{B}, 2I - z \,\square\, \bar{z} > 0 \}$.

LITERATUR

[1] H. BRAUN and M. KOECHER. — *Jordan-Algebren*, Springer (1966).

[2] K. H. HELWIG. — Jordan-Algebren und kompakte symmetrische Räume I, *Math. Z.*, 115 (1970), pp. 315-349.

[3] U. HIRZEBRUCH. — Über Jordan-Algebren und kompakte symmetrische Räume vom Rang 1, *Math. Z.*, 90 (1965), pp. 339-354.

[4] M. KOECHER. — Jordan algebras and their applications, *Lectures notes*, U. of Minnesota, Minneapolis (1962).

[5] —. — An elementary approach to bounded symmetric domains, *Lecture notes*, Rice University, Houston (1969) and *Appendix* (1970).

[6] O. LOOS. — *Symmetric spaces I*, Benjamin (1969).

[7] K. MEYBERG. — *Jordan-Tripelsysteme und die Koecher-Konstruktion von Lie-Algebren*, Hab. Schrift, U München (1969).

[8] H. C. WANG. — Two-point homogeneous spaces, *Ann. of Math.*, 55 (1952), pp. 177-191.

Mathematisches Institut
der Universität
Roxeler Strasse 64
44-Münster
(République Fédérale Allemande)

Actes, Congrès intern. math., 1970. Tome 1, p. 285 à 292.

VARIATIONS MODULAIRES SUR UN THÈME DE CARTAN

par A. I. KOSTRIKIN

Il s'agira ici d'algèbres de Lie simples de dimension finie sur un corps k algébriquement clos de caractéristique $p > 0$. Tout à fait remarquables à de nombreux points de vue, elles portent la marque des propriétés de deux classes d'algèbres de Lie complexes (sur $\boldsymbol{C}$), à savoir : simples de dimension finie et simples transitives infinies correspondant aux pseudo-groupes de Lie primitifs. L'étude de ces classes et la détermination exhaustive des algèbres qu'elles contiennent est indissolublement liée au nom de E. Cartan [2].

La théorie des algèbres de Lie modulaires est toujours en plein développement et propose tout un éventail de problèmes parfois inattendus. Ce n'est que tout à fait récemment, par exemple, que Block [1] a complètement décrit les algèbres de Lie semi-simples en termes simples, résultat dont la démonstration était attendue depuis longtemps. On trouvera les autres aspects de la théorie dans l'analyse complète de Seligman [8].

1. Types d'algèbres simples.

Choisissons dans chaque algèbre de Lie simple de dimension finie sur $\boldsymbol{C}$ une base de Chevalley [4] et effectuons la réduction modulo p (et également le passage à l'algèbre quotient par le centre de dimension 1 dans le cas A_{kp-1}) nous obtenons les algèbres simples sur k

$$A_n,\ n \geqslant 1;\quad B_n,\ n \geqslant 2;\quad C_n,\ n \geqslant 3;\quad D_n,\ n \geqslant 4;\quad E_i,\ i = 6, 7, 8;\quad F_4;\quad G_2,$$

qu'il est traditionnel d'appeler classiques (y compris E_i, F_4 et G_2).

Il est bien connu que sur le corps $\boldsymbol{C}$, il n'existe, à un isomorphisme près, que quatre séries d'algèbres de Lie simples infinies transitives :

$$W_n,\ n \geqslant 1;\quad S_n,\ n \geqslant 2;\quad H_n,\ n \geqslant 1;\quad K_n,\ n \geqslant 2,$$

appelées algèbres de type Cartan. A partir de leurs réalisations dans l'algèbre des différentiations continues de l'anneau des séries entières formelles, I. R. Shafarevitch et l'auteur [13] et [14] ont construit les algèbres de type Cartan en caractéristique $p > 0$. Soit E un espace vectoriel de dimension finie sur k avec une base $\{X_1, \ldots, X_n\}$ et soit $O(E) = \langle X_1^{(i_1)}, \ldots, X_n^{(i_n)} \rangle$ l'algèbre des puissances divisées sur E. L'algèbre $O(E)$ apparaît de manière naturelle dans les problèmes d'algèbre liés d'une façon ou d'une autre aux nombres premiers p (cf. [3], [5]). Toutes les dérivations spéciales

$$\mathscr{D} : X^{(h)} \to X^{(h-1)} \mathscr{D} X, \qquad X \in E,$$

de l'algèbre $O(E)$ forment une algèbre de Lie simple de dimension finie $W_n(E)$. De plus, par analogie avec la caractéristique nulle, on introduit les trois autres séries d'algèbres : $S_n(E) \subset W_{n+1}(E)$, $H_n(E) \subset W_{2n}(E)$, $K_n(E) \subset W_{2n-1}(E)$ déterminées par les formes différentielles extérieures $\omega = dX_1 \wedge \ldots \wedge dX_{n+1}$:

$$\omega = \sum_{1 \leqslant i \leqslant n} dX_i \wedge dX_{i+n} \quad \text{et} \quad \omega = dX_0 + \sum_{1 \leqslant i \leqslant n-1} (X_i dX_{i+n} - X_{i+n} dX_i)$$

respectivement. Posons $\partial_i X_j^{(h)} = \delta_{ij} X_j^{(h-1)}$, et $\deg X_i = -\deg \partial_i = 1$, $i > 0$, $\deg X_0 = 2 = -\deg \partial_0$; on obtient ainsi des graduations standard dans toutes les algèbres $L(E)$. Comme d'habitude, il faut entendre par drapeau généralisé de hauteur l un système

$$\mathscr{F} : E = E_0 \supseteq E_1 \supseteq \ldots \supseteq E_1 \supseteq E_{l+1},$$

de sous-espaces de E inclus l'un dans l'autre. Au drapeau $\mathscr{F}$ correspond de manière unique une sous-algèbre graduée de dimension finie $O(\mathscr{F})$, invariante pour toutes les dérivations $\partial_\xi : X^{(h)} \to X^{(h-1)}\xi(X)$, $\xi \in E^*$, et aussi une algèbre graduée simple de dimension finie $W(\mathscr{F}) \subset W(E)$ constituée par les dérivations de $O(\mathscr{F})$ dans elle-même. Une définition équivalente est

$$W(\mathscr{F}) = \langle \mathscr{D} \in W(E) \,|\, (\mathrm{ad}\, \partial_\xi)^{p^i} \mathscr{D} = 0, \quad \xi \in \mathrm{Ann}\, E_i \subset E^* \}$$

En général $\tilde{L}(\mathscr{F}) = L(E) \cap W(\mathscr{F})$, où $L = S$, H ou K, n'est pas une algèbre simple mais son algèbre dérivée seconde $L(\mathscr{F}) = \tilde{L}(\mathscr{F})''$ est déjà simple. Toute algèbre de Lie graduée M telle que $L(\mathscr{F}) \subseteq M \subseteq \tilde{L}(\mathscr{F})$ s'appelle une algèbre de type Cartan relative au drapeau $\mathscr{F}$. Les algèbres $W(\mathscr{F})$ (générales), $S(\mathscr{F})$ (spéciales), $H(\mathscr{F})$ (hamiltoniennes) et $K(\mathscr{F})$ (de contact) ne sont pas seulement des représentants caractéristiques des algèbres de Lie simples non classiques. Enrichissant quelque peu la construction dans les cas $S(\mathscr{F})$ et $H(\mathscr{F})$, Wilson [9] a établi le théorème suivant

Théorème 1. — Toutes les algèbres simples non classiques du livre [8] sont contenues dans les algèbres « croisées » de type Cartan.

La notion de « croisement », dont je ne donnerai pas ici de définition précise, est, visiblement, une forme commode pour la réalisation de toutes sortes de déformations des algèbres graduées dont il sera question plus bas. *Il est important de souligner que l'accumulation, pendant trente ans, d'exemples ingénieux (ou, comme le disent certains, pathologiques) au niveau des conjectures n'a pas conduit au chaos.* Au contraire le point de vue modulaire dans cette approche nouvelle est assez naturel et attirant pour les chercheurs. Des considérations heuristiques, appuyées par une série de résultats, ont conduit I. R. Chafarevitch et l'auteur à la conviction que la conjecture fondamentale suivante est vraie.

(C_1) Toute algèbre de Lie $\mathscr{L}$ simple de dimension finie sur un corps k algébriquement clos de caractéristique $p > 5$ est isomorphe à une algèbre de Lie classique ou à une déformation d'une algèbre graduée de type Cartan.

2. Résultats relatifs à la classification.

Dans ce qui suit, on suppose $p > 5$. La limitation $p \neq 2,3$ résulte de l'essence même de notre entreprise tandis que la valeur $p = 5$ s'exclut plutôt pour simplifier les énoncés.

Soit $\mathscr{L}$ une algèbre de Lie simple de dimension finie sur k, $\mathscr{L}_0$ sa sous-algèbre maximale. Parmi les sous-espaces propres $\mathscr{L}_{-1}$ tels que $[\mathscr{L}_{-1}, \mathscr{L}_0] \subseteq \mathscr{L}_{-1}$, choisissons-en un minimal. Posant

$$\mathscr{L}_{-i}=\mathscr{L}^i_{-1}=[\ldots [\mathscr{L}_{-1}, \mathscr{L}_{-1}],\ldots, \mathscr{L}_{-1}], \quad \mathscr{L}_i=\{x\in\mathscr{L}_{i-1} \mid [x, \mathscr{L}_{-1}]\subseteq\mathscr{L}_{i-1}\}, \quad i>0,$$

étant donné la maximalité de $\mathscr{L}_0$, nous obtenons l'égalité $\mathscr{L}_{-q} = \mathscr{L}$ et étant donné la simplicité de $\mathscr{L}$, l'égalité $\mathscr{L}_{r+1} = 0$ pour certains q, $r \in \mathbf{Z}$, $q > 0$, $r \geqslant 0$. Il est facile de voir que

$$[\mathscr{L}_i, \mathscr{L}_j] \subseteq \mathscr{L}_{i+j}.$$

On obtient la filtration

$$\mathscr{L} = \mathscr{L}_{-q} \supset \ldots \supset \mathscr{L}_{-1} \supset \mathscr{L}_0 \supset \mathscr{L}_1 \supset \ldots \supset \mathscr{L}_r \supset 0$$

de profondeur q et de longueur r, qui dépend bien entendu du choix de $\mathscr{L}_0$. L'algèbre de Lie graduée associée à cette filtration est

$$\operatorname{gr} \mathscr{L} = L = L_{-q} \oplus \ldots \oplus L_{-1} \oplus L_0 \oplus L_1 \oplus \ldots \oplus L_r;$$

comme d'habitude nous désignerons par $(x, y) \to [x, y]$ sa multiplication qui possède pour $r \geqslant 1$ les propriétés suivantes

1) $[L_i, L_j] \subseteq L_{i+j}$;
2) L_{-1} est un L_0-module simple;
3) $x \in L_{\pm i}$, $[x, L_{\mp 1}] = 0$, $i \geqslant 0 \Rightarrow x = 0$

(transitivité de l'algèbre graduée).

Une algèbre de Lie $\mathscr{M}$ dans laquelle il existe une filtration $\{\mathscr{M}_i\}$ avec $\operatorname{gr} \mathscr{M} \cong L$ (isomorphisme d'algèbres graduées) s'appelle une déformation de l'algèbre graduée L; (ce n'est pas la notion usuelle de déformation, au sens de Kuranishi, Spencer, Kerstenhaber, etc.). La déformation L est triviale si $\mathscr{M} \cong L$. Sans imposer la simplicité du L_0-module L_{-1}, on peut se limiter aux filtrations de profondeur 1 comme cela s'est presque toujours fait en caractéristique nulle (cf. [7]). La technique correspondante est exposée par exemple dans l'article [6] où l'on rappelle les résultats obtenus par Tanaka. Elle a aussi été donnée indépendamment dans la note [10] de Veisfeiler.

Bien que la composante L_0 donne une représentation irréductible exacte sur L_{-1}, on ne peut rien dire de précis sur sa structure (c'est une des bizarreries de la caractéristique p). Dans un cas particulier, on a le résultat suivant

Théorème 2. — Une algèbre de Lie L semi-simple sur K, qui admet une représentation exacte de dimension $n < p - 1$, se décompose en somme directe d'algèbres de Lie simples classiques (cf. [15] et les remarques à la fin de [14]).

D'autre part V. G. Katz [11], [12] a établi le théorème suivant

Théorème 3. — Soit L une algèbre de Lie de dimension finie transitive graduée, admettant une déformation simple, dont la composante L_0 — somme directe d'algèbres classiques M_i et du centre, et de L_{-1} — est un p-module compatible avec la p-structure dans les M_i; alors L est isomorphe à une algèbre de Lie classique ou de type Cartan (avec les restrictions $q = 1$ et $n = \dim L_{-1} < p - 1$ ce théorème est démontré aussi dans [14]).

Enfin, je formulerai un résultat qui met la conjecture (C_1) sur un terrain solide.

THÉORÈME 4. — La conjecture (C_1) est vraie s'il existe dans $\mathscr{L}$ une sous-algèbre de codimension $n < p - 1$.

Pour la démonstration, il faut construire une filtration à partir d'une sous-algèbre maximale de codimension $< p - 1$, passer à l'algèbre graduée, et appliquer les théorèmes 2 et 3, si cette filtration est de longueur $r \geqslant 1$ (transitivité !). Dans le cas $r = 0$, il faut utiliser des résultats exposés dans [15] et [16]. Remarquons, en particulier, qu'une algèbre de Lie simple avec une sous-algèbre de codimension 1 est isomorphe soit à l'algèbre A_1, soit à une algèbre générale $W_1(\mathscr{F})$ de dimension p^m, $m = 1, 2, \ldots$

3. Sous-algèbres invariantes.

Une sous-algèbre maximale $\mathscr{L}_0 \subset \mathscr{L}$ choisie au hasard conduit à une filtration de $\mathscr{L}$ de longueur nulle qui est sans intérêt. Cependant, il y a des raisons de croire qu'on peut effectuer une construction absolument invariante, comme le suggère la conjecture suivante.

(C_2) Dans toute algèbre de Lie $\mathscr{L}$ sur un corps k, simple et non classique, il existe une sous-algèbre de Lie (propre) maximale $\mathscr{L}_{\text{inv}}$, invariante par le groupe Aut $\mathscr{L}$ de tous les automorphismes de l'algèbre, et contenant toute autre sous-algèbre invariante.

Cette intéressante situation, liée à la structure du groupe Aut $\mathscr{L}$ et de l'algèbre $\mathscr{L}$ elle-même, s'explique par la présence de nilpotents dans les schémas des automorphismes des algèbres non classiques. V. A. Kreknine a démontré le théorème suivant

THÉORÈME 5. — La filtration standard (cf. § 1) d'une algèbre simple $L(\mathscr{F})$ de type Cartan est invariante pour Aut $L(\mathscr{F})$. Toutes les sous-algèbres invariantes sont contenues dans $\mathscr{L}_0 = L_0 \oplus L_1 \oplus \ldots$

Pour les différentes déformations des algèbres $M \subseteq \tilde{L}(\mathscr{F})$, la conjecture (C_2) n'est pas démontrée. La conjecture plus forte suivante suggère une méthode effective de démonstration.

(C_3) La sous-algèbre maximale invariante $\mathscr{L}_{\text{inv}}$ est le normalisateur dans $\mathscr{L}$ de la sous-algèbre invariante

$$\mathscr{C} = \langle c \in \mathscr{L} \mid (\text{ad } c)^2 = 0 \rangle \neq 0.$$

Comme on le montre dans l'article [16], la filtration relative à $\mathscr{L}_{\text{inv}} = N_{\mathscr{L}}(\mathscr{C})$ est sûrement de longueur $r > 1$. On y établit aussi le théorème suivant

THÉORÈME 6. — La sous-algèbre non nulle $\mathscr{C}$ (elle est toujours nilpotente) existe dans toute algèbre simple non classique avec une décomposition de Cartan

$$\mathscr{L} = H + \Sigma \mathscr{L}_\alpha$$

et un élément $0 \neq a \in \bigcup_\alpha \mathscr{L}_\alpha$ tel que $(\text{ad } a)^{p-1} = 0$.

Bien entendu, la question suivante se pose : existe-t-il une algèbre de Lie simple $\mathscr{L}$ sur k $(p \neq 2, 3)$ dans laquelle $(\text{ad } x)^{p-1} \neq 0$ pour tout élément non nul $x \in \mathscr{L}$?

A l'aide du théorème 5 on établit instantanément la non-isomorphie des algèbres $L(\mathscr{F})$ des différentes séries et en résout le problème des isomorphismes à l'intérieur de ces séries. Ainsi, la filtration standard relative à $\mathscr{L}_{\text{inv}}$ montre qu'à toutes les décompositions ordonnées différentes $m = m_1 + \ldots + m_n$, $1 \leqslant m_1 \leqslant \ldots \leqslant m_n$, correspondent des algèbres $W_n(\mathscr{F})$ non isomorphes de dimension $\dim W_n(\mathscr{F}) = np^m$, $m \geqslant n$. On obtient des résultats analogues pour les autres séries.

4. Familles paramétriques.

Soit $p = \operatorname{car} k = 3$, $\varepsilon \in k$, $\varepsilon \neq 0$ et soit $\{ \alpha, \beta \}$ un système fondamental de racines pour le type B_2. On se propose d'examiner la p-algèbre de Lie simple graduée de dimension dix

$$L(\varepsilon) = L_{-2} \oplus L_{-1} \oplus L_0 \oplus L_1 \oplus L_2, \qquad L(-1) = B_2$$

où

$$L_{\pm 2} = \langle E_{\pm(2\alpha+\beta)} \rangle,$$
$$L_{\pm 1} = \langle E_{\pm(\alpha+\beta)}, E_{\pm\alpha} \rangle,$$
$$L_0 = \langle E_{-\beta}, H_\beta, E_\beta \rangle + \langle Z \rangle,$$
$$[Z, X_i] = iX_i, \quad X_i \in L_i; \quad [H_\beta, E_{i\alpha+j\beta}] = (-i+2j)E_{i\alpha+j\beta}.$$

Par rapport à la base donnée, les constantes de structure de $L(\varepsilon)$ sont les mêmes que celles de l'algèbre simple complexe B_2 à l'exception des cas suivants

	E_α	$E_{\alpha+\beta}$	$E_{2\alpha+\beta}$
$E_{-2\alpha-\beta}$	$-\varepsilon E_{-\alpha-\beta}$	$\varepsilon E_{-\alpha}$	$-\varepsilon^2 Z$
$E_{-\alpha-\beta}$	$2E_{-\beta}$	$-H_\beta + \varepsilon Z$	εE_α
$E_{-\alpha}$	$H_\beta + \varepsilon Z$	$2E_\beta$	$-\varepsilon E_{\alpha+\beta}$

Dans l'article [17] on montre le théorème suivant:

THÉORÈME 7. — Les p-algèbres de Lie simples $L(\varepsilon)$ et $L(\varepsilon')$ pour des éléments ε et ε' de k distincts, $\varepsilon\varepsilon' \neq 1$, ne sont pas isomorphes.

Par suite, la normalisation du type de Chevalley [4] n'est pas réalisable dans une algèbre quelconque. Probablement, pour $p = 2,3$, il existe d'autres familles paramétriques (de même puissance que le corps k), mais je me risquerai malgré tout à énoncer la conjecture suivante.

(C_4) Il n'existe pas de famille paramétrique d'algèbres de Lie simples quand la caractéristique p du corps de base k (supposé, bien entendu, algébriquement clos) est suffisamment grande.

En ce qui concerne les algèbres graduées, c'est très vraisemblable car, sinon, la conjecture (C_1) perdrait toute signification. D'autre part, il n'y a pas de correspondance biunivoque entre les cohomologies de Spencer et les classes d'isomorphisme de déformations et de très nombreux exemples montrent qu'il n'existe pas non plus de paramètres continus dans les déformations. Voici une situation typique. Soit $\mathscr{F}$ le drapeau de hauteur 1 d'un espace vectoriel $E = \langle X_1, X_2 \rangle$ de dimension 2 sur k. Introduisons dans $O(\mathscr{F})/k$ la structure d'algèbre de Lie simple $\mathscr{L}(\varepsilon)$, $0 \neq \varepsilon \in k$, en posant

$$U \circ V = (\partial_1 U \cdot \partial_2 V - \partial_2 U \cdot \partial_1 V)(1 + \varepsilon X_1^{(p-1)} X_2^{(p-1)}), \quad U, V \in O(\mathscr{F})/k.$$

Par construction, $\mathscr{L}(\varepsilon)$ est une déformation de l'algèbre graduée

$$L = H_1(\mathscr{F}) \oplus \langle X_1^{(p-1)} X_2^{(p-1)} \rangle \subset \tilde{H}_1(\mathscr{F}),$$

dans laquelle la p-algèbre de Lie hamiltonienne $H_1(\mathscr{F})$ est un idéal de codimension 1. Cette déformation correspond au cocycle $f \in H^{2p-3,2}(L)$:

$$f(X_1, X_2) = X_1 \circ X_2 = X_1^{(p-1)} X_2^{(p-1)} \in L_{2p-4}.$$

Comme il est facile de le vérifier, pour tout $\varepsilon \neq 0$, il existe un isomorphisme $\mathscr{L}(\varepsilon) \cong \mathscr{L}(1)$ et il n'existe donc aucun paramètre.

Il est traditionnel de qualifier de rigide une algèbre de Lie qui n'admet pas de déformations non triviales. L'algèbre générale $W_n(\mathscr{F})$ est rigide.

5. **Remarques isolées.**

I. Comme me l'a communiqué V. G. Katz, il est possible de réduire le problème fondamental de la classification des algèbres de Lie simples de dimension finie à celui de la maximalité du sous-schéma le plus réduit du schéma des automorphismes de ces algèbres. On ne sait pas si on réussira à obtenir (ou pas) la démonstration des conjectures (C_2) et (C_3) en utilisant la technique des groupes algébriques.

II. De nombreuses questions restent ouvertes dans la théorie des représentations des algèbres de Lie de caractéristique $p > 0$, même dans le cas des algèbres classiques. Tout récemment, A. N. Roudakov [19] a montré que $p^{m(L)}$, $m(L) = \frac{1}{2}(\dim L - \text{rang } L)$, est la dimension maximum possible des représentations irréductibles d'une algèbre de Lie L classique sur k, avec car $k = p > 3$, et que cette dimension est atteinte dans la classe des p-représentations irréductibles. Cette dernière affirmation n'est pas vraie pour les p-algèbres de type Cartan pour lesquelles l'exposant $m(L)$ n'est pas calculable, sauf pour $m(W_1) = \frac{p-1}{2}$. La paramétrisation des représentations de l'algèbre L sur k par une variété algébrique (suivant l'idée de Zassenhaus) et la recherche de cette variété ne sont en fait résolues que pour l'algèbre A_1 (cf. [20]).

III. Soit L une des algèbres de type Cartan simples sur le corps fini F_q, soit

$$L = L_{-q} \oplus \ldots \oplus L_{-1} \oplus L_0 \ldots \oplus L_r, \qquad q \leqslant 2,$$

sa graduation standard et soit Γ une p-représentation irréductible. Pour tout élément $X \in L_i$, $i \neq 0$, $\Gamma(X)^p = 0$, considérons les exponentielles $\exp \Gamma(X)$ et le groupe

$$G_q(L, \Gamma) = \langle \exp \Gamma(X) \rangle$$

qu'elles engendrent. Cela ressemble de loin aux groupes de Chevalley [4]. La structure du groupe $G_q(L, \Gamma)$ dépend autant de L que de Γ. Dans le cas $L = W_1$ et $\dim \Gamma = p - 1$, on a un isomorphisme $G_q(W_1, \Gamma) \cong C_{\frac{p-1}{2}}(q)$, alors que $C_q(W_1, \text{ad}) \cong A_{p-1}(q)$. Rappelons que le groupe Aut W_1 est résoluble. Le manque de matériel expérimental ne permet de faire aucune hypothèse précise sur la structure de $G_q(L, \Gamma)$ dans le cas général.

IV. Il convient enfin d'expliquer que l'indice inférieur dans la notation des algèbres de type Cartan W_n, S_n, H_n, K_n a la même signification que pour les algèbres classiques $A_n, \ldots, G_2$; cet entier n (qui est la dimension de la sous-algèbre torique maximale) est appelé le rang de l'algèbre. A la différence du cas classique, les tores maximaux de la p-algèbre de Lie simple L de type Cartan ne sont pas conjugués. Plus précisément, ils se répartissent en $n + 1$ orbites relatives à Aut L, déterminées par l'intersection des tores avec la sous-algèbre invariante L_{inv} (S. P. Démouchkine ; article sous presse). Ce résultat est vrai aussi pour les sous-algèbres de Cartan (normalisateurs des tores maximaux). Pour les algèbres de type Cartan $L(\mathscr{F})$, relatives à un drapeau $\mathscr{F}$ quelconque, la question des classes de conjugaison des tores maximaux reste ouverte. En tout cas, les sous-algèbres de Cartan de $L(\mathscr{F})$ ne sont plus tenues d'avoir la même dimension. Par exemple, l'algèbre $W_1(\mathscr{F})$, dim $W_1(\mathscr{F}) = p^m$, a des sous-algèbres de Cartan de dimensions 1 et p^{m-1}. Comme m'en a informé R. Block à ce congrès, H. Strade a découvert récemment l'existence d'algèbres simples avec des sous-algèbres de Cartan non commutatives. Ce fait était longtemps resté conjectural.

6. Conclusion.

Les idées du paragraphe 3 ont été énoncées sous une forme naïve et pas tout à fait exacte dans mon exposé au congrès de Stockholm de 1962 (cf. [18]) où il était en fait question d'autres problèmes. Finalement, il s'est trouvé que l'idée inattendue d'introduire la sous-algèbre $\mathscr{C}$ est bien compatible avec la construction des algèbres de type Cartan. Les idées de E. Cartan, issues de l'analyse et de la géométrie, ont permis, grâce aux efforts conjugués d'une série d'algébristes, de faire avancer le problème de la classification. Ne me départissant pas de mon optimisme, qui s'est déjà largement manifesté dans les conjectures exprimées ci-dessus, je me permets de formuler le vœu que les travaux de ces huit dernières années permettront d'élaborer le bon cadre dans lequel des recherches à long terme seront possibles.

BIBLIOGRAPHIE

[1] R. Block. — *Bull. Amer. Math. Soc.*, 74, No. 6 (1968), pp. 1086-1090.
[2] E. Cartan. — *Ann. Sci. École Norm. Sup.*, 26 (1909), pp. 93-161.
[3] P. Cartier. — Séminaire « Sophus Lie », 2e année (1955-1956), pp. 307.
[4] C. Chevalley. — *Tohoku Math. J.*, 7 (1955), pp. 14-66.
[5] J. Dieudonné. — *Proc. Internat. Congr. Math.*, Amsterdam (1955).
[6] Sh. Kobayashi and T. Nagano. — Proc. Seminar in dif. geometry, Kyoto, Japan (1965).
[7] I. M. Singer et Sh. Sternberg. — *J. d'analyse Math.*, 15, No. 1 (1965), pp. 4-114.
[8] G. B. Seligman. — Modular Lie algebras, Springer-Verlag (1967).
[9] R. L. Wilson. — Nonclassical simple Lie algebras, A dissertation, Yale Univ. (1969).
[10] Б. Ю. Вейсфейлер. — Бесконечномерные фильтрованные алгебры Ли и их связь с градуированными алгебрами Ли, Функц. анализ и его приложения, №o 1, 2 (1968), 94-95.
[11] В. Г., Кац. — Простые неприводимые градуированные алгебры Ли конечного роста, Изв. АН СССР, сер. матем., 32 (1968), pp. 1323-1367.
[12] —. — О классификации простых алгебр Ли над полем с ненулевой хар., Изв. АН СССР, сер. матем., 34 (1970), pp. 385-408.

[13] А. И. Кострикин, И. Р. Шафаревич. — Псевдогруппы Картана и p-алгебры Ли, Докл. АН СССР, № 4, 168 (1966), pp. 740-742.
[14] —, —. — Градуированные алгебры Ли конечнои хар., Изв. АН СССР, сер. матем., 33 (1969), pp. 251-322.
[15] —. — Теорема о полупростых p-алгебрах Ли, матем. заметки, № 5, 2 (1967), pp. 465-474.
[16] —. — Квадраты присоединенных эндоморфизмов в простых p-алгебрах Ли, Изв. АН СССР, 31 (1967), pp. 445-487.
[17] —. — Параметрическое семейство простых алгебр Ли, Изв. АН СССР, сер. матем., № 4, 34 (1970), pp. 744-756.
[18] —. — Proc. Internat. Congr. Math., 1962.
[19] А. Н. Рудаков. — Изв. АН СССР, сер. матем., 34 (1970), pp. 735-743.
[20] —, И. Р. Шафаревич. — Матем. заметки, вып. 2 (1967), pp. 439-454.

Institut mathématique
V. A. Steklov,
Moscou
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 293 à 296.

PROPERTIES OF COUNTABLE CHARACTER

by B. H. NEUMANN

1. **Preliminaries.**

We deal with algebraic systems, or briefly *algebras*, and abstract classes, or *properties* of algebras: the class $\mathfrak{X}$ is abstract if with an algebra also all its isomorphic copies belong to $\mathfrak{X}$.

As usual we denote by $S\mathfrak{X}$ the class of subalgebras, by $Q\mathfrak{X}$ the class of epimorphic images, by $R\mathfrak{X}$ (" residually $\mathfrak{X}$ ") the class of subcartesian products of algebras in $\mathfrak{X}$; and by $L\mathfrak{X}$ (" locally $\mathfrak{X}$ ") the class of those algebras all of whose finitely generated subalgebras belong to $\mathfrak{X}$. To these we add $C\mathfrak{X}$ (" countably $\mathfrak{X}$ "), which we define to be the class of those algebras all of whose countable subalgebras belong to $\mathfrak{X}$. We say that the property $\mathfrak{X}$ is *of countable character* if $C\mathfrak{X} = \mathfrak{X}$; this is analogous to properties of local character, defined by $L\mathfrak{X} = \mathfrak{X}$. Clearly $CC\mathfrak{X} = C\mathfrak{X}$ and $LL\mathfrak{X} = L\mathfrak{X}$, so that " countably $\mathfrak{X}$ " has countable character and " locally $\mathfrak{X}$ " has local character.

The following assumptions are made once and for all:

(i) All algebras considered belong to a fixed species defined by finitely many finitary operations;
(ii) All algebras are " small ", in the sense that their carriers (or sets of elements) and the finitely iterated power sets of their carriers can be well-ordered.

An immediate consequence of the first assumption is that *countably generated algebras are countable*, and it follows that

$$C\mathfrak{X} \subseteq L\mathfrak{X}. \tag{1}$$

It is easy to see that if $S\mathfrak{X} = \mathfrak{X}$ then $\mathfrak{X} \subseteq C\mathfrak{X}$ and $\mathfrak{X} \subseteq L\mathfrak{X}$; and that always $SC\mathfrak{X} = C\mathfrak{X}$ and $SL\mathfrak{X} = L\mathfrak{X}$; and it then follows that *a property of local character also has countable character*. The converse is not true.

2. **Simple facts.**

The ordered set $(S, \leq)$ is *directed* if every pair of elements of S, and consequently also every finite subset of S, has an upper bound in S. We define $(S, \leq)$ to be *σ-directed* if every countable subset of S has an upper bound in S, or, equivalently, if it is directed and every countable chain in S has an upper bound in S.

The properties of being directed and of being σ-directed are preserved under isotone mappings. The following fact is an immediate consequence of this:

LEMMA. — *Let $(S, \leq)$ be σ-directed, and let $(\omega, \leq)$ be the set $\omega = \{0, 1, 2, \ldots\}$ of non-negative integers in its natural order. If $f\colon S \to \omega$ is an isotone function, then f is bounded.*

This leads at once to the following simple theorems.

THEOREM 1. — *Finiteness is of countable character.*

If $\mathfrak{F}$ denotes the class of finite algebras then clearly $\mathfrak{F} \subseteq C\mathfrak{F}$, so that only $C\mathfrak{F} \subseteq \mathfrak{F}$ need be shown. Let $A \in C\mathfrak{F}$, and denote by S the set of countable subalgebras of A, ordered naturally by the subalgebra relation $\leq$. Then $(S, \leq)$ is σ-directed. For $C \in S$ put $f(C) = |C|$, the order of C. Then f is an isotone mapping of $(S, \leq)$ into $(\omega, \leq)$, hence bounded, say by n. Now $|A| \leq n$; for if A contained $n + 1$ distinct elements, they would generate a countable subalgebra $C \in S$, and then $n + 1 \leq |C| = f(C) \leq n$, which is absurd.

THEOREM 2. — *Let*

$$\mathfrak{V}_0 \subseteq \mathfrak{V}_1 \subseteq \mathfrak{V}_2 \subseteq \ldots$$

be an ascending sequence of properties of countable character, and let $\mathfrak{U}$ be their union. Then $\mathfrak{U}$ also has countable character.

Proof. — As $C\mathfrak{V}_i = \mathfrak{V}_i$ implies $S\mathfrak{V}_i = \mathfrak{V}_i$, we have $S\mathfrak{U} = \mathfrak{U}$, and thus $\mathfrak{U} \subseteq C\mathfrak{U}$, and it only remains to prove the reverse inclusion. Let then $A \in C\mathfrak{U}$ and again denote by S the set of countable subalgebras of A, with the natural order $\leq$, so that $(S, \leq)$ is σ-directed. For $C \in S$ put

$$f(C) = \min\,(i \in \omega \mid C \in \mathfrak{V}_i).$$

Then $f\colon S \to \omega$ is isotone, hence bounded, say by n. Thus $A \in C\mathfrak{V}_n = \mathfrak{V}_n \subseteq \mathfrak{U}$.

Among the applications of this theorem we mention the case that each $\mathfrak{V}_i$ is a variety or a quasivariety; for they are even of local character, while their unions $\mathfrak{U}$ are in general not of local character; for example we have [1]:

COROLLARY. — *Nilpotency, polynilpotency, and solubility of groups are properties of countable character.*

In fact if the $\mathfrak{V}_i$ in Theorem 2 are assumed to be quasivarieties, one can prove a stronger theorem:

THEOREM 3. — *Let*

$$\mathfrak{V}_0 \subseteq \mathfrak{V}_1 \subseteq \mathfrak{V}_2 \subseteq$$

be an ascending sequence of quasivarieties, and let $\mathfrak{U}$ be their union. Then $R\mathfrak{U}$ has countable character.

The proof is not very difficult but lengthy and omitted. Again we obtain as an example [1]:

COROLLARY. — *Residual nilpotency, residual polynilpotency, residual solubility of groups are properties of countable character.*

3. Residual finiteness.

THEOREM 4. — *Residual finiteness is a property of countable character.*

We only sketch the proof, as it is very similar to the proof of the same fact for groups in [1]. If $\mathfrak{F}$ is the class of finite algebras of our given species, then $S\mathfrak{F} = \mathfrak{F}$, hence $SR\mathfrak{F} = R\mathfrak{F}$ and $R\mathfrak{F} \subseteq CR\mathfrak{F}$, and only $CR\mathfrak{F} \subseteq R\mathfrak{F}$ remains to be proved. Let $A \in CR\mathfrak{F}$ and let a, b be two distinct elements of A. Denote by S the set of those countable subalgebras of A that contain a and b, and again order it naturally by $\leq$; then $(S, \leq)$ if σ-directed. If $C \in S$ then there is an algebra $F \in \mathfrak{F}$ and an epimorphism $\eta : C \twoheadrightarrow F$ with $a\eta \neq b\eta$. Denote by $f(C)$ the least integer that occurs here as order of F as η varies. Then f is isotone, hence bounded, say by n.

In every isomorphism class of algebras of order not exceeding n in the given species we choose a representative, and we denote by $\mathfrak{R}_n$ the set of the representatives so chosen and of their subalgebras. We note that assumption (i) in the introduction ensures that $\mathfrak{R}_n$ is finite. Next we consider the set T of finitely generated subalgebras of A that contain a, b, and note that, again as a consequence of assumption (i), $T \subseteq S$. Thus to each $D \in T$ there is an algebra $R \in \mathfrak{R}_n$ and an epimorphism $\eta : D \twoheadrightarrow R$ such that $a\eta \neq b\eta$. This means that the set Γ_D, say, of epimorphisms $\eta : D \twoheadrightarrow R \in \mathfrak{R}_n$ with $a\eta \neq b\eta$ is not empty; it is also finite; for η is completely determined once the images of the members of some set of generators of D in some member of R are specified: but D is generated by a finite set, and there are only finitely many R in $\mathfrak{R}_n$, and each of them is finite. Next we notice that if $D \leq E \in T$ and $\delta \in \Gamma_E$, then $\gamma = \delta \mid D \in \Gamma_D$, and thus there is then a mapping, the restriction mapping, of Γ_E into Γ_D. These mappings, say $\varphi_{ED} : \Gamma_E \to \Gamma_D$, form a coherent inverse system, and by a theorem involving something like well-order, and thus relying on assumption (ii)—say, for example, Steenrod's theorem—the inverse limit is not empty. This leads to the existence of a homomorphism of A to some member of $\mathfrak{R}_n$, say some $\gamma_* : A \twoheadrightarrow R \in \mathfrak{R}_n$, with $a\gamma_* \neq b\gamma_*$. As $a \neq b$ were arbitrary in A, A is indeed residually finite, and the theorem follows.

4. Further results.

If $\mathfrak{G}$ denotes the class of finitely generated algebras, what is $C\mathfrak{G}$? It can not be $\mathfrak{G}$ itself, as $SC\mathfrak{G} = C\mathfrak{G}$ but $S\mathfrak{G} \neq \mathfrak{G}$. Instead one has, almost obviously:

THEOREM 5. — *The class $C\mathfrak{G}$ of algebras whose countable subalgebras are finitely generated is the class of noetherian algebras, that is the class of algebras with maximum condition for subalgebras.*

A noetherian algebra clearly belongs to $C\mathfrak{G}$, as all its subalgebras are finitely generated, hence countable. Conversely a non-noetherian algebra contains a properly ascending chain of subalgebras, which may be assumed finitely generated; and the limit of this chain is countable but not finitely generated, and thus the algebra is not in $C\mathfrak{G}$.

Finally we remark that if $\mathfrak{N}$ denotes the property of being non-simple, that is to say, of possessing congruences that are properly between the identity congruence and the universal congruence, then $C\mathfrak{N} \subseteq \mathfrak{N}$. In fact we have:

THEOREM 6. — *If A is a simple algebra and C a countable subalgebra of A, then C is contained in a simple countable subalgebra D of A.*

We again omit the proof, which is an easy adaptation of that in the case of groups [1]. It is not difficult to see that $C\mathfrak{N} \neq \mathfrak{N}$, and one can also show that $L\mathfrak{N} \nsubseteq \mathfrak{N}$ (see [1]).

REFERENCE

[1] B. H. NEUMANN. — Group properties of countable character, *Algebra i Logika* (to be published).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Box 4, PO,
Canberra, ACT 2600.
(Australie)

Actes, Congrès intern. math., 1970. Tome 1, p. 297 à 300.

SUMS OF SQUARES IN REAL FUNCTION FIELDS

by A. PFISTER

1. **Introduction.**

Let $f(x) = \dfrac{g(x)}{h(x)} \in R(x) = R(x_1, \ldots, x_n)$ be a rational function in n variables with real coefficients. f is called positive definite if

$$f(a) \geqslant 0 \quad \text{for all} \quad a = (a_1, \ldots, a_n) \in R^n \quad \text{with} \quad h(a) \neq 0.$$

Hilbert's problem 17 is the following:

Is every positive definite function f a sum of squares in $R(x)$

This is trivial for $n = 1$ and was proved for $n = 2$ by Hilbert in 1893 [4]. He showed that in this case every positive definite function is a sum of 4 squares. The general n-variable case was settled by E. Artin in 1926 [1]. However, his proof is purely abstract and does not give an estimate for the number of squares needed. In this quantitative direction progress was made in 1966 by J. Ax (unpublished) who showed that positive definite functions in 3 variables are sums of 8 squares. At the same time he simplified the proof for 2 variables and he gave a precise conjecture for the n-variable case, namely that every positive definite function should be a sum of 2^n squares. In 1967 I have been able to prove this conjecture (see [7] or Corollary 1 below).

One of the main ideas of Ax is to make use of a well-known theorem of Tsen [11] which has been rediscovered by Lang [6]:

THEOREM 1. — Let C be an algebraically closed field, let K be a field of transcendence degree n over C. Let f be a form of degree d in more than d^n variables with coefficients in K. Then f has a non-trivial zero in K. In particular, every quadratic form of dimension greater than 2^n has a non-trivial zero.

By means of the abstract theory of so-called multiplicative quadratic forms we can deduce from Theorem 1 the following result about function fields over R:

THEOREM 2. — Let R be a real closed field, let K be an extension field of transcendence degree n over R. Let $\varphi \cong (1, a_1) \otimes \ldots \otimes (1, a_n)$ be a multiplicative quadratic form of dimension 2^n over K and let $b \neq 0$ be a totally positive element of K, i. e. an element which can be represented as a finite sum of squares in K. Then φ represents b over K.

COROLLARY 1. — Let $K = R(x_1, \ldots, x_n)$ and let $f \in K$ be positive definite. Then f is a sum of 2^n squares in K.

Proof. — By Artin's Theorem f is totally positive. By Theorem 2 f is represented by $\varphi \cong (1, 1) \otimes \underset{n\,\text{times}}{\ldots} \otimes (1, 1)$, i. e. f is a sum of 2^n squares.

COROLLARY 2. — Let K be a non-real function field of transcendence degree n over R. Then $\varphi \cong (1, a_1) \otimes \ldots \otimes (1, a_n)$ is universal in K.

Proof. — Every element of K is a sum of squares.

2. **Preliminaries about quadratic forms.**

In this section K can be an arbitrary field of characteristic different from 2. Without restriction quadratic forms over K are assumed to be in diagonal form and non-degenerate. The form $\varphi(x) = \sum_1^n a_i x_i^2$ is abbreviated by $\varphi = (a_1, \ldots, a_n)$, $\prod_1^n a_i \neq 0$. Equivalence is denoted by $\cong$, direct orthogonal sum by $\oplus$, tensor product by $\otimes$. φ is called universal if φ represents every element of K, φ is called isotropic if φ has a non-trivial zero in K.

The following results are well-known:

PROPOSITION 1. — φ represents $b \in K^* \Leftrightarrow \varphi \oplus (-b)$ isotropic.

In particular, every isotropic form is universal.

PROPOSITION 2. — $(a, b) \cong (c, abc)$ for $c = a + b \neq 0$.

We are now able to prove the essential result of this section (see also [8], [10]):

PROPOSITION 3. — Let $n \geqslant 0$, $a_1, \ldots, a_n \in K^*$ and suppose that

$$\varphi \cong (1, a_1) \otimes \ldots \otimes (1, a_n).$$

Then φ is multiplicative in the following sense: If $c \in K^*$ is represented by φ then $\varphi \cong c\varphi$.

Proof. — By induction on n:

The case $n = 0$, $\varphi = (1)$ is trivial.

Suppose now that Proposition 3 is true for φ and let us prove it for

$$\psi = \varphi \otimes (1, a_{n+1}) \cong \varphi \oplus a_{n+1}\varphi.$$

An element c which is represented by ψ can be written in the form $c = a + a_{n+1}b$ where a and b are represented by φ. The cases $a = 0$ or $b = 0$ are done by the induction hypothesis. Suppose now $ab \neq 0$. Using Proposition 2 we have

$$\psi \cong \varphi \oplus a_{n+1}\varphi \cong a\varphi \oplus a_{n+1}b\varphi \cong (a, a_{n+1}b) \otimes \varphi \cong (c, caa_{n+1}b) \otimes \varphi$$
$$\cong c\varphi \oplus ca_{n+1}ab\varphi \cong c\varphi \oplus ca_{n+1}\varphi \cong c\psi.$$

COROLLARY. — Let $G_k(K) = \{ c \in K^* : c \text{ is a sum of } k \text{ squares in } K \}$. If $k = 2^n$ is a power of 2 then G_k is a subgroup of K^*.

For later application we also need:

LEMMA. — Let $\varphi \cong (1, a_1) \otimes \ldots \otimes (1, a_n) \cong (1) \oplus \varphi'$ and let $b_1 \in K^*$ by represented by φ'. Then there exist $b_2, \ldots, b_n \in K^*$ such that $\varphi \cong (1, b_1) \otimes \ldots \otimes (1, b_n)$.

Proof. — See [8] or [10].

3. Proof of theorem 2.

a) We may suppose that φ is anisotropic since otherwise φ is universal which immediately gives the result. Also the case $b = b_1^2$ is trivial. We will first treat the case $b = b_1^2 + b_2^2$, $b_1 b_2 \neq 0$. By Tsen's Theorem we know that φ is universal over the field $K(i) = K(\sqrt{-1})$. If $K = K(i)$ then the result follows. If not, then $\beta = b_1 + ib_2$ generates $K(i)$ over K and φ represents β over $K(i)$. This shows that there are vectors u, v with components in K such that $\varphi(u + \beta v) = \beta$, $v \neq 0$. Hence

$$\varphi(u) + 2\beta \langle u, v \rangle_\varphi + \beta^2 \varphi(v) = \beta.$$

Comparing with $\beta^2 - 2b_1\beta + b = 0$ we find $\varphi(u) - b\varphi(v) = 0$ (and

$$2 \langle u, v \rangle_\varphi + 2b_1 \varphi(v) = 1).$$

Since φ is multiplicative this gives the result.

b) We will now suppose that Theorem 2 holds for all forms φ of the given type and for all elements $b \in K^*$ which are sums of k squares ($k \geqslant 2$) and will proceed by induction on k. Up to a square factor a sum of $k + 1$ squares looks like $c = 1 + b$ where b is a sum of k squares. Putting $\varphi = (1) \oplus \varphi'$ the induction hypothesis gives $b = b_1^2 + b_2$ where b_2 is represented by φ', and without restriction $b_2 \neq 0$. We want to show that φ represents c.

Consider the form $\psi = \varphi \otimes (1, -c) = (1) \oplus \varphi' \oplus (-c\varphi) = (1) \oplus \psi'$. ψ' represents $b_2 - c = (b - b_1^2) - (1 + b) = -1 - b_1^2$. By the Lemma we have therefore $\psi \cong (1, -1 - b_1^2) \otimes \chi$ with a form $\chi \cong (1, c_1) \otimes \ldots \otimes (1, c_n)$. Applying the induction hypothesis to χ we have χ represents $1 + b_1^2$. Hence $\psi \cong \varphi \oplus (-c\varphi)$ is isotropic. Therefore $\varphi(u) - c\varphi(v) = 0$ with non-zero vectors u, v over K. Since φ is anisotropic and multiplicative it follows that φ represents c over K.

4. Open problems.

If K is a field, denote by $t = t(K)$ the minimal number such that every sum of squares in K is already a sum of t squares (Of course t may be infinite).

PROBLEM 1. — Corollary 1 of Theorem 2 shows that $t(R(x_1, \ldots, x_n)) \leqslant 2^n$. On the other hand a theorem of Cassels [2] shows that $1 + x_1^2 + \ldots + x_n^2$ is not a sum of n squares in $R(x_1, \ldots, x_n)$, hence $t \geqslant n + 1$. What is the true value of $t(R(x_1, \ldots, x_n))$?

Recently it has been shown [3] that $t(R(x_1, x_2)) = 4$, but the method is special to the case $n = 2$.

PROBLEM 2. — Let K be as in Corollary 2 of Theorem 2. Is every quadratic form φ of dimension 2^n universal in K?

PROBLEM 3. — Replace R by the field Q of rational numbers. Is $t(Q(x_1, \ldots, x_n))$ bounded by some function of n?

The only known results in this direction are: $t(Q) = 4$ (Theorem of Lagrange), $t(Q(x)) = 5$ (Landau [5], Pourchet [9]).

REFERENCES

[1] E. ARTIN. — Über die Zerlegung definiter Funktionen in Quadrate, *Hamb. Abh.*, 5, (1927), pp. 100-115 (Collected Papers, pp. 273-288).

[2] J. W. S. CASSELS. — On the representation of rational functions as sums of squares, *Acta Arithm.*, 9 (1964), pp. 79-82.

[3] —, W. J. ELLISON and A. PFISTER. — On sums of squares and on elliptic curves over function fields. To appear in *J. of Number Theory*.

[4] D. HILBERT. — Über ternäre definite Formen, *Acta Math.*, 17 (1893), pp. 169-197; *Ges. Abh.*, II, pp. 345-366.

[5] E. LANDAU. — Über die Darstellung definiter Funktionen durch Quadrate, *Math. Ann.*, 62 (1906), pp. 272-285.

[6] S. LANG. — On quasi-algebraic closure, *Ann. of Math.*, 55 (1952), pp. 373-390.

[7] A. PFISTER. — Zur Darstellung definiter Funktionen als Summe von Quadraten, *Invent. math.*, 4 (1967), pp. 229-237.

[8] —. — Quadratic forms over fields. To appear in vol. 20 of *Proc. of Symposia in Pure Mathematics.*

[9] Y. POURCHET. — Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *A paraître.*

[10] W. SCHARLAU. — Quadratic Forms, *Queen's Papers on Pure and Applied Mathematics*, No. 22, Kingston, Ontario (1969).

[11] C. TSEN. — Zur Stufentheorie der Quasi-algebraisch-Abgeschlossenheit kommutativer Körper, *J. Chinese Math. Soc.*, 1 (1936), pp. 81-92.

Mathematisches Institut
der Universität
Saasstrasse 21, Postfach 3980
65-Mainz
(République Fédérale Allemande)

Actes, Congrès intern. math., 1970. Tome 1, p. 301 à 308.

B_2 - CATÉGORIES - ALGÈBRE HOMOLOGIQUE

HOMOLOGIE DES ALGÈBRES COMMUTATIVES

par MICHEL ANDRÉ

A une A-algèbre commutative B, on sait associer un complexe de B-modules $L_{B/A}$ défini à une homotopie près. Ce complexe peut être utilisé pour définir des groupes d'homologie $H_n(A, B, W)$ et des groupes de cohomologie $H^n(A, B, W)$ en présence d'un B-module W. Pour le faire on considère simplement l'homologie des deux complexes suivants :

$$L_{B/A} \otimes_B W \qquad \text{et} \qquad \mathrm{Hom}_B(L_{B/A}, W).$$

La définition du complexe $L_{B/A}$ utilisée par D. Quillen [9] et l'auteur [1] permet de donner aux groupes d'homologie deux propriétés essentielles, aussi importantes que la suite exacte et la propriété d'excision pour les groupes relatifs en homologie singulière. D'une part il existe une suite exacte $*$

$$\ldots \to H_n(A, B, W) \to H_n(A, C, W) \to H_n(B, C, W) \\ \to H_{n-1}(A, B, W) \ldots \to H_0(B, C, W) \to 0$$

en présence d'une A-algèbre commutative B, d'une B-algèbre commutative C et d'un C-module W. D'autre part il existe un isomorphisme naturel $**$

$$H_n(A, B, W) \oplus H_n(A, C, W) \cong H_n(A, B \otimes_A C, W)$$

en présence de deux A-algèbres commutatives B et C et d'un $B \otimes_A C$-module W et cela sous la condition

$$\mathrm{Tor}_i^A(B, C) = 0 \qquad i = 1, 2, \ldots, n.$$

A l'aide de ces deux propriétés, de quelques suites spectrales et de résultats concernant les basses dimensions, il est possible de développer une théorie assez complète de l'homologie des anneaux commutatifs. D. Quillen a publié un premier résumé de cette théorie [8]. A un niveau plus élémentaire, l'auteur a publié des notes [2] qui contiennent une bibliographie relativement complète du sujet. On peut considérer les pages suivantes comme une suite du résumé de D. Quillen.

1. **Anneau gradué associé.**

Si l'on excepte les dimensions 0 et 1, tous les groupes d'homologie peuvent se ramener au type suivant : $H_n(A, A/I, W)$ où A est un anneau commutatif quelconque, où I est un idéal de A quelconque et où W est un A/I-module quelconque. Le foncteur Tor est apparu une première fois à propos de l'isomorphisme $**$ de l'introduction, il apparaît une deuxième fois dans la suite spectrale de D. Quillen (section 6 de [8]), suite spectrale qui joue un rôle important dans l'étude de $H_*(A, A/I, W)$.

THÉORÈME 1.1. — *Soient un anneau A et un idéal I et considérons $B = A/I$. Alors il existe une suite spectrale*

$$E^2_{pq} = H_{p+q}[S^B_q L_{B/A}] \Rightarrow \mathrm{Tor}^A_n(B, B)$$

où S^B_q est la q-ième composante du foncteur « algèbre symétrique » S^B de la catégorie des B-modules dans la catégorie des B-algèbres.

Le corollaire suivant de ce théorème sera utilisé ci-dessous.

COROLLAIRE 1.2. — *Soient un anneau A et un idéal I tels que le A/I-module I/I^2 soit projectif. Alors l'algèbre graduée $\mathrm{Tor}^A_*(A/I, A/I)$ est isomorphe à l'algèbre extérieure du A/I-module $\mathrm{Tor}^A_*(A/I, A/I) \cong I/I^2$ si et seulement si les groupes d'homologie $H_n(A, A/I, A/I)$ sont nuls sauf en dimension $n = 1$.*

Considérons toujours un anneau A et un idéal I et en outre l'anneau gradué associé

$$\mathrm{Gr}(A) = \sum_{n \geq 0} I^n/I^{n+1}.$$

En géométrie algébrique, on sait passer de la A-algèbre A/I à la $\mathrm{Gr}(A)$-algèbre A/I et inversement. En particulier il existe une suite spectrale (voir la p. II-17 de [10]), qui converge vers le module gradué $\mathrm{Tor}^A_*(A/I, A/I)$ et dont le terme E^1 jouit de la propriété suivante

$$\sum_{p+q=n} E^1_{pq} = \mathrm{Tor}^{\mathrm{Gr}(A)}_n(A/I, A/I).$$

Il existe un résultat analogue pour les groupes d'homologie étudiés ici (proposition 23.8 de [1]).

PROPOSITION 1.3. — *Soient un anneau noethérien A et un idéal I. Alors il existe une suite spectrale qui converge vers $H_*(A, A/I, A/I)$ et dont le terme E^1 satisfait à l'égalité suivante*

$$\sum_{p+q=n} E^1_{pq} = H_n(\mathrm{Gr}(A), A/I, A/I)$$

Il est assez difficile d'utiliser cette suite spectrale. On obtient de meilleurs résultats si l'on approche l'anneau A non pas par l'anneau $\mathrm{Gr}(A)$ mais par l'ensemble des anneaux A/I^k. En bref : on répète pour la cohomologie des anneaux munis de topologies adiques ce qui se fait classiquement pour la cohomologie des groupes topologiques totalement discontinus, les anneaux noethériens correspondant aux groupes discrets. On considère donc un anneau A, un idéal I et un A/I-module W et pour chaque $n \geq 0$, on définit un nouveau groupe de cohomologie

$$\tilde{H}^n(A, A/I, W) = \lim_{k \to \infty} H^n(A/I^k, A/I, W)$$

qui doit approcher le groupe de cohomologie $H^n(A, A/I, W)$ dans une certaine mesure. Pour la définition de $\tilde{H}^n$, on a utilisé le fait que H^n est un foncteur contravariant de la première variable.

Dans l'introduction, il a été question d'un isomorphisme naturel pour l'homologie et dualement pour la cohomologie

$$H^n(A, B \otimes_A C, W) \cong H^n(A, B, W) \oplus H^n(A, C, W)$$

si l'égalité suivante est satisfaite

$$\operatorname{Tor}_i^A(B, C) = 0 \qquad i = 1, 2, \ldots, n.$$

Ce résultat peut être généralisé.

PROPOSITION 1.4. — *Soit un diagramme commutatif d'homomorphismes d'anneaux*

$$\begin{array}{ccccccccc} B = B_0 & \to & B_1 & \to & \ldots & B_{n-1} & \to & B_n = B' \\ \uparrow & & \uparrow & & & \uparrow & & \uparrow \\ A = A_0 & \to & A_1 & \to & \ldots & A_{n-1} & \to & A_n = A' \\ \downarrow & & \downarrow & & & \downarrow & & \downarrow \\ C = C_0 & \to & C_1 & \to & \ldots & C_{n-1} & \to & C_n = C' \end{array}$$

Supposons nul l'homomorphisme

$$\operatorname{Tor}_i^{A_{i-1}}(B_{i-1}, C_{i-1}) \to \operatorname{Tor}_i^{A_i}(B_i, C_i)$$

pour $i = 1, 2, \ldots, n$. *Soit* W *un* $B' \otimes_{A'} C'$*-module. Alors le carré commutatif suivant composé d'homomorphismes naturels peut être complété d'une diagonale* Δ

$$\begin{tikzcd} H^n(A', B' \otimes_{A'} C', W) \arrow[r] \arrow[d] & H^n(A', B', W) \oplus H^n(A', C', W) \arrow[d] \arrow[dl, "\Delta"'] \\ H^n(A, B \otimes_A C, W) \arrow[r] & H^n(A, B, W) \oplus H^n(A, C, W). \end{tikzcd}$$

Considérons toujours un anneau A et un idéal I. Une résolution d'Artin-Rees d'un A-module M est une résolution projective de ce module

$$\ldots \xrightarrow{d} P_n \xrightarrow{d} P_{n-1} \xrightarrow{d} \ldots P_1 \xrightarrow{d} P_0$$

qui jouit de la propriété suivante : pour tout $n \geqslant 0$ et pour tout $k \geqslant 0$, il existe un $l = l(k, n) \geqslant k$ avec

$$(I^l P_n) \cap (dP_{n+1}) \subset I^k(dP_{n+1}).$$

Il revient au même d'affirmer que l'homomorphisme naturel

$$\operatorname{Tor}_{n+1}^A(M, A/I^l) \to \operatorname{Tor}_{n+1}^A(M, A/I^k)$$

est nul. Si le module M possède une résolution d'Artin-Rees, alors toute résolution projective de ce module est une résolution d'Artin-Rees. En particulier un module de type fini sur un anneau noethérien possède une résolution d'Artin-Rees.

Lorsque le A-module A/I possède une résolution d'Artin-Rees, on peut faire usage de la proposition 1.4 et démontrer que l'homomorphisme naturel

$$H^n(A, A/I^r, W) \to H^n(A, A/I^s, W)$$

est nul pour s suffisamment grand par rapport à r. On a donc l'égalité suivante

$$\lim_{k \to \infty} H^n(A, A/I^k, W) = 0$$

Par l'intermédiaire de la suite exacte $*$ de l'introduction pour chacune des situations suivantes

$$A \to A/I^k \to A/I$$

de l'égalité ci-dessus découle un isomorphisme

$$\lim_{k\to\infty} H^n(A/I^k, A/I, W) \cong H^n(A, A/I, W)$$

THÉORÈME 1.5. — *Soient un anneau A et un idéal I. Supposons que le A-module I possède une résolution d'Artin-Rees. Alors l'homomorphisme naturel*

$$\tilde{H}^n(A, A/I, W) \to H^n(A, A/I, W)$$

est un isomorphisme pour tout $n \geqslant 0$ et pour tout A/I-module W.

En particulier pour un anneau A noethérien, on a toujours un isomorphisme

$$\tilde{H}^n(A, A/I, W) \cong H^n(A, A/I, W)$$

On peut aussi démontrer le théorème précédent en utilisant la suite spectrale du théorème 1.1 (voir le théorème 6.15 de [8]).

Il est possible de calculer les deuxièmes groupes d'homologie grace à l'égalité

$$H_2(A, A/I, W) \cong \mathrm{Tor}_2^A(A/I, W)/\mathrm{Tor}_1^A(A/I, A/I).\mathrm{Tor}_1^A(A/I, W).$$

Par conséquent (d'après un résultat de S. Eilenberg) un anneau local et noethérien A d'idéal maximal I est régulier si et seulement si le groupe $H_2(A, A/I, A/I)$ est nul. Il est possible de généraliser ce résultat en prenant soin d'utiliser les groupes de cohomologie $\tilde{H}^n$.

THÉORÈME 1.6. — *Soient un anneau A et un idéal I. Alors les trois conditions suivantes sont équivalentes:*

1. *le A/I-module I/I^2 est projectif et la A/I-algèbre graduée* Gr (A) *est isomorphe à l'algèbre symétrique du A/I-module I/I^2,*
2. *le groupe $\tilde{H}^2(A, A/I, W)$ est nul pour tout A/I-module W,*
3. *le groupe $\tilde{H}^n(A, A/I, W)$ est nul pour tout $n \neq 1$ et pour tout A/I-module W.*

La démonstration utilise les deux propriétés fondamentales $*$ et $**$ décrites dans l'introduction et aussi l'égalité suivante

$$H^1(A, A/I^k, W) \cong \mathrm{Hom}_{A/I}(I^k/I^{k+1}, W).$$

En fait toute la démonstration est basée sur un diagramme commutatif

$$\begin{array}{ccc} B & \to & B/J \\ \downarrow & & \downarrow \\ A & \to & A/I \end{array} \qquad \text{avec} \qquad A \otimes_B B/J \cong A/I$$

où l'anneau B et l'idéal J sont suffisamment simples pour que la cohomologie de la B-algèbre B/J soit triviale. A vrai dire le procédé fonctionne parfaitement seulement sous certaines conditions: par exemple A local noethérien ou encore I nilpotent. On est amené à remplacer l'anneau A et l'idéal I par la famille des anneaux A/I^k et des idéaux nilpotents I/I^k. Comme conséquence il faut remplacer le groupe

$H^n(A, A/I, W)$ par l'ensemble des groupes $H^n(A/I^k, A/I, W)$. Une démonstration complète se trouve dans [2], pages 212-229.

COROLLAIRE 1.7. — *Soit une algèbre topologique A sur un anneau topologique C. Supposons que la topologie de A est donnée par un idéal I et que la C-algèbre topologique discrète A/I est formellement lisse. Alors la C-algèbre topologique A est formellement lisse si et seulement si le A/I-module I/I^2 est projectif et donne une algèbre symétrique qui est isomorphe à la A/I-algèbre graduée* Gr (A).

Il suffit de démontrer que l'hypothèse de lissité pour la C-algèbre A/I implique l'existence d'un isomorphisme

$$\text{Exalcotop}\, C(A, W) \cong \tilde{H}^2(A, A/I, W).$$

Pour une démonstration directe de ce corollaire on se reporte au corollaire 19.5.4 de [4].

Il est possible de résumer les résultats précédents à l'aide d'une proposition dont la démonstration fait usage de la proposition 1.2, du théorème 1.5 et du théorème 1.6.

PROPOSITION 1.8. — *Soient un anneau A et un idéal I tels que le A/I-module I/I^2 soit projectif. Alors les quatre conditions suivantes sont équivalentes :*

1. *l'algèbre graduée* $\mathrm{Tor}_*^A(A/I, A/I)$ *est isomorphe à l'algèbre extérieure du A/I-module* $\mathrm{Tor}_1^A(A/I, A/I) \cong I/I^2$,
2. *l'algèbre graduée* Gr (A) *est isomorphe à l'algèbre symétrique du A/I-module I/I^2 et le A-module I possède une résolution d'Artin-Rees,*
3. *le groupe $H_2(A, A/I, A/I)$ est nul et le A-module I possède une résolution d'Artin-Rees,*
4. *le groupe $H_n(A, A/I, W)$ est nul pour tout $n \neq 1$ et pour tout A/I-module W.*

2. **Basses dimensions.**

Il a déjà été question de l'isomorphisme suivant qui, entre autre, permet d'identifier nos deuxièmes groupes d'homologie avec ceux de Lichtenbaum-Schlessinger [7] :

$$H_2(A, A/I, W) \cong \mathrm{Tor}_2^A(A/I, W)/\mathrm{Tor}_1^A(A/I, A/I) . \mathrm{Tor}_1^A(A/I, W).$$

On peut démontrer le résultat suivant qui en fait ne concerne que des algèbres et modules gradués Tor.

THÉORÈME 2.1. — *Soient un anneau B et un idéal J, un anneau A avec un idéal I et un homomorphisme de B dans A qui envoie J dans I. Alors il existe une suite exacte naturelle*

$$H_2(B, B/J, A/I) \to H_2(A, A/JA, A/I) \to \mathrm{Tor}_1^B(B/J, A)/I\, \mathrm{Tor}_1^B(B/J, A) \to$$
$$H_1(B, B/J, A/I) \to H_1(A, A/JA, A/I) \to 0.$$

Si A est un anneau local d'idéal maximal I et si $\underline{x} = (x_1, \ldots, x_n)$ est un système minimal de générateurs d'un idéal K de l'anneau A, alors on peut choisir un anneau B

et un idéal J avec $JA = K$ comme dans la démonstration du théorème 1.6 et la suite exacte ci-dessus donne un isomorphisme

$$H_2(A, A/K, A/I) \cong H_1(\underline{x}, A)/IH_1(\underline{x}, A)$$

où $H_1(\underline{x}, A)$ désigne le premier groupe d'homologie de Koszul pour l'ensemble $\underline{x}$ d'éléments de A et pour le A-module A. Cet isomorphisme démontre de manière immédiate le cas particulier du théorème 1.6 dû à S. Eilenberg et mentionné ci-dessus.

COROLLAIRE 2.2. — *Soient un anneau B, local et noethérien, d'idéal maximal J, un anneau A, local et noethérien, d'idéal maximal I et un homomorphisme de B dans A qui envoie J dans I. On munit B de la topologie J-adique, B/J de la topologie discrète, A de la topologie I-adique et A/JA de la topologie I/JA-adique. Alors la B-algèbre A est formellement lisse si et seulement si d'une part la B/J-algèbre A/JA est formellement lisse et d'autre part le B-module A est plat.*

Il s'agit du théorème 19.7.1 de [4]. D'après le théorème 1.5 et l'égalité des foncteurs H^1 et Exalcom, on sait que la B-algèbre A (respectivement la B/J-algèbre A/JA) est formellement lisse si et seulement si le groupe $H_1(B, A, A/I)$ (respectivement le groupe $H_1(B/J, A/JA, A/I)$) est nul. L'homomorphisme naturel de ce groupe-là dans ce groupe-ci est un épimorphisme et même un isomorphisme si le B-module A est plat, d'après les propriétés $*$ et $**$. Il reste donc à démontrer que le B-module A est plat si la B-algèbre A et la B/J-algèbre A/JA sont formellement lisses. Si les groupes $H_1(B, A, A/I)$ et $H_1(B/J, A/JA, A/I)$ sont nuls, alors l'homomorphisme naturel de $H_n(B, B/J, A/I)$ dans $H_n(A, A/JA, A/I)$ est une monomorphisme pour $n = 1$ et un épimorphisme pour $n = 2$. D'après la suite exacte du théorème précédent le groupe $\mathrm{Tor}_1^B(B/J, A)$ est donc nul. Le B-module A est idéalement séparé, il est donc plat d'après le critère de platitude.

Sur un corps de caractéristique 0, une algèbre est formellement lisse si et seulement si elle est régulière. En caractéristique positive, on a le théorème 22.5.8 de [4] qui est un corollaire du résultat suivant.

THÉORÈME 2.3. — *Soit A une algèbre locale et noethérienne sur un corps K de caractéristique p. Alors il existe un isomorphisme naturel*

$$H_1(K, A, R) \otimes_R T \cong H_2(A \otimes_K K^{1/p}, T, T)$$

où R désigne le corps résiduel de l'anneau local A et T celui de l'anneau local $A \otimes_K K^{1/p}$. Soit L une extension de degré fini du corps K, contenue dans le corps $K^{1/p}$. Alors il existe un monomorphisme naturel

$$H_2(A \otimes_K L, S, S) \otimes_S T \to H_2(A \otimes_K K^{1/p}, T, T)$$

où S désigne le corps résiduel de l'anneau local et noethérien $A \otimes_K L$. En outre la réunion des images des monomorphismes précédents est égale à $H_2(A \otimes_K K^{1/p}, T, T)$ tout entier.

On démontre la première partie du théorème à l'aide des propriétés $*$ et $**$ et du diagramme commutatif suivant

$$\begin{tikzcd}
H_2(K^{1/p}, T, T) \arrow[d] & H_1(K, A, T) \arrow[r] \arrow[d] & H_1(K, T, T) \arrow[d] \\
H_2(A \otimes_K K^{1/p}, T, T) \arrow[r] & H_1(K^{1/p}, A \otimes_K K^{1/p}, T) \arrow[r] & H_1(K^{1/p}, T, T).
\end{tikzcd}$$

Dans la démonstration de la deuxième partie du théorème on utilise le fait que les deuxièmes et troisièmes groupes d'homologie d'une extension de corps sont nuls. Dans la démonstration de la troisième partie du théorème on utilise le fait que l'homologie des algèbres commute aux limites filtrantes.

COROLLAIRE 2.4. — *Soit A une algèbre locale et noethérienne sur un corps K de caractéristique p. On munit K de la topologie discrète et A de la topologie I-adique, I étant l'idéal maximal de l'anneau local A. Alors la K-algèbre topologique A est formellement lisse si et seulement si pour toute extension L de degré fini du corps K, contenue dans le corps* $K^{1/p}$, *l'anneau local et noethérien* $A \otimes_K L$ *est régulier.*

La K-algèbre A est formellement lisse si et seulement si $H_1(K, A, R)$ est nul et l'anneau $A \otimes_K L$ est régulier si et seulement si $H_2(A \otimes_K L, S, S)$ est nul, d'après les théorèmes 1.5 et 1.6.

PROPOSITION 2.5. — *Soient deux corps* $K \subset M$. *Alors l'espace vectoriel* $H_n(K, M, M)$ *est nul pour n différent de* 0 *et de* 1. *L'espace vectoriel* $H_1(K, M, M)$ *est nul si et seulement si l'extension* M/K *est séparable. Dans le cas d'une extension de type fini, son degré de transcendance est égal à la différence de Cartier*

$$\operatorname{rg} H_0(K, M, M) - \operatorname{rg} H_1(K, M, M).$$

Lorsque l'extension M/K est monogène alors ou bien l'anneau M est le quotient d'une K-algèbre libre par un idéal principal (cas algébrique) ou bien l'anneau M est le corps des quotients d'une K-algèbre libre (cas transcendant). Cette remarque permet de démontrer les première et troisième parties de la proposition dans ce cas particulier. Le cas général est obtenu à l'aide de suites exactes $*$ et de limites filtrantes. On démontre la deuxième partie de la proposition comme suit. D'après le théorème 2.3, le groupe $H_1(K, M, M)$ est nul si et seulement si chacun des anneaux locaux et noethériens $M \otimes_K L$ est régulier. L'idéal maximal de $M \otimes_K L$ est formé des éléments nilpotents. L'anneau $M \otimes_K L$ est régulier si et seulement s'il s'agit d'un corps. Donc le groupe $H_1(K, M, M)$ est nul si et seulement si $M \otimes_K K^{1/p}$ est un corps, ou encore d'après le critère de MacLane, si et seulement si l'extension M/K est séparable.

Le fait que le groupe $H_n(K, M, M)$ est toujours nul pour $n = 2$ et est nul pour $n = 1$ si et seulement si l'extension est séparable démontre le résultat de Gerstenhaber-Knudson : la K-algèbre M est une algèbre commutative rigide si et seulement si l'extension est séparable.

Terminons par une généralisation du théorème 5.3 de [5]. On démontre de manière analogue une généralisation du théorème 5.2 de [5] : la condition de finitude semble nécessaire pour pouvoir passer de la lissité pour une topologie adique à la lissité pour une topologie discrète.

PROPOSITION 2.6. — *Soient deux corps* $K \subset M$. *Alors l'algèbre graduée* $\operatorname{Tor}_*^{M \otimes_K M}(M, M)$ *est isomorphe à l'algèbre extérieure de l'espace vectoriel sur M des différentielles de Kaehler de la K-algèbre M si et seulement si l'extension* M/K *est séparable.*

Pour la démonstration, on utilise les propositions 1.8 et 2.5 et les isomorphismes suivants

$$H_{n+1}(M \otimes_K M, M, M) \cong H_n(M, M \otimes_K M, M) \cong H_n(K, M, M).$$

On peut trouver dans les travaux [3] et [6] deux aspects de la théorie de l'homologie des anneaux commutatifs, deux aspects qui n'ont pas pu être traités dans ce résumé.

BIBLIOGRAPHIE

[1] M. ANDRÉ. — Méthode simpliciale en algèbre homologique et algèbre commutative, Springer *Lecture Notes*, 32 (1967).

[2] —. — Rapport sur l'homologie des algèbres commutatives, *Notes Battelle* (1970).

[3] —. — L'algèbre de Lie d'un anneau local. Symposia Mathematica Istituto Nazionale di Alta, *Matematica*, 4 (1970), pp. 337-375.

[4] A. GROTHENDIECK. — Éléments de géométrie algébrique. IV. Première partie. *Publications Mathématiques I. H. E. S.*, 20 (1964).

[5] G. HOCHSCHILD, B. KONSTANT and A. ROSENBERG. — Differential forms on regular affine algebras, *Trans. Amer. Math. Soc.*, 102 (1962), pp. 383-408.

[6] L. ILLUSIE. — Complexe cotangent relatif d'un faisceau d'algèbres, *C. R. Acad. Sci.* (Paris), 268 (1969), pp. 278-281 et 323-326.

[7] S. LICHTENBAUM and M. SCHLESSINGER. — The cotangent complex of a morphism, *Trans. Amer. Math. Soc.*, 128 (1967), pp. 41-70.

[8] D. QUILLEN. — On the (co)-homology of commutative rings, *Proceedings of Symposia in Pure Mathematica A. M. S.*, 17 (1970), pp. 65-87.

[9] —. — On the homology of commutative rings, *Notes M. I. T.* (1967).

[10] J.-P. SERRE. — Algèbre locale. Multiplicités. Springer *Lecture Notes*, 11 (1965).

Département de Mathématiques
École Polytechnique Fédérale
Lausanne (Suisse).

Actes, Congrès intern. math., 1970. Tome 1, p. 309 à 312.

NON-ABELIAN FULL EMBEDDING: OUTLINE

by MICHAEL BARR

1. Introduction.

If exactness is properly defined it is possible to formulate the theorems of Freyd-Heron-Lubkin and Mitchell in the following way (see [Fr] and [Mi]).

THEOREM (Freyd-Heron-Lubkin). — Let $\underline{X}$ be a small abelian category. Then there is an exact, isomorphism reflecting embedding $\underline{X} \to \underline{S}$, the category of sets.

THEOREM (Mitchell). — Let $\underline{X}$ be a small abelian category. Then there is a monoid M and a full exact embedding $\underline{X} \to \underline{S}^M$, the category of M-sets.

The definition of exactness used here is as follows.

DEFINITION. — Let $\underline{X}$ be a category with finite limits. A morphism $f: X \to X'$ of $\underline{X}$ is called a regular epimorphism if the sequence $X \underset{f}{\times} X \rightrightarrows X \to X'$ is a coequalizer diagram, where, of course, $X \underset{f}{\times} X$ is the kernel pair of f. If $U: \underline{X} \to \underline{Y}$ is a functor we say that U is exact if U preserves finite limits (= projective limits) and regular epimorphisms. We call it reflexively exact if it preserves and reflects them.

From this definition, such a functor $\underline{X} \to \underline{S}$ lifts uniquely, when $\underline{X}$ is additive, through $\underline{Ab}$, the category of abelian groups by virtue of preserving finite products. When X is abelian moreover, this definition of exactness translates to the usual definition of exactness of the lifted functor. Similar remarks apply to $\underline{S}^M$ and $\underline{Ab}^M$. Thus the usual formulations of these theorems are readily recovered.

The point of this paper is to show that by a suitable reformulation it is possible to prove analogous results for categories which are not additive but which satisfy " exactness " type properties. As I am not entirely convinced that this is the most appropriate definition, I avoid elevating this to the status of a definition.

We must define one more notion. An object $\phi \in \underline{X}$ is called an empty object if it is initial and if any map to ϕ is an isomorphism.

2. Statement of the theorem.

THEOREM. — Suppose the small category $\underline{X}$ has finite inverse limits and that the kernel pair of every map have a coequalizer. Then the following are equivalent.

1. There is a monoid M and a full, faithful exact functor $\underline{X} \to \underline{S}^M$.

2. There is a faithful reflexively exact functor $\underline{X} \to \underline{S}$.

3. *a*) For any non-empty object X of $\underline{X}$, the terminal morphism $X \to 1$ is a regular epi.

b) In any pullback diagram

$$\begin{tikzcd} & \bullet \arrow[dr] & \\ \bullet \arrow[ur, "f'"] \arrow[dr] & & \bullet \\ & \bullet \arrow[ur, "f"'] & \end{tikzcd}$$

f regular epi implies f' regular epi.

A full embedding reflects isomorphisms and an exact functor reflects isomorphisms if and only if it is reflexively exact. From this remark, $1 \Rightarrow 2$ and $2 \Rightarrow 3$ are easy. Thus the main interest is $3 \Rightarrow 1$. We will sketch the main argument here. The full paper will appear elsewhere.

In unpublished work, M. Tierney has shown that an additive category is abelian if and only if it satisfies $3b$ together with the condition that every equivalence is effective. It is easy to see that $3a$ is automatic in the additive case so that this theorem is in fact a proper generalization of the above mentioned theorems. The example of torsion free abelian groups (in a small universe) shows that the generalization is proper. In addition it shows that in an additive-but-not-abelian category exactness may not coincide with the usual idea (of preserving all finite limits and colimits).

3. **Outline of proof.**

For convenience use the term *diagram in* $\underline{X}$ to mean a functor with codomain $\underline{X}$. If $D : \underline{I} \to \underline{X}$ we will either say that D is a diagram or that $(\underline{I}, D)$ is a diagram. If $(\underline{I}, D)$ is a diagram and $X \in \underline{X}$, define $(D, X) = \operatorname{colim}(Di, X)$, the colimit taken over $i \in \underline{I}$. If $(\underline{I}, D)$ and $(\underline{J}, E)$ are two diagrams then define $(D, E) = \lim (D, Ej)$ the limit taken over $j \in \underline{J}$. Explicitly, a map $D \to E$ is represented by choosing a function σ : objects $\underline{J} \to$ objects $\underline{I}$ together with a map $fj : D\sigma j \to Ej$ for each $j \in \underline{J}$ subject to the coherence condition required by lim and the equivalence relation entailed by colim. With this definition it is obvious how to compose representations of morphisms between diagrams and we can show that this gives a category Diag $\underline{X}$. There is an obvious full embedding $\underline{X} \to$ Diag $\underline{X}$ in which X goes to the singleton diagram X. It is not hard to show that Diag $\underline{X}$ is precisely the opposite category to the functor category $(\underline{X}, \underline{S})$. However, for the purposes of this proof, it is much easier to deal directly with diagrams than with functors.

At this point we must interpose a recent result of M. Tierney (unpublished).

THEOREM. — If a category $\underline{X}$ has finite limits, if the kernel pair of any map have a coequalizer and if condition $3b$ of the main theorem is satisfied, then the regular epis and monos give a factorization system.

The definition of a factorization system can be found, for example, in [Ba], 8.2. The implications of this result, among others, are that every map has such a factorization, that a composite of regular epis is regular epi and that if fg is regular epi, so is f.

Now we define a diagram $(\underline{I}, D)$ to be projective if

P1. $\underline{I}$ is an inverse directed set.

P2. For any $i \in \underline{I}$ and any regular epi $f : X \to Di$ there is a $j \leqslant i$ such that $D(i, j) = f$.

We define a diagram $(\underline{I}, D)$ to be acyclic if

A1. $\underline{I}$ is an inverse directed set.

A2. For any $i < j$ in $\underline{I}$, the interval $[i, j] = \{ k \mid i \leqslant k \leqslant j \}$ is finite.

A3. For any $i < j$ in $\underline{I}$, the natural map $Di \to \lim \{ Dk \mid i < k \leqslant j \}$ is a regular epimorphism.

LEMMA. — Let $(\underline{I}, D)$ be projective, $(\underline{J}, E)$ acyclic. For any $j_0 \in \underline{J}$, any map $D \to Ej_0$ can be extended to a map $D \to E$.

For technical reasons A1 will be replaced by

A1'. $\underline{I}$ is an inf semilattice.

If $(\underline{I}, D)$ satisfies A1', A2 and A3 we call it strongly acyclic.

It should be noted that these definitions are not isomorphism invariant. However in the argument below we will be dealing with the actual diagrams so this will not cause any problems.

The following is due, almost without change, to Lubkin [Lu].

PROPOSITION. — Under the hypotheses of the main theorem, part 3, every diagram $(\underline{I}, D)$ in which $\underline{I}$ is an inverse directed set can be embedded in a projective diagram.

By a careful analysis of Lubkin's argument, one can show.

PROPOSITION. — Every strongly acyclic diagram can be embedded in a projective, strongly acyclic diagram.

By applying the above diagram to the singleton diagram whose value is the terminal object we find a projective, acyclic diagram $(\underline{I}, D)$ in which every non-empty $X \in \underline{X}$ appears at least once, since the terminal map $X \to 1$ is a regular epi and hence by P2 is represented. Since for any $i < j$ the interval $[i, j]$ is finite, there is a chain

$$i = i_1 < i_2 < \ldots < i_r = j$$

such that there is no k between i_s and i_{s+1}. Then A3 implies that $Di_s \to Di_{s+1}$ is a regular epi and since the class of regular epis is closed under composition, it follows that $Di \to Dj$ is regular epi. From this it will follow that $(D, -) : \underline{X} \to \underline{S}$ reflects regular epis. It obviously preserves finite limits which then implies that it reflects isomorphisms, is faithful and reflexively exact. Now we let U denote the obvious lifting of $(D, -)$ to $\underline{S}^M$, the category of right M sets where M is the monoid of endomorphisms of D. U is also a reflexively exact embedding. To show it is full it is required to show that is $\varphi : (D, X) \to (D, Y)$ is a map with $\varphi(gu) = \varphi g . u$ for any $g : D \to X$, $u : D \to D$ then there is some $f : X \to Y$ with $\varphi g = f . g$. Let $X \in \underline{X}$ and $i \in \underline{I}$ be some vertex with $Di = X$. Let F be the diagram D, truncated above i. Then $D \cong F$ since I is directed. Let $d : F \to X$ be the map represented by the identity on Fi. Let E be the diagram, defined on $(\underline{I}, i)$ by

$$Ej \underset{d^1 j}{\overset{d^0 j}{\rightrightarrows}} Fj \to X$$

is a kernel pair. Then is may be shown that E is acyclic and that

$$E \underset{d^1}{\overset{d^0}{\rightrightarrows}} F \xrightarrow{d} X$$

is a coequalizer diagram. The fact that E is acyclic implies that there are enough maps $D \to E$ to separate maps from E. Now replace D by F and suppose $\varphi : (F, X) \to (F, Y)$ is given with $\varphi(g.u) = \varphi g.u$ for $g : F \to X$, $u : F \to F$. Now $\varphi d \in (F, Y)$. If $\varphi d.d^0 \neq \varphi d.d^1$ then there is some $U : F \to E$ with $\varphi d.d^0.u \neq \varphi d.d^1.u$. But $\varphi d.d^1.u = \varphi(d.d^0.u)$ since $d^0.U : F \to F$. But then $\varphi(d.d^0.u) = \varphi(d.d^1.u) = \varphi d.d^1.u$ for the same reason. Thus there is an $f : X \to Y$ with $\varphi d = f.d$. If $g \in (F, X)$ is an other map it factors, again using the projective/acyclic comparison lemma as $g = d.u$ for some $u : F \to F$. But then $\varphi g = \varphi(d.u) = \varphi d.u = f.d.u = f.g$.

Added note. — The main theorem of this paper can be improved to the following.

Theorem. — Suppose the small category $\underline{X}$ has finite inverse limits and that the kernel pair of every map have a coequalizer. Then the following are equivalent:

1. There is a small category $\underline{\dot{M}}$ and a full, faithful exact functor $\underline{X} \to \underline{S}^{\underline{M}}$.
2. There is a small discrete category $\underline{M}$ and a faithful, reflexively exact functor $\underline{X} \to \underline{S}^{\underline{M}}$.
3. In any pullback diagram

$$\begin{tikzcd}[row sep=small] & \bullet \arrow[dr] & \\ \bullet \arrow[ur, "f'"] \arrow[dr] & & \bullet \\ & \bullet \arrow[ur, "f"'] & \end{tikzcd}$$

f regular epi implies f' regular epi.

Moreover the objects of $\underline{M}$ can be taken to be the set of non-empty subobjects of the terminal object.

It is easily shown that 3*a*) of the original theorem is equivalent to the assertion that the terminal object has no proper non-empty subobjects. Just factor the terminal map $X \to 1$ into a regular epi and a mono. Thus this theorem generalizes the original.

REFERENCES

[Fr] P. Freyd. — *Abelian Categories*, Harper and Row, New York (1964).
[Mi] B. Mitchell. — *Theory of Categories*, Academic Press, New York (1965).
[Ba] M. Barr. — Coequalizers and free triples, *Math. Zeitschrift*, 116 (1970), pp. 307-322.
[Lu] S. Lubkin. — Imbedding of abelian categories, *Trans. Amer. Math. Soc.*, 97 (1960), pp. 410-417.

McGill University
Department of Mathematics,
Montreal, Québec (Canada)

Actes, Congrès intern. math., 1970. Tome 1, p. 313 à 317.

UTILISATION DES CATÉGORIES EN GÉOMÉTRIE ALGÉBRIQUE

par JEAN GIRAUD

En choisissant le titre de cette conférence, j'avais l'intention de montrer par des exemples comment les catégories fournissent un langage et, en même temps, une algèbre qui permettent de mettre de l'ordre dans des questions parfois fort touffues, de montrer aussi comment les applications que l'on a en vue servent de mentor au catégoricien, plus enclin qu'un autre, peut-être, aux digressions. Pour limiter les préréquisites, je me contenterai d'un exemple, déjà ancien, mais que l'on peut aborder (au § 3) en n'utilisant que la notion de champ sur un site (§ 1); au § 2, j'explique une construction permettant d'attacher un topos à un champ de groupoïdes et qui a son utilité pour l'étude des extensions de groupes (algébriques ou topologiques), mais je ne parlerai pas de ce dernier point.

§ 1. — On rappelle qu'un *champ* sur un topos (ou, plus généralement un site) X est une catégorie fibrée $p: C \to X$ satisfaisant à une condition supplémentaire qui exprime que les objets et les flèches se recollent. L'*image directe* de C par un morphisme de topos $f: X \to Y$ est, par définition, le produit fibré $C \times_X Y$, où Y est considéré comme une X-catégorie grâce au foncteur image inverse $f^*: Y \to X$; on la note $f_*(C)$. L'*image inverse* par f d'un champ D sur Y est un champ $f^*(D)$ sur X muni d'un morphisme $D \to f_*f^*(D)$ tel que, pour tout champ C sur X, le foncteur naturel

$$\mathrm{Cart}_X(f^*(D), C) \to \mathrm{Cart}_Y(D, f_*(C))$$

soit une équivalence, où $\mathrm{Cart}_X(A, B)$ désigne la catégorie des foncteurs cartésiens d'un X-champ A dans un autre B. En particulier, si S est un objet d'un topos X et si $x: X \mid S \to X$ est le morphisme naturel, on peut prendre pour image inverse d'un X-champ C celui qui s'en déduit par le changement de base $x_! : X \mid S \to X$, $x_!(T/S) = T$; de plus, si $q: G \to X \mid S$ est un champ sur $X \mid S$, le composé $x_! \circ q: G \to X$ est encore un champ noté $x_!(G)$ et, pour tout X-champ C, on a un isomorphisme

$$\mathrm{Cart}_X(x_!(G), C) \approx \mathrm{Cart}_{X|S}(G, x^*(C)).$$

THÉORÈME 1.1. — *Soit C un champ de groupoïdes sur un topos X. Il existe un objet S de X et une gerbe G sur le topos induit $X \mid S$ tels que $x_!(G)$ soit isomorphe à C.*

Un champ de groupoïdes est un champ dont les fibres sont des groupoïdes; on dit que c'est une gerbe s'il est localement équivalent au champ des torseurs (espaces principaux homogènes) sous un faisceau de groupes. On prend pour S l'objet de X qui représente le faisceau associé au préfaisceau qui, à tout objet T de X, associe l'ensemble des classes à isomorphisme près d'objet de la fibre C_T. On dit que S est le *faisceau des* *sous-gerbes maximales de C*, car il est facile de vérifier qu'une section $s \in S(T)$ de S au-dessus d'un objet T de X s'interprète comme une sous-gerbe de la restriction de C à $X \mid T$ qui est maximale en ce sens que toute sous-gerbe qui la contient lui est égale. On prend alors pour G la catégorie C elle-même, munie du foncteur $q: G \to X \mid S$ qui, à un objet c de C de projection T, associe la sous-gerbe maximale de $C \mid T$ qui contient c, considérée comme un morphisme $T \to S$, c'est-à-dire un objet de $X \mid S$. Le couple (C, q) est bien une gerbe G et l'on a $p = x_! \circ q$, d'où la conclusion. L'intérêt de cette construction tient à ce qu'elle est fonctorielle par rapport au site.

COROLLAIRE 1.2. — *Soit encore $f: X' \to X$ un morphisme de topos. L'image inverse C' de C par f est un champ de groupoïdes, le faisceau S' des sous-gerbes maximales de C' est l'image inverse de S et la gerbe G' sur $X' \mid S'$ attachée à C' est l'image inverse de G par le morphisme induit $f \mid S: X' \mid S' \to X \mid S$.*

La démonstration repose sur l'étude du procédé général de construction de l'image inverse d'un champ.

§ 2. — Puisque les topos forment une 2-catégorie, pour tout topos X, les X-topos (topos munis d'un morphisme de topos $f: X' \to X$) forment une 2-catégorie ; si X' et X'' sont deux X-topos, on notera $\mathrm{Mor}_X(X', X'')$ la catégorie des X-morphismes de X' dans X''. On a en fait une catégorie fibrée $\underline{\mathrm{MOR}}_X(X', X'')$ sur X, dont la fibre en $S \in Ob(X)$ est $\mathrm{Mor}_{X|S}(X' \mid S', X'' \mid S'')$, où S' et S'' sont les images inverses de S sur X' et X''. D'après M. Hakim, cette catégorie fibrée est *un champ*, ce qui exprime que les morphismes de topos se recollent.

THÉORÈME 2.1. — *Soit $p: C \to X$ un champ de groupoïdes sur un topos X. Il existe un X-topos $\tau_C(X): B_C(X) \to X$ et une section c de l'image inverse de C par $\tau_C(X)$ tels que, pour tout X-topos $f: X' \to X$, le foncteur*

$$\mathrm{Mor}_X(X', B_C(X)) \to f^*(C)(X'), \qquad m \mapsto m^*(c), \tag{1}$$

soit une équivalence de catégories.

2.1.1. Le *topos classifiant* $B_C(X)$, aussi noté B_C, est donc défini par sa « propriété universelle », mais il n'est connu qu'à équivalence près, comme il arrive souvent dans ce genre de questions. Lorsque les fibres de C sont discrètes, C admet un scindage, donc est défini par un faisceau d'ensemble S, à savoir $S(T) = Ob(C_T)$, qui est d'ailleurs celui de (1.1). Dans ce cas, il est clair que le topos induit $X \mid S$ est un classifiant. Par ailleurs, si C est la gerbe des torseurs sous un groupe A de X, on prend pour classifiant le topos $B_A(X)$ des objets de X munis d'opérations à gauche de A, le morphisme $\tau_A(X): B_A(X) \to X$ étant défini par son foncteur image inverse qui, à $E \in Ob(X)$, associe l'objet E^τ obtenu en faisant opérer A trivialement. D'après une remarque de Grothendieck, le topos $B_A(X)$ jouit de la propriété universelle voulue : à un $f^*(G)$-torseur P sur un X-topos $f: X' \to X$, on associe le X-morphisme de topos $\omega_P: X' \to B_G(X)$ dont le foncteur image inverse est $\omega_P^*(E) = P^{f^*(G)} f^*(E)$.

2.1.2. Indiquons maintenant comment le cas général se déduit des deux cas particuliers précédents. On définit d'abord $B_C(X)$ en considérant la catégorie $FL(X)$ des flèches de X munie de son foncteur but : c'est un champ dont les fibres sont des topos et les foncteurs image inverse des morphismes de topos (en bref, un champ de topos).

On pose $B_C(X) = \mathrm{Cart}_X(C, FL(X))$. On vérifie que cette définition est en accord avec les précédentes lorsque C est à fibres discrètes ou bien est un champ de groupoïdes. Grâce à (1.1), on montre ensuite que l'on a une équivalence de catégories $B_C(X) \approx B_G(X \mid S)$, avec les notations de (1.1). Pour voir que $B_C(X)$ est un topos, on peut donc supposer que C est une gerbe, il reste à trouver un procédé de localisation; or il est clair que $B_C(X)$ est la fibre en l'objet final d'une X-catégorie fibrée, laquelle est localement un champ de topos puisque C est localement équivalente à une gerbe de torseurs et que ce cas a été traité; d'où la conclusion, car, jointe à une condition supplémentaire que nous n'expliciterons pas, la condition d'être un champ de topos est de nature locale. On définit le morphisme $\tau_C(X)$ par son foncteur image inverse, lequel associe, à un objet T de X, le foncteur cartésien constant $t\colon C \to FL(X)$, $t(a) = p(a) \times T$. Par le même procédé de réduction au cas d'une gerbe de torseurs, on vérifie que c'est bien un morphisme de topos. Il reste à prouver la propriété universelle. Par dévissage et localisation, on montre qu'elle est satisfaite pour les X-topos de la forme $X \mid T$, $T \in Ob(X)$. On montre ensuite que si $f\colon X' \to X$ est un morphisme de topos et si $C' = f^*(C)$, on a un carré commutatif à isomorphisme près

$$\begin{array}{ccc} B_{C'}(X') & \to & B_C(X) \\ \downarrow & & \downarrow \\ X' & \to & X \end{array}$$

et que celui-ci est 2-cartésien dans la 2-catégorie des X-topos.

2.2. La construction de $B_C(X)$ à partir de X fournit un (« vrai ») 2-foncteur de la 2-catégorie des champs de groupoïdes dans celle des X-topos, qui est pleinement fidèle, c'est-à-dire que l'on a la proposition suivante.

PROPOSITION 2.2. — *Soient C et C' deux champs de groupoïdes sur un topos X. Le foncteur naturel*

(1) $$\mathrm{Cart}_X(C, C')^0 \to \mathrm{Mor}_X(B_C(X), B_{C'}(X))$$

est une équivalence de catégories.

Il nous faut expliquer le retournement des flèches. Un morphisme de champs $m\colon C \to C'$ induit par composition un foncteur $B_m^*\colon B_{C'} \to B_C$ qui est le foncteur image inverse d'un morphisme de topos $B_m\colon B_C \to B_{C'}$, et un morphisme de morphismes de champs $u\colon m \to m'$ induit, par composition un morphisme de foncteurs $B_u\colon B_m^* \to B_{m'}^*$, d'où, d'après les conventions habituelles, un morphisme de morphismes de topos en sens inverse $B_u\colon B_{m'} \to B_m$.

§ 3. — Nous allons maintenant montrer comment on peut, en utilisant seulement la notion d'image directe et inverse de champs, formuler et démontrer les variantes non commutatives du théorème de changement de base pour un morphisme propre en cohomologie étale; nous indiquerons en gros la marche de la démonstration.

THÉORÈME 3.1. — *Soit un carré cartésien de schémas*

$$\begin{array}{ccc} X & \xleftarrow{g'} & X_0 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f_0} \\ Y & \xleftarrow[g]{} & Y_0 \end{array}$$

tel que f soit propre et Y localement noethérien. Pour tout champ ind-fini C sur le site étale $X_{\acute{e}t}$ de X, le morphisme naturel $u: g^*f_*(C) \to f_{0*}g'^*(C)$ est une équivalence de catégories.

On dit qu'un champ C est ind-fini (resp. constructible) si, pour tout objet c de C de projection $S \in Ob(X_{\acute{e}t})$, le faisceau $Aut_S(c)$ des S-automorphismes de c est ind-fini (resp. constructible) [1]. Qu'un morphisme de champs soit une équivalence, se voit fibre par fibre, la fibre en un point $x: (U\text{-ens}) \to Y_{0\acute{e}t}$ du site étale $Y_{0\acute{e}t}$ de Y_0 étant l'image inverse de u par x. On réduit ainsi l'énoncé au suivant.

PROPOSITION 3.2. — *Si, de plus, Y est le spectre d'un anneau local hensélien et noethérien et si Y_0 est le spectre du corps résiduel, le foncteur restriction $v: C(X) \to C_0(X_0)$ est une équivalence.*

Si Z, ou F, ou C, est un schéma, ou un faisceau, ou un champ sur X, on note Z_0, ou F_0, ou C_0 son image inverse sur X_0. Lorsque C est la gerbe des torseurs sous un faisceau de groupes F (resp. le champ à fibres discrètes attaché à un faisceau d'ensembles F), la conclusion de l'énoncé signifie que l'application $H^i(X, F) \to H^i(X_0, F_0)$ est bijective pour $i \leqslant 1$ (resp. $i = 0$). En particulier, la condition (A) ci-dessous n'est autre que le théorème de spécialisation du groupe fondamental ; on la démontre (ainsi que (B)) en utilisant le théorème d'approximation de M. Artin, qui permet de supposer que Y est le spectre d'un anneau local complet, auquel cas le résultat est dû à Grothendieck [2]. Du point de vue de la géométrie algébrique, ceci est évidemment l'ingrédient essentiel de la démonstration.

(A) Pour tout X-schéma fini X', le foncteur restriction $C(X') \to C(X'_0)$ est une équivalence de catégories.

(B) Pour tout faisceau d'ensembles F sur X, l'application $F(X) \to F_0(X_0)$ est bijective.

(C) Pour tout champ ind-fini C sur X, le foncteur $v: C(X) \to C_0(X_0)$ est une équivalence.

On montre que v est toujours pleinement fidèle en appliquant (B) au faisceau des morphismes entre deux sections quelconques de C. Soit alors $c_0 \in Ob(C_0(X_0))$; la sous-gerbe de C_0 engendrée par c_0 s'interprète comme une section de l'image inverse sur X_0 du faisceau des sous-gerbes maximales de C (1.2), elle provient donc d'après (B) d'une sous-gerbe de C, ce qui permet de supposer que C est une gerbe. Introduisons la catégorie fibrée sur SCH/X qui, à un X-schéma $z: Z \to X$ associe la catégorie $C(Z)$ des sections de l'image inverse $z^*(C)$ de C. Il se trouve que c'est un champ pour une topologie qui est plus fine que la topologie étale et pour laquelle sont couvrants les morphismes surjectifs qui sont de plus entiers, ou propres, ou plat et localement de présentation finie. De plus, on prouve que les conditions (A) et (B) sont stables si l'on remplace X par un X-schéma entier X' et X_0 par $X'_0 = X' \times_X X_0$ (ou même par $X'_1 = X' \times_X X_1$, où X_1 est un fermé de X qui contient X_0). L'on en déduit par descente que v est une équivalence s'il en est ainsi de $C(X') \to C(X'_0)$. Il est alors facile de voir que l'on peut supposer que X est intègre et, par récurrence noethérienne, il suffit de prouver qu'il existe un fermé $X_1 \supset X_0$ tel que $C(X) \to C(X_1)$ soit une équivalence. On construit X' et X_1 grace au lemme suivant.

LEMME 3.3. — *Soit X un schéma intègre, quasi-compact et quasi-séparé et soit C une gerbe constructible (resp. ind-finie) sur X. Il existe un morphisme entier $s: X' \to X$,* *un faisceau de groupes fini et constant (resp. ind-fini) F sur X', un ouvert dense U de X et un morphisme de gerbes $r: s^*(C) \to T$, où T est la gerbe des F-torseurs, tels que la restriction de r à $s^{-1}(U)$ soit une équivalence.*

On note K' une clôture séparable du corps des fonctions K de X et l'on prouve le lemme en utilisant le fait que le site zariskien de X' est équivalent à son site étale. Prenant pour X_1 un fermé contenant X_0 et tel que $U \supset (X - X_1)$, il reste à prouver que $C'(X') \to C'(X'_1)$ est une équivalence, où $C' = s^*(C)$. Soit c_1 une section de C' sur X'_1 et soit K la catégorie fibrée sur $X'_{1\,\text{ét}}$ dont les objets de projection S sont les (c, i), où $c \in Ob(C'_S)$ et où $i: (c \mid S_1) \to (c_1 \mid S_1)$ est un S_1-isomorphisme. C'est une gerbe car X'_1 est fermé dans X', et pour que c_1 provienne d'un $c \in Ob(C(X'))$, il faut et il suffit que K ait une section ; soit K' la gerbe construite de façon analogue en remplaçant C par T et c_1 par $d_1 = r(c_1)$. On a un morphisme naturel $K \to K'$, qui est une équivalence comme on voit fibre par fibre : aux points de X'_1, ces fibres sont équivalentes à la catégorie finale, aux points de U, le morphisme r est une équivalence. Il suffit donc de prouver que d_1 provient d'une section de T. Puisque nous avons vu que le couple (X', X'_1) satisfait à la condition (A), cela est vrai lorsque C est constructible car alors F est constant. D'où la condition (C) pour un champ constructible, donc aussi, par passage à la limite pour la gerbe des torseurs sous un groupe ind-fini, d'où le cas général, en reprenant le même raisonnement et en invoquant cette fois la partie respée de (3.3).

Par un raisonnement tout analogue mais plus simple, car on peut ici se contenter de localiser pour la topologie étale, on démontre les variantes non commutatives du *théorème de changement de base lisse.* On doit à Mme Raynaud l'énoncé suivant qui est la variante non commutative du *théorème de finitude* des images directes supérieures par un morphisme propre.

THÉORÈME 3.4. — *Soit $f: X \to S$ un morphisme propre de type fini, S étant localement noethérien et soit C un champ sur X. Si X et son faisceau des sous-gerbes maximales sont constructibles, il en est de même de $f_*(C)$ et de son faisceau des sous-gerbes maximales.*

RÉFÉRENCES

[1] M. ARTIN, A. GROTHENDIECK et J.-L. VERDIER. — Séminaire de Géométrie Algébrique de l'I. H. E. S., 1963-1964, Cohomologie Étale des schémas.

[2] A. GROTHENDIECK. — Séminaire de Géométrie Algébrique de l'I. H. E. S., 1960.

École normale supérieure
de Saint-Cloud
92-Saint-Cloud (France)

Actes, Congrès intern. math., 1970. Tome 1, p. 319 à 322.

EXTENSIONS OF STRUCTURES AND FULL EMBEDDINGS OF CATEGORIES

by Z. HEDRLÍN

Introduction.

The objects of study of mathematics are often sets with some additional information. E. g. for a group the additional information is the binary operation, for a topological space the family of open sets, for a graph the set of its edges. Equivalences and mutual relations between objects are studied by means of a special class of mappings which is chosen according to the pourpose of the study. The choice of the mappings usually depends on the additional information about the objects. Frequently used choices are e. g. isomorphisms or homomorphisms for groups, continuous mappings, open mappings or homeomorphisms for topological spaces, isomorphisms or compatible mappings for graphs.

We shall study the following problem: given objects and their mappings by means of a choice, under what condition we can simplify the additional information and the choice of mappings preserving in the same time all information about the original mappings. The main result can be roughly described as follows: no matter how many and how complicated objects are given, for any choice of mappings which is closed under composition and contains all identity mappings, it is always possible to replace the additional information by means of a binary relation and the choice of mappings by means of the choice of compatibility with the relations, maintaining all the information about the original mappings.

Definitions and conventions.

We shall work simultaneously in two set theories. In the usual Gödel-Bernays set theory with the axiom of choice for classes and with the assumption that there is no measurable cardinal as specified in [2]. The other, finite set theory, is again the Gödel-Bernays set theory with the axiom of choice for classes but with the negation of the axiom of infinity. Our results considered in the latter set theory give theorems in combinatorics and finite algebra.

We use the following convention: by a list we mean any ordered n-touple, n being a non-zero ordinal. We shall assume that a list can be distinguished from any ordinary set, which can be achieved by proper indexing.

Let U_1, U_2 be sets. By a mapping from U_1 into U_2 we mean a triple $f = \langle U_1, U_2, f \rangle$, where $f \subset U_1 \times U_2$ is a functional relation. Let

$$f = \langle U_1, U_2, f \rangle, \qquad g = \langle U_3, U_4, g \rangle$$

be mappings. Their composition $g \circ f$ is defined if and only if $U_2 = U_3$ and then $g \circ f = \langle U_1, U_4, g \circ f \rangle$, where $g \circ f$ designates the composition of relations. The mapping g will be called an extension of f if and only if $U_3 \supset U_1$, $U_4 \supset U_2$, $g \supset f$ and $g(U_3 - U_1) \subset U_4 - U_2$. By an object O we mean a list on the first place of which there is a set U called the underlying set of O, We shall write $O = \langle U, \dots \rangle$. The elements on the other places describe the additional information.

Let $O_1 = \langle U_1, \dots \rangle$, $O_2 = \langle U_2, \dots \rangle$ be objects. By a morphism m from O_1 into O_2 we mean a triple $m = \langle O_1, O_2, f \rangle$, where f is a mapping from U_1 into U_2. f will be called the mapping of m. Let $m_1 = \langle O_1, O_2, f \rangle$, $m_2 = \langle O_3, O_4, g \rangle$ be morphisms. Their composition $m_2 \circ m_1$ will be defined if and only if $O_2 = O_3$ and in this case $m_2 \circ m_1 = \langle O_1, O_4, g \circ f \rangle$. The morphism m_2 is called an extension of the morphism m_1 if and only if g is an extension of f. The identity morphism of an object O is the morphism $\langle O, O, i \rangle$, where i is the identity mapping of the underlying set of O.

We shall use also the standard categorical language.

Structures and extensions.

By a structure we mean a class S, whose elements are only objects and morphisms, such that

(i) with each morphism S contains its range and domain,
(ii) with each object it contains its identity morphism,
(iii) if $m_1, m_2 \in S$, $m_2 \circ m_1$ is defined, then $m_2 \circ m_1 \in S$.

Observe that an object is never a morphism and the other way around, since lists and sets differ. Thus a structure S can be written as $S = {}^mS \cup {}^0S$, where ${}^mS$ contains only morphisms and ${}^0S$ only objects.

Let S be a structure. ${}^mS$ is then a class on which the partial binary operation $\circ$ is defined. ${}^mS$ together with this partial binary operation will be designate by alg (S). Obviously, alg (S) is a category. If we associate with every morphism its mapping we get a faithfull functor from alg (S) into the category of sets. Thus, alg (S) is a concrete category. On the other hand, it is obvious that each concrete category is isomorphic with alg (S) for some structure S.

Let S be a structure. A structure S_1 is called a substructure of S if $S_1 \subset S$. S_1 is called a full substructure of S if $S_1 \subset S$ and $m = \langle O_1, O_2, f \rangle \in S$, $O_1, O_2 \in S_1$ implies $m \in S_1$. Obviously, if S_1 is a full substructure of S then alg (S_1) is a full subcategory of alg (S).

Examples of structures. — Alg (1, 1) : objects-all algebras with two unary operations, morphisms—all their homomorphisms. Tlh: objects—all topological spaces, morphisms—all their local homeomorphisms. Gra: objects—all graphs, morphisms—all their compatible mappings (see [2]).

Now, we are going to define a notion which will enable us to compare structures. Let O_1, O_2, O_1', O_2' be objets, M a set of morphisms from O_1 into O_2, M' a set of morphisms from O_1' into O_2'. M' is called an extension of M if each $m' \in M'$ is an extension of some $m \in M$, and for every $m \in M$ there is exactly one $m' \in M'$ such that m'

is an extension of m. Let S and S' be structures. We say that S has an extension *onto* S' if there exists a class bijection F from ${}^0S$ onto ${}^0S'$ with the following property: for every objects $O_1, O_2 \in {}^0S$, the set of all morphisms from $F(O_1)$ into $F(O_2)$ in S' is an extension of the set of all morphisms from O_1 into O_2 in S. We say that S has an extension *into* S' if it has extension onto a full substructure of S'.

Obviously, if S has extension onto S' then the categories alg (S) and alg (S') are isomorphic. If S has extension into S' then the category alg (S) can be fully embedded into the category alg (S').

Main extension theorem.

THEOREM. — Every structure has an extension into each of the structures Alg (1, 1), Tlh and Gra.

COROLLARY. — Every concrete category can be fully embedded into the category of all algebras with two unary operations.

The theorem has been proved combining a few lemmas by L. Kučera and by myself. In the lemmas we used results by P. Goralčik, J. de Groot, J. R. Isbell, J. Lambek, A. Pultr, J. Sichler, V. Trnková and P. Vopěnka. The proof is rather long. Since it uses new structural techniques not much from the already published results can be used which, together with the absence of L. Kučera in the civil life, postponed the publishing of the proof. The complete proof was presented in full at Charles University in Prague and at Tulane University in New Orleans.

The theorem suggests to define: a structure S is called a super-structure if every structure has an extension into S.

In addition to the structures Alg (1, 1), Tlh and Gra some other structures are known to be super-structures. J. Sichler developed a deep theory of superstructures which are primitive classes of algebras. P. Hell, E. Mendelsohn and J. Nešetřil investigate similar questions for various substructures of Gra and related structures.

All the results so far mentioned are true both in the infinite and finite set theories. There are two results which hold only in the infinite set theory. The structure of semigroups and all their homomorphisms is a super-structure (see [1]; this paper can serve as an introduction to the ideas) and so is the structure of antireflexive partly ordered sets with all order preserving mappings (common result with R. H. McDowell).

Our proof shows a natural hierarchy of structures which can serve as a tool for a classification of some branches of mathematics.

Kučera theorem and a new approach to categories.

Examples of P. Freyd and J. R. Isbell show that not every category is concrete. Moreover, P. Freyd proved that the often used category, whose objects are topological spaces and morphisms are classes of homotopically equivalent mappings is not concrete. The Kučera theorem will show that every category can be obtained from algebraization of a structure in a similar way as the last category was obtained from the category of topological spaces and continuous mappings.

Let K, L be categories. L is called an m-factorization (m for morphisms), if there is a functor F from K onto L which is one-to-one on objects and maps K onto L.

KUČERA THEOREM. — For every category K there exists a structure S such that K is an m-factorization of alg (S).

The proof can be presented on a few pages and can be found in the already mimeographed part of my lecture notes at Tulane University. An independent proof is announced by P. Freyd together with an internal characterization of concrete categories by means of an Isbell condition.

Combining the previous theorems we get:

COROLLARY. — Every category is isomorphic with an m-factorization of the algebraization of a full substructure of each of the structures Alg (1, 1), Tlh, Gra.

Thus, the Kučera theorem enables to study even non-concrete categories by means of structures. In fact, the corollary to the main extension theorem, which was our aim to prove for a few years, could be proved only by introduction of structural methods.

Further results.

In addition to the mentioned results many other results have been obtained along these lines. They concern full embeddings of categories, functor theory, universal algebra, topology, graph theory, theory of semigroups and some other questions. Since the theory is developing, some of the papers are available only in the form of preprints. The mimeographed list of these papers and preprints can be obtained upon request from Prague.

REFERENCES

[1] Z. HEDRLÍN and J. LAMBEK. — How comprehensive is the category of semigroups, *J. of Algebra*, 11 (1969), pp. 195-212.
[2] — and P. VOPĚNKA. — An undecidable theorem concerning full embeddings into categories of algebras, *Comment. Math. Univ. Carolinae*, 7 (1966), pp. 401-409.

Charles University
Department of Mathematics,
Sokolovska 83,
Praha 8 (Tchécoslovaquie)

Actes, Congrès intern. math., 1970. Tome 1, p. 323 à 328.

EXTENSIONS OF FUNCTORS ON GROUPS AND COEFFICIENTS IN A COHOMOLOGY THEORY

by PETER HILTON

1. Introduction.

It was shown in [7] (see also [1, 8]) how to use co-Moore spaces to put finitely-generated coefficients G into a cohomology theory h. The extension to arbitrary coefficients (modulo a difficulty with 2-torsion) was then effected using a direct limit process.

If $\mathscr{F}$ is a nice pointed category of topological spaces, and h is a cohomology theory on $\mathscr{F}$, we say that h is *good* if the Hopf map $\gamma : S^3 \to S^2$ induces

$$0 = h(1_X \wedge \gamma) : h(X \wedge S^2) \to h(X \wedge S^3)$$

for all X in $\mathscr{F}$. If h is multiplicative it is easily seen that h is good if $h(\gamma) = 0$ and this follows if $h(S^0)$ is 2-torsion-free. Let $\mathscr{G}_0$ be the category of finitely-generated abelian groups, $\mathscr{G}_1$ the category of abelian groups if h is good; otherwise let $\mathscr{G}_0$ be the category of finitely-generated 2-torsion-free abelian groups, $\mathscr{G}_1$ the category of 2-torsion-free abelian groups. Then we have a functor $W_h : \mathscr{G}_0 \to Coh$, the category of cohomology theories on $\mathscr{F}$, given by:

$$W_h(G) = h(- ; G) \qquad G \text{ in } \mathscr{G}_0. \tag{1.1}$$

Here $h(X ; G)$ is obtained by " smashing " X with the co-Moore space LG and then applying h [7]. We extend W_h to $\mathscr{G}_1$ by taking direct limits, the argument being justified in [6] and relying heavily on the universal coefficient theorem (Actually, only the second case was discussed in detail in [7], but the first case, when h is good, is handled in exactly the same way).

Ulmer pointed out that the extension given in [7] is, in fact, the Kan extension; his argument (see the last section of [6]) rested on the additivity of W_h. This suggests the general question of when an extension of a functor from some category $\mathscr{G}_0$ to a category $\mathscr{G}_1$, effected by a direct limit process, is, in fact, the Kan extension. We give an answer in Section 3, in the form of some sufficient conditions, but this answer requires us to pass from direct limits over directed sets to direct limits over filtering categories (see [2]; filtering categories were called " quasi-filtered " in [4, 5]). This extension of the theory of [6] is given in Section 2. In Section 4, we show that, to speak informally, a natural universal coefficient sequence always splits (here our arguments were suggested by a study of Mislin's work on the Künneth theorem [9]), while there is essentially only one non-split sequence which can arise as a (non-natural) universal coefficient sequence, namely:

$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0$$

Details of results in this section are to be found in [3]; details of those in Section 2 and 3 will be published later.

We remark that if h is not good we still get a " quasi-functor " (in a sense made precise and studied by Paul Kainen in his doctoral thesis) W_h from the category of finitely-generated abelian groups to *Coh* and that this may be extended to countable abelian groups by restricting attention to special direct systems consisting of sequences of inclusions. We still see no way of extending the quasi-functor (1.1) to uncountable groups with 2-torsion (unless, of course, the cohomology theory h is good).

2. On filtered families of groups and direct limits

Our object in this section is to generalise the results of Sections 2 and 3 of [6] by allowing direct systems over filtering categories instead of merely over directed sets. Thus we define, for a given category $\mathscr{L}$, the category $\mathscr{L}^{\Sigma}$ as follows:

— An *object* of $\mathscr{L}^{\Sigma}$ is a pair (I, F), abbreviated to F, where I is a filtering category (" quasi-filtered " in [4, 5]) and $F: I \to \mathscr{L}$ is a functor.

— A *morphism* of $\mathscr{L}^{\Sigma}$, $\Phi: (I, F) \to (J, G)$ is a pair $\Phi = (T, u)$ where $T: I \to J$ is cofinal [2, 4] and $u: F \to GT$ is a natural transformation.

Evidently, $\mathscr{L}^{\Sigma}$ is a category under the law of composition:

$$(S, v)(T, u) = (ST, vT \circ u) \tag{2.1}$$

We will also need the category $\not f$ of filtering categories and cofinal functors defined in the obvious way. We note that there is a canonical embedding of $\mathscr{L}$ in $\mathscr{L}^{\Sigma}$ which associates with $X \in |\mathscr{L}|$ the pair $(1, F_X)$ where F_X maps the object of 1 to X. This embedding is full and faithful. If $\mathscr{L}$ is cocomplete, there is a left adjoint $L: \mathscr{L}^{\Sigma} \to \mathscr{L}$ to this embedding yielding direct limits of objects of $\mathscr{L}^{\Sigma}$. We assume $\mathscr{L}$ cocomplete and remark that:

$$\begin{aligned} (T, u) &= (T, 1_{GT})(1_I, u), \\ L(T, 1) &= 1 \qquad \text{since } T \text{ is cofinal.} \end{aligned} \tag{2.2}$$

We say that $T: I \to J$ in $\not f$ is a *fibre map* if, given $T(i) \xrightarrow{\psi} j'$ in J, we have $i \xrightarrow{\varphi} i'$ in I with $T(\varphi) = \psi$.

THEOREM 2.3. — *Given $(T, u): F \to G$ in $\mathscr{L}^{\Sigma}$, there is a canonical factorization*

$$\begin{tikzcd} & \overline{F} \arrow[dl, shift left, "(\overline{S},1)"] \arrow[d, "(\overline{T},\overline{u})"] \\ F \arrow[ur, shift left, "(S,1)"] \arrow[r, "(T,u)"'] & G \end{tikzcd}$$

such that:

(*a*) $(\overline{T}, \overline{u})(S, 1) = (T, u)$
(*b*) $(\overline{S}, 1)(S, 1) = 1$
(*c*) $\overline{T}$ *is a fibre map.*

THEOREM 2.4. — *Let*

$$\begin{tikzcd} & I \arrow[d, "T"] \\ J \arrow[r, "S"'] & K \end{tikzcd}$$

be a diagram in $\mathscr{F}$ *with* T *a fibre map. By taking pull-backs in the category of sets, one obtains a diagram of categories and functors*

$$\begin{tikzcd} A \arrow[r, "S'"] \arrow[d, "T'"] & I \arrow[d, "T"] \\ J \arrow[r, "S"'] & K \end{tikzcd} \tag{2.5}$$

Then:

(*a*) A *is filtering*
(*b*) T' *is a fibre map*
(*c*) S' *is in* $\mathscr{F}$
(*d*) (2.5) *is a pull-back in* $\mathscr{F}$

THEOREM 2.6. — *Let*

$$\begin{tikzcd} & (I, F) \arrow[d, "(T,u)"] \\ (J, G) \arrow[r, "(S,u)"'] & (K, H) \end{tikzcd}$$

be a diagram in $\mathscr{L}^{\Sigma}$ *with* T *a fibre map. Using* (2.5) *construct:*

$$\begin{tikzcd} (A, E) \arrow[r, "(S', v')"] \arrow[d, "(T', u')"] & (I, F) \arrow[d, "(T,u)"] \\ (J, G) \arrow[r, "(S,v)"'] & (K, H) \end{tikzcd} \tag{2.7}$$

where for (i, j) *with* $T(i) = S(j)$, $E(i, j)$ *is the pull-back in* $\mathscr{L}$ *of:*

$$\begin{tikzcd} & F(i) \arrow[d, "u_i"] \\ G(j) \arrow[r, "v_j"'] & HT(i) = HS(j) \end{tikzcd}$$

Then (2.7) *is a pull-back in* $\mathscr{L}^{\Sigma}$.

THEOREM 2.8. — *Let* $\mathscr{G}$ *be the category of groups. Then the direct limit in* $\mathscr{G}^{\Sigma}$ *commutes with pull-backs of fibre-maps.*

We remark that Theorem 2.8 certainly holds for categories other than the category of groups. Our results apply to precisely those categories (including the category of sets) for which Theorem 2.8 holds.

Now let $\mathscr{G}_0 \subseteq \mathscr{G}_1 \subseteq \mathscr{G}$ be a triple of categories in which $\mathscr{G}_0$, $\mathscr{G}_1$ are full subcategories of $\mathcal{G}$, and the groups in $\mathcal{G}_1$ are precisely the direct limits of filtered families of groups in $\mathcal{G}_0$. Suppose further that; for any diagram:

$$\begin{array}{ccc} & & G_0 \\ & & \downarrow \\ G'_0 & \rightarrow & G_1 \end{array}$$

with G_0, G'_0 in $\mathcal{G}_0$ and G_1 in $\mathcal{G}_1$, the pull-back is in $\mathcal{G}_0$. We then say that $\mathcal{G}_0$ has *property P*. Let $L: \mathcal{G}_0^\Sigma \rightarrow \mathcal{G}_1$ be the direct limit functor, and let $\overline{L}: \overline{\mathcal{G}_0^\Sigma} \rightarrow \mathcal{G}_1$ be the canonical extension of L to the category of fractions with respect to L. Then we deduce from Theorems 2.3, 2.6 and 2.8 the following proposition and main theorem.

PROPOSITION 2.9. — *If $\mathcal{G}_0$ has property P, then $\overline{L}: \overline{\mathcal{G}_0^\Sigma} \rightarrow \mathcal{G}_1$ is full and faithful and surjective on objects:*

THEOREM 2.10. — *Let $W_0 : \mathcal{G}_0 \rightarrow \mathcal{E}$ be a functor from $\mathcal{G}_0$ to the cocomplete category $\mathcal{E}$ such that, for any Φ in $\mathcal{G}_0^\Sigma$,*

(2.11) $$\varinjlim W_0^\Sigma(\Phi) \textit{ is an equivalence if } \varinjlim \Phi \textit{ is an equivalence.}$$

Then, if $\mathcal{G}_0$ has property P, W_0 extends to a unique functor $W_1 : \mathcal{G}_1 \rightarrow \mathcal{E}$ such that:

(2.12) $$W_1 \varinjlim = \varinjlim W_0^\Sigma \quad \textit{on } \mathcal{G}_0^\Sigma$$

It is evident that condition (2.11) is necessary in order that W_1 exist satisfying (2.12). We will be concerned in the next section with the question whether W_1 is the Kan extension of W_0.

3. Relation to the Kan extension.

We again consider $\mathcal{G}_0 \subseteq \mathcal{G}_1 \subseteq \mathcal{G}$ as in Section 2, and construct the Kan extension of $W_0 : \mathcal{G}_0 \rightarrow \mathcal{E}$ to $\mathcal{G}$. Given G in $\mathcal{G}$, we consider the category I_G of *$\mathcal{G}_0$-objects over G.* Thus an object of I_G is a homomorphism $\chi : G_0 \rightarrow G$ where G_0 is in $\mathcal{G}_0$ and a morphism $\varphi : \chi \rightarrow \chi'$ in I_G is a commutative triangle

$$\begin{tikzcd} G_0 \arrow[rr, "\varphi"] \arrow[dr, "\chi"'] & & G'_0 \arrow[dl, "\chi'"] \\ & G & \end{tikzcd}$$

We define $W_G : I_G \rightarrow \mathcal{E}$ by $W_G(\chi) = W_0(G_0)$, $W_G(\varphi) = W_0(\varphi)$ and then the Kan extension W of W_0 is given by

(3.1) $$W(G) = \varinjlim W_G$$

Notice that there is an underlying functor $U : I_G \rightarrow \mathcal{G}_0$ and that $W_G = W_0 U$. Suppose now that I_G is filtering. Then:

$$W(G) = \varinjlim W_G = \varinjlim W_0 U = \varinjlim W_0^\Sigma(U).$$

Thus if $\mathcal{G}_0$ has property P and (2.11) holds we may apply Theorem 2.10 and infer that:

$$W_1 \varinjlim U = W(G) \tag{3.2}$$

We have thus proved.

THEOREM 3.3. — *Let $\mathcal{G}_0 \subseteq \mathcal{G}_1 \subseteq \mathcal{G}$ be as in Section 2 with $\mathcal{G}_0$ having property P and assume that $W_0 : \mathcal{G}_0 \to \mathcal{E}$ satisfies* (2.11). *Suppose further that, for a given G in $\mathcal{G}_1$,*

$$\begin{array}{ll} (a) & I_G \text{ is filtering} \\ (b) & G = \varinjlim U \end{array}$$

Then $W_1(G) = W(G)$ where W is the Kan extension of W_0 to $\mathcal{G}$.

COROLLARY 3.4. — *Let $\mathcal{G}_0 \subseteq \mathcal{G}_1 \subseteq \mathcal{G}$ be as in Section 2 with $\mathcal{G}_0$ having property P and assume that $W_0 : \mathcal{G}_0 \to \mathcal{E}$ satisfies* (2.11). *Suppose further that there exists (I, F) in $\mathcal{G}_0^\Sigma$ such that $\varinjlim F = G$. Then I is embedded canonically in I_G and we suppose the embedding cofinal. We conclude that:*

$$W_1(G) = W(G)$$

where W is the Kan extension of W_0 to $\mathcal{G}$.

For the hypotheses imply (*a*) and (*b*) of Theorem 3.3 (see [2, 4]).

APPLICATION. — Let h be a good cohomology theory in the sense of Section 1. Then we suppose given (see [1, 7, 8]) a procedure for putting finitely-generated abelian coefficients into the theory h. Thus we are given a functor $W_0 : \mathcal{G}_0 \to$ *Cohg*, where $\mathcal{G}_0$ is the category of finitely-generated abelian groups and *Cohg* is the category of good cohomology theories. Then $\mathcal{G}_1 = \mathcal{A}b$, the category of abelian groups, $\mathcal{G}_0$ has property P, and one uses the universal coefficient theorem ([7]; see also (4.1)) to verify (2.11). Thus $W_1 : \mathcal{A}b \to$ *Cohg* is defined by (2.12). However it is plain in this case that the hypotheses of Corollary 3.4 are satisfied for all G in $\mathcal{A}b$, so that W_1 is just the Kan extension of W_0 to $\mathcal{A}b$. This argument is, of course, quite different from Ulmer's, which was based on the additivity of W_0, of which no apparent use is made in Corollary 3.4.

If h is not a good theory, we may carry out the same argument with $\mathcal{G}_0$ the category of finitely-generated 2-torsion-free abelian groups, $W_0 : \mathcal{G}_0 \to$ *Coh*, the category of cohomology theories. Again we conclude that W_1 is the Kan extension of W_0 to the category of 2-torsion-free abelian groups.

4. The splitting of universal coefficient sequences.

We confine attention to the universal coefficient sequence in general cohomology

$$0 \to h^n(X) \otimes G \to h^n(X; G) \to \operatorname{Tor}(h^{n+1}(X), G) \to 0 \tag{4.1}$$

though our arguments apply more broadly (see [3] for details). Then (4.1) is natural in G on $\mathcal{A}b$ if h is a good theory, and is natural in G on $\mathcal{A}b_{(2)}$, the category of 2-torsion-free abelian groups, for any theory h. If G is countable with 2-torsion and h is not good, then (4.1) still subsists and is *quasi-natural* in the sense that we may associate with $\varphi : G \to G'$ a set of homomorphisms

$$\varphi_{\#} : h^n(X ; G) \to h^n(X ; G')$$

in a quasi-functorial way such that:

$$\begin{array}{ccccccccc} 0 & \to & h^n(X) \otimes G & \to & h^n(X ; G) & \to & \operatorname{Tor}(h^{n+1}(X), G) & \to & 0 \\ & & \downarrow{\scriptstyle 1 \otimes \varphi} & & \downarrow{\scriptstyle \varphi_{\#}} & & \downarrow{\scriptstyle \operatorname{Tor}(1,\varphi)} & & \\ 0 & \to & h^n(X) \otimes G' & \to & h^n(X ; G') & \to & \operatorname{Tor}(h^{n+1}(X), G') & \to & 0 \end{array}$$

commutes.

PROPOSITION 4.2. — *If* (4.1) *is pure (i. e., $h^n(X) \otimes G$ is pure in $h^n(X : G)$) then it splits provided the torsion subgroup of $h^{n+1}(X)$ or G has bounded exponent.*

THEOREM 4.3. — *Whenever* (4.1) *is natural it is pure.*

Let us say that an abelian group A is 2-*high* if every element $a \in A$ such $2a = 0$ can be halved. Thus, if A is finitely-generated, A is 2-high if and only if $\mathbb{Z}_2$ is not a summand.

THEOREM 4.4. — *The sequence* (4.1) *is pure provided at least one of $h^n(X)$, $h^{n+1}(X)$, G is 2-high.*

Thus, if we confine attention to finitely-generated groups, (4.1) splits unless $h^n(X) \otimes G$ and Tor $(h^{n+1}(X), G)$ have $\mathbb{Z}_2$ summands yielding $\mathbb{Z}_4$ in $h^n(X ; G)$ and this can only happen when $h^n(X)$, $h^{n+1}(X)$, G all have $\mathbb{Z}_2$ summands. Such a situation does indeed arise with real K-theory or stable cohomotopy theory mod 2.

BIBLIOGRAPHY

[1] S. ARAKI and H. TODA. — Multiplicative structures in mod q cohomology theories I, *Osaka J. Math.*, 2 (1965), pp. 71-115.

[2] M. ARTIN and B. MAZUR. — Etale Homotopy, *Lecture notes* (Springer), No. 100 (1969).

[3] A. DELEANU and P. J. HILTON. — On the splitting of universal coefficient sequences, *Proc. Coll. Alg. Top.*, Aarhus (1970), pp. 180-201.

[4] —. — Remark on Cech extensions of cohomology functors, *Ibid.*, pp. 44-66.

[5] B. ECKMANN and P. J. HILTON. — Commuting limits with colimits, *Journ. Alg.*, 11 (1969), pp. 116-144.

[6] P. J. HILTON. — On the category of direct systems and functors on groups, *Journ. Pure and Appl. Alg.*, 1 (1971), pp. 1-26.

[7] —. — Putting coefficients into a cohomology theory, *Proc. Neth. Acad. Sci.*, 73 (1970), pp. 196-216.

[8] C. R. F. MAUNDER. — Mod p cohomology operations and the Bokstein spectral sequence, *Proc. Cam. Phil. Soc.*, 63 (1967), pp. 23-43.

[9] G. MISLIN. — The splitting of the Künneth sequence for generalised cohomology (to appear).

Cornell University
Department of Mathematics,
Ithaca, N. Y. 14850 (U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 329 à 334.

QUANTIFIERS AND SHEAVES

by F. W. LAWVERE

The unity of opposites in the title is essentially that between logic and geometry, and there are compelling reasons for maintaining that geometry is the leading aspect. At the same time, in the present joint work with Myles Tierney there are important influences in the other direction: a Grothendieck " topology " appears most naturally as a modal operator, of the nature " it is locally the case that ", the usual logical operators such as $\forall$, $\exists$, $\Rightarrow$ have natural analogues which apply to families of geometrical objects rather than to propositional functions, and an important technique is to lift constructions first understood for " the " category $\underline{S}$ of abstract sets to an arbitrary topos. We first sum up the principal contradictions of the Grothendieck-Giraud-Verdier theory of topos in terms of four or five adjoint functors, significantly generalizing the theory to free it of reliance on an *external* notion of infinite limit (in particular enabling one to claim that in a sense logic is a special case of geometry). The method thus developing is then applied to intrinsically define the concept of Boolean-valued model for $\underline{S}$ ($\underline{\underline{BVM}/\underline{S}}$) and to prove the independence of the continuum hypothesis free of any use of transfinite induction. The second application of the method outlined here is an intrinsic geometric construction of the Chevalley-Hakim global spectrum of a ringed topos free of any choice of a " site of definition ".

When the main contradictions of a thing have been found, the scientific procedure is to summarize them in slogans which one then constantly uses as an ideological weapon for the further development and transformation of the thing. Doing this for " set theory " requires taking account of the experience that the main pairs of opposing tendencies in mathematics take the form of adjoint functors, and frees us of the mathematically irrelevant traces ($\in$) left behind by the process of accumulating ($\cup$) the power set (P) at each stage of a metaphysical " construction ". Further, experience with sheaves, permutation representations, algebraic spaces, etc., shows that a " set theory " for geometry should apply not only to *abstract* sets divorced from time, space, ring of definition, etc., but also to more general sets which do in fact develop along such parameters. For such sets, usually logic is " intuitionistic " (in its formal properties) usually the axiom of choice is false, and usually a set is not determined by its points defined over 1 only.

1. By a topos we mean a category $\underline{E}$ which has finite limits and finite colimits, which is (*a*) cartesian closed and which (*b*) has a subobject classifier T. That is (*a*) on the one hand there is for each object A an internal hom functor $(\ )^A$ right adjoint to cartesian product $(\ ) \times A$, and (*b*) on the other hand there is a single map true: $1 \to T$ such that any monomorphism $X' \rightarrowtail X$ in $\underline{E}$ is the pullback of true along a unique characteristic map $X \to T$. This is the principal struggle in the internal theory of an arbitrary topos, and leads to very rapid development. The " set " T of

" truth-values " for $\underline{E}$ is shown to be a Heyting-algebra object which is complete in the sense that for any map $f: X \to Y$ in $\underline{E}$ there is a left adjoint $\exists_f$ to the induced map T^f and also a right adjoint

$$\forall_f : T^X \to T^Y$$

to T^f. Usually T is not a Boolean-algebra; for example if $\underline{E}$ = all $\underline{S}$-valued sheaves on a topological space, T is that sheaf whose sections over any U is the set of open subsets of U, while if $\underline{E} = \hat{\underline{C}} = \underline{C}^{\mathrm{op}}\underline{S}$ is set-valued functors on a small category $\underline{C}$, then $T(C)$ = all cribles of C. For any $\varphi : X \to T$, we denote by $\{ X/\varphi \}$ the corresponding subobject, correctly suggesting that to appropriate formulas of higher-order logic, a corresponding actual subobject exists.

All of the usual exactness properties of a topos follow quickly, most of them from the fact that there is for any $f: X \to Y$ a functor

$$\prod_f : \underline{E}/X \to \underline{E}/Y$$

right adjoint to pulling back families $E \to Y$ over Y along f to families $E \underset{Y}{\times} X$ indexed by X. This extends to the case where the fibers are being acted upon as follows: If $\underline{C}$ in Cat ($\underline{E}$) is an internal category object in $\underline{E}$ with object-of-objects X, we can consider all actions of $\underline{C}$ on arbitrary families $E \to X$ of objects internally parameterized by X, obtaining a new *topos* $\hat{\underline{C}} = C^{\mathrm{op}}\,\underline{E}$ of internal $\underline{E}$-valued presheaves on $\underline{C}$. If $f: \underline{C} \to \underline{C}'$ is any internal functor, there is a right adjoint $f_* : \hat{\underline{C}} \to \hat{\underline{C}}'$ to the induced functor (as well as a left adjoint f_0), which means that in a very useful sense, any topos (even if countable) is internally complete.

Let us denote by σ_X the " support " functor which to any family $E \to X$ assigns the caracteristic map of the image of the structure map. This then allows consideration of particular direct contradictions between logic and geometry of a kind arising in proof theory and reminiscent of virtual vector bundles:

(Π)

For every map $f: X \to Y$,
$$\begin{tikzcd} \underline{E}/X \arrow[r, "\prod_f"] \arrow[d, "\sigma_X"'] & \underline{E}/Y \arrow[d, "\sigma_Y"] \\ \underline{E}(X, T) \arrow[r, "\forall_f"'] & \underline{E}(Y, T) \end{tikzcd}$$

The above diagram commutes for permutation representations of a group, but not for the category $\underline{2}\,\underline{S}$ of maps in sets. On the other hand, both in intuitionistic logic and algebraic geometry we have to consider the extent to which the internal algebraicly defined operator $\exists$ actually means existence, which is essentially means whether

($\exists$) For every object E, the epi part *splits* in the following diagram

$$\begin{tikzcd} \underline{E} \arrow[r] & \{1 \mid \sigma_1(E)\} \arrow[r] \arrow[l, bend left, dashed] & 1 \end{tikzcd}$$

Now the latter condition *fails* for $\underline{G}\,\underline{S}$, $\underline{G}$ a non-trivial group, but *holds* for $\underline{P}\,\underline{S}$ where $\underline{P}$ is any well-ordered set (such as $\underline{2}$). Actually the conjunction of the two conditions (Π) and ($\exists$) is equivalent to the condition that every epi splits, which geometrically we would call 0-dimensionality and logically we would call the axiom of choice. If $\underline{E}$ is the category of equivalence classes of formulas in some higher theory, the condition ($\exists$) is a Skolem condition, but the problem arises also if $\underline{E}$ is of a geometrical nature since $\exists\varphi =$ true usually means actual existence only locally.

Often in a topos we have to make use of a further adjoint reflecting the contradiction between primitive recursion data and the family of sequences which it defines (T-valued sequences being the case known as mathematical induction), for example in analyzing a coequalizer or forming the free group or free ring object generated by a given object:

(ω) $\underline{E}^{\circlearrowleft} \to E$ is not an equivalence and has a left adjoint $(\ ) \times \omega$. Here $E^{\circlearrowleft}$ is the usual category of objects-together-with an-endomap. However we did not include this axiom in the definition of topos partly because of the useful generality and partly because it is automatically lifted to any topos $\underline{E}$ " defined over " another one $\underline{E}_0$ in which it is true.

" Defined over " refers to a given *geometrical morphism* of topos, by which we mean a functor having an exact left adjoint. There are also *logical morphisms* of topos, which means a functor preserving up to isomorphism all the structure involved in the concept of topos. The two unite in *local homeomorphism*, which is a geometrical morphism u whose left adjoint part u^* is actually a logical morphism.

THEOREM. — Any geometrical morphism $u : \underline{E}' \to \underline{E}''$ of topos can be factored into

$$\begin{tikzcd} \underline{E}' \arrow[rr, "u"] \arrow[dr, "u'"'] & & \underline{E}'' \\ & \underline{E} \arrow[ur, "u''"'] & \end{tikzcd}$$

Where $\underline{E}$ is also a topos, where u', u'' are geometrical morphisms of topos with the additional properties that $(u'')_*$ is full and faithful $\underline{E} \to \underline{E}''$ while the left adjoint $(u')^* : \underline{E} \to \underline{E}'$ reflects isomorphisms. Further, u'' (hence any full and faithful geometrical morphism) is entirely determined by a single map $j_u : T'' \to T''$ in $\underline{E}''$ of the kind we call a Grothendieck " topology ", in fact as the j_u-sheaves.

Shifting to a topos denoted by $\underline{E}$ (rather than $\underline{E}''$) the conditions which such a modal operator $j : T \to T$ should satisfy are that it is (*a*) idempotent and that it (*b*) commutes with true and with the conjunction map $\wedge : T \times T \to T$. Such induces functorially a closure operator on the set of subobjects of any object (not a Kuratowski closure; for example in presheaves on a topological space the appropriate j assigns to any order ideal of open sets the principal ideal determined by its union). In order to show that j yields a full and faithful geometrical morphism $\underline{E}_j \to \underline{E}$ of topos, we show that the usual condition of being a j-sheaf is equivalent to having a diagonal j-closed in the square (" separated ") and being j-closed in any separated object into which embedded. Then the associated sheaf functor is constructed without any appeal to infinite direct limits by using the following four observations about a Grothendieck " topology " (= modal operator j satisfying axioms (*a*) and (*b*): 1) The image T_j of j is a j-sheaf. 2) Y^X is a j-sheaf if Y is. 3) For any X, the j-closure in $X \times X$ of the diagonal is an equivalence relation. 4) If $X \to Y$ is any mono of X into any sheaf Y, then the j-closure in Y of X is the associated sheaf of X. (The first step (prior to applying the four observations) is to consider the singleton map $\{\ \} : X \to T^X$). One then proves that the associated sheaf functor is exact by studying the morphisms which it inverts.

An important example in which we use the above factorization theorem is (lifted to an arbitrary base topos $\underline{E}$ instead of $\underline{S}$) the Godement construction of sheaves on a topology basis by the method of resolving the contradiction between presheaves and (" discrete ") espace étalé. By a topology basis is meant a triplet consisting of an object X (of " points "), an object A (of " indices for the basis elements "), and a pairing $X \times A \to T$ which satisfies a directness condition so that the induced pair of adjoints

$$\underline{E}/X \underset{\Gamma}{\overset{\varinjlim}{\leftrightarrows}} \underline{A}^{\mathrm{op}}\underline{E}$$

is a geometrical morphism of topos (Here by $\underline{A}$ we mean the poset whose " hom " order relation $F \rightrightarrows A$ on " objects " in A is just thepullback along $A \to T^X$ of the standard order relation on subobjects of X). Then the " image " topos is the usual category of sheaves, describable either using a Grothendieck " topology " in $\underline{A}^{\mathrm{op}}\underline{E}$ or a left exact cotriple (standard construction) in $\underline{E}/X$.

There is a standard Grothendieck topology in any topos, namely double negation, which is more appropriately put into words as " it is cofinally the case that ". The category $\underline{E}_{\neg\neg}$ of double negation sheaves always satisfies the additional condition that the logic is classical:

$$(\neg) \qquad 1 + 1 \xrightarrow{\sim} T$$

which is equivalent with the condition that T (e. g. $T_{\neg\neg}$ in $\underline{E}_{\neg\neg}$) is a Boolean algebra object, which again geometrically is equivalent with the condition that every mono $X' \rightarrowtail X$ is part of a (unique) direct sum diagram $X' + (\neg X') \xrightarrow{\sim} X$.

For constructing logical morphisms of topos we need to use geometrical morphisms, but also another construction, a generalized ultraproduct, which does *not* give a geometrical morphism in general and hence leads outside the realm of externally complete (i. e. defined over given $\underline{E}_0$) topos considered up to now in geometry. The data needed for the generalized ultraproduct is a pair consisting of a functor $u_*: \underline{E} \to \underline{E}_0$ between two topos, which may be a geometrical morphism but which in general is only required to preserve finite inverse limits, and of a homomorphism $h: u_*(T) \to T_0$ of Heyting algebra objects of $\underline{E}_0$. A new category $\underline{E}_h$ is then obtained from $\underline{E}$ by formally inverting all monomorphisms $X' \rightarrowtail X$ in $\underline{E}$ whose " universal quantification belongs to the ultrafilter " in the sense that

$$h(u_*(\sigma_1(\prod_{X\to 1} X'))) = \mathrm{true}_0$$

THEOREM. — $\underline{E}_h$ is a topos and $\underline{E} \to \underline{E}_h$ a logical morphism. $\underline{E}_h$ is defined over $\underline{E}_0$ *in the sense of closed categories* but usually not in the geometrical sense of topos.

The above is needed, for example, to show that a $\underline{BVM}/\underline{S}$ can always be collapsed to a two-valued model, allowing most work on independence results to take place in higher topos without actually choosing h and making the collapse.

2. We can now make more precise what it is usually necessary to assume about " the " category $\underline{S}$ of abstract sets: it can be any topos satisfying conditions (Π), ($\exists$), (ω), ($\neg$) above as well as the following " irreducibility of 1 " condition:

$$(\vee) \quad \text{If } \varphi_i: 1 \to T \qquad \text{and} \qquad \varphi_1 \vee \varphi_2 = \text{true},$$

then

$$\varphi_1 = \text{true} \quad \text{or} \quad \varphi_2 = \text{true}.$$

Now conditions ($\neg$) and ($\vee$) together imply that there are only two subobjects of 1, but not conversely as $\underline{M}^{\mathrm{op}}\underline{S}$, for $\underline{M}$ a monoid but not a group, shows. On the other hand ($\exists$) and ($\neg$) together imply that the subobjects of 1 (which form a " complete " Boolean algebra then) also form a *generating* family for the category; a topos satisfying ($\exists$) and ($\neg$) we call " Boolean ", and in such usually write $2 = T$. By a Boolean-valued model $\underline{E}$ of $\underline{S}$ (in symbols $\underline{E} \in \underline{\underline{BVM}}/\underline{S}$) we mean then simply that $\underline{E}$ is a Boolean topos defined over $\underline{S}$. We can then show that any BVM over $\underline{S}$ actually also satisfies (Π) i. e. the axiom of choice, and indeed that the bi-category $\underline{\underline{BVM}}/\underline{S}$ is equivalent to the category $\underline{CBA}(\underline{S})$ of $\underline{S}$-complete Boolean algebra objects in $\underline{S}$.

Actually the BVM's can be constructed another way, namely as double negation sheaves $\tilde{\underline{P}} = (\underline{P}\,\underline{S})_{\neg\neg}$ in the category of $\underline{S}$-valued functors on some poset $\underline{P}$ in $\underline{S}$. In this case (as well as others) the terminology of Cohen is suggestive: if $X \in \tilde{\underline{P}}$, $q \geq p$ in $\underline{P}$, $\varphi : X \to 2$ and x is an element of X defined at p, say that " q forces $\varphi(x)$ " iff $\varphi(x/q) = \text{true}$. Then in $\tilde{\underline{P}}$, q forces $\varphi(x)$ iff r forces $\varphi(x)$ for a set of r cofinal beyond q.

To refute the continuum hypothesis in some $BVM\,\tilde{\underline{P}}$ we also follow Cohen by choosing a set I in $\underline{S}$ with $2^\omega < I$ in the sense that there is a mono but no epi. Then $\underline{P}$ is the poset (ordered by extension) of all partial maps $\omega \times I \to 2$ with finite domain (definable as an object in any topos). Then in $\tilde{\underline{P}}$

$$\omega < u^*(2^\omega) < 2^\omega$$

where u^* is the " constant sheaf " functor left adjoint to the " global sections " functor $u_* : \tilde{\underline{P}} \to \underline{S}$. For the proof, one notes that $\underline{P}$ itself is essentially the definition of a map $u^*(I) \rightarrowtail 2^\omega$ *on a covering*, hence for sheaves there is such a map. The main point is then the

LEMMA. — If $\underline{P}$ is any poset in $\underline{S}$ satisfying a suitable " countable chain condition ", X in $\underline{S}$ and Y in $\underline{S}$ with $Y \times \omega \cong Y$, then

$$\mathrm{Epi}\,(X, Y) = 0 \text{ in } \underline{S} \qquad \text{implies} \qquad \mathrm{Epi}\,(u^*(X), u^*(Y)) = 0 \text{ in } \tilde{\underline{P}}.$$

Here Epi (X, Y) is an object defined in any topos by pulling back " image " along " true ".

3. A particular sort of topology basis arises if an object A has the structure of a (multiplicative) commutative monoid and one is given a *homomorphism* $u : A \to T^X$ into the monoid of subobjects of an object X, where multiplication is defined as conjunction (intersection). In this case we have moreover that the order-relation-object $F \rightrightarrows A$ determines a submonoid of the constant functor $\overline{A}$ in $\underline{A}^{\mathrm{op}}\underline{E}$ and that the " membership " relation $P \rightarrowtail X \times A$ induced by the pairing determines a submonoid of the constant family $\dot{A}$ in $\underline{E}/X$. We may then form fractions to obtain new commutative monoid objects $(\dot{A})_P$ in $\underline{E}/X$ and $(\overline{A})_F$ in $\underline{A}^{\mathrm{op}}\underline{E}$ and in particular $\tilde{A}$ (in the intermediate sheaf category) which is the reflection of $(\overline{A})_F$ and which is reflected to $(\dot{A})_P$.

Suppose now that A is actually a commutative *ring* in $\underline{E}$. Because of the intuitionistic nature of logic (already for $\underline{E} = \underline{2}\,\underline{S}$) we are forced to define a *prime* x of A

to be, not an ideal, but a subobject of A satisfying rather four conditions of the form

1) $[1 \in x] = \text{true}$
2) $[f.g \in x] = [f \in x] \wedge [g \in x]$
3) $[0 \in x] = \text{false}$
4) $[f + g \in x] \leq [f \in x] \vee [g \in x]$

Note that 2) is an if-and-only-if condition and that the disjunction in the conclusion of the implication in 4) means essentially sup of two subobjects, which in a general topos may mean actual disjunction only locally. We further say that a ring is *local* iff the subobject of units is a prime. By a finite inverse limit, we get $X \rightarrowtail T^A$, " the subobject of T^A consisting of all subobjects of A which are prime ". This gives a topology basis in $\underline{E}$ whose sheaves form the topos Spec (A) known as the global spectrum of $\underline{E}, A$; in Spec (A), $\tilde{A}$ is a local ring object, and indeed the universal local A-algebra in topos defined over $\underline{E}$. Note that in the process, the membership relation is exactly transformed into its opposite.

4. While the application of our method to algebraic geometry has only begun, other questions also immediately arise. Unpublished work of George Rousseau shows that the semantics often given for intuitionistic logic is simply ordinary (i. e. for abstract sets) semantics done in a suitable topos $\Lambda\,\underline{S}$; a similar statement is true for Läuchli's proof-theoretic interpretation, as was recently shown by Anders Kock. But it would seem also possible to consider parameters designed to be applied to actual materialist time rather than just to stages in an imagined " construction ". In any topos satisfying (ω) each definition of the real numbers yields a definite object, but it is not yet known what theorems of analysis can be proved about it.

BIBLIOGRAPHY

MAO TSETUNG. — *On contradiction. Where do correct ideas come from?* Peking (1966).
GROTHENDIECK-GIRAUD-VERDIER. — *Topologie et faisceaux.*
Mme HAKIM. — *Schemas relatifs* (Thesis), Orsay (1967), S. G. A.
SOLOVAY-SCOTT. — *Boolean valued models of set theory.* To appear.
LAWVERE. — Adjointness in Foundations (Dialectica), vol. 23 (1969), pp. 281-296. Equality in Hyperdoctrines and the Comprehension Scheme as an Adjoint Functor, *Proc. of A. M. S. Symposium on Pure Math. XVII-Applications of Category Theory*, Providence (1970).

Department of Mathematics
Dalhousie University
Halifax, Nova Scotia,
Canada

Actes, Congrès intern. math., 1970. Tome 1, p. 335 à 339.

DIFFERENTIAL HOMOLOGICAL ALGEBRA

by JOHN C. MOORE

§ 1. A commentary on differential homological algebra.

Homological algebra since its first formal appearance in the book of H. Cartan and S. Eilenberg more than fifteen years ago has proved useful in many parts of mathematics, and indeed influenced their development. The original homological algebra was principally concerned with the study of various so called Hom(,) and tensor product functors defined on categories of modules, and with the derived functor of these functors. There have been many different generalizations and extensions of the original work, including the development of relative homological algebra, extensions to appropriate Abelian category contexts of the original formalism, and introduction and study of the derived functors of certain non-additive functors. However, the application to topology of homological algebra lead to somewhat different developments than those mentioned above, which may be generally included under the heading of differential homological algebra.

Before the formal advent of homological algebra there was already considerable evidence that it was necessary to study certain functors associated with differential algebras (i. e. differential graded algebras). This was to be found principally in the work of Eilenberg and MacLane on the homology of $K(\pi, n)$'s. Later the work of H. Cartan including the calculation of the homology of the $K(\pi, n)$'s gave further evidence in this direction, and many indications as to how to formulate a theory of homological algebra which would contain most of the original work, and the work of Eilenberg and MacLane on $K(\pi, n)$'s together with his own work. This theory is differential homological algebra.

Another development of the last fifteen years has been the gradual realization that in the applications of homological algebra to algebraic topology the notion of differential coalgebra (differential graded coalgebra) would play almost as important a role as that of differential algebra. Though from a modern point of view the idea of coalgebra is natural and straightforward it seems not to have appeared formally until some of the work of P. Cartier of the middle '50's.

The notions of differential coalgebra, comodule over a coalgebra, and differential comodule over a differential coalgebra came into being and started to receive considerable study in the following years.

Differential homological algebra is essentially the study of differential algebras and the derived functors of the tensor product and Hom(,) functors defined on appropriate categories of differential modules over differential algebras on the one hand, and the study of differential coalgebras and the derived functor of the cotensor product and Hom(,) functors defined on appropriate categories of differential comodules ovet differential coalgebras on the other hand.

While differential homological algebra may be defined abstractly this is essentially a unifying process which clears the head a bit. It is the standard natural cases which are of principal interest, as with ordinary homological algebra.

The process of defining derived functors in differential homological algebra is quite similar to that in ordinary homological algebra. One usually starts by forming " projective " resolutions or " injective " resolutions as required by the case under study. However, there are almost always two differences from the most classical homological algebra. First the resolutions are usually taken vis a vis a projective class or an injective class, and hence are part of relative homological algebra. Second the process of assembling the resolutions using the functor under study is slightly more complicated than classically; due to the fact that the differential in the complex which one forms comes in part from the morphisms in the resolution and in part from the fact that everything in sight had a differential to start out with. One of the early examples of this phenomenon occurred in the development of hyperhomology by Cartan and Eilenberg. Indeed hyperhomology may be viewed as the primitive basic example of differential homological algebra. The Künneth spectral theorem of hyperhomology is typical of the phenomena of differential homological algebra. This is in part the case because of the spectral sequence itself which relates certain classical derived functors with those of differential homological algebra which are sometimes called differential derived functors.

§ 2. Some relations between differential algebras and differential coalgebras.

Let R be a commutative ring, and let Diff alg (R) denote the full subcaterogy of the category of supplemented differential R-algebras generated by those objects A such that $A_q = 0$ for $q < 0$, and A_q is flat for all q. Let Diff coalg (R) denote the full subcategory of the category of supplemented differential R-coalgebras generated by those objects C such that $C_q = 0$ for $q < 0$, $C_0 = R$, and C_q is flat for all q.

THEOREM. — There are functors

$$B(\ ): \text{Diff alg}\ (R) \to \text{Diff coalg}\ (R),$$

and

$$\Omega(\ ): \text{Diff coalg}\ (R) \to \text{Diff alg}\ (R)$$

and morphism of functors $\alpha : \Omega B \to 1_{\text{Diffalg}(R)}$, and $\beta : 1_{\text{Diffcoalg}(R)} \to B\Omega$ such that

1) $(\alpha, \beta) : \Omega \dashv B$ is an adjoint pair of functors,
2) for any object C of Diff coalg (R)

the morphism $H\beta(C): H(C) \to HB\Omega(C)$ is an isomorphism, and

3) for any object A of Diff alg (R) such that $A_0 = R$,

the morphism $H\alpha(A): 4\Omega B(A) \to H(A)$ is an isomorphism.

The functor $B(\ )$ is called the *classifying functor* of the category Diff alg (R), and is aside from the emphasis on its coalgebra structure the reduced bar construction of Eilenberg and MacLane. The functor $\Omega(\ )$ is called the *loop functor* of the category Diff coalg (R), and is essentially the cobar construction of J. F. Adams.

For X and Y differential graded R-modules, if $f: X \to Y$ is a morphism of degree n of the underlying graded structures, then $Df: X \to Y$ is the morphism of degree $(n-1)$ of the underlying graded structures, defined by $Df = d(Y)f - (-1)^n fd(X)$. Note f is a differential morphism of degree n if and only if $Df = 0$, $DDf = 0$, and two differential morphisms of degree n, f, g, are homotopic if and only if there exists $h: X \to Y$ a morphism of degree $n+1$ of the underlying graded structures such that $Dh = f - g$.

If C in an object of Diff coalg (R), A is an object of Diff alg (R), $f: C \to A$ is a morphism of degree p of the underlying graded structures, and $g: C \to A$ is one of degree q, then $f \cup g: C \to A$ is the morphism of degree $p+q$ which is the composite

$$C \xrightarrow{\Delta(C)} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\phi(A)} A$$

where $\Delta(C)$ is the comultiplication of C and $\phi(A)$ is the multiplication of A. A morphism of degree -1 of the underlying graded structures, $\tau: C \to A$ is a *twisting morphism* (cochain) if $D\tau = + \tau \cup \tau$. The notion of twisting morphism was introduced by E. H. Brown and further studied by V. K. A. M. Guggenheim and others. Its importance lies in its relationship with (A, C) bundles. An (A, C) object X is a differential left A-module right C-comodule such that the diagram

$$\begin{tikzcd} A \otimes X \arrow[rr, "\phi(X)"] \arrow[d, "A \otimes \Delta(X)"] & & X \arrow[d, "\Delta(X)"] \\ A \otimes X \otimes C \arrow[rr, "\phi(X) \otimes C"] & & X \otimes C \end{tikzcd}$$

is commutative where $\phi(X)$ determines the module structure of X and $\Delta(X)$ the comodule structure. Such an object is an (A, C) bundle if neglecting differentials

1) X admits the structure of an extended A – module,
2) X admits the structure of an extended C – comodule,
3) the natural morphism $R \bigotimes_A X \to C$ is an isomorphism, and
4) the natural morphism $A \to X \,\square_C\, R$ is an isomorphism.

Any twisting morphism $\tau: C \to A$ determines an (A, C) bundle and any (A, C) bundle is isomorphic with one determined by a twisting morphism.

Given any object A of Diff alg (R), there is an $(A, B(A))$ bundle $W(A)$ determined by a twisting morphism $\tau A: B(A) \to A$ such that $H(W(A)) = R$. This universal bundle is essentially the acyclic bar construction of Cartan. If C is any object of Diff coalg (R), and X is any (A, C) bundle, then there is a morphism $f: C \to B(A)$ in Diff coalg (R) such that the (A, C) bundle X is isomorphic with that determined by the twisting morphism $\tau_A f: C \to A$.

Given any connected DGR-module X (i. e. such that $X_q = 0$ for $q \leq 0$) there is associated with X a connected differential coalgebra $T(X)$ and a morphism of DGR-modules $\alpha(X): T(X) \to X$ such that if C is a connected differential coalgebras and $g: C \to X$ a morphism of DGR-modules, then there is a unique morphism of differential coalgebras $\bar{g}: C \to T(X)$ such that $\alpha(X)\bar{g} = g$, i. e. $X \rightsquigarrow T(X)$ is an adjoint functor. Further if X_q is flat for all q, then so is $T(X)_q$.

If A is an object of Diff alg (R) with augmentation ideal $I(A)$, and $\gamma: s(I(A)) \to I(A)$

is the canonical isomorphism of degree -1 of the suspension of $I(A)$ with $I(A)$, then there is a unique $d'': T(sI(A)) \to T(sI(A))$ which is a morphism of degree -1 of the underlying graded structures and having the following properties:

i) $Dd'' = 0$,
ii) $d''d'' = 0$,
iii) if θ is the composite $T(sI(A)) \xrightarrow{\gamma(sI(A))} sI(A) \to I(A) \xrightarrow{\gamma} A$, then $\theta d'' = +\theta \cup \theta$, and
iv) $(d'' \otimes 1_T + 1_T \otimes d'')\Delta(T) = \Delta(T)d''$.

The classifying coalgebra of A, $B(A)$, has the same underlying coalgebra structure as does $T(sI(A))$, its differential is the sum of the differential of $T(sI(A))$ and d'', and $\tau_A : B(A) \to A$ is θ.

Given any object C of Diff coalg (R), there is an $(\Omega(C), C)$ bundle $E(C)$ determined by a twisting morphism $\tau_C : C \to \Omega(C)$ such that $H(E(C)) = R$. This universal bundle has the property that if A is any object of Diff alg (R) and X is an (A, C) bundle, there is a morphism $f: \Omega(C) \to A$ in Diff alg (R) such that the (A, C) bundle X is isomorphic with that determined by twisting morphism $f\tau_C : C \to A$.

The loop construction may be explicitly given in a manner dual to that sketched for the classifying construction. The flatness hypotheses are not necessary for part 1) of the theorem stated early in this paragraph or for the constructions indicated. However, they are needed for parts 2) and 3) of the theorem, and other homological properties.

§ 3. Some relation between differential Lie algebras and commutative differential coalgebras.

In this paragraph the ground ring will be assumed to be a field k of characteristics different from two. Let Diff coalg $^C(k)$ denote the full subcategory of Diff coalg (k), generated by those objects with commutative diagonal. Given an object C of Diff coalg $^C(k)$, there is a natural morphism of graded vector spaces $\tau_C : s^{-1}(J(C)) \to \Omega(C)$ where $J(C)$ is the augmentation coideal of C, and the sub Lie algebra of $\Omega(C)$ generated by the image of τ_C is a differential sub Lie algebra of $\Omega(C)$, where $\Omega(C)$ is considered as a Lie algebra via $[X, Y] = XY - (-1)^{rs}YX$ for $X \in \Omega(C)_r$, $Y \in \Omega(C)_s$. Proceeding one obtains a functor $L(\ ): \text{Diff coalg}\ ^C(k) \to \mathscr{L}(k)$, the category of differential Lie algebras over k.

If X is an object of $\mathscr{L}(k)$, its universal enveloping algebra $U(X)$ may be considered as an object of Diff alg (k). There is a natural diagram of graded vector spaces $s(X) \to sIU(X) \to B(U(X))$, and one lets $C(X)$ be the largest sub coalgebra of $B(U(X))$ which is commutative, and has $s(X)$ as its subspace of primitive elements. The coalgebra $C(X)$ is a differential sub coalgebra of $BU(X)$, and one has a functor

$$C(\ ): \mathscr{L}(k) \to \text{Diff coalg}\ ^C(k),$$

special cases of which are classical. There are morphisms of functors $\alpha : LC \to 1_{\mathscr{L}(k)}$ and $\beta : 1_{\text{Diff coalg}\, C(k)} \to CL$ such that $(\alpha, \beta): L \dashv C$ is an adjoint pair of functors.

Given an object Y of $\mathscr{L}(k)$, there is a twisting morphism $\tau_Y : C(Y) \to U(Y)$ which is the composite $C(Y) \to BU(Y) \xrightarrow{\tau(Y)} U(Y)$. The $(U(Y), (C(Y))$ determined by this twisting morphism is acyclic, and then the natural morphism $HC(Y) \rightarrow HBU(Y)$ is an isomorphism. Further this bundle admits additional structure so that it becomes a principal fibration in Diff coalg ${}^{C}(k)$ with base $C(Y)$ and structural group $U(Y)$.

PARTIAL BIBLIOGRAPHY

[1] J. F. ADAMS. — On the cobar construction, *Proc. N. A. S.*, U. S. A., 42 (1956), pp. 409-412.
[2] E. H. BROWN Jr. — Twisted tensor products I, *Ann. of Math.*, 69 (1959), pp. 223-246.
[3] H. CARTAN and S. EILENBERG. — *Homological algebra*, Princeton (1956).
[4] Sèminaire H. CARTAN, *E. N. S.*, Paris (1954-1955).
[5] Sèminaire H. CARTAN, *E. N. S.*, Paris (1959-1960).
[6] S. EILENBERG and S. MACLANE. — On the groups $H(\pi, n)$, I, *Ann. of Math.*, 58 (1953), pp. 55-106.
[7] — and J. C. MOORE. — Foundation of relative homological algebra, *Memoirs A. M. S.*, 55 (1965).
[8] —. — Homology and fibrations I, *Comm. Math. Helv.*, 40 (1966), pp. 199-236.
[9] V. GUGENHEIM. — *On the chain complex of a fibration* (to appear).
[10] S. MACLANE. — *Homology*, New York (1963).
[11] J. C. MOORE and L. SMITH. — Hopf algebras and multiplicative fibrations I, *Amer. J. Math.*, 90 (1968), pp. 752-780.
[12] —. — Hopf algebras and multiplicative fibrations II, *Amer. J. Math.*, 90 (1968), pp. 1113-1150.
[13] J. C. MOORE. — *Some properties of the loop homology of commutative coalgebras* (to appear).
[14] D. QUILLEN. — Rational homotopy theory n, *Ann. of Math.*, 90 (1969), pp. 205-295.

Princeton University
Department of Mathematics,
Fine Hall,
Princeton, New Jersey 08540
(U. S. A.

Actes, Congrès intern. math., 1970. Tome 1, p. 341 à 345.

B_3 - GROUPES FINIS

BLOCKS OF CHARACTERS

by RICHARD BRAUER

§ 1. Let G be a group of finite order g. Let p be a fixed prime number and take an algebraically closed field Ω of characteristic p. We can write the group algebra $\Omega[G]$ as a direct sum

$$\Omega[G] = \oplus \Sigma B \tag{1}$$

of two-sided ideals B of $\Omega[G]$ which themselves cannot be written non-trivially as direct sums of two-sided ideals. Equivalently, we can consider the algebra-homomorphisms ω_B of the *class algebra* (i. e. of the center $Z(\Omega[G])$ of $\Omega[G]$) of G over Ω onto the field Ω. These are in one-to-one correspondence with the ideals B in (1), if we require that ω_B maps the unit element of B non-trivially.

We are concerned with the influence of the decomposition (1) on the linear representations of G. For instance, if F is an irreducible representation of G in Ω, we associate F with the *block* B in (1), if the linear extension of F to a representation of $\Omega[G]$ maps B non-trivially. If X is an irreducible complex representation of G, we associate X with B, if the modular irreducible constituents F of X are associated with B. We then say that the character χ of X belongs to the *block* B.

I have studied these questions for a number of years, cf. [2] [3]. I wish to present here some newer developments. Since the theory is rather elaborate, it will be necessary to remain somewhat vague. Our main interest is to obtain results which can be applied to a study of the complex irreducible characters of G.

I may perhaps mention that it was recognized early in this work that especially strong results are available, if the prime p divides the order g with the exact exponent 1. For instance, such primes p occur for all known simple sporadic groups G, and for most of these, it is possible to obtain the characters of G assuming only the value of the order g and the simplicity of G.

It seems therefore highly desirable to generalize these results to the case that an arbitrary power of p divides g. Unfortunately, the results are here far less precise. They are of importance, if we wish to study finite groups G with a given Sylow-p-subgroup, especially for $p = 2$.

§ 2. It will be necessary to describe briefly some back ground material. Each block B determines a class of p-subgroups D of G, the *defect groups* of B. If $|D| = p^d$, d is called the *defect* of B. If $m \neq 0$ is a rational integer, m_p will denote the exact power of p dividing m. The degree $\chi(1)$ of an irreducible character χ in B is divisible by g_p/p^d and we may set $\chi(1)_p = g_p p^{h-d}$ with $h \geqslant 0$. Here, h is called the *height* of χ. Since B contains characters of height 0, the defect d of B can be characterized in this manner.

Consider a block b of a subgroup H of G with the defect group D_0 in H. Assume that the centralizer $C_G(D_0)$ of D_0 in G is contained in H. Then b determines a unique block B of G which is denoted by $B = b^G$. The relation between b and B is given by

$$\omega_B(SK) = \sum_L \omega_b(SL). \tag{2}$$

Here ω_B is the algebra-homomorphism of $Z(\Omega[G])$ corresponding to B; ω_b has the same significance for b. Further, K is a conjugacy class of G and L ranges over the conjugacy classes of H contained in K. Finally, $SK \in \Omega[G]$ denotes the *class sum* of K, i. e. the sum of the elements of K; SL has the analogous significance. For fixed B, the set of all blocks b of H with $b^G = B$ is denoted by $\mathscr{B}l(H, B)$. The defect group D_0 of b then is contained in a suitable defect group of B. If an irreducible character $\psi \in b$ is known, ω_b can be found, and (2) provides already some information concerning the characters in $B = b^G$.

If B is again a block of G with the defect group D, there exist blocks b of $DC(D)$ with $b^G = B$. All these b are conjugate under the action of $N(D)$ on $DC(D)$. They all have the defect group D. Each b contains a unique *canonical character* θ with the properties:

(*i*) θ is *trivial* on D, i. e. the kernel of the corresponding representation of $DC(D)$ contains D. Hence θ can be considered as irreducible character of

$$DC(D)/D \simeq C(D)/Z(D)$$

or as an irreducible character of $C(D)$ which is trivial on the center $Z(D)$ of D.

(*ii*) We have

$$\theta(1)_p = | C(D)/Z(D) |_p .$$

In other words, as character of $C(D)/Z(D)$, θ is the unique character of a block of defect 0.

(*iii*) If M is the stabilizer of θ in $N(D)$ acting on $DC(D)$ under conjugation, we have $| M\colon DC(D) |_p = 1$.

Conversely, if θ is an irreducible character of $DC(D)$ satisfying conditions (*i*) and (*ii*) and if b is the block of $DC(D)$ containing θ, then $B = b^G$ has a defect group containing D. The block B has the defect group D, if and only if (*iii*) holds.

We see that we can characterize blocks by means of irreducible characters θ of centralizers $C(D)$ of p-subgroups D of G. If we apply this type of characterization not only to blocks B of G but also to blocks b of subgroups, we can describe the set $\mathscr{B}l(H, B)$, cf. [3, I, **6**].

§ 3. We state what appears to be a basic result on blocks. For a given p and d, the p-blocks of defect d for the category of all finite groups G are distributed into a finite number of *types* T. In order to avoid to become too technical, I shall not define precisely what is meant by a type of blocks but will only indicate the idea and describe some properties.

First of all, all blocks B of a type T have the same defect group D considered as an abstract group. Moreover, we always have the same " fusion " of the elements of D in G. This is to say that the elements of this abstract group D are partitioned into subsets such that for each block B of type T, the defect group of B in the corresponding group G can be identified with the abstract group D in such a way that two elements of D are conjugate in G, if and only if they belong to the same subset. In particular, we can then find a set Π of elements π of D which represent the conjugacy classes of G which meet D, and which is the same for all blocks of type T.

Next, the number r_π of members b of $Bl(C(\pi), B)$ is the same for each $\pi \in \Pi$ for all B of the type T. Moreover, these b can be taken in such an order $b_1, b_2, \ldots, b_{r_\pi}$ that the number of modular irreducible representations in b_j does not depend on B $(j = 1, 2, \ldots, r_\pi)$. Finally, the arrangement can be chosen such that the decomposition numbers as well for B as for the b_j are the same for all B in question, provided that for each b_j, a suitable " basic set " is chosen.

It follows from this that, for all B of a given type, the number $k(B)$ of irreducible characters χ in B is the same. Likewise, the number $l(B)$ of modular irreducible characters in B is the same for all B of given type.

Because of the finiteness of the number of types, it is clear that $k(B)$ lies below a bound depending only on p^d. It is not known if always $k(B) \leqslant p^d$, but a weaker result has been obtained by W. Feit and the author by a different method.

It can also be shown that the number $k^{(0)}(B)$ of irreducible characters of height 0 is the same for all B of type T. If the degrees of these $k^{(0)}(B)$ characters are $x_1, x_2, \ldots$ the value of the quotients $x_i/x_j \pmod p$ can be found.

The really important properties of a block B of given type T appear, if we assume that we have additional information. Suppose for instance that, for each $\pi \in \Pi$ with $\pi \neq 1$, we know the irreducible characters of $C(\pi)$. If we know how the conjugacy classes of $C(\pi)$ are embedded in those of G, then we can find the values of all irreducible characters χ in B for all elements of G of order divisible by p. The known properties of group characters yield information concerning the remaining values of χ. It will be clear how much this will mean for a discussion of the characters of G.

There are further formulas available in the case $p = 2$ which express the group order g and which often lead to rather unexpected results.

§ 4. If B is a block with the defect group D, the problem arises to determine its type. We assume that B is characterized by the character θ of $C(D)$ as described in § 2.

The first step is to characterize the blocks $b \in \mathscr{B}l(C(\pi), B)$ for each $\pi \in D$. This can be done by the method of [3], cf. § 2. We require a certain amount of information concerning the centralizers of non-trivial p-subgroups of D and their characters. It suffices to take π in the system Π.

For the further discussion of the type of B, we have to use the known properties of characters, for instance, the orthogonality relations for decomposition numbers. This leaves us with a finite number of possibilities. Unfortunately, this number can be very large.

The whole discussion is considerably simpler for a special class of blocks B which we call flat blocks. First of all, B has *full defect*, i. e. the defect group D is a Sylow-p-subgroup P of G. *Here*, $PC(P) = P \times V$ where V is a group of order prime to p. We may then consider θ as an irreducible character of V.

We say that B is *flat*, if for each p-subgroup $Q \neq 1$ of G, we have a character ψ_Q of $C(Q)$ of degree 1 which is trivial on $Z(Q)$ such that the following conditions are satisfied:

(*i*) If $Q_0 = Q^\sigma$ with $\sigma \in G$, we have $\psi_{Q_0} = \psi_Q^\sigma$.

(*ii*) If $Q_1 \supset Q \supset 1$ are p-subgroups of G, then ψ_{Q_1} is the restriction of ψ_Q to $C(Q_1)$.

(*iii*) $$\psi_P = \theta.$$

In particular, $\theta(1) = 1$.

It can be shown that if a block B contains characters of degree 1, then B must be flat. In particular, the *principal block* B_0 (i. e. the block containing the principal character of G) is flat. Here ψ_Q is the principal character of $C(Q)$.

It can be seen that $| VG'\colon G' |$ blocks B of G contain characters of degree 1 and that each such B contains $| G\colon VG' |$ such characters: thus, the number of flat blocks is at most $| VG'\colon G' |$. Since the number of flat blocks can often be determined directly, we obtain upper bounds for $| VG'\colon G' |$.

It is remarkable that there are cases where each flat block contains characters of degree 1. For instance, this is so, if $p = 2$ and if the Sylow 2-group of G is either quasi-dihedral or a wreathed 2-group, cf. [1]. The discussion of the type of B_0 here shows that if G has no normal subgroup of order 2, B_0 contains only one character of degree 1. Thus, $VG' = G$ and we obtain a formula for $| G : G' |$.

J. Alperin, D. Gorenstein and the author have recently studied finite groups with quasi-dihedral and wreathed Sylow 2-subgroups. In particular, they have determined all simple groups of this type [1]. The character theoretic part of this work is based on a study of the possible types of flat blocks. Also, the formula for $| G\colon G' |$ plays an important role as well as some results discussed below in § 5.

§ 5. E. C. Dade [5] has determined the types of blocks with cyclic defect groups. This generalizes older results of the author for the case $d = 1$. This requires methods finer than the ones described above. Unfortunately, it has not been possible so far to find extensions of these methods to more general cases.

Even in the case of abelian defect groups D, our information about the possible types of flat blocks seems rather incomplete, except when $| D |$ is rather small. (It may be mentioned that for instance for $| D | = 9$, the results are sufficient to show that groups G of certain special orders g cannot be simple).

We mention a result for blocks B with abelian defect groups D which improves results of [3]. If D has rank r, then the height h of any character χ in B is less than $r(r + 1)/2$. If p lies above a bound depending only on r, then $h \leqslant r$.

This indicates that there are connections between the heights of the characters in blocks and the structure of D. It is not known whether or not characters of positive height occur in B, if and only if the defect group is non-abelian.

The situation is somewhat more favorable, when $p = 2$. For instance, all types of blocks B with dihedral defect group D of order $2^n \geqslant 4$ can be determined. We mention that we have here $k(B) = 2^{n-2} + 3$, $1 \leqslant l(B) \leqslant 3$. In each case, we obtain formulas for the group order g, similar to the formulas which had been known previously for the case that the Sylow 2-subgroup P of G itself is dihedral and B is the principal 2-block of G.

It seems certain that other 2-groups D can be studied successfully in a similar manner. Each result of this kind is of interest for an investigation of groups of even order.

REFERENCES

[1] J. ALPERIN, R. BRAUER and D. GORENSTEIN, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroup, To appear in the *Trans. Amer. Math. Soc.*, 151.
[2] R. BRAUER, Zur Darstellungstheorie der Gruppen endlicher Ordnung, *Math. Zeitschrift*, 63 (1956), pp. 406-444; 72 (1959), pp. 25-46.
[3] —. — On blocks and sections in finite groups, *Amer. J. of Math.*, 89 (1967), pp. 1115-1136; 90 (1968), pp. 895-925.
[4] —. — Some applications of the theory of blocks of characters of groups, IV, To appear in the *Journal of Algebra.*
[5] E. C. DADE, Blocks with cyclic defect groups, *Ann. of Math.*, 84 (1966), pp. 20-48.

Harvard University
Department of Mathematics,
2 Divinity Avenue,
Cambridge, Mass. 02138
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 347 à 348.

THE SUBGROUP STRUCTURES OF THE EXCEPTIONAL SIMPLE GROUPS

by J. H. CONWAY

The exceptional simple groups are those simple groups which have not yet been fitted into natural infinite families. They comprise the 5 Mathieu groups (M_{11}, M_{12}, M_{22}, M_{23}, M_{24}), 3 Janko groups ($J_1 = J$, $J_2 = HJ$, $J_3 = HJM$), 3 Conway groups (C_1, C_2, C_3), 3 Fischer groups (F_{22}, F_{23}, F_{24}), and individual groups discovered by Higman and Sims (HS), McLaughlin (Mc), Suzuki (Sz), Held (HTH), as well as a putative group discovered by Lyons (Ly?).

The relationships between these groups are not yet fully understood, although it is clear that there are many connexions. One informative approach is to investigate the subgroups of each of the groups above, and one purpose of this note is to record some of the progress made in this direction, mostly by the students of Professor D. Livingstone, of Birmingham University.

Let M be a maximal proper subgroup of a non-abelian simple group G, and let N be a minimal normal subgroup of M. Then the normaliser of N in G is certainly not all of G, since G is simple, and so it must coincide with M, since it certainly contains M. On the other hand, N is characteristically simple, and so a direct product of isomorphic simple groups. If these are cyclic p-groups C_p, N is an elementary abelian subgroup of G, and so may be supposed to be contained within a fixed Sylow p-subgroup P of G. So in this case it is sufficient to classify elementary abelian subgroups of P, find their normalisers in G, and check maximality.

In the remaining case, N is a direct product of isomorphic copies of a non-abelian simple group S, say, and consideration of possible orders will often show that $N = S$. Here there is no general technique, but there are a number of restrictions on the order of S that can be deduced from the character table of G and the Sylow theory, and it might be possible to identify all possible subgroups of permitted orders.

The programme has been completed for all the Mathieu groups, and for the groups J, HS, Mc, C_3, and it would probably be fairly easy to add the groups J_2 and J_3 to this list. A certain amount is known about the geometric interpretations of the subgroups in some of these cases when G has a natural geometric representation.

On the other hand, a certain amount of work has been done on the larger groups, although not in an exhaustive fashion. In C_1 there are many naturally defined subgroups which arise in a geometric manner, and which have been partially classified by R. T. Curtis, they include the Mathieu groups, the other Conway groups, the Higman and Sims and McLaughlin groups, the Hall-Janko group J_2, and a covering group of Suzuki's group. In F_{24}' Fischer has classified those subgroups generated by involutions of the defining class, and in the Lyons group, if it exists, there is a triple cover of McLaughlin's group, and probably a copy of the simple group $G_2(5)$.

Character tables have been computed for all the groups except the two largest Fischer groups, in most cases by hand computation, and in many cases before the construction of the group. But for the larger groups machine computation is essential, thus for C_0 (the double cover of C_1) the printed table measures 4 feet by 8, and required considerable calculations both by machine and by hand, the collaborators being M. J. T. Guy, J. G. Thompson and N. S. Patterson. It would be useful to have improved machine methods for calculating such tables, which are essential in any detailed investigation of a particular group.

In addition to the cases where one group is known or believed to be a subquotient of another, there seems to be a curious relation between the groups F_{24} and C_0 on which I have commented elsewhere. I think that a complete explanation of this " twinning " phenomenon would probably shed light on most of the problems concerned with the reasons for the existence of these apparently isolated groups.

Department of Mathematics,
16 Mill Lane,
Cambridge
(Grande-Bretagne)

Actes, Congrès intern. math., 1970. Tome 1, p. 349 à 353.

LOCAL AND GLOBAL PROPERTIES OF FINITE GROUPS

by GEORGE GLAUBERMAN

Let p be a prime and S be a Sylow p-subgroup of a finite group G. Suppose we are given information about the normalizers of several non-identity subgroups of S, perhaps all the non-identity subgroups of S, or perhaps a single characteristic subgroup of S. What does this tell us about the structure of G as a whole?

We will discuss two special cases of this problem and one related result. Let $O_p(G)$ denote the largest normal p-subgroup of G and $O^p(G)$ denote the subgroup of G generated by the p'-elements of G. Define $d(S)$ to be the maximum of the orders of the Abelian subgroups of S and define $J(S)$ to be the *Thompson subgroup* of S, generated by the Abelian subgroups of order $d(S)$. The characteristic subgroups $K_\infty(S)$ and $K^\infty(S)$ of S mentioned in Theorem 1 will be discussed below. We say that an element x of S is *weakly closed* in S with respect to G if the only element of S that is conjugate to x in G is x itself. Let D_8, S^4, and S^5 denote the dihedral group of order eight and the symmetric groups of degree four and five.

THEOREM 1 [5, II]. — *Suppose $p \geq 5$. Let N be $N_G(K_\infty(S))$ or $N_G(K^\infty(S))$. Then $G/O^p(G)$ is isomorphic to $N/O^p(N)$.*

THEOREM 2 [7, II]. — *Suppose $|S/O_p(G)| = p$. Then there exists a characteristic subgroup K of S such that $K \trianglelefteq G$ and such that the nilpotence class of S/K is at most three if $p = 3$ and at most two if $p \neq 3$.*

THEOREM 3 [4, II]. — *Suppose $p = 2$, $x \in S \cap Z(N_G(J(S)))$, and x is not weakly closed in S with respect to G. Then S contains a subgroup R that satisfies at least one of the following conditions:*

(*a*) *R has index two in S, $x \in R$, and $x \notin Z(N_G(R))$;*

(*b*) *R is an elementary Abelian group of order 16 and $N_G(R)/C_G(R)$ is isomorphic either to S^5 or to an extension of an elementary Abelian group of order 9 by D_8;*

(*c*) *$O^2(C_G(R))$ has a dihedral or semi-dihedral Sylow 2-subgroup of order at least 8, and $O^2(C_G(R)) \cap R = 1$.*

The proof of Theorem 1 naturally depends on the definitions of $K_\infty(S)$ and $K^\infty(S)$. They are obtained as " limits " of sequences of subgroups of S in the following way:

For every finite p-group P and every subgroup Q of P, we define two subgroups

$K_*(P; Q)$ and $K^*(P; Q)$ of P. Our definitions are designed so that both subgroups contain $Z(P)$ and

if $P \supseteq P_1 \supseteq Q_1 \supseteq Q$, then $K_*(P_1; Q_1) \subseteq K_*(P; Q)$ and $K^*(P_1; Q_1) \subseteq K^*(P; Q)$.

We then define

$K_{-1}(P) = P$;

$K_i(P) = K_*(P; K_{i-1}(P))$ if i is even and $i \geq 0$; and

$K_i(P) = K^*(P; K_{i-1}(P))$ if i is odd and $i \geq 1$.

Clearly, $K_{-1}(P) \supseteq K_1(P)$. By induction, $K_i(P) \supseteq K_{i+2}(P)$ for all odd i and $K_i(P) \subseteq K_{i+2}(P)$ for all even i. We define $K_\infty(P)$ to be the set-theoretic union of the groups $K_i(P)$, i even, and $K^\infty(P)$ to be the intersection of the groups $K_i(P)$, i odd. Then both of these groups contain $Z(P)$ and are therefore non-identity groups if $P \neq 1$. A short argument shows that if Q is a subgroup of P that contains $K_\infty(P)$ and $K^\infty(P)$, then $K_\infty(P) = K_\infty(Q)$ and $K^\infty(P) = K^\infty(Q)$.

Returning to our group G, we require some commutator notation to express the properties of $K_\infty(S)$ and $K^\infty(S)$. Let G' denote the commutator subgroup of G. Suppose $x \in G$. For every subgroup H of G, let $[H, x]$ be the subgroup of G generated by all the commutators $h^{-1}x^{-1}hx$ as h ranges over H. Let $[H, x; 1] = [H, x]$ and $[H, x; i+1] = [[H, x; i], x]$ for $i = 1, 2, 3, \ldots$ If $x \in S$ define the *degree* of x (relative to G) to be the smallest integer n such that $[H, x; n] \subseteq K$ for every chief factor of H/K of G such that $H \subseteq O_p(G)$.

The main property of $K_\infty(S)$ and $K^\infty(S)$ used in the proof of Theorem 1 is the following:

(1.1) *If $K_\infty(S) \ntrianglelefteq G$ or $K^\infty(S) \ntrianglelefteq G$, then S contains an element x such that $x \notin O_p(G)$ and x has degree at most four.*

To obtain (1.1), assume that no element of S satisfies the conclusion. Let $T = O_p(G)$. Let Q be a characteristic subgroup of T such that $[T, Q] \subseteq Z(Q) = C_T(Q)$; the existence of Q was proved by Thompson ([8], p. 185). We prove (1.1) by showing that $Q \subseteq K_i(S) \subseteq T$ for every non-negative integer i. By our remarks above, it follows that $K_\infty(S) = K_\infty(T) \trianglelefteq G$ and $K^\infty(S) = K^\infty(T) \trianglelefteq G$.

To apply (1.1), we use the following slight extension of some work of Feit [2], obtained independently by L. Scott and the author:

(1.2) *Let S^* be the subgroup of S generated by the elements of degree less than p. Let $T = O_p(G)$. Then $S^* \trianglelefteq S$ and $T \cap G' = T \cap (N_G(S^*))'$.*

This result can be obtained by transfer techniques similar to those of Wielandt [14].

Given (1.1) and (1.2), the proof of Theorem 1 reduces to the proof of an earlier, similar theorem [5, I] which required $p > 5$. A theorem of Tate [11], [13] shows that it is sufficient to prove that $G/S'O^p(G)$ is isomorphic to $N/S'O^p(N)$. Let $T = O_p(G)$. By some basic work of Alperin and Gorenstein [1], we may assume that $T \neq 1$. By using induction on G/T, we see that it suffices to obtain that $T \cap G' = T \cap N'$. Since $p > 4$, this follows from (1.1), (1.2), and induction.

The proof of Theorem 1 suggests several possibilities for improvement. It would be interesting if (1.1) could be strengthened, perhaps by the use of different characteristic subgroups, to yield x of degree at most three. If one could obtain x of degree at most two, an analogue of Theorem 1 for $p = 3$ would follow.

There are many other problems concerning local and global properties of groups that reduce to the case where $O_p(G) \neq 1$ and it is desired that some characteristic subgroup of S be normal in G. If p is odd, $C_G(O_p(G)) \subseteq O_p(G)$, and the special linear group $SL(2, p)$ of degree two over $GF(p)$ is not involved in G, then $Z(J(S)) \trianglelefteq G$ ([8], Theorems 8.1.2 and 8.2.11). Although this result is false for $p = 2$ ([3], p. 1132-1133), it is an open question whether some other non-identity characteristic subgroup of S must be normal in G. Even if $SL(2, p)$ is involved in G, result (1.1) suggests that when $O_p(G)$ is sufficiently " large " or complicated, then some non-identity characteristic subgroup of S must be normal in G. Theorem 2 represents a small step in this direction.

Theorem 2 is proved by considering various isomorphisms of subgroups of S. The main tool is a generalization of some results of Sims [10]:

(2.1) [7, *I*] *Let Q and R be subgroups of index p in a finite p-group P. Suppose ϕ is an isomorphism of R onto Q. Let $N(\phi)$ be the largest subgroup of R that is mapped onto itself by ϕ. Then $N(\phi) \trianglelefteq P$, and the nilpotence class of $P/N(\phi)$ is at most two if $p = 2$ and at most three if p is odd.*

To apply (2.1), take an arbitrary automorphism α of S and an arbitrary Sylow p-subgroup S^* of G. Let $T = O_p(G)$ and let $\hat{T}$ be the largest characteristic subgroup of S contained in T. Since T contains the Frattini subgroup of S, $S/\hat{T}$ is an elementary Abelian group. Take $h \in G$ such that h lies in the group generated by S and S^* and $h^{-1}Sh = S^*$. Let U be the inverse image of T under α. Define an isomorphism ϕ of U onto T by

$$\phi(x) = (x^{\alpha})^{h}, \quad \text{for all} \quad x \in U.$$

Take $N(\phi)$ as in (2.1). A short argument shows that $N(\phi) \trianglelefteq S^*$ and hence that α maps $N(\phi)$ onto itself. A more extensive investigation shows [7, I] that the nilpotence class of $S/N(\phi)$ is at most two unless $p = 3$.

Let $S = S_1, S_2, S_3, \dots$ and $T = T_1, T_2, T_3, \dots$ be the terms of the lower central series of S and T. Letting α and S^* vary above, we define four sets of conditions, at least one of which must be satisfied by S and G. An examination of each of these cases yields the following:

(2.2) [7, II] *Assume the hypothesis of Theorem 2 and assume the above notation. Then S and G enjoy at least one of the following properties*:

(*a*) $Z(S) \trianglelefteq G$;

(*b*) $J(S) = J(T)$;

(*c*) $S_i = T_i$ for all $i \geq 4$, and for $i = 3$ if $p \neq 3$;

(*d*) $\hat{T} \trianglelefteq G$.

Theorem 2 follows easily from (2.2) and induction.

By using Theorem 2 and the method of proof of Thompson's factorization theorem [12], we can prove the following corollary:

(2.3) *Suppose H is a subgroup of G, $p = 2$, and P is a Sylow 2-subgroup of H. Assume that $H/O_2(H)$ is a dihedral group, $P \subseteq S$, and $P = N_S(Q)$ for every non-identity normal subgroup of H contained in $O_2(H)$. Suppose $P \neq S$. Then $|P| \leq 2^4$.*

Actually, (2.3) was obtained in an earlier result (Theorem 2 of [6]). This result also describes the structure of S if $P \neq 1$, based on some results of W. J. Wong [15].

Now let us consider the proof of Theorem 3. By a short argument, there exists a p-subgroup D of $C_G(x)$ such that $x \in D$ and $x \notin Z(N_G(D))$. Replacing D by $J(D)$ if necessary, we may assume that $J(D) = D$. Let $P = N_S(D)$. We choose D to be maximal with respect to a certain partial ordering (Theorem 6 of [4, I]). By the results of [4, I] and an additional argument, P is a Sylow 2-subgroup of $N_G(D)$ and P contains a subgroup T of index two that satisfies the following conditions: $d(P) = d(T)$; $x \in T$; $x \notin Z(N_G(T))$; and P is a Sylow 2-subgroup of $N_G(T)$.

Now we obtain condition (*a*) of Theorem 3 if $P = S$. Assume that $P \neq S$. Take $T_0 \subseteq T$ maximal such that $T_0 \trianglelefteq H$ and $N_S(T_0) \supset U$. We may assume that $N_S(T_0)$ is a Sylow 2-subgroup of $N_G(T_0)$. Of course, it is entirely possible that $T_0 = 1$.

At this point, it does not seem possible to stretch the methods of [4, I] any further, even in the case where $T_0 = 1$. In fact, we were stuck at this point for several years. Here (2.3) seems to be necessary. From our above conditions, there exists a subgroup H of $N_G(T)$ such that $H \supseteq P$, $x \notin Z(H)$, and H/T is dihedral. Replacing H by H/T_0 and G by $N_G(T_0)/T_0$ in (2.3), we see that $|P/T_0| \leq 2^4$. We also obtain the structure of $N_S(T_0)/T_0$, by the remark after (2.3). By an application of McLaughlin's Theorem [9] on transvections over $GF(2)$ and by a transfer argument, we obtain condition (*b*) of Theorem 3 if $x \in T_0$ and condition (*c*) if $x \notin T_0$.

REFERENCES

[1] J. L. Alperin and D. Gorenstein. — Transfer and fusion in finite groups, *J. Algebra*, 6 (1967), pp. 242-255.

[2] W. Feit. — Some properties of the Green correspondence, in *Theory of Finite Groups, A Symposium*, W. A. Benjamin, New York (1969).

[3] G. Glauberman. — A characteristic subgroup of a p-stable group, *Canad. J. Math.*, 20 (1968), pp. 1101-1135.

[4] —. — Weakly closed elements of Sylow subgroups I, II, *Math. Zeit.*, 107 (1968), pp. 1-20; 112 (1969), pp. 89-100.

[5] —. — Prime-power factor groups of finite groups I, II, *Math. Zeit.*, 107 (1968), pp. 159-172; to appear.

[6] —. — Normalizers of p-subgroups in finite groups, *Pacific J. Math.*, 29 (1969), pp. 137-144.

[7] —. — Isomorphic subgroups of finite p-groups I, II, to appear.

[8] D. Gorenstein. — *Finite Groups*, Harper and Row, New York (1968).

[9] J. McLaughlin. — Some subgroups of $SL_n(F_2)$, *Ill. J. Math.*, 13 (1969), pp. 108-115.

[10] C. C. Sims. — Graphs and finite permutation groups, *Math. Zeit.*, 95 (1967), pp. 76-86.

[11] J. Tate. — Nilpotent quotient groups, *Topology*, 3 (1964), pp. 109-111.

[12] J. G. Thompson. — Factorizations for p-solvable groups, *Pacific J. Math.*, 16 (1966), pp. 371-372.

[13] —. — Normal p-complements and irreducible characters, *J. Algebra*, 14 (1970), pp. 129-134.

[14] H. WIELANDT. — p-Sylowgruppen and p-Factorgruppen, *J. Reine angew. Math.*, 182 (1940), pp. 180-193.

[15] W. J. WONG. — Determination of a class of primitive permutation groups, *Math. Zeit.*, 99 (1967), pp. 235-246.

University of Chicago
Department of Mathematics,
Eckhart Hall,
Chicago, Illinois 60637
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 355 à 360.

CENTRALIZERS OF INVOLUTIONS IN FINITE SIMPLE GROUPS

by DANIEL GORENSTEIN

It has been known for a long time that the structure of a finite simple group is intimately connected with the structure of the centralizers of its involutions. An old result of Brauer and Fowler asserts, in fact, that there are at most a finite number of simple groups in which the centralizer of an involution has a given structure. A more specific, pioneering result of Brauer established that the groups $PSL(3, q)$ with $q \equiv -1 (\text{mod } 4)$ and the Mathieu group M_{11} were the only simple groups in which the centralizer of an involution was isomorphic to a homomorphic image of $GL(2, q)$ by a central subgroup of odd order.

This last theorem was certainly one of the first of what has now become a major area of finite group theory, the characterization of the presently known simple groups in terms of the structure of the centralizers of their involutions. This work is developing at such a pace that it is not unreasonable to hope that within a very few years such characterizations will exist for all the known simple groups. We should mention that some of these investigations have led to the discovery of certain of the new sporadic simple groups. In fact, the first of these was discovered by Janko while studying groups in which the centralizer of an involution was isomorphic to the direct product of a group of order 2 and A_5.

In all these theorems one specifies to begin with the structure of the centralizer of one or more involutions of an abstract simple group G and then tries to prove that the structure of G (that is, its multiplication table) is essentially uniquely determined in terms of a set of generators and relations by the given conditions. On the other hand, in more general classification problems the objective of the analysis is, in contrast, the determination of the structure of these centralizers in the group under investigation. Once this is accomplished, the problem is thus reduced to precisely the kind of characterization theorem just described.

For example, in the study of simple groups whose Sylow 2-subgroups are either quasi-dihedral or a wreath product of a cyclic group of order at least 4 by a group of order 2, which have recently been completely characterized by Alperin, Brauer, and myself, almost all of our effort was devoted to establishing that in such a group G the centralizer of an involution is necessarily isomorphic to a homomorphic image of either $GL(2, q)$ or $GU(2, q)$ for some odd q by a central subgroup of odd order. Using the above-mentioned result of Brauer together with other related characterization theorems of Brauer, O'Nan, and Suzuki, we were able to conclude that G was isomorphic to one of the groups $PSL(3, q)$, $PSU(3, q)$, or M_{11}.

Even a cursory glance at the various general classification problems solved to date will reveal the essential role played by the centralizers of involutions in each of the proofs. It is therefore natural to raise the following general question:

What can one say about the centralizers of involutions in arbitrary finite simple groups?

Put in this form, the question is actually too general and probably unattackable, for it omits an essential ingredient of each of the successfully completed general classification problems: namely, the role played by induction. For example, in the quasi-dihedral and wreathed problem, our group G was by assumption a minimal counterexample to the desired classification theorem. But then using induction together with the previously obtained classification of groups with dihedral Sylow 2-subgroups together with the solvability of groups of odd order, we were able to determine the general shape of every proper subgroup of G. Without such knowledge, it would have been impossible for us to have carried out the so-called *local group-theoretic* analysis that constitutes the non character-theoretic portion of the proof. Moreover, it is precisely by means of extensions of this type of local group-theoretic analysis that the attack on the general problem posed above is to be made.

We see then that some hypotheses on the proper subgroups of G must be imposed if we are to expect to obtain any reasonable answers to our question. The most natural general condition is clearly the following: the composition factors of every proper subgroup of G are among the presently known simple groups. Indeed, in any specific general classification problem a minimal counterexample will always be a simple group of this type.

Of course, in each particular argument only certain properties of the known simple groups will actually be used. It turns out, in fact, that only very few of what appear to be general properties of the presently known simple groups enter into the analysis. These properties can actually be systematically formalized and, moreover, it is important to proceed formally since we want our results to remain valid, if at all possible, even if new simple groups are discovered in the future.

It is not surprising that not every composition factor of every proper subgroup of our group G plays a role; in fact, only certain composition factors of the centralizers of the involutions of G are critical. To describe these, we introduce some terminology. A *quasisimple* group is by definition a perfect central extension of a simple group and a *semisimple* group is any central product of quasisimple groups. Observe that any group H possesses a unique largest normal semisimple subgroup. As usual, $O(H)$ denotes the unique largest normal subgroup of H of odd order, the so-called (2-regular) *core* of H.

The key notion is that of $L(G)$, which is a certain collection of quasisimple groups associated with the group G. A given quasisimple group L is in $L(G)$ if and only if L is isomorphic to one of the quasisimple components of the largest normal semisimple subgroup of

$$C_G(x)/O(C_G(x))$$

for some involution x of G. It is primarily properties of the elements of $L(G)$ that are needed for our arguments.

For a given group G, $L(G)$ may, of course, be empty. Since each element of $L(G)$ is nonsolvable, this will clearly be the case if the centralizer of every involution of G

is solvable. Actually $L(G)$ is empty if and only if each such centralizer is 2-constrained. By definition, a group H is *2-constrained* if $C_{\bar{H}}(O_2(\bar{H})) \subseteq O_2(\bar{H})$, where $\bar{H} = H/O(H)$ and $O_2(\bar{H})$ denotes the largest normal 2-subgroup of $\bar{H}$.

What kind of results about the centralizers of involutions would one hope to establish? Obviously we would like to prove that these centralizers resemble those in the presently known simple groups, the closer, the better. Let us then briefly examine the centralizers of involutions in these groups. Apart from the alternating groups and the sporadic groups (and, of course, those of prime order), all the remaining known groups are of Lie type. Moreover, for a group L of the latter type, the centralizer of an involution t of L has sharply divergent form according as L is defined over a field of even or odd characteristic. This is natural since t is correspondingly a unipotent or semisimple element of L.

In the even characteristic case, it appears that $H = C_L(t)$ is always 2-constrained and has a trivial core. In particular, the largest normal semisimple subgroup K of H is trivial. By contrast, in the odd characteristic case, it appears to be generally true that H/K is a small solvable group and that K has 1 or 2 components which are of Lie type of odd characteristic (except in certain degenerate cases in which the number of components is 0, 3, or 4). Thus in the odd case, K dominates the structure of H. The centralizers of involutions in the sporadic groups have structures similar to those in the groups of Lie type of even characteristic period. (In some instances, K is non-trivial, but in such cases $K/Z(K)$ is isomorphic to a group of Lie type of even characteristic). In A_n, the centralizers of involutions have features of those in groups of Lie type of both even and odd characteristic.

I should like now to illustrate these considerations by describing two general results which pertain to the even and odd characteristic cases respectively. These results represent a joint effort with John Walter.

We have seen above that $O(C_L(t)) = 1$ in the characteristic 2 case. Let us say that any quasisimple group L with this property is *1-balanced*. In general, this property is false if L is of Lie type of odd characteristic or isomorphic to A_n with $n \equiv 3 \pmod 4$, but holds for the remaining known simple groups. A second condition which we need to state our first result is called *2-generation*. A quasisimple group L is said to be 2-generated if for any Sylow 2-subgroup R of L, we have

$$L = \langle N_L(Q) \mid Q \subseteq R,\ Q \text{ contains a noncyclic abelian subgroup} \rangle.$$

(We have here simplified both these definitions slightly; actually it is necessary to impose the conditions on certain collections of groups which contain L as a normal subgroup).

The so-called Bender groups $PSL(2, 2^n)$, $Sz(2^n)$, and $PSU(3, 2^n)$ and any of their central extensions by a group of order 2 are not 2-generated, as is easily checked, since in any of these groups a Sylow 2-subgroup is disjoint from its conjugates. Apart from the Bender groups, the only other known quasisimple groups that are not 2-generated are Janko's first group mentioned above and the perfect central extension $\hat{A}_9$ of A_9 by a group of order 2. For brevity, we call any one of the groups on this list *exceptional*.

Finally a group G is said to have *2-rank* or *normal 2-rank* at least k if a Sylow 2-subgroup of G possesses respectively an abelian or normal abelian subgroup of rank at least k. In particular, G has 2-rank 1 if and only if G possesses no non-cyclic abelian 2-subgroups and hence by a well-known result if and only if G has cyclic or generalized quaternian Sylow 2-subgroups.

We can now state our first result.

THEOREM. — Let G be a simple group of normal 2-rank at least 3. If every element of $L(G)$ is 1-balanced and either 2-generated or exceptional, then $O(C_G(x)) = 1$ for every involution x of G.

Actually in this degree of generality, some technical additional assumptions must be made. However, the stated result does hold if $L(G)$ is empty and hence if the centralizer of every involution of G is 2-constrained. Likewise it holds if every element of $L(G)$ is 2-generated.

This result, although very powerful in certain situations, still leaves one, in general, a long way from pinning down the structure of the centralizers of the involutions in such a group G, which we may view as the general group of " characteristic 2 " type. The central problem in the classification of simple groups of characteristic 2 type (which we note includes all the presently known sporadic groups along with the groups of Lie type of characteristic 2) is the development of general methods which will enable one to restrict the structure of these centralizers much more sharply. A major portion of Thompson's celebrated N-group paper (sections 8, 9, 13, 14, and 15) deals with a particular case of this problem. It will be important in this connection to determine how far his methods and results can be extended.

In contrast, our results in the odd characteristic case are already quite definitive. We shall not attempt to state here the exact set of conditions which we impose on the elements of $L(G)$, as some are fairly technical. Again they involve certain notions of balance and generation. They are embodied in the concepts of what we call a *Λ-group* and a *weak Λ-group.* The central point about a Λ-group or weak Λ-group G is that, in effect, we assume that the elements of $L(G)$ are of known type with at least one of these elements (but not necessarily all) being a group of Lie type of odd characteristic (and not isomorphic to one of even characteristic). The sole distinction between a Λ-group and a weak Λ-group is that in the former case the groups A_n and $\hat{A}_n$ with $n - 3$ divisible by a high power of 2 are excluded from $L(G)$. These particular groups require special treatment in our analysis, being the only known groups which do not have the property of what we call *3-balance.*

To state our principal result in the odd characteristic, we need one further notion. A group H is said to have *standard form* if H possesses a *normal* quasisimple subgroup L such that $C_H(L)$ has cyclic or generalized quaternion Sylow 2-subgroups. L is called the *standard component* of H.

Note that the possible structures of $C_H(L)$ are very restricted in this case and are completely known. Moreover, $H/LC_H(L)$ is isomorphic to a group of outer automorphisms of L. Hence the structure of H is essentially completely detérmined once the standard component L of H is specified.

Our main result asserts

THEOREM. — If G is either a simple Λ-group of normal 2-rank at least 13 or a simple weak Λ-group of normal 2-rank at least 17, then the centralizer of some involution of G is in standard form.

Our theorem actually asserts that the corresponding standard component satisfies conditions similar to those which hold in the groups of Lie type of odd characteristic. Thus, in effect, our result reduces the further study of such simple groups to the following general problem:

Determine all simple groups in which the centralizer of some involution is in standard form with standard component of Lie type of odd characteristic.

This statement is simply a more precise formulation of the general question which we discussed at the beginning: characterize the simple groups in terms of the structure of the centralizers of their involutions. Indeed, apart from a few degenerate cases of low Lie rank, every group of Lie type of odd characteristic possesses an involution whose centralizer is in standard form.

As indicated before, considerable progress has been made in this whole area and there is reasonable hope that the entire problem can be completely solved. If and when this is accomplished, our theorem could then be used as a basis for an inductive characterization of the groups of Lie type of odd characteristic. To complete such a characterization, it would be necessary, in addition, to determine all simple Λ-groups of normal 2-rank less than 13. Although some of our general arguments break down in such cases, there exist a number of special methods for handling the difficulties that arise.

We note also that our result in the odd characteristic case gives further evidence that the sporadic simple groups are somehow more related to the groups of Lie type of even characteristic.

We shall conclude now with a few remarks concerning the nature of the proof of the two stated theorems. Let S be a Sylow 2-subgroup of the group G satisfying the respective conditions. In each instance one proceeds by contradiction and the entire aim of the analysis is to demonstrate that the group

$$\langle\, C_G(x) \mid x \text{ ranging over the involutions of } S \,\rangle$$

is a *proper* subgroup of G.

Once this is established, the theorem in question follows immediately from a theorem of Bender. Indeed, the preceding assertion implies that G contains what is called a *strongly embedded* subgroup and Bender has completely classified all such groups. In particular, he has shown that $PSL(2, 2^n)$, $Sz(2^n)$, and $PSU(3, 2^n)$ are the only simple groups which possess a strongly embedded subgroup.

Thus the proof of both theorems comes down to what we may call " piecing together " the centralizers of the involutions of S. This will explain why our analysis requires conditions primarily on the centralizers of involutions. Furthermore, the need for S to contain abelian subgroups of suitably high rank comes about from the fact that we must continually compare the centralizers of different involutions of S and some degree of freedom is required to carry this out effectively.

The entire piecing together process is very general, most of it being almost formal in nature. In fact, I have come to think of the main steps in the argument as being essentially " functorial ". Indeed, the proof rests ultimately on what I have previously termed a *signalizer functor* and the so-called *signalizer functor theorem.*

If A is an elementary abelian 2-subgroup of the group G, we say that θ is an *A-signalizer functor on G* if for each involution a in A there is associated an A-invariant subgroup $\theta(C_G(a))$ of $O(C_G(a))$ which satisfies the compatibility condition

$$\theta(C_G(a)) \cap C_G(b) \subseteq \theta(C_G(b))$$

for any pair of involutions a, b of A.

The signalizer functor theorem asserts that if A has rank at least 3, then the subgroup

$$\langle\, \theta(C_G(a)) \mid \ a \text{ ranging over the involutions of } A \,\rangle$$

is of *odd* order.

Since, in practice, G will be non-solvable, this result implies that the given subgroup is a proper subgroup of G. David Goldschmidt has recently given an improved version and much simpler proof of the signalizer functor theorem than the original one that appears in the *Journal of Algebra.*

We note finally that under the assumptions of our first theorem, it turns out that $\theta(C_G(a)) = O(C_G(a))$ defines an A-signalizer functor on G. The aim of the proof is then to show that this θ is, in fact, the *trivial* signalizer functor. From this, the desired conclusion follows easily.

In summary, we have attempted to indicate that in simple groups whose proper subgroups have composition factors of known type and whose Sylow 2-subgroups are suitably large, general methods exist which enable one to determine, at least partially, the structure of the centralizers of their involutions.

Rutgers University
Department of Mathematics,
New Brunswick,
New Jersey 08.903
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 361 à 365.

A SURVEY OF SOME QUESTIONS AND RESULTS ABOUT RANK 3 PERMUTATION GROUPS

by D. G. HIGMAN

1. Rank 3 groups and strongly regular graphs.

We use throughout the notation of [5], to which we refer for the basic theory of finite rank 3 permutation groups G. The solvable primitive rank 3 permutation groups have been determined by Foulser [4] and, independently, by Dornhoff [2]. Since rank 3 groups of odd order are solvable we assume that G has even order. Then the graphs $\mathscr{I}_\Delta$ and $\mathscr{I}_\Gamma$ associated with the non-trivial orbitals Δ and Γ of G are a complementary pair of strongly regular graphs, both of which are connected if and only if G is primitive. We call a strongly regular graph *primitive* if it and its complement are connected. *A rank* 3 *graph* is defined to be a strongly regular graph whose automorphism group has rank 3 on the vertices.

The imprimitive rank 3 groups are certainly of interest, but our attention here is directed at the primitive ones.

2. Simple rank 3 groups.

Interest in rank 3 groups stems largely from the fact that many of the known finite simple groups have rank 3 representations, 3 being the minimal rank in many cases. The alternating groups of degree at least 5 and the classical groups of degree at least 4 have parabolic representations of rank 3, as do the groups $E_2(q)$. At least 12 of the 18 or 19 sporadic simple groups have rank 3 representations (the 5 Mathieu groups, the Hall-Janko group HJ, the Higman-Sims group HS, the McLaughlin group M^c, and the 3 Fischer groups). A question which arises at once is

QUESTION I. — What are the rank 3 subgroups of the known rank 3 groups?

We mention the following results in this connection:

(2.1) [8] The rank 3 subgroups of the symmetric group Σ_n, $n > 4$, in its action on the 2-element subsets are precisely the 4-fold transitive groups, together with $P\Gamma L_2(8)$ in case $n = 9$.

(2.2) [9] For $q \neq 2$, the rank 3 subgroups of $P\Gamma L_n(q)$, $n \geq 4$, in its action on the lines of the $(n-1)$-dimensional projective space $\mathbb{P}_{n-1}(q)$ are precisely those containing $PSL_n(q)$.

In proving (2.2) we use Perrin's result [16] that for $q \neq 2$ and $3 \leqslant k \leqslant \left[\dfrac{n}{2}\right] - 1$, a subgroup of $P\Gamma L_n(q)$ transitive on the k-dimensional linear varieties of $\mathbb{P}_{n-1}(q)$ contains $PSL_n(q)$. Perrin has proved the analogues of (2.2) for the symplectic and unitary groups acting on the absolute points, again under the assumption that $q \neq 2$.

3. The case $k = l = 2\mu$.

From now on we assume that G is a rank 3 group of even order with parameter set $\Phi = (n, k, l, \lambda, \mu, r, s, f, g)$. A question which arises in connection with any transitive permutation group is: what is the rank of its normalizer in the symmetric group? In our present case an application of Clifford's theorem gives

(3.1) If the normalizer of G is doubly-transitive, then

$$k = l = 2\mu. \tag{*}$$

For any integer μ, (*) determines a parameter set satisfying the standard conditions. Solvable groups of this type of degree q exist for every prime power $q \equiv 1$ (4), $q > 1$. Two results are

(3.2) (J. J. Seidel, cf. [5]). If G satisfies (*), then n is a sum of two squares.

(3.3) [10] If G satisfies (*) with μ a prime, then G is solvable.

QUESTION II. — Are there non-solvable rank 3 groups satisfying (*)?

4. Normal subgroups.

Assume that G is primitive. There is a unique minimal normal subgroup M of G, which is elementary abelian if regular and simple if primitive. In contrast to the doubly transitive case it can happen that M is neither regular nor primitive, but the possibilities for this are severely limited. In fact

(4.1) If G is primitive, M is not regular and N is a normal subgroup $\neq 1$ of G which is not primitive, then, for suitable choice of Δ, $\{ a, b \} \cup (\Delta(a) \cap \Delta(b))$, $(a, b) \in \Delta$, is an imprimitive block for N of minimal length > 1 and is a clique.

QUESTION III. — Is there a bound on the number of simple factors of M in case M is not regular?

QUESTION IV. — Is there a bound on the rank of M in case M is not regular?

As with doubly transitive groups there does not seem to be much information aside from the solvable case about

QUESTION V. — What are the rank 3 groups with regular normal subgroups?

Such groups arise in the theory of affine planes, since

(4.2) (Kallaher [12], Liebler [13]). A finite affine plane admitting a group of collineations having rank 3 on the points is a translation plane.

5. **Local to global.**

The first general question here is to obtain information about G form knowledge of G_a, the rank 3 extension problem being the case in which complete information about G_a is given and the question is that of the existence of G. Several sporadic simple groups were first constructed as solutions to this problem by first constructing a strongly regular graph, namely HS, M^c, Sz, and the three Fischer groups [7, 14, 20, 3].

We list some examples of results obtained for primitive G from information about the constituents of G_a. We easily see that if $G_a \mid \Delta(a)$ and $G_a \mid \Gamma(a)$ are both doubly transitive, then $n = 5$.

(5.1) [6, 6′] If $G_a \mid \Delta(a)$ is doubly transitive and $\mu = 1$, then either $n = 5$ and G is dihedral of order 10, $n = 10$ and G is isomorphic with one of A_5 or Σ_5, or $n = 50$ and G is isomorphic with $U_3(5)$ or $U_3(5)$ with the field automorphism adjoined.

(5.2) (M. Smith [19]. If $G_a \mid \Delta(a)$ is doubly transitive and $G_a \mid \Gamma(a)$ has rank 3, and if $\mu \geq 2$, then there exists an odd integer $s \geq 3$ such that (*i*) $\mu = \frac{1}{4}(s^2 - 1)$, $k = \frac{1}{8}(s^3 + 3s^2 - 5s + 1)$ and $n = \frac{1}{16}(s - 1)^2(s + 5)^2$, (*ii*) if $s = 3$, then G is a split extension of an elementary abelian group of order 16 by A_5 or Σ_5, (*iii*) if $s = 5$, then G is isomorphic with HS or its automorphism group, and (*iv*) $s = 7$ is impossible.

(5.1) and (5.2) are proved under weaker assumptions than stated here, and we have not given the full conclusion of Smith's result. (5.1) can be obtained as a consequence of a purely graph theoretic theorem of Hoffman and Singleton (cf. [18]) except that the case $n = 3250$ has only been eliminated under the rank 3 assumption.

(5.3) (S. Montague [15]). If $G_a \mid \Delta(a)$ is faithful and isomorphic with $PSL_2(q)$ in its action of degree $q + 1$, then $q = 4$ or 9.

Under the assumption that $l = k(k - 1)/2$, Montague gets the same conclusion for $PGL_2(q)$ and rules out $PSU_3(q)$, A_n, the Ree groups and the Suzuki groups $Sz(q)$, in their usual doubly transitive actions.

(5.4) (D. Perrin [16]). If $G_a \mid \Delta(a)$ is Frobenius, then G is either solvable or isomorphic with A_5 or Σ_5.

Question VI. — What are the G with $G_a \mid \Delta(a)$ and $G_a \mid \Gamma(a)$ both doubly transitive?

6. **Rank 3 graphs with given minimum eigenvalue.**

The rank 3 graphs with minimum eigenvalue $s = -2$ have been determined by Seidel ([17]; see also [18, 5]). A corresponding determination for $s = -3$ is much more difficult, including as it does the determination of the Steiner triple systems. On the other hand we should soon have a reliable answer to

Question VII. — What are the primitive rank 3 graphs with minimum eigenvalue -3?

For a given prime power $q \geq 2$ there are two infinite families of primitive rank 3 graphs with minimum eigenvalue $s = -(q+1)$, namely (1) the graph having as vertices the lines of $\mathbb{P}_n(q)$, $n \geq 3$, two being adjacent if they intersect, and (2) the subgraph of this graph having as vertices the lines not meeting a given coline. An important result proved by Sims [18] is

(6.1) For a fixed integer $m > 2$ there are at most finitely many non-isomorphic primitive rank 3 graphs with $s = -m$ not belonging to one of the families (1) or (2).

The proof, which depends on a general graph theoretic result of A. Hofmman, does not give a useful bound for the number of vertices in such graphs.

7. Characterization by the subdegrees.

Coincidences of parameter sets of non-isomorphic rank 3 graphs do occur, for example, the symplectic and orthogonal groups of degrees $2m$ and $2m+1$ respectively over $\mathbb{F}_q$, $m \geq 2$, have parabolic rank 3 representations with the same parameter sets. On the other hand, some rank 3 groups are already determined by the subdegrees, or, what is the same thing, by n and k. As an example of a result of this kind we state the following in which $Q_m = q^{m-1} + q^{m-2} + \ldots + 1$ and $Q_{m,2} = \dfrac{Q_m Q_{m-1}}{Q_2}$.

(7.1) [8, 9] Let $n = Q_{m,2}$ and $k = qQ_2Q_{m-2}$ with $m \geq 4$ and $q \geq 1$ integers. Then

I. For $q = 1$, either (*a*) G is isomorphic with a 4-fold transitive subgroup of degree m in its action on the 2-element subsets, (*b*) $m = 9$ and $G \approx P\Gamma L_2(8)$, or (*c*) $\mu = 6$ and $m = 9, 17, 27$ or 57, $\mu = 7$ and $m = 51$, or $\mu = 8$ and $m = 28, 36, 385, 903$ or 8128.

II. For $q \geq 2$, either (*a*) G is isomorphic with a subgroup of $P\Gamma L_m(q)$ in its action of the lines of $\mathbb{P}_{m-1}(q)$, (*b*) $m = 4$ or 5, or (*c*) m is odd, $7 \leqslant m \leqslant 17$ and $\mu \neq (q+1)^2$.

The case $\mu = 6$, $m = 9$ is realized by the automorphism group of $E_2(2)$.

QUESTION VIII. — Which of the remaining exceptional cases in (7.1) are realized?

8. Partial geometries.

The importance of partial geometries in the study of rank 3 permutation groups, and especially of Bose's results [1] giving sufficent conditions for a strongly regular graph to be the graph of a partial geometry, was demonstrated by Sims in his proof of (6.1), and they play a similar role in the proof of (7.1). We conclude with two questions about partial geometries which we are forced to ask on the basis of present evidence.

QUESTION IX. — Does there exist a partial geometry (whose automorphism group has rank 3 on the points or on the lines) with parameters (R, K, T) such that

$$1 < T < \min(R-1, K-1)?$$

The partial geometries with parameters $(R, K, 1)$ are precisely the generalized 4-gons in the sense of Tits.

QUESTION X. — Is a rank 3 graph with $\mu = -s$ necessarily the graph of a generalized 4-gon?

A result in this direction, with various applications, is given in [11].

REFERENCES

FG : *Theory of finite groups*, A symposium, edited by R. Brauer and C. S. Sah, Benjamin, New York (1969).

[1] R. C. BOSE. — Strongly regular graphs, partial geometries and partially balanced designs, *Pac. J. Math.*, 13 (1963), pp. 389-419.

[2] Larry DORNHOFF. — Primitive solvable rank 3 permutation groups, *Yale University notes* (1968).

[3] B. FISCHER. — Finite groups generated by 3-transpositions, *Inventiones Math.* (to appear).

[4] D. FOULSER. — Solvable primitive permutation groups of low rank, *Trans. Amer. Math. Soc.*

[5] M. D. HESTENES and D. G. HIGMAN. — Rank 3 permutation groups and strongly regular graphs, *Proceedings of the symposium on computers in number theory and algebra* (March 1970).

[6] D. G. HIGMAN. — Finite permutation groups of rank 3, *Math. Z.*, 86 (1964), pp. 145-156.

[6′] —. — Primitive rank 3 groups with a prime subdegree, *Math. Z.*, 91 (1966), pp. 70-86.

[7] — and C. C. SIMS. — A simple groups of order 44, 352, 000, *Math. Z.*, 105 (1968), pp. 110-113.

[8] —. — Characterization of families of rank 3 permutation groups by the subdegrees I, *Archiv der Mathematik*, 21 (1970), pp. 151-156.

[9] —. — Characterization of families of rank 3 permutation groups by the subdegrees II, *Archiv der Mathematik*.

[10] —. — Solvability of a class of rank 3 permutation groups, *Nagoya Math. J.*, vol. 41.

[11] —. — Strongly regular graphs and partial geometries (in preparation).

[12] M. J. KALLAHER. — On finite affine planes of rank 3, *J. Alg.*, 13 (1969), pp. 544-553.

[13] R. A. LIEBLER. — Finite affine planes of rank 3 are translative planes, *Math. Z.*

[14] J. E. MCLAUGHLIN. — A simple group of order 898, 128, 000 (Fg, 109-111).

[15] S. MONTAGUE. — On rank 3 groups with a multiply transitive constituent, *J. Alg.* (1970), pp. 506-522.

[16] D. PERRIN. — To appear.

[17] J. J. SEIDEL. — Strongly regular graphs with (− 1, 1, 0) adjacency matrix having eigenvalue 3, *Lin. alg. and its appl.*, 1 (1968), pp. 281-298.

[18] C. C. SIMS. — On graphs with rank 3 automorphism groups, *J. Comb. Theory.*

[19] M. SMITH. — On a class of rank three permutation groups, *Math. Z.* (to appear).

[20] M. SUZUKI. — A simple group of order 448, 345, 497, 600 (FG, 113-119).

University of Michigan
Department of Mathematics,
Ann Arbor, Michigan 48104
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 367 à 369.

A CLASS OF NON-SOLVABLE FINITE GROUPS

by ZVONIMIR JANKO

Let X be a finite group. If P is a p-subgroup of X different from identity (p is a prime), then the normalizer $N_X(P)$ of P in X is called a p-local subgroup of X.

A subgroup Y of X is called a local subgroup of X if Y is a p-local subgroup of X for some prime p.

The purpose of this work is to determine the structure of every non-solvable finite group G which has the following property:

(S) *Each 2-local subgroup H of G is solvable and all odd order Sylow subgroups of H are cyclic.*

We remark that John G. Thompson has considered in Section 15 of the N-groups paper all non-solvable finite groups X with the property that every local subgroup of X is solvable and every 2-local subgroup of X has cyclic Sylow p-subgroups for all odd primes p. Therefore this work can be considered as a generalization of the Thompson's (unpublished) work. Also the occurrence of the Tits simple group of order $2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$ which is an N-group makes the above problem very complicated. Here an N-group is a non-solvable finite group all of whose local subgroups are solvable.

The only known non abelian finite simple groups with the property (S) are: $L_2(r)$, $r > 3$, $L_3(3)$, M_{11}, $U_3(3)$, $Sz(q)$, $U_3(q)$ where $q = 2^n \geq 4$ and the Tits simple group. We shall call these groups SK-groups,

Let G be a non-abelian finite simple group of the smallest possible order which has the property (S) but which is not isomorphic to any SK-group. We have proved so far that the group G has the following properties:

(1) *Let T be a fixed Sylow 2-subgroup of G. Then T possesses a normal elementary abelian subgroup of order ≥ 8. Also T does not normalize any non-identity odd order subgroup of G.* Here we have used a joint result with J. G. Thompson and also some unpublished results of D. Gorenstein and J. H. Walter about centralizers of involutions.

(2) *A fixed Sylow 2-subgroup T of G is contained in at least two distinct maximal 2-local subgroups of G.* This result in particular rules out the possibility that T is a maximal subgroup of G. Also the chances to determine the structure of T are therefore increased.

(3) *Let H be any 2-local subgroup of G. Then the maximal normal odd order subgroup $O(H)$ of H is equal* 1. This is an immediate consequence of (1) and a result of D. Gorenstein about simple groups of characteristic 2 type.

(4) *The group G does not have a maximal* 2-*local subgroup M with the following properties*: (*i*) *Every normal abelian* 2-*subgroup of M is generated by at most two elements.* (*ii*) *M possesses a non-cyclic normal abelian* 2-*subgroup A such that $C_G(a) \subseteq M$ for every involution a of A.* The proof of this result is a straightforward adaptation of the corresponding result in Section 13 of the N-groups paper of J. G. Thompson.

(5) *The group G does not have a maximal* 2-*local subgroup M such that the maximal normal* 2-*subgroup $O_2(M)$ of M is of symplectic type.* Here a 2-group X is of symplectic type if X is non-cyclic and every characteristic abelian subgroup of X is cyclic. The proof of this result is also a straightforward adaptation of the proof of the corresponding results in Section 13 of the N-groups paper of J. G. Thompson.

(6) *Let T be a fixed Sylow* 2-*subgroup of G. Let M_1 and M_2 be two distinct maximal* 2-*local subgroups of G which contain T. Then we have $M_1 \cap M_2 = T$.*

This difficult result is proved in the following way. Assume that the result (6) is false. Then it is shown at first that G possesses one and only one maximal 2-local subgroup M containing T such that the order of M is divisible by a prime $p \geq 7$. Also $N_G(T) \subseteq M$. Let N be a maximal 2-local subgroup of G containing T which is different from M. Then we have $M \cap N = T \cdot D$, where $D \neq 1$, D is a cyclic odd order subgroup and T is normal in $T \cdot D$. Let E be a Hall $2'$-subgroup of M containing D and let F be a Hall $2'$-subgroup of N containing D. Then it is shown that E is a Frobenius group with kernel E' and a complement D and F is cyclic. We have $| F/D | = 3$ or 5 or 15. Also D is a Hall subgroup of F. The following result is crucial. For every subgroup D_0 of prime order p of D, D_0 centralizes a four subgroup of T, $C_G(D_0)$ is non-solvable and a Sylow p-subgroup of G is non-cyclic. By the methods of Section 13 of the N-groups paper of J. G. Thompson it is shown that $\Omega_1(Z(T))$ has order ≤ 4 and that $T_0 = \Omega_1(Z(T))$ is a normal subgroup of M. This last result is very strong and leads quickly to a contradiction. It is shown that D possesses a subgroup P of prime order p such that P centralizes T_0. It follows that the order of D is in fact equal p and that $p = 5$ or 7. Also $T_0 = \langle z \rangle$ has order 2, M has no normal four subgroups and $M = C_G(z)$. We have that $T_1 = C_T(D)$ is a Sylow 2-subgroup of $N_G(D) = C_G(D)$ and T_1 is either a dihedral group of order 8 or T_1 is a direct product of a group of order 2 and a dihedral group of order 8. If $p = 5$, then $C_G(D) = D \times L$ where L is isomorphic to A_6, S_5 or S_6 and if $p = 7$, then $C_G(D) = D \times L$ with $L \simeq L_2(7)$. Finally, we also get that $| F/D | = 3$. In all these results the minimality of $| G |$ is used several times. After that we show that $N_G(T) = M$. There are normal elementary abelian 2-subgroups of M of order ≥ 8. Let F be one of these of the smallest possible order. Then for every subgroup F_0 of index 2 of F we show that $C_G(F_0) \subseteq M$. After that a standard consideration of the weak closure of F in T yields a contradiction.

(7) *A Sylow* 2-*subgroup T of G is self-normalizing in G.* In the proof of this result the minimality of $| G |$ is used together with a result of C. Sims about primitive permutation groups.

(8) *Let M be any maximal* 2-*local subgroup of G containing the fixed Sylow* 2-*subgroup T of G. Then $T = TU$ where the subgroup U has order* 3 *or* 5 *or* 15. This result is proved by using the methods of Section 13 of the N-groups paper of J. G. Thompson.

As a direct consequence of this result we also get that every maximal 2-local subgroup of G has order $2^a k$ where $a > 0$ and $k = 3$ or 5 or 15.

As a conclusion we may say that the last result heavily restricts the structure of 2-local subgroups of G and so it is hoped that the final contradiction will be reached showing that there is no counter-example G. This will then show that every non-abelian finite simple group with the property (S) is an *SK-group.*

It is also easily seen that G is an N-group.

In the future work the following characterization of the Tits simple group given by D. Parrott (unpublished) will be very useful.

Let X be a finite simple group which possesses an involution z such that the centralizer H of z in X has the following properties:

(*i*) $O_2(H)$ *has order* 2^9 *and class at least* 3.

(*ii*) $H/O_2(H)$ *is a Frobenius group of order* 10 *or* 20.

(*iii*) *If P is a subgroup of order* 5 *of H, then the centralizer of P in $O_2(H)$ is contained in* $Z(O_2(H))$.

Then $H/O_2(H)$ *has order* 20 *and X is isomorphic to the Tits simple group.*

The Ohio State University
Department of Mathematics,
Columbus, Ohio 43210
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 371 à 373.

CHARACTERIZATIONS OF SOME FINITE SIMPLE GROUPS

by MICHIO SUZUKI

There have been many works done on the problem of characterizing some of the finite simple groups by the structure of the centralizers of some elements of order two. In a recent paper [4], we gave such a characterization of the special linear groups $L_n(q)$ over a finite field of characteristic 2. The purpose of this note is to report on similar characterizations of the unitary and the symplectic groups of arbitrary dimension over a finite field of characteristic 2.

We denote by $U = U_n(q)$ the projective special unitary group of dimension n defined over the field of q^2 elements. If φ is a non-degenerate hermitian form defined over an n-dimensional vector space V over the field of q^2 elements, the group U is isomorphic to the factor group of the group of unimodular linear transformations of V leaving φ invariant by the subgroup of the scalars. Thus U is a simple group except when $q = 2$ and $n = 3$. In this note we consider only the case:

$$q \quad \text{is a power of 2 and} \quad n \geqq 4.$$

Let t be an element of U, which corresponds to a unitary transvection on V with respect to φ. Then t is an involution in the center of a Sylow subgroup of U. It is easy to study the structure of the centralizer $C_U(t)$. In particular the center of $C_U(t)$ is an elementary abelian group of order q. The main result is the following theorem.

THEOREM. — Let G be a finite group and H be a subgroup of G satisfying the following two conditions:

(*i*) H is isomorphic to $C_U(t)$, and
(*ii*) if j is any involution of the center of H, then we have

$$C_G(j) \cong H.$$

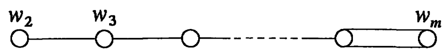
Then one of the following three holds:

(*a*) H is a normal subgroup of G;
(*b*) H has a normal complement in G;
(*c*) G is isomorphic to the unitary group $U_n(q)$.

The special cases of $n = 4$ and $n = 5$ of this theorem have been discussed by Suzuki [3] and Thomas [5] respectively. The same result is almost true for $n = 3$; the only exception occurs when $q = 2$. We remark that in case (*a*) the structure of the group G/H is very restricted. It is a group of order dividing $q - 1$. The case (b) is possible only when q is equal to 2.

The proof of the above theorem is similar to the one for the linear groups in [4] and we will omit the details here.

We may assume that $n \geqq 6$. The group H involves the unitary group of lower dimension. So H has a (BN)-pair of type B_{m-1} where $n = 2m$ or $2m + 1$. The main step of the proof is a construction of a (BN)-pair of type B_m in G. Suppose that the Weyl group of the (BN)-pair of H is generated by the distinguished set of generators $w_2, w_3, \ldots, w_m$. We can choose the notation so that the corresponding diagram is



Then the construction of a (BN)-pair of type B_m in G amounts to the addition of an involution w_1 to the left of the above diagram. We can find a candidate for w_1 in the normalizer of certain subgroup of H, and prove the required properties. This process is essentially similar to the corresponding step in the special linear group case [4] and depends on the detailed study of fusions of involutions. We use the Z^*-theorem of Glauberman, and remark that a recent theorem of Shult on fusions of involutions [2] is helpful in the proof. If the fusion pattern is the same with the unitary group, we can prove that the case (c) holds. Otherwise we have the non-simple cases (a) and (b). Although the proofs are similar we have to treat two cases separately in some points according as n is even or odd.

The final identification is done by applying a theorem of Tits [6], which characterizes the simple groups of Lie type of rank at least 3 as finite simple groups with (BN)-pairs. Tits' theorem is applicable since we assumed that $n = 6$. In our situation we have so much informations on hand that we could prove the uniqueness of the structure without appealing the work of Tits.

In the symplectic group case we have a similar result, which we omit to state. The proof is similar but in some sense harder. One reason is that there is an exceptional case when $n = 6$ and $q = 2$. This case has been treated by Yamaki [7]. We use a method similar to Yamaki's to treat the general case.

Similar theorems are expected to hold for other type of classical groups. Recently Dempwolff [1] generalized the main theorem of [4] by assuming only that the structure of the centralizer of an involution in the center of a Sylow 2-subgroup is the right one. Similar generalization will be true in the unitary or symplectic case.

REFERENCES

[1] U. Dempwolff. — *A characterization of L (2^m) by the centralizer of one 2-central involution.* To appear.

[2] E. Shult. — *On the fusion of an involution in its centralizer.* To appear.

[3] M. Suzuki. — *On characterizations of linear groups, V and VI.* To appear.

[4] —. — Characterizations of linear groups, *Bull. Amer. Math. Soc.*, 75 (1969), pp. 1043-1091.

[5] G. THOMAS. — A characterization of the unitary groups $PSU_5(q^2)$, $q = 2^n$. To appear in *Jour. of Algebra.*
[6] J. TITS. — *Buildings of spherical types and finite (BN)-pairs.* To appear.
[7] H. YAMAKI. — A characterization of the simple group $S_p(6, 2)$, *Jour. Japanese Math. Soc.*

University of Illinois
at Urbana-Champaign
Department of Mathematics,
Urbana, Illinois 61801
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 375 à 376.

QUADRATIC PAIRS

by J. G. THOMSON

DEFINITION. — (G, M) is a quadratic pair for p if

1. G is a finite group $\neq 1$.
2. M is an irreducible F_pG-module ($F_p = \mathbb{Z}/p\mathbb{Z}$).
3. G acts faithfully on M.
4. $G = \langle Q \rangle$, where $Q = \{ x \in G - \{ 1 \} \mid M(x-1)^2 = 0 \}$.

CENTRAL PRODUCT THEOREM. — If (G, M) is a quadratic pair for p and $p \geqslant 5$, then for some $n \geqslant 1$:

1. $G = G_1, \ldots, G_n$, $[G_i, G_j] = 1$ if $i \neq j$ and $G_i = G_i'$, $G_i/Z(G_i)$ is simple.
2. For suitable M_i, (G_i, M_i) is a quadratic pair for p.
3. $M \cong M_1 \otimes \ldots \otimes M_n$ as F_pG-modules.

MAIN THEOREM. — If (G, M) is a quadratic pair for p, $p \geqslant 5$, $G = G'$ and $\overline{G} = G/Z(G)$ is simple, then $\overline{G}$ is isomorphic to one of the following groups:

$$A_n(q),\quad B_n(q),\quad C_n(q),\quad D_n(q),\quad G_2(q),\quad F_4(q),\quad E_6(q),\quad E_7(q),$$
$$^2A_n(q),\quad {}^2D_n(q),\quad {}^3D_4(q),\quad {}^2E_6(q).$$

Here q is the order of the center of a Sylow p-subgroup of G.

The proofs are not short, and begin with considerable notation. If $x \in Q$, let $p^{d(x)} = |M(x-1)|$, and set $Q_e = \{ x \in Q \mid d(x) = e \}$. Let $d = \min_{x \in Q} (d(x))$. The set Q_d is singled out for special study. If $x, y \in Q_d$, write $x \sim y$ if and only if $\ker(x-1) = \ker(y-1)$ and $\operatorname{im}(x-1) = \operatorname{im}(y-1)$. Let $E(x)^{\#} = \{ y \in Q_d \mid y \sim x \}$. Then it is easy to see that $E(x)^{\#} \cup \{ 1 \} = E(x)$ is a subgroup of G for each $x \in Q_d$, and we let Σ be the set of such subgroups.

An important preliminary result is that if $E, F \in \Sigma$ and $H = \langle E, F \rangle$ then one of the following holds:

(*a*) H is abelian.
(*b*) $H' \in \Sigma$.
(*c*) $H \cong SL(2, |E|)$.

This result immediately raises the question of classifying groups which are generated by a collection of subgroups Σ whose subgroups H satisfy (*a*), (*b*) or (*c*), and such that if $E \in \Sigma$, then all conjugates of E are in Σ. This problem seems quite difficult. For example, the groups of Fischer (F_{22}, F_{23}, F_{24}) satisfy this condition.

Keeping to our quadratic pair, let $\mathcal{O}(E) = \{ F \in \Sigma \mid \langle E, F \rangle \cong SL(2, |E|) \}$. By a theorem of R. Baer, $\mathcal{O}(E) \neq \phi$ for all $E \in \Sigma$. It turns out that it is possible to parametrize $\mathcal{O}(E)$ in an exploitable fashion. To do this, define $M_E = \ker(x - 1)$, $M^E = M(x - 1)$ $(x \in E - \{1\})$. By the construction of Σ, M_E, M^E do not depend on our choice of x. Let $U(E)$ be the largest subgroup of G which is 1 on M/M_E, M_E/M^E and on M^E. Choose $F \in \mathcal{O}(E)$. Then there is a bijection of $U(E)$ and $\mathcal{O}(E)$ given by $\eta \mapsto \eta^{-1}F\eta$. This labelling of $\mathcal{O}(E)$ is very helpful. In proving this result, we get a remarkable property of G. Namely, if F_1, $F_2 \in \mathcal{O}(E)$ and the unique involution of $\langle E, F_1 \rangle$ coincides with the unique involution of $\langle E, F_2 \rangle$, then

$$\langle E, F_1 \rangle = \langle E, F_2 \rangle.$$

This result reduces the study of $\mathcal{O}(E)$ to the study of $I(E)$, the set of involutions i of G such that for some $F \in \mathcal{O}(E)$, $i \in \langle E, F \rangle$.

The previous results lead quickly to a proof of the central product theorem, so we can concentrate on the main theorem. Again let $E \in \Sigma$, $F \in \mathcal{O}(E)$, and set $S = \langle E, F \rangle$, $C = C_G(E)$, $D = C_G(S)$. Then $C = U(E) \cdot D$ and $U(E) \lhd C$, $U(E) \cap D = 1$. Furthermore, $Z(C_G(E)) = E \times Z(G)$ and we obtain all the possibilities for the isomorphism class of $C_G(E)/Z(G)$. Let P be a Sylow p-subgroup of $C_G(E)$. Then P is a Sylow p-subgroup of G. Let $N_G(P) = P \cdot H$, where H is of order prime to p. A crucial but easy result is that if Σ_0 is the set of elements of Σ which are normalized by H, then for each $E_0 \in \Sigma_0$, $\Sigma_0 \cap \mathcal{O}(E_0)$ has precisely one element. Also, $N_G(H)$ is transitive on Σ_0. It is then relatively straightforward to construct the multiplication table of G via a Bruhat decomposition.

It is to be hoped that the quadratic pairs for the prime 3 can be classified, but this is a substantially more difficult problem.

The reason for studying quadratic pairs is that they seem to arise frequently in simple groups. More particularly, if G is simple and p is a prime such that for every p-local subgroup N of G, $O_p(N)$ contains its centralizer, then often quadratic pairs appears as (G_0, M) where G_0, M are subquotients of G. The study of such groups G is a vast program, a small corner of which is occupied by quadratic pairs.

University of Cambridge
Department of Mathematics,
16 Mill Lane,
Cambridge
(Grande-Bretagne)

Actes, Congrès intern. math., 1970. Tome 1, p. 377 à 379.

B_4 - CORPS LOCAUX ET GLOBAUX ANALYSE P-ADIQUE

ON CUBIC TRIGONOMETRIC SUMS

by J. W. S. CASSELS

0. We are concerned with a conjecture relating Gauss sums constructed with a character of order 3 (Kummer sums) and certain products of values of elliptic functions.

1. Let

$$p \equiv 1 \ (3)$$

be a rational prime. Then

$$4p = l^2 + 27m^2$$

for integers l, m, where l is uniquely determined by the normalization

$$l \equiv 1 \ (3)$$

but m is allowed to take either sign. Then

$$\varpi = (l + 3m\sqrt{-3})/2$$

is a prime in the ring $\mathbb{Z}[\omega]$, where $\omega^3 = 1$, $\omega \neq 1$.

A character χ of order 3 on $\mathbb{Z}/p\mathbb{Z}$ is defined by the congruence

$$\chi(a) \equiv a^{(p-1)/3} \ (\varpi)$$

The trigonometric sum in question is

$$\tau = \sum_{0<j<p} \chi(j)\xi^j \ (*)$$

where

$$\xi = e^{2\pi i/p}.$$

Gauss showed that

$$\tau^3 = p\varpi$$

but there is very little additional information about τ.

2. The elliptic curve

$$\mathscr{C}: \quad y^2 = 4x^3 - 1$$

with the usual Weierstrass parametrization

$$x = \wp(z) \quad , \quad y = \wp'(z)$$

has the module of periods

$$\theta\mathbb{Z}[\omega]$$

where

$$\theta = 3.0599\ \ldots$$

As was probably known to Eisenstein,

$$\prod_{\beta} \wp(\beta\theta/\varpi) = 1/\varpi^2,$$

where β runs through all residue classes modulo ϖ prime to ϖ.

A 1/3-set $\mathfrak{S}$ of residues mod ϖ is one such that

$$\beta, \quad \omega\beta, \quad \omega^2\beta \qquad (\beta\in\mathfrak{S})$$

is a complete set of residues prime to ϖ. By Wilson's Theorem

$$\prod_{\beta\in\mathfrak{S}}\beta \equiv -\Omega_{\mathfrak{S}}$$

for some cube root of unity $\Omega_{\mathfrak{S}}$. The product

$$P = \Omega_{\mathfrak{S}}^{-1}\prod_{\beta\in\mathfrak{S}}\wp(\beta/\varpi)$$

is independent of the choice of $\mathfrak{S}$ and satisfies

$$P^3 = \varpi^{-2}.$$

3. The following conjecture has been verified for all $p < 5.000$:

$$\tau = p^{1/3}\varpi P,$$

where $p^{1/3}$ is the real cube root.

4. The conjecture can be formulated in purely algebraic terms, i. e. independent of any embedding into the complex numbers. Let $\mathfrak{e}$ be a ϖ-division point on $\mathscr{C}$. With an obvious convention we write

$$P(\mathfrak{e}) = \Omega_{\mathfrak{S}}^{-1}\prod_{\beta\in\mathfrak{S}}x(\beta\mathfrak{e}).$$

Let $P'(\mathfrak{d})$ be the analogous quantity for a ϖ'-division point $\mathfrak{d}$. Let ξ be the Weil pairing of $\mathfrak{d}$, $\mathfrak{e}$ and now define τ by (*). The abstract version of the conjecture is

$$\tau = \chi(3)^2\,\{P(\mathfrak{e})\}^{-1}\varpi' P'(\mathfrak{d}).$$

The factor $\chi(3)^2$ occurs here because $e^{2\pi i/p}$ is not in general the Weil pairing of the points with parameters θ/ϖ and θ/ϖ'.

5. The p-adic treatment of the conjecture leads to the following problem for $\mathscr{C}$ over the finite field $\mathbb{F}$ of p elements. Working modulo ϖ, complex multiplication by ϖ is just the Frobenius, but complex multiplication by ϖ' is a separable isogeny. Let $\mathfrak{X}$ be a generic point and put $\mathfrak{x} = \varpi'\mathfrak{X}$. Then $\overline{\mathbb{F}}(\mathfrak{X})/\overline{\mathbb{F}}(\mathfrak{x})$ is an Artin-Schreier extension, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$. As a particular case of results of Deuring, there is a $g \in \mathbb{F}(\mathfrak{X})$ (note: $\mathbb{F}$ not $\overline{\mathbb{F}}$) such that the automorphism group is generated by

$$g \to g + j\mathfrak{A} \qquad (j \in \mathbb{F}),$$

where

$$\mathfrak{A}^{p-1} = \frac{1}{\left\{\frac{1}{3}(p-1)!\right\}^3}.$$

On the other hand, the automorphism group is just

$$\mathfrak{X} \to \mathfrak{X} + \mathfrak{d}$$

where $\mathfrak{d}$ is a ϖ'-division point. The problem is to give the coordinates of the $\mathfrak{d}$ corresponding to $g \to g + \mathfrak{A}$.

The author obtained formulae which are good enough for machine computation, and these led to the formulation of the conjecture. The formulae are deduced from the mod p analogues of some apparently quite new symmetry properties of the coefficients of classical elliptic functions.

REFERENCES

There is much more about the history of the problem and a complete set of references in my paper « On Kummer sums » in the Proceedings of the London Mathematical Society, (3), **21** (1970), pp. 19-27. It gives a fuller account of aspects slurred over in the foregoing resume.

University of Cambridge
Department
of Pure Mathematics
and Mathematical Statistics,
16 Mill Lane, Cambridge
(Grande-Bretagne)

Actes, Congrès intern. math., 1970. Tome 1, p. 381 à 389.

NON-ABELIAN CLASSFIELDS OVER FUNCTION FIELDS IN SPECIAL CASES

by YASUTAKA IHARA

1. General formulations and conjectures.

1.1. *Primes and Conjugacy Classes Principle.*

One of our basic ideas is that a certain type of infinite *discrete* groups Γ plays a central role in arithmetic of non-abelian extensions of algebraic function fields of one variable over finite fields (abbrev. function fields). An origin of this idea was the following question: *is there any identity between the Riemann ζ-function of an arithmetic field K and a " Selberg type ζ-function " of a discrete group Γ, in some cases?* Indeed, if we assume such an identity for a function field K, then we can proceed and meet, in a fairly natural way, the concept of " *primes and conjugacy classes principle* " (abbrev. p. & c.c. principle), and then of " *non-abelian classfield theory of Γ-type* ". We shall begin with this explanation. Another origin was an observation that if we introduce such a group as $\Gamma = PSL_2(\mathbf{Z}^{(p)})$, where p is a prime number and

$$\mathbf{Z}^{(p)} = \{ a/p^t \mid a, t \in \mathbf{Z} \},$$

then this theory holds for such a group [5]. But this explanation will be left to § 2.

Recall that the original Selberg ζ-function is defined with respect to a discrete subgroup Γ of $G = PSL_2(\mathbf{R})$ with finite volume quotient. While the Riemann ζ-function describes the distribution of prime divisors of an arithmetic field, the Selberg ζ-function describes that of Γ-conjugacy classes in the space of G-conjugacy classes. By " Selberg type ζ-functions, " we vaguely mean some " ζ-functions " connected with the distribution problems of Γ-conjugacy classes, where G is some more general topological group, say, of Lie type. Since the space of G-conjugacy classes of a Lie type group G is roughly identical to the disjoint union of mutually non-conjugate tori T of G, we may fix one torus T in considering such a " ζ-function ".

Let us formulate the above question in a more explicit way. Take an infinite discrete subgroup Γ of a topological group G, and let T be a closed abelian subgroup of G. Call T^* the set of all such element $t \in T$ that the centralizer of t in G coincides with T. Then $g^{-1}tg = t'$ ($t, t' \in T^*, g \in G$) implies $g^{-1}Tg = T$. Now suppose that T contains an open compact subgroup T_0 with $T/T_0 \cong \mathbf{Z}$ [1]. For each $t \in T$, call deg (t) (the *degree* of t) the absolute value of the image of t by the induced homomorphism $T \to \mathbf{Z}$. Since T_0 is the unique maximal compact subgroup of T, it is clear that deg (t) is inva-

[1] This assumption is natural, when we presuppose an identity between a Selberg type ζ-function w.r.t (G, Γ, T) and a congruence ζ-function.

riant by any topological automorphism of T. In particular, if $t, t' \in T^*$ are G-conjugate and hence conjugate by the normalizer of T, then $\deg(t) = \deg(t')$. Assume now that if some element $\neq 1$ of Γ is G-conjugate to some $t \in T$, then $t \in T^*$. Call a subset S of Γ, *T-bolic*, if there is some $g \in G$ with $g^{-1}Sg \subset T$. It is easy to see that a subgroup H of Γ is *maximal T-bolic* if and only if either of the following two equivalent conditions (*i*), (*ii*) is satisfied: (*i*) H is the centralizer of *some* T-bolic element $\neq 1$ of Γ; (*ii*) for *every* $\gamma \in H$ with $\gamma \neq 1$, γ is T-bolic and H coincides with its centralizer. It is clear that if H, H' are two distinct maximal T-bolic subgroups, then $H \cap H' = \{1\}$. Now let $\mathscr{H}$ denote the set of all *infinite* (2) maximal T-bolic subgroups of Γ. Then if $H \in \mathscr{H}$, its torsion subgroup H^0 is finite and the quotient $\overline{H} = H/H^0$ is isomorphic to $\mathbf{Z}$. Suppose that we can assign one choice of isomorphism $\overline{H} \cong \mathbf{Z}$ *for each* $H \in \mathscr{H}$, in such a way as to be compatible with the conjugations by elements of Γ (3). Let Γ act on $\mathscr{H}$ by the conjugation. From each Γ-conjugacy class of subgroups in $\mathscr{H}$, choose a representative H, and for each representative H, let $\overline{\pi}$ denote the *positive generator* of $\overline{H}$; i. e., the generator of $\overline{H}$ that corresponds to 1 by the above chosen isomorphism $\overline{H} \cong \mathbf{Z}$. Thus, $H, \overline{\pi}$ and its Γ-conjugacy class $\{\overline{\pi}\}_\Gamma$ (which is more intrinsic than $H, \overline{\pi}$) are in one-to-one correspondence with each other. Note that if Γ is torsion-free, $\{\overline{\pi}\}_\Gamma^{\pm 1}$ *runs over all primitive T-bolic Γ-conjugacy classes*; i. e., the Γ-conjugacy classes of such T-bolic elements of Γ that generate some $H \in \mathscr{H}$. Now, define the *degree* $\deg\{\overline{\pi}\}_\Gamma$ of $\{\overline{\pi}\}_\Gamma$, by $\deg\{\overline{\pi}\}_\Gamma = \deg(t)$, where $t = g^{-1}\pi g \in T$ and $\pi \in H$ is a representative modulo H^0 of $\overline{\pi}$. By the above remarks, it is well-defined, and is a positive integer. Now define the ζ-function by

$$\zeta_\Gamma(u) = \prod_{\{\overline{\pi}\}_\Gamma} (1 - u^{\deg\{\overline{\pi}\}_\Gamma})^{-1}.$$

This is an analogue of Selberg ζ-function in idea, but in form, it is an analogue of congruence ζ-functions (4) (5).

Now we can raise our question more concretely: *is there any* (G, Γ, T) *of the above type and a function field* K, *such that* $\zeta_\Gamma(u)$ *essentially coincides with the congruence ζ-function of* K, *at least for the principal parts?* Since the ζ-function of K is by definition $\prod_P (1 - u^{\deg P})^{-1}$, ($P$: prime divisors of K,) this question is refined to the following:

Is there any (G, Γ, T) *and* K, *and a " natural " degree-preserving one-to-one correspondence between a set* $\mathfrak{p}(\Gamma)$ *of almost all* $\{\overline{\pi}\}_\Gamma$ *and a set* $\mathfrak{p}(K)$ *of almost all prime divisors of* K?

If there is such a correspondence, we shall say that the *primes and conjugacy classes principle* holds between $\mathfrak{p}(K)$ and $\mathfrak{p}(\Gamma)$. That this principle actually holds for some K

(2) If G/Γ is compact, then any maximal T-bolic subgroup H is infinite, since if $g^{-1}Hg \subset T$, then $T/g^{-1}Hg$ is compact.

(3) This is possible if and only if the mutually inverse elements of $\overline{H}$ are not Γ-conjugate to each other for any H; and when possible, in many ways so. But the " reciprocity ", i. e., (*ii*) (*b*) of § 1.2, can be expected only for good choices of isomorphisms. Thus, our conjectures and results that follow depend on their good choices.

(4) If G/Γ is compact, or if (G, Γ, T) belongs to the type that we consider in § 1.3, there are at most finitely many $\{\overline{\pi}\}_\Gamma$ with the given degree, and hence $\zeta_\Gamma(u)$ is well-defined as a formal power series.

(5) Note that $\zeta_\Gamma(u)$ does not depend on the choice of the isomorphisms $\overline{H} \cong \mathbf{Z}$.

and Γ, is a basic point in making our program and proving some results on " non-abelian classfield of Γ-type ". Indeed, then Γ would play the role of the ideal class group (in the sense of Takagi) of abelian classfield theory, and the conjugacy class $\{\bar{\pi}\}_\Gamma \in \mathfrak{p}(\Gamma)$ corresponding to a prime divisor P of K would play the role of the ideal class determined by P.

1.2. *Abstract formulation of non-abelian classfield theory of* Γ-*type*. We assume that the p. & c. c. principle holds between some $\mathfrak{p}(K)$ and $\mathfrak{p}(\Gamma)$;

$$\mathfrak{p}(\Gamma) \ni \{\bar{\pi}\}_\Gamma \underset{1:1}{\leftrightarrows} P \in \mathfrak{p}(K).$$

We shall say that a *non-abelian classfield theory of* Γ-*type* is valid between K and Γ *if* there is an infinite Galois extension $\mathfrak{K}$ of K and an injective isomorphism ι of Γ into the Galois group $\mathfrak{g} = \mathrm{Gal}\,(\mathfrak{K}/K)$, satisfying the following conditions (*i*), (*ii*):

(*i*) $\iota(\Gamma)$ *is dense in* $\mathfrak{g}$. *The subgroups* $\Gamma' \subset \Gamma$ *of finite indices and the closed subgroups* $\mathfrak{g}' \subset \mathfrak{g}$ *of finite indices are in a natural one-to-one correspondence.*

Hence Γ' also correspond in a one-to-one manner with finite extensions K' of K contained in $\mathfrak{K}$. The next condition (*ii*) comes out naturally from the idea that the p. & c. c. principle should be assumed for all corresponding K' and Γ', *in a compatible way.*

(*ii*) *Let* $P \in \mathfrak{p}(K)$ *and let* $\{\bar{\pi}\}_\Gamma \in \mathfrak{p}(\Gamma)$ *be the corresponding* Γ-*conjugacy class. Then, there is a prime factor* $\mathfrak{p}$ *of* P *in* $\mathfrak{K}$ *such that*

(*a*) $\iota(H^0)$, *resp. the topological closure of* $\iota(H)$ *in* $\mathfrak{g}$, *are the inertia group, resp. the decomposition group, of* $\mathfrak{p}$ *in* $\mathfrak{K}/K$;

(*b*) $\iota(\bar{\pi})$ *is the Frobenius automorphism of* $\mathfrak{p}$ *in* $\mathfrak{K}/K$.

This condition (*ii*) would describe the law of decompositions of prime divisors P of $\mathfrak{p}(K)$ in $\mathfrak{K}/K$ completely, and would imply that the p. & c. c. principle holds for all corresponding K' and Γ' in a compatible way. In fact, it is enough to connect

$$\iota(\gamma)\mathfrak{p}\,|_{K'} \qquad \text{with} \qquad \gamma H \gamma^{-1} \cap \Gamma'$$

for each $\gamma \in \Gamma$ and $P \in \mathfrak{p}(K)$. It is clear by definition that if the classfield theory of Γ-type is valid between K and Γ, then it is also valid for all corresponding pairs K' and Γ'.

1.3. *Main conjectures.* The detailed studies of some selected cases gave us a strong hope that the classfield theory of Γ-type is actually valid for the groups Γ of the type defined below, and tempted us to propose a following series of conjectures (C 1) $\sim$ (C 5). It is stronger than the classfield theory of Γ-type defined in § 1.2. So far, it is proved only for some special cases of Γ, but seems to be supported also by some other results on Γ (e. g., § 3.1).

We shall specify (G, Γ, T) as follows:

$$G = PSL_2(R) \times PSL_2(k_\mathfrak{p}) \qquad \text{(topological group)},$$

where R and $k_\mathfrak{p}$ are the real and a p-adic field respectively, and $PSL_2 = SL_2/\pm 1$. For each subset $S \subset G$, S_R resp. $S_\mathfrak{p}$ denote its projection to $G_R = PSL_2(R)$ resp. $G_\mathfrak{p} = PSL_2(k_\mathfrak{p})$. Now, Γ is a discrete subgroup of G with finite volume quotient G/Γ, which is *essentially indecomposable*, in the sense that Γ_R resp. $\Gamma_\mathfrak{p}$ are dense in G_R resp. $G_\mathfrak{p}$.

For simplicity's sake, *we shall assume* Γ *to be torsion-free.* We shall take

$$T = PSO_2(R) \times (\text{the diagonals}),$$

so that $T/T_0 \cong \mathbf{Z}$ with $T_0 = PSO_2(R) \times$ (unit diagonals). It is easy to check all assumptions of § 1.1 on (G, Γ, T). Let $\mathfrak{p}(\Gamma)$ be the set of *all* $\{\bar{\pi}\}_\Gamma$. It is an infinite set, and the ζ-function can be explicitly calculated (§ 3.1). Besides $\mathfrak{p}(\Gamma)$, a certain finite set $\mathfrak{p}_\infty(\Gamma)$, and the degrees of its elements are defined ([7], vol. 2, Chap. 1). $\mathfrak{p}_\infty(\Gamma)$ is empty if and only if G/Γ is compact. Put $\Gamma^0 = \Gamma \cap (G_R \times V)$, where $V = PSL_2(\mathcal{O}_\mathfrak{p})$ and $\mathcal{O}_\mathfrak{p}$ is the ring of integers of $k_\mathfrak{p}$. Then its projection Γ_R^0 is a discrete subgroup of G_R with finite volume quotient. Let g denote the genus of Γ_R^0, and let s be the number of distinct cusps in a fundamental domain of Γ_R^0. Then $g - 1 + s/2 > 0$, and

$$s = \sum_{P \in \mathfrak{p}_\infty(\Gamma)} \deg P.$$

Put $q = N\mathfrak{p}$, and $\mathbb{H} = (q-1)(g - 1 + s/2)$. Then $\mathbb{H}$ is always a *positive integer* ([7], vol. 2, Chap. 1). Now, our main conjectures are the following $(C\,1) \sim (C\,5)$:

$(C\,1)$ *Each* Γ *defines a function field* K *with genus* g *and with exact constant field* F_{q^2}, *and the* p. & c. c. *principle holds between* $\mathfrak{p}(K)$ *and* $\mathfrak{p}(\Gamma)$. *More precisely, the set of all prime divisors of* K *is decomposed into three mutually disjoint subsets* $\mathfrak{p}(K)$, $\mathfrak{p}_\infty(K)$ *and* $\mathfrak{S}(K)$; *and we have degree-preserving one-to-one correspondences*

$$\mathfrak{p}(K) \leftrightarrow \mathfrak{p}(\Gamma), \qquad \mathfrak{p}_\infty(K) \leftrightarrow \mathfrak{p}_\infty(\Gamma),$$

which agree with $(C\,2) \sim (C\,5)$.

We shall call the prime divisors of $\mathfrak{p}(K)$, $\mathfrak{p}_\infty(K)$ and $\mathfrak{S}(K)$ *ordinary, cuspidal,* and *special,* respectively.

$(C\,2)$ *There are exactly* $\mathbb{H}$ *special prime divisors, and they are of degree one over* F_{q^2}. *Moreover, there is a differential* ω *of* K *of degree* $(q-1)/2$ (*resp.* $q - 1$, *if* $2 \mid q$), *whose divisor* (ω) *equals*

$$W = \{\prod_{P \in \mathfrak{S}(K)} P\}\{\prod_{Q \in \mathfrak{p}_\infty(K)} Q\}^{-(q-1)/2} \qquad (\text{resp. } W^2).$$

$(C\,3)$ *Non-abelian classfield theory of* Γ*-type is valid between* K *and* Γ (*for the above* $\mathfrak{p}(K) \leftrightarrow \mathfrak{p}(\Gamma)$).

$(C\,4)$ (*i*) *The ordinary and the special prime divisors are unramified in* $\mathfrak{K}$; (*ii*) *the special prime divisors are decomposed completely in* $\mathfrak{K}$ [6]; (*iii*) *the cuspidal prime divisors are at most tamely ramified in* $\mathfrak{K}$; (*iv*) *the inertia group and the Frobenius of cuspidal prime divisors in* $\mathfrak{K}$ *can also be described in the language of* $\mathfrak{p}_\infty(\Gamma)$ [7].

$(C\,5)$ $\mathfrak{K}$ *is the maximum Galois extension of* K *satisfying the conditions* (*i*) (*ii*) (*iii*) *of* $(C\,4)$.

Note. — Our conjectures implicitly contain the following. Let $G_R = PSL_2(R)$ act on the complex upper half plane $\mathfrak{H}$ by $\tau \to (a\tau + b)(c\tau + d)^{-1}$ $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_R\right)$.

(6) This is the very reason why the special prime divisors do not correspond to any Γ-conjugacy classes (the Frobenius conjugacy class is trivial!).

(7) We omit this detail here. It can be formulated easily by referring to [7], vol. 2 (Chap. 1, Th. 3 and Chap. 5, Th. 5).

Let $H \in \mathscr{H}$. Then since $T_R = PSO_2(R)$, H_R has a common fixed point z on $\mathfrak{H}$. Let Γ' be any subgroup of Γ with finite index and put $\Delta' = \Gamma' \cap (G_R \times V)$, so that Δ'_R is a fuchsian group. Then, we conjecture that there is a *suitable* algebraico-geometric model $\mathscr{C}_{\Delta'}$ of $\Delta'_R \backslash \mathfrak{H}$, such that the reduction of $\mathscr{C}_{\Delta'}$ modulo some extension of p gives a model of K' (of § 1.2 (*i*)), and that the reduction of the point z gives the element of $\mathfrak{p}(K')$ corresponding to $H' = H \cap \Gamma' \in \mathfrak{p}(\Gamma')$. In the special cases where our conjectures are solved, the compatible p. & c. c. principle is established in this way.

2. Solved cases.

2.1. *Elliptic modular case.*

Let p be a prime number, and consider the ring $\mathbf{Z}^{(p)} = \{ a/p^t \mid a, t \in \mathbf{Z}\}$. Let Γ be a subgroup of $\Gamma(1) = PSL_2(\mathbf{Z}^{(p)})$ with finite index. Then by the diagonal embedding Γ can be considered as a discrete subgroup of $G = PSL_2(\mathbf{R}) \times PSL_2(\mathbf{Q}_p)$ ($\mathbf{Q}_p$: the p-adic field) with finite volume quotient, and with dense image of projection in each component of G.

THEOREM. — *Let Γ be as above, and moreover torsion-free. Then Γ satisfies* $(C\,1) \sim (C\,4)$. *The torsion-freeness assumption can be dropped if we modify* $(C\,2)$ $(C\,4)$ *in a suitable way.* (*In particular, the non-abelian classfield theory of Γ-type is valid for these groups*).

The proof is given in [7], vol. 1, 2; Chap. 5. To prove them by our method is equivalent to synthesizing and reconstructing carefully in the language of the group $\Gamma(1)$ the various results, on complex multiplication theory of elliptic curves (Deuring [1]), and on modernized and generalized Kroneckerian type theory of elliptic modular functions (Shimura [14] for char. 0, Igusa [4] for char. p) ([8]). The congruence subgroup property of $\Gamma(1)$ proved by Mennicke [10], Serre [13] is also used. See also § 4. As an example, take $\Gamma = \Gamma(2)$ (the principal congruence subgroup of level 2; $p \neq 2$). It is torsion-free. The corresponding K is rational; $K = F_{p^2}(x)$. Identify the prime divisor P of K with the residue class of x, and write $P = P_a$ for $x \equiv a \pmod{P}$. Then, $\mathfrak{p}_\infty(K) = \{ P_0, P_1, P_\infty \}$, and $\mathfrak{S}(K) = \{ P_a \mid u(a) = 0 \}$; where $u(x)$ is a polynomial of degree $(p-1)/2$ defined by

$$u(x) = \Sigma_{i=0}^{r} \binom{r}{i}^2 x^i \qquad (r = (p-1)/2) \ (^9).$$

The p. & c. c. principle $\mathfrak{p}(K) \leftrightarrow \mathfrak{p}(\Gamma)$ is established by the process described in the above *note* (§ 1.3). Namely, let $\Delta_R = \Gamma_R^0 =$ the principal congruence subgroup of $PSL_2(\mathbf{Z})$ of level 2. Let $\lambda(z)$ be the λ-function; i. e., a generator of the field of automorphic functions *w. r. t.* Δ_R, whose values at the three cusps are 0, 1, ∞. Then

$$\mathfrak{p}(\Gamma) \ni \{ \bar{\pi} \}_\Gamma \to H \to z \to \lambda_0 = \lambda(z) \bmod \mathfrak{P} \to P = P_{\lambda_0}$$

([8]) IGUSA [4] is *directly* used in constructing $\mathfrak{K}$ and proving $(C\,4)$ (*i*), (*iii*).

([9]) By HASSE-DEURING (cf. [1]), $u(a) = 0$ if and only if $Y^2 = X(X-1)(X-a)$ is a supersingular elliptic curve. That $a \in F_{p^2}$ and $a \neq 0, 1$ follows from this (or also directly, by using our definition of ω given in [9]). That all roots a of $u(x) = 0$ are simple was directly proved by IGUSA [3]. I am grateful to IGUSA and DWORK, since I was much inspired by [3] and DWORK [2] (§ on elliptic curves).

defines the bijection $\{\bar{\pi}\}_\Gamma \leftrightarrow P$ of $\mathfrak{p}(\Gamma) \leftrightarrow \mathfrak{p}(K)$. Here $\mathfrak{P}$ is a *fixed* prime factor of p ([10]). The field $\mathfrak{K}$ is obtained from the composite of Igusa's fields of modular functions for all levels $\not\equiv 0 \pmod p$, by lowering the field of constant down to F_{p^2} in a suitable way. Once this is proved, the ramification properties (i. e., the prime divisors $P \neq P_0, P_1, P_\infty$ of K are unramified and $P = P_0, P_1, P_\infty$ are at most tamely ramified in $\mathfrak{K}$) are reduced to the Igusa's theorem [4]. Moreover, by our theorem, $P \in \mathfrak{S}(K)$ are decomposed completely in $\mathfrak{K}$. But we do not know whether $\mathfrak{K}$ is characterized by these ramifications and decompositions properties. For example, $\mathfrak{S}(K) = \{P_{-1}\}$ for $p = 3$; hence $(C\,5)$ is to conjecture that $\mathfrak{K}$ is the maximum Galois extension of K in which $P \neq P_0, P_1, P_\infty$ are unramified, P_0, P_1, P_∞ are at most tamely ramified, and P_{-1} is decomposed completely.

The differential ω of $(C\,2)$ is quite an interesting one. It is given by

$$\omega = \frac{u(x)}{\{x(1-x)\}^{(p-1)/2}} (dx)^{(p-1)/2}$$

for the above example. We can prove that:

THEOREM. — *ω is invariant, up to the signs, by all separable modular transforms $x \to x'$* (cf. [8]).

Here, $x \to x'$ is called a separable modular transform if the elliptic curve

$$Y^2 = X(X-1)(X-x')$$

is separably isogenous to $Y^2 = X(X-1)(X-x)$. The above theorem is also equivalent to that *ω is invariant, up to the signs, by all automorphisms of $\mathfrak{K}/F_{p^2}$*. Conversely, a differential $\eta \neq 0$ of $\mathfrak{K}$ (of higher degree) having this invariance property must have the form: $\eta = c\cdot\omega^h$; $c \in F_p^\times$, $h \in \mathbf{Z}$, $h \geq 0$. There is *no* analogue of ω in characteristic 0. Another theorem on ω is the following. Take a $(p-1)/2$-*th* root ω_1 of ω in a separable extension of K. Then:

THEOREM. — *(i) ω_1 is invariant by the Cartier operator. (ii) Let $z = z(\lambda)$ be the inverse of $\lambda(z)$, and let $(\#)$ be the Schwarz' equation for dz:*

$$(\#) \qquad \frac{2(dz/d\lambda)(d^3z/d\lambda^3) - 3(d^2z/d\lambda^2)^2}{(dz/d\lambda)^2} = \frac{\lambda^2 - \lambda + 1}{\lambda^2(1-\lambda)^2}.$$

Replace λ by x and consider $(\#)$ in characteristic p. Then it is satisfied by ω_1 in place of dz. (iii) ω_1 is uniquely characterized by (i), (ii) up to $F_p^\times$-multiples.

The differential ω can be defined in a very natural way in more general cases. This, and the proof of the theorem (in generalized form) are given in [9].

Note. — The differential dz of the inverse of automorphic functions is always transcendental (unlike the elliptic functions case, where dz is the invariant differential on the elliptic curve). Nevertheless, [9] shows that in certain cases there is a natural *algebraic* differential ω_1 in characteristic p which plays a role of " $dz \pmod p$ ".

([10]) The choice of one isomorphism $\bar{H} \cong \mathbf{Z}$ for each H, and the injection $\iota: \Gamma \to \mathfrak{g}$ of § 1.2 are also defined w.r.t a fixed prime factor $\mathfrak{P}$ of p. We must take the *same* $\mathfrak{P}$ to validate our theorem. The effect of changing $\mathfrak{P}$ is of subtle nature ([7], vol. 2; Chap. 5).

2.2. *Some quaternion modular cases.*

Other known examples of Γ are obtained from some quaternion algebras B. If F is the center of B, Γ is defined w. r. t. an order Θ of B and a prime divisor $\mathfrak{P}$ of F (cf. [7], vol. 1, Chap. 4). In these cases, Γ_R^0 is the unit group of Θ, and hence belongs to the fuchsian groups of Poincaré-Fricke type. For these fuchsian groups, Shimura [15] [16] proved beautiful arithmetic properties of the quotient $\Gamma_R^0\backslash\mathfrak{H}$. His theories, combined with some detailed studies of endomorphism rings of abelian varieties (esp. their behavior under the reduction processes), may give us enough tool for proving some of our conjectures. Partial results along this line were obtained by Shimura and by (our student) Morita:

THEOREM (Shimura) (11). — *For almost all prime numbers p that remain träge in F (i. e., $\mathfrak{P} = p$), Γ satisfies the p. & c. c. principle in the way explained in the note* (§ 1.3). *Moreover, the number of special prime divisors can be computed, which agrees with* (C 2).

If $F = \mathbf{Q}$, this result would imply the main parts of (C1) $\sim$ (C4), but for *almost all p*. Recently, Y. Morita [11] claimed:

THEOREM (Morita). — *If $F = \mathbf{Q}$, the main parts of* (C 1) $\sim$ (C 4) *are valid for all p not dividing the discriminant of B.*

His proof is based on Shimura's and Mumford's theory of moduli of abelian varieties, Tate's result on endomorphisms of abelian varieties, and on our theorem on $\zeta_\Gamma(u)$ (immediately below) (12).

3. Some related results.

3.1. *The ζ-function of* Γ.

Here we sketch the results of our computations of $\zeta_\Gamma(u)$, where (G, Γ, T) is as in § 1.3.

THEOREM (13). — $$\zeta_\Gamma(u) \times \prod_{P \in \mathfrak{p}_\infty(\Gamma)} (1 - u^{\deg P})^{-1} = \frac{\prod_{i=1}^{g}(1 - \rho_i u)(1 - \rho_i' u)}{(1 - u)(1 - q^2 u)} \times (1 - u)^{\mathbb{H}},$$
with $\rho_i\rho_i' = q^2$; $|\rho_i|, |\rho_i'| \leq q^2$; $\rho_i, \rho_i' \neq 1, q^2$. $\mathbb{H}$ is a positive integer defined in § 1.3.

If Γ is not assumed torsion-free, then the formula is somewhat more complicated. In any case, this result agrees with (C 1) (C 2).

(11) This was informed by Shimura's letter to the speaker dated May, 1968. He announced a somewhat stronger result, but it cannot be explained briefly.

(12) Thus, it is very long and involved. We may say that an interest of the (partial) proof of our conjectures in quaternion modular cases *along this line* lies more on the *corelation* between some problems on abelian varieties and our problems (see also § 4).

(13) This has been announced in [5] in the case G/Γ: compact, Γ: torsion-free, and proof for this case is given in [7], vol. 1, Chap. 1. The general case is proved in [7], vol. 2, Chap. 1. It is on one hand based on Eichler-Selberg trace formula but on the other hand, it requires a detailed study of T-bolic and parabolic elements of Γ. Labesse then offered an alternative proof in the G/Γ: compact, Γ: torsion-free case, by using $L^2(G/\Gamma)$ in place of Eichler-Selberg (a letter to the speaker; Oct. 1969).

Note. — We can express $\prod_{i=1}^{g}(1-\rho_i u)(1-\rho_i' u)$ by some Hecke polynomial. By combining this with Shimura's work [16], it can be shown that the first term on the right side is a congruence ζ-function for *almost all* $\mathfrak{P}$, *in quaternion modular cases.* But this is weaker than the " p. & c. c. principle ", since this still does not guarantee any *natural and compatible* one-to-one correspondence between $\mathfrak{p}(K)$ and $\mathfrak{p}(\Gamma)$.

3.2. *The* $G_{\mathfrak{p}}$*-fields.*

The groups Γ of § 1.3 correspond in a one-to-one manner with the $G_{\mathfrak{p}}$-fields over **C** ([7]), vol. 1, Chap. 2). Roughly speaking, $G_{\mathfrak{p}}$-field is an algebraic function field having non-compact automorphism group $G_{\mathfrak{p}} = PSL_2(k_{\mathfrak{p}})$ and satisfying some conditions on ramifications. One basic theorem is that we can lower the field of constant of $G_{\mathfrak{p}}$-fields down to algebraic number fields, and that under a certain (not too restrictive) condition on Γ, it can be done *in a unique way* ([7], vol. 1, Chap. 2, Pt. 2). This proof is long, but uses only some group theories of $G_{\mathfrak{p}}$ and a deformation theory of Γ given in [7]. In our proof, *a basic point is that* $G_{\mathfrak{p}}$*-fields have sufficiently many automorphisms* ([14]). The relation between the $G_{\mathfrak{p}}$-fields and our problems (which seems essential) is roughly explained in [6], [7].

4. Concluding remarks.

Our knowledge on non-abelian mathematics is so narrow that we could only have touched a part of " an iceberg above water ". Here we are satisfied by giving a concrete program for " non-abelian classfield theory of Γ-type " (which seems fairly probable), solving some special cases, and by showing that the problem is closely related to other arithmetical problems. We shall conclude this talk by the following remark. Function field is often compared with algebraic number field. The former has analogous but simpler structure than the latter, and also allows geometric treatments. Thus, some problems that offer no clues at all for number fields may offer some for function fields. This was first shown by Weil's proof of the Riemann hypothesis for function fields. So far, it does not help prove the Riemann hypothesis for number fields, but the related works of Hasse, Weil, etc. have shown that (some) arithmetic problems on function fields are closely related to some other problems (esp. complex multiplication theory) on number fields, *not by a formal analogy between two problems, but more closely, by a " relation between warps and wooves of the same (if not apparently so) problem ".* Now, a relation of our problem with complex multiplication theory is also of this sort. We have been talking in a view-point of *trying some non-abelian mathematics on function fields* (which are too difficult for number fields), but from another view-point, *it is a " woof " of complex multiplication theory.* Namely, if we call a " warp " of complex multiplication theory that theory of " fixed imaginary quadratic lattice and variable p ", then a woof is that theory of " fixed p and variable imaginary quadratic lattices ". There is an admirable generalization of warps (of complex multiplication theory) by Shimura [16], but its wooves are by no means

([14]) Usefulness of this point is also stressed in a recent work of Pjatezkii-Sapiro [12].

complete (only touched), and these are almost equivalent to our problems (C 1) $\sim$ (C 4) for the quaternion modular groups! Finally, we note that the use of the groups Γ (of type § 1.3, § 2) is very natural and convenient for " woof theories ".

REFERENCES

[1] M. Deuring. — Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg*, 14 (1941), pp. 197-272.

[2] B. Dwork. — A deformation theory for the zeta function of a hypersurface, *Proceedings International Congress Math.*, Stockholm (1962).

[3] J. Igusa. — Class number of a definite quaternion with given discriminant, *Proc. Nat. Acad. Sci.*, 44 (1958), pp. 312-314.

[4] —. — Fiber systems of Jacobian varieties III, *Amer. J. Math.*, 81 (1959), pp. 453-476.

[5] Y. Ihara. — Algebraic curves mod p and arithmetic groups, *Proc. symposia in pure math.*, 9 (1966), pp. 265-271.

[6] —. — The congruence monodromy problems, *J. Math. Soc. Japan*, 20-1 $\sim$ 2 (1968), pp. 107-121.

[7] —. — On congruence monodromy problems, vol. 1, 2, *Lecture notes* 1, 2, Univ. of Tokyo (1968-1969).

[8] —. — An invariant multiple differential attached to the field of elliptic modular functions of characteristic p, to appear in *Amer. J. Math.*

[9] —. — Modular transforms of p-power degrees and induced multiple differentials of characteristic p, Mimeographed note (1970).

[10] J. Mennicke. — On Ihara's modular group, *Invent. Math.*, 4 (1967), pp. 202-228.

[11] Y. Morita. — Ihara's conjectures and moduli space of abelian varieties, *Mimeographed note* (1970).

[12] Pjateckii-Saprio. — Reduction of the fields of modular functions and the rings of functions on p-adic manifolds, *Lecture note* at Maryland Univ. (1970).

[13] J.-P. Serre. — Le problème des groupes des congruences pour SL_2, to appear.

[14] G. Shimura. — Correspondances modulaires et les fonctions ζ de courbes algébriques, *J. Math. Soc. Japan*, 10 (1958), pp. 1-28.

[15] —. — On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, *J. Math. Soc. Japan*, 13 (1961), pp. 275-331.

[16] —. — Construction of class fields and zeta functions of algebraic curves, *Ann. of Math.*, 85-1 (1967), pp. 58-159.

[17] —. — Local representations of Galois groups, *Ibid.*, 89-1 (1969), pp. 99-124.

[18] —. — On canonical models of arithmetic quotients of bounded symmetric domains, *Ibid.*, 91-1 (1970), pp. 144-222.

University of Tokyo
Department of Mathematics,
Hongo, Bunkyo-ku,
Tokyo (Japon)

Actes, Congrès intern. math., 1970. Tome 1, p. 391 à 394.

ON SOME INFINITE ABELIAN EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

by KENKICHI IWASAWA

Let l be a prime number and let Z_l and Q_l denote the ring of l-adic integers and the field of l-adic numbers respectively; their additive groups will be also denoted by the same letters.

Now, an extension K of a field k is called a Z_l-extension if K/k is a Galois extension and its Galois group is topologically isomorphic to the additive group Z_l (1). For such an extension K/k, there exists a sequence of fields

$$k = k_0 \subset k_1 \subset \ldots \subset k_n \subset \ldots$$

such that each k_n/k is a cyclic extension of degree l^n and K is the union of all k_n, $n \geqq 0$. Conversely, if there is a sequence of cyclic extensions k_n/k such as mentioned above, then the union K of all k_n, $n \geqq 0$, is a Z_l-extension of k.

In the following, we shall consider Z_l-extensions of which the ground fields are finite algebraic number fields, i. e. finite extensions of the rational field Q. We first give some examples. For each $n \geqq 0$, let $P_{l,n}$ denote the cyclotomic field of l^{n+1}-th or 2^{n+2}-th roots of unity according as $l > 2$ or $l = 2$. Let $P_l = P_{l,0}$ and let $P_{l,\infty}$ be the union of all $P_{l,n}$, $n \geqq 0$. Then $P_{l,\infty}/P_l$ is a Z_l-extension with intermediate fields $P_{l,n}$, $n \geqq 0$. The field $P_{l,\infty}$ has a unique subfield $Q_{l,\infty}$ such that $P_l \cap Q_{l,\infty} = Q$, $P_l Q_{l,\infty} = P_{l,\infty}$, and this $Q_{l,\infty}$ gives us the unique Z_l-extension of the rational field Q. Furthermore, for any finite algebraic number field k, the composite $kQ_{l,\infty}$ is a Z_l-extension of k. Hence each k has at least one Z_l-extension over it.

Let K be a Z_l-extension of a finite algebraic number field k and let k_n, $n \geqq 0$, be the intermediate fields of k and K. Let C_n denote the ideal-class group of k_n, and A_n the Sylow l-subgroup of C_n. Denote by l^{e_n} *the* order of A_n, i. e. the highest power of l dividing the class number of k_n. Then, for all sufficiently large n, the exponent e_n is given by a formula

$$e_n = \lambda n + \mu l^n + \nu,$$

where λ, μ, and ν are integers ($\lambda, \mu \geqq 0$), independent of n. Since these integers are uniquely determined for given K/k by the above formula, we shall denote them by $\lambda(K/k)$, $\mu(K/k)$, and $\nu(K/k)$ respectively. For the special Z_l-extension $K = kQ_{l,\infty}$ over k, they will be denoted also by $\lambda_l(k)$, $\mu_l(k)$, and $\nu_l(k)$ respectively; furthermore we

---

(1) In earlier papers, the author called such extensions Γ-extensions.

simply put $\lambda_l = \lambda_l(P_l)$, $\mu_l = \mu_l(P_l)$, $\nu_l = \nu_l(P_l)$. Thus we obtain arithmetic invariants $\lambda_l(k)$, $\mu_l(k)$, $\nu_l(k)$ depending upon k and l, and λ_l, μ_l, ν_l for each prime number l.

Let O denote the ring of all algebraic integers in K, I the group of all invertible O-modules in K, and C the factor group of I modulo the principal O-modules (2); we may simply call I and C the ideal group and the ideal-class group of O in K, respectively. Let A be the Sylow l-subgroup (i. e. the l-primary component) of C. Then C is the direct limit of C_n, $n \geqq 0$, and A that of A_n, $n \geqq 0$, and the Galois group Gal (K/k) acts on C and A in the obvious manner. The above formula for e_n is obtained by analysing the structure of this Gal (K/k)-module A. Thus we see in particular that the Tate module $T_l(A)$ for the abelian l-group A is a free Z_l-module and its rank over Z_l is equal to the invariant λ.

At the present, little is known on the nature of the invariants $\lambda(K/k)$, $\mu(K/k)$, and $\nu(K/k)$ defined above. Yet it is clear that they play an essential role in the theory of Z_l-extensions. It seems particularly interesting to see when $\lambda = 0$ or $\mu = 0$ or $\lambda = \mu = 0$. It is easy to find a Z_l-extension K/k for which $\lambda(K/k)$ is arbitrary large. On the other hand, no example of K/k with $\mu(K/k) > 0$ is yet found. Although the number of such examples for which we have verified $\mu(K/k) = 0$ is quite limited, we are tempted to conjecture that $\mu(K/k) = 0$ for every Z_l-extension K/k, or at least that $\mu_l(k) = 0$ for every k and l or $\mu_l = 0$ for every l.

For the invariants λ_l and μ_l, we know that $\lambda_l = \mu_l = 0$ if and only if l is a regular prime, and if this is the case, then $\nu_l = 0$ also. Let P_l' denote the maximal real subfield of P_l and put

$$\lambda_l' = \lambda_l(P_l'), \quad \mu_l' = \mu_l(P_l'), \quad \nu_l' = \nu_l(P_l').$$

Then $\lambda_l' \leqq \lambda_l$, $\mu_l' \leqq \mu_l$. Now, a well-known conjecture of Vandiver states that the class number of P_l' is not divisible by l for every prime number l; it is checked by numerical computation for a large number of primes. For given l, the conjecture is equivalent with $\lambda_l' = \mu_l' = \nu_l' = 0$. Unlike what is said above for λ_l, μ_l, and ν_l, it is not known whether $\lambda_l' = \mu_l' = 0$ implies $\nu_l' = 0$ and, hence, Vandiver's conjecture. Nevertheless, it would be an interesting problem to find out if $\lambda_l' = \mu_l' = 0$ for every l.

Let $T_l(A)$ be the Tate module defined above and let V denote the tensor product of $T_l(A)$ and Q_l over Z_l: $V = V_l(A) = T_l(A) \otimes Q_l$. V is a vector space of dimension λ over Q_l and the Galois group Gal (K/k) acts on V continuously so that it defines an l-adic representation of Gal (K/k). It is clear that the definition of V above is completely parallel to the usual construction of such l-adic representations by means of, say, abelian varieties (3). Note also that if k' is a subfield of k such that K/k' is a Galois extension, then the same vector space V defines an l-adic representation of the larger group Gal (K/k').

Let $l > 2$ and $k = P_l$, $K = P_{l,\infty}$ in the above (4). Then V is decomposed into the direct sum of $l - 1$ subspaces V_i, $0 \leqq i < l - 1$, with respect to the action of

(2) In other words, C = Pic (O). Note that the ring O is not noetherian.

(3) See J.-P. Serre, Abelian l-adic representations of elliptic curves, Benjamin (New York, Amsterdam), 1968.

(4) For $l = 2$, slight modification is needed in what is said below about the decomposition of V and the definition of σ_0.

$\mathrm{Gal}(P_l/Q)$. Let W denote the group of all roots of unity in $P_{l,\infty}$ with order a power of l. Let σ_0 be the automorphism of K/k such that $\sigma_0(\zeta) = \zeta^{1+l}$ for every ζ in W and let $f_i(x)$ be the characteristic polynomial of σ_0 acting on V_i. Assuming Vandiver's conjecture for the prime l, we can describe the representation of $\mathrm{Gal}(K/k)$ on each V_i rather explicitly. It then follows ([5]) in particular that the characteristic polynomials $f_i(x)$, $0 \leqq i < l-1$, are closely related to the l-adic L-functions of Kubota-Leopoldt associated with the characters $\mathrm{Gal}(P_l/Q) \to Z_l^{\times}$.

For a Z_l-extension K/k in general, we know very little on the structure of the l-adic representation $\mathrm{Gal}(K/k) \to GL(V)$. However the following fact might be of some interest, in particular when viewed as an analogue of a similar result in algebraic geometry. Let k be any finite algebraic number field containing P_l and let

$$K = kQ_{l,\infty} = kP_{l,\infty}.$$

Let O' denote the ring of all l-integers in K, i. e. the union of all $l^{-n}O$, $n \geqq 0$. Let C' be the ideal class group of O' in K, and A' the Sylow l-subgroup of C'. Let $V' = T_l(A') \otimes Q_l$ over Z_l, where $T_l(A')$ denotes the Tate module for A'. As before, V' defines an l-adic representation of $\mathrm{Gal}(K/k)$, and the natural map $A \to A'$ induces an epimorphism $T_l(A) \to T_l(A')$ so that V' is a factor space of the representation space V. Now, an element α in K will be called l^n-hyperprimary ($n \geqq 0$) if α is an l^n-th power in the v-completion K_v for every place v of K lying above the place l of Q ([6]), and an O'-module $\mathfrak{a}$ of K will be called hyperprimary if, for some $n \geqq 0$, $\mathfrak{a}^{l^n} = (\alpha)$ with an l^n-hyperprimary element α in K. Let B' be the subgroup of all classes in A' which are represented by hyperprimary O'-modules and let $V'' = T_l(B') \otimes Q_l$ over Z_l. Then V'' again defines an l-adic representation of $\mathrm{Gal}(K/k)$, and $B' \to A'$ induces a monomorphism $T_l(B') \to T_l(A')$ so that V'' is a subspace of V'. Hence V'' is involved in the original representation space V. Let W be the group of roots of unity as defined above and let $V_0 = T_l(W) \otimes Q_l$ over Z_l. Then V_0 defines a one-dimensional l-adic representation of $\mathrm{Gal}(K/k)$ through its action on W.

Now, suppose that the ground field k is abelian either over the rational field or over an imaginary quadratic field. Then we can prove ([7]) that there exists a non-degenerate skew-symmetric Q_l-bilinear form

$$V'' \times V'' \to V_0$$

such that

$$\langle \sigma u, \sigma v \rangle = \sigma(\langle u, v \rangle)$$

for all u, v in V'' and σ in $\mathrm{Gal}(K/k)$. It follows that V'' is even dimensional and that the characteristic polynomial of each σ in $\mathrm{Gal}(K/k)$ acting on V'' satisfies a functional equation similar to the one for the zeta-function of an algebraic curve defined over a finite field ([8]).

([5]) See K. Iwasawa, On p-adic L-functions, *Ann. Math.*, 89 (1969), pp. 198-205.

([6]) There exist only a finite number of such places v in K.

([7]) The proof will be published elsewhere.

([8]) Actually we can prove the above result for a wider class of ground fields including those mentioned above. It seems likely that the same result holds for an arbitrary ground field k containing P_l, without any further assumption on k.

As already mentioned, the skew-symmetric form defined above is essentially an analogue of the classical Riemann forms on complex tori, of which a purely algebraic construction was given by Weil for abelian varieties of arbitrary characteristic ([9]). It would be interesting to pursue such analogy further in studying the structure of the representation space V''.

([9]) The original idea of Weil appears in his paper: Sur les fonctions algébriques à corps de constantes fini, *C. R. Paris*, 210 (1940), pp. 592-594.

Princeton University
Department of Mathematics,
Princeton, New Jersey 08540
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 395 à 399.

SOME RESULTS CONCERNING RECIPROCITY AND FUNCTIONAL ANALYSIS

by TOMIO KUBOTA

There is an old, well-known relationship between the quadratic reciprocity and analytic functions. Briefly speaking, the transformation formula of a theta-function yields the quadratic reciprocity law. This fact is essentially contained in Gauss' work (see e. g. [10]), and has been generalized by Hecke [1]. It is not quite simple to find a corresponding result for the higher reciprocity, but it may motivate the investigation of a new branch of the number theory.

In the present note, we shall review principal results which we can prove in the analytic theory of the reciprocity law, and after that we shall pick up some important problems which are still open.

For the sake of simplicity, we take as our basic field once for all an imaginary quadratic field $F = \mathbf{Q}(\sqrt{-d})$ with discriminant $-d$, and we denote by n a natural number such that F contains a primitive n-th root of unity, i. e. $n = 2, 3, 4$, or 6. This setting causes no restriction of generality; what is stated in this note can be obtained for a general algebraic number field in the routine way of generalization, e. g. by taking a direct product of spaces in stead of a single one on which automorphic functions are considered.

At the beginning of this note, it was mentioned that the theta-function yields the quadratic reciprocity law. What we propose to state now is that this procedure is invertible, i. e. by means of the general reciprocity law, we can construct generalized theta-functions.

More precisely speaking, denote by H the three dimensional upper half space, whose points are of the form $u = (z, v)$, $(z \in \mathbf{C}, v > 0)$. Then, H is the non-hermitian symmetric space $SL(2, \mathbf{C})/SU(2)$, and the operation of $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{C})$ on H is given by the linear transformation $\sigma u = (au + b)(cu + d)^{-1}$, where we identify u with the matrix $\begin{pmatrix} z & -v \\ v & \bar{z} \end{pmatrix}$, and any $t \in \mathbf{C}$ with the matrix $\begin{pmatrix} t & \\ & \bar{t} \end{pmatrix}$.

Let now $\mathfrak{o}$ be the ring of integers of F, denote by (a/b) the n-th power residue symbol of F, and let Γ be a certain subgroup of $SL(2, \mathbf{C})$ which is commensurable with $SL(2, \mathfrak{o})$. Then, there exists a character χ of Γ, which is, for a congruence subgroup of $SL(2, \mathfrak{o})$ modulo a sufficiently high power of n, given by $\chi(\sigma) = (c/d)$ or 1 according to $c \neq 0$ or $= 0$, $\left(\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$, [3]. This result is equivalent to the reciprocity law of the power residue symbol (a/b). The condition which the group Γ should satisfy will not be discussed here, but we can take as Γ for instance the group generated by a certain congruence subgroup of $SL(2, \mathfrak{o})$ and by some elements of finite order in $SL(2, C)$ including $\omega = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$, and in this case we can fix the character χ such that $\chi(\omega)=1$.

The kernel of χ is a non-congruence subgroup of Γ. On the other hand, the group Γ operates on H discontinuously, and the fundamental domain $D = \Gamma\backslash H$ is of finite volume.

Putting $v(u) = v$ for $u = (z, v) \in H$, let us now define an Eisenstein series by

$$E(u, s) = \Sigma\bar{\chi}(\sigma)v(\sigma u)^s, \qquad (\sigma \in \Gamma_\infty\backslash\Gamma),$$

where s is a complex variable, and Γ_∞ is the group of $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ with $c = 0$. This series does not converge absolutely unless Re $s > 2$, but, as a consequence of Selberg's theory (see e. g. [11]) which is fully applicable to the present case, $E(u, s)$ has a meromorphic continuation onto the whole s-plane, has a pole of first order at $s = (n + 1)/n$, and the residue $\theta(u)$ of $E(u, s)$ at the pole is a square integrable function on D satisfying $\theta(\sigma u) = \chi(\sigma)\theta(u)$ for $\sigma \in \Gamma$.

The function θ is nothing else than a generalized theta-function which we have mentioned earlier. The series $E(u, s)$ is so to speak the Eisenstein series attached to the cusp ∞ of D, so that a similar series can be defined for each cusp of D, and the residues at $s = (n + 1)/n$ of all such Eisenstein series spans a finite dimensional complex vector space Θ of generalized theta-functions. A generalized theta-function $\theta \in \Theta$ not only reduces to a classical theta-function when $n = 2$, but also is in many aspects completely analogous to ordinary theta-functions. For example, the construction of a special type of unitary representation of a metaplectic group investigated in [12] finds some analogy also for generalized theta functions [5]. Since generalized theta-functions are defined on a non-hermitian space, it is impossible to use the theory of complex analytic functions in the study of them, and consequently our whole investigation should be based upon the functional analysis.

We now propose to introduce some byproducts of our analytic investigation of the reciprocity law. Most important things are results on the value distribution of Gauss sums. Put $e(z) = \exp(2\pi\sqrt{-1}(z + \bar{z}))$ for $z \in C$; then the Eisenstein series $E(u, s)$ has a Fourier expansion of the following form:

$$E(u, s) = v^s + \phi(s)v^{2-s} + \Sigma\phi(s, m)\,||\,m\,||^{(s-1)/2}(2\pi)^s\Gamma(s)^{-1}vK_{s-1}(4\pi\,|\,\beta m\,|\,v)\cdot e(\beta mz), \quad (m \in \mathfrak{o},\ m \neq 0),$$

where K is a modified Bessel function, β is a number in F, and

$$\phi(s, m) = c_0\Sigma\frac{g_m(c)}{||\,c\,||^s}, \qquad (c \in \mathfrak{o},\ c \neq 0).$$

Here, c_0 is a positive constant, and, denoting by $\{ c \}$ the set of double cosets $\Gamma_\infty\sigma\Gamma_\infty$ represented by an element $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a fixed c, $g_m(c)$ is given by

$$g_m(c) = \sum_{\{c\}}\bar{\chi}(\sigma)e(\beta md/c).$$

Furthermore, if we denote by $\zeta(s)$ the Dedekind's zeta-function of F, then $\phi(s)$ is equal to $(s-1)^{-1}\zeta(ns-n)\zeta(ns-(n-1))^{-1}$ up to an elementary factor. It is easily seen that $g_m(c)$ is essentially a classical Gauss sum defined for a power residue character of degree n modulo c.

From the theory of the analytic continuation of Eisenstein series, one can extract various properties of the functions $\phi(s, m)$. Among others, it is proved that $\phi(s, m)$ is meromorphic, and its only singularity in the region Re $s > 1$ is possibly the simple pole at $s = (n+1)/n$. Only from this fact, it follows that

$$G(Y) = \Sigma g_m(c)/\| c \|^{1/2}, \qquad (\| c \| < Y),$$

has the asymptotic property $G(Y) = o(Y)$ for $n > 2$ [4]. Observing Eisenstein series containing not only χ but also a representation of the compact group $SU(2)$, we can get a similar result for the product of $g_m(c)$ and the value of a Grössencharacter at c [7].

To improve the asymptotic property of $G(Y)$, we fix a fundamental domain D of Γ such that the set D_Y of all points $u = (z, v)$ in D with $v > Y$ is an infinitely long column parallel to the v-axis, and observe the function $E^Y(u, s)$ defined on D by

$$E^Y(u, s) = \begin{cases} E(u, s) - v^s, & u \in D_Y, \\ & \text{for} \\ E(u, s) & u \in D - D_Y. \end{cases}$$

By the general theory of the Eisenstein series, the function $E^Y(u, s)$ satisfies

$$\int_D | E^Y(u, s) |^2 du = \frac{Y^{2s-2}}{2S-2} + \frac{\overline{\phi(s)}Y^{2it} - \phi(s)Y^{-2it}}{2it}$$

for $s = S + it$, $S > 1$, where du is the invariant measure of H. This formula enables us to evaluate each non-constant term in the Fourier expansion of $E(u, s)$ on the line Re $s = S$ with a fixed $S > 1$. On the other hand, the behaviour of K_s on the same line as the function of s can be investigated by the integral representation

$$K_s(z) = \frac{1}{2}\left(\frac{1}{2}z\right)^{-s} \int_0^\infty \exp\left(-t - \frac{z^2}{4t}\right) t^{s-1} dt.$$

Using well-known properties of Γ-functions, we can therefore determine the growth of $\phi(S + it, m)$ with respect to t, and, combining these results with the theorem of Schnee-Landau type [8], we can attain an asymptotic property of $G(Y)$. The best result which one can expect in this way is

$$G(Y) = O\left(Y^{\frac{1}{2}+\frac{1}{n}+\varepsilon}\right)$$

for any $\varepsilon > 0$. Such a result may have some connection with [2], [9].

There are various open problems in the functional-analytic study of the reciprocity law. The most important one is to find a satisfactory relationship between the Fourier-Bessel transformation and the automorphic property of the function $\theta(u)$.

To speak more precisely, assume that the group Γ contains the element $\omega = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ with $\chi(\omega) = 1$, and denote by $\theta(v)$ the restriction to the v-axis of the function $\theta(u)$ derived from the Eisenstein series $E(u, s)$ for the cusp ∞ which we introduced earlier, i. e. $\theta(v) = \theta((0, v))$. Then, we have $\theta(v) = \theta(1/v)$, and from various reasons it is likely that there exists a function $f(t)$, $t \geqq 0$, satisfying the following properties:

i) $f\left(|z|^{\frac{n}{n-1}}\right)$, $z \in C$, belongs to the Schwartz space $S(C)$ over C.

ii) $f\left(t^{\frac{n}{n-1}}\right)$ is invariant under a Fourier-Bessel transformation, i. e.

$$2\pi \int_0^\infty f\left(t^{\frac{n}{n-1}}\right) J_0(2\pi tw) t dt = f\left(w^{\frac{n}{n-1}}\right), \qquad w \geqq 0.$$

iii) Put $\delta_F = |\sqrt{-d}/2|$, and $\mathfrak{m} = \delta_F^{1/2}\mathfrak{o}$; then $\mathfrak{m}$ is a self-dual module with respect to the additive character $e(z/2\sqrt{-1})$ of complex numbers, and we have

$$v^{-\frac{n-1}{n}} \theta(v) = \Sigma f\left(|\nu|^{\frac{n}{n-1}} v\right), \qquad (\nu \in \mathfrak{m}).$$

If $n = 2$, then we may take $e^{-\pi t}$ as $f(t)$, and the series in *iii)* reduces to an ordinary theta-series. Therefore, the main meaning of the conditions *i)*, *ii)*, *iii)* is that, under these conditions, the general reciprocity law can be viewed as a theorem which is based upon analytic properties of the Schwartz function f, in such a way that the quadratic reciprocity comes from the Fourier transformation of $e^{-\pi t^2}$.

The conditions *i)*, *ii)*, *iii)* have, however, also some other consequences. For example, it is possible to deduce from them an asymptotic property of Fourier coefficients of $\theta(u)$ derived from the Fourier expansion of $E(u, s)$. This will imply again an asymptotic property of Gauss sums, because the Fourier coefficients of $\theta(u)$ is closely related to Gauss sums like $g_1(m)$, $(m \in \mathfrak{o})$ [7]. The results which we obtain in this way are different from the assertions on $G(Y)$ which we have given above.

REFERENCES

[1] H. HECKE. — *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig (1923).

[2] E. KRÄTZEL. — Kubische und biquadratische Gausssche Summen, *Journ. reine angew. Math.*, 228 (1967), pp. 159-165.

[3] T. KUBOTA. — Ein arithmetischer Satz über eine Matrizengruppe, *Journ. reine angew. Math.*, 222 (1966), pp. 10-24.

[4] —. — On a special kind of Dirichlet series, *Journ. Math. Soc. Japan*, 20 (1968), pp. 193-207.

[5] —. — On automorphic functions and the reciprocity law in a number field, *Lectures in Math.*, 2, Kyoto Univ. (1969).

[6] —. — Some results concerning reciprocity law and real analytic automorphic functions, Proc. Summer Institute on Number Theory held at State Univ. of New York at Stony Brook (1969), to appear.

[7] —. — Some number theoretical results on real analytic automorphic forms, Proc. Conference on Several Complex Variables held at Univ. of Maryland (1970), to appear.

[8] E. LANDAU. — *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig (1909).

[9] H. MELLIN. — Bemerkungen im Anschluss an den Beweis eines Satzes von Hardy über die Zetafunktion, *Ann. Acad. Sci. Fennicae*, A-11, No. 3 (1917), 17 pages.

[10] H. REICHARDT. — *C. F. Gauss Gedenkband anlässlich des 100. Todestages am 23, Februar 1955*, Leipzig (1957).

[11] A. SELBERG. — Discontinuous groups and harmonic analysis, *Proc. Int. Congr. Stockholm* (1962), pp. 177-189.

[12] A. WEIL. — Sur certains groupes d'opérateurs unitaires, *Acta Math.*, 111 (1964), pp. 143-211.

Mathematical Institute
Faculty of Science
Nagoya University
Chikusaku, Nagoya
(Japon)

Added in proof. — Shortly after the Congress, the author found an adequate way of interpreting the transformation formula of $\theta(u)$ through an integral transformation. This requires, however, some changes in the statements *i*), *ii*), *iii*).

Actes, *Congrès intern. math.*, 1970. Tome 1, p. 401 à 411.

LE GROUPE DE BRAUER-GROTHENDIECK EN GÉOMÉTRIE DIOPHANTIENNE

par Y. I. MANIN

Introduction.

Soit k un corps, $[k:\mathbf{Q}] < \infty$, $\mathscr{V}$ une classe de variétés algébriques sur k. Soit $V \in \mathscr{V}$ et soit k_v un complété de k.

La première condition nécessaire pour l'existence d'un k-point sur V est que, pour tout v, $V(k_v)$ ne soit pas vide. Si pour tout $V \in \mathscr{V}$ cette condition est suffisante, on dit que le principe de Hasse est vérifié par $\mathscr{V}$.

Si $\mathscr{V}$ est la classe des espaces homogènes principaux sur une variété abélienne V_0, Cassels [1] et Tate ont donné une obstruction au principe de Hasse et cette obstruction est effectivement calculable. Plus précisément, soit $V \in \mathscr{V}$ et soit $b \in H^1(G, V_0(\bar{k}))$ la classe de cohomologie correspondante, où $G = \mathrm{Gal}(\bar{k}/k)$. Si tous les $V(k_v)$ sont non vides, b appartient au groupe de Chafarevitch-Tate $Ш(V_0)$. Soit $\hat{V}_0$ la variété abélienne duale de V_0 et soit $Ш(V_0) \times Ш(\hat{V}_0) \to \mathbf{Q}/\mathbf{Z}$ l'accouplement canonique de Cassels-Tate. Pour que $V(k)$ soit non vide, il faut que la classe b de V appartienne au noyau (à gauche) de cet accouplement.

Le premier but de cet exposé est de démontrer que l'utilisation du groupe de Brauer-Grothendieck $\mathrm{Br}(V)$ de la variété V permet de construire une obstruction parfaitement générale au principe de Hasse. En calculant cette obstruction pour différentes classes $\mathscr{V}$, nous obtenons tout d'abord une démonstration simple et unifiée d'une série de résultats déjà connus. On obtient ainsi :

a) La forme de Cassels-Tate et la « suite duale » de Cassels [1, 2].

b) Le théorème de Voskresensky sur le groupe Ш pour les tores [14].

c) Les contre-exemples de Swinnerton-Dyer [12], de Mordell [9] et de Cassels et de Guy [3] au principe de Hasse pour certaines surfaces cubiques.

La construction de l'obstruction est liée à l'existence d'un accouplement général $\mathrm{Br}(V) \times Z(V) \to \mathrm{Br}(k)$, où $Z(V)$ est le groupe des cycles de dimension zéro sur V. En appliquant cet accouplement lorsque $V(k)$ est non vide, on peut obtenir des résultats qui vont plus loin :

d) Des minorations pour le « rang » de la surface cubique V (nombre de points de $V(k)$ à partir desquels on peut construire tous les autres par la méthode « des sécantes et des tangentes » ; voir [7]).

e) Un certain accouplement de $\mathrm{Br}(V)$ et du noyau d'Albanese dans le groupe de Chow de dimension zéro, cet accouplement étant à valeurs dans $\mathrm{Br}(k)$. Comme l'a démontré récemment Mumford [10], le deuxième groupe est de dimension infinie si

$k = C$, dim $V = 2$ et $p_g(V) > 0$. L'étude de ce groupe par voie arithmétique peut présenter un intérêt.

Construction de l'obstruction.

Soit V une variété sur k et soit $\mathrm{Br}(V)$ son groupe de Brauer-Grothendieck (voir Grothendieck [5]). A tout élément $a \in \mathrm{Br}(V)$ et à tout point géométrique $x \in V(K)$, $K \supset k$, est attachée une spécialisation $a(x) \in \mathrm{Br}(K)$. (Si a est la classe d'une algèbre d'Azumaya A sur V, $a(x)$ est la classe de la fibre géométrique $A(x)$).

Supposons que k soit un corps de nombres et que $V(k_v)$ soit non vide pour tout v. Soit $V(A)$ l'espace des k-adèles de V.

Fixons un sous-groupe B de $\mathrm{Br}(V)$.

DÉFINITION. — *a) Les adèles* (x_v), $(y_v) \in V(A)$ *sont B-équivalents si*

$$\forall a \in B, \quad \forall v, \quad a(x_v) = a(y_v) \in \mathrm{Br}(k_v).$$

b) On désignera par E l'espace quotient de V(A) par la relation de B-équivalence.

c) Soit $X \in E$; on définit un caractère $i_X : B \to Q/Z$ par la formule

$$i_X(a) = \sum_v \mathrm{inv}_v(a(x_v)),$$

où (x_v) adèle quelconque de la classe X et où $\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow Q/Z$ est le plongement classique (c'est un isomorphisme si v n'est pas archimédienne).

1. THÉORÈME DE L'OBSTRUCTION : $V(k) \subset \bigcup_{i_X = 0} X \subset V(A)$.

La démonstration est triviale : si l'adèle $(x_v) \in X$ est un adèle principal et correspond au point $x \in V(k)$, alors $a(x)$ appartient à $\mathrm{Br}(k)$ pour tout $a \in B$ et, par conséquent,

$$\sum_v \mathrm{inv}_v a(x) = 0.$$

Si l'on choisit convenablement V et B, *il se peut que* $i_X \neq 0$ *pour tout* X : alors $V(k)$ est vide, bien que $V(A)$ soit non vide.

Avant de passer aux exemples, donnons quelques propriétés du *groupe de Brauer-Grothendieck* $\mathrm{Br}(V)$.

Les k-morphismes canoniques $V \to k$ et $V \otimes \bar{k} \to V$ induisent des homomorphismes $\mathrm{Br}(k) \to \mathrm{Br}(V)$ et $\mathrm{Br}(V) \to \mathrm{Br}(V \otimes \bar{k})$. Désignons par $\mathrm{Br}_0(V)$ l'image du premier homomorphisme et par $\mathrm{Br}_1(V)$ le noyau du deuxième.

La filtration

$$\mathrm{Br}_0(V) \subset \mathrm{Br}_1(V) \subset \mathrm{Br}_2(V) = \mathrm{Br}(V)$$

joue un rôle essentiel dans l'étude du groupe de Brauer. Il est évident que, quels que soient B et X, on a $B \cap \mathrm{Br}_0(V) \subset \mathrm{Ker}\, i_X$. Ici, seuls les sous-groupes B contenus dans $\mathrm{Br}_1(V)$ nous intéressent. C'est pourquoi il faut savoir calculer $\mathrm{Br}_1(V)/\mathrm{Br}_0(V)$. Ce groupe est décrit, dans une large mesure, par le résultat suivant, dans lequel on suppose que V est une varité projective lisse :

Soit V_0 la variété d'Albanese de V, $\hat{V}_0$ la variété duale et NS le groupe de Néron-Severi.

2. THÉORÈME. — *Si $H^3(G, \bar{k}^*) = 0$, on a une suite exacte*

$$\mathrm{Pic}(V\otimes\bar{k})^G \to NS(V\otimes\bar{k})^G \to H^1(G, \hat{V}_0(\bar{k})) \xrightarrow{\varphi} \mathrm{Br}_1(V)/\mathrm{Br}_0(V) \xrightarrow{\psi} H^1(G, NS(V\otimes\bar{k})) \to H^2(G, \hat{V}_0(\bar{k})).$$

Cas particuliers

a) Si $H^1(G, NS(V\otimes\bar{k})) = 0$ (par exemple, si V est une courbe, ou, plus généralement, si $NS(V\otimes\bar{k})$ est libre et G opère dessus de façon triviale), il existe un épimorphisme à noyau fini

$$H^1(G, \hat{V}_0(\bar{k})) \xrightarrow{\varphi} \mathrm{Br}_1(V)/\mathrm{Br}_0(V) \to 0.$$

b) Si $V_0 = \{0\}$, alors $\mathrm{Br}_1(V)/\mathrm{Br}_0(V) \cong H^1(G, NS(V\otimes\bar{k}))$.

Pour la démonstration, nous aurons besoin de deux lemmes.

3. LEMME. — $\mathrm{Br}_1(V)/\mathrm{Br}_0(V) \cong H^1(G, \mathrm{Pic}(V\otimes\bar{k})$.

Démonstration. — Soit $\bar{k}(\xi)$ le corps des fonctions rationnelles sur $V\otimes\bar{k}$. De la lissité de V, on déduit facilement, par passage à la fibre générique, la suite exacte (cf. Grothendieck [5], II)

$$0 \to \mathrm{Br}_1(V) \to H^2(G, \bar{k}(\xi)^*) \to H^2(G, \mathrm{Div}(V\otimes\bar{k})).$$

On peut l'inclure dans le diagramme commutatif:

$$\begin{array}{ccccccc}
 & & \mathrm{Br}(k) & \xrightarrow{\sim} & \mathrm{Br}(k) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Br}_1(V) & \to & H^2(G, \bar{k}(\xi)^*) & \to & H^2(G, \mathrm{Div}(V\otimes\bar{k})) \\
 & & & & \downarrow & & \downarrow\wr \\
0 & \to & H^1(G, \mathrm{Pic}(V\otimes\bar{k})) & \to & H^2(G, \bar{k}(\xi)^*/\bar{k}^*) & \to & H^2(G, \mathrm{Div}(\xi\otimes\bar{k})) \\
 & & & & \downarrow & & \\
 & & & & H^3(G, \bar{k}^*) = 0 & &
\end{array}$$

La ligne du bas de ce diagramme provient de la suite exacte de G-modules

$$0 \to \bar{k}(\xi)^*/\bar{k}^* \to \mathrm{Div}(V\otimes\bar{k}) \to \mathrm{Pic}(V\otimes\bar{k}) \to 0,$$

tandis que la colonne provient de la suite $0 \to \bar{k}^* \to \bar{k}(\xi)^* \to \bar{k}(\xi)^*/\bar{k}^* \to 0$.

En utilisant la partie gauche de ce diagramme, on obtient facilement le résultat cherché. (Ce raisonnement a été utilisé par Lichtenbaum [6] dans le cas où V est une courbe et où, par conséquent, $\mathrm{Br}_1(V) = \mathrm{Br}(V)$).

Remarque. — La condition $H^3(G, \bar{k}^*) = 0$ peut être remplacée par la suivante: $V(k)$ est dense pour la topologie de Zariski.

4. LEMME. — $\mathrm{Pic}^0(V\otimes\bar{k}) = \hat{V}_0(\bar{k})$ *en tant que G-modules.*

Démonstration. — Pic^0 est le groupe des classes des diviseurs qui sont algébriquement équivalents à zéro. L'application canonique $\alpha\colon V\times V \to V_0$ induit un plongement

$$\alpha^*\colon \mathrm{Pic}^0(V_0) \to \mathrm{Pic}^0(V\times V);$$

en outre, l'application $L \mapsto p_1^*L \otimes p_2^*L^{-1}$ (où $p_i: V \times V \to V$ est la $i^{\text{ème}}$ projection) définit un plongement

$$\beta^*: \mathrm{Pic}^0(V) \to \mathrm{Pic}^0(V \times V).$$

On voit facilement que α^* et β^* ont même image, formée des classes des faisceaux inversibles sur $V \times V$ qui sont triviaux sur la diagonale. Ceci donne des isomorphismes $\hat{V}_0(k) \to \mathrm{Pic}^0(V_0)$; on a une construction analogue sur le corps $\bar{k}$.

Démonstration du théorème 2. — On l'obtient en considérant la suite exacte de cohomologie associée à la suite de G-modules

$$0 \to \mathrm{Pic}^0(V \otimes \bar{k}) \to \mathrm{Pic}\,(V \otimes \bar{k}) \to NS(V \otimes \bar{k}) \to 0$$

et en appliquant les lemmes 3 et 4.

Applications. — Nous nous limiterons à deux exemples :

5. La surface de Swinnerton-Dyer [12]. — Cette surface V est donnée par l'équation homogène sur $\boldsymbol{Q}$:

$$T_3(T_0 + T_3)(T_0 + 2T_3) = \prod_{i=1}^{3} (T_0 + \theta^{(i)}T_1 + \theta^{(i)2}T_2) \tag{1}$$

où les $\theta^{(i)}$ sont les trois racines du polynôme $\theta^3 + 7(\theta + 1)^2 = 0$. On vérifie facilement que $V(\boldsymbol{Q}_p)$ et $V(\boldsymbol{R})$ sont non vides. Soit $K = \boldsymbol{Q}(\theta)$. C'est une extension cubique normale ; $V \otimes K$ est birationnellement équivalente à $\boldsymbol{P}_K^2$. On a donc $\mathrm{Br}(V) = \mathrm{Br}_1(V)$ et $V_0 = 0$. Il découle du théorème 2 que

$$\mathrm{Br}_1(V)/\mathrm{Br}_0(V) = H^1\,(\mathrm{Gal}\,K/k, \mathrm{Pic}\,(V \otimes K)) \cong \boldsymbol{Z}_3 \times \boldsymbol{Z}_3.$$

Étant donné que $G_0 = \mathrm{Gal}\,(K/k)$ est cyclique, il est commode d'identifier $\mathrm{Br}(V)$ au sous-groupe de $\mathrm{Br}(\boldsymbol{Q}(\xi))$ que voici :

$$\begin{aligned} &\mathrm{Ker}\,[H^2(G_0, K(\xi)^*) \to H^2(G_0, \mathrm{Div}\,(V \otimes K))] \\ &\qquad \cong \mathrm{Ker}\,[H^0(G_0, K(\xi)^*) \to H^0(G_0, \mathrm{Div}\,(V \otimes K))] \subset k(\xi)^*/N_{K/k}(K(\xi)^*), \end{aligned}$$

où ξ est un point générique de V.

Désignons par B le sous-groupe de $\mathrm{Br}_1(V)$ engendré par les deux éléments de $k(\xi)^*/N_{K/k}(K(\xi)^*)$ représentés par les fonctions

$$f_1 = \frac{T_0 + T_3}{T_3} \quad , \quad f_2 = \frac{T_0 + 2T_3}{T_3}.$$

(Leurs diviseurs sont des normes, comme on le voit sur l'équation (1) ; c'est pourquoi les cocycles fonctionnels correspondants se décomposent dans la cohomologie à coefficients dans $\mathrm{Div}\,(V)$. Un calcul facile montre que $\mathrm{Br}(V)$ est engendré par $\mathrm{Br}_0(V)$ et B).

Une étude locale élémentaire permet d'établir le fait suivant :

Proposition. — *a) Soit* $x \in V(\boldsymbol{R})$ *ou* $V(\boldsymbol{Q}_p)$, *avec* $p \neq 7$, $T_3(T_0 + T_3)(T_0 + 2T_3)(x) \neq 0$. *Alors*

$$\mathrm{inv}_v(f_1(x)) = \mathrm{inv}_v(f_2(x)) = 0.$$

b) Soit $x \in V(\boldsymbol{Q}_7)$. *Alors, ou bien* $\mathrm{inv}_7(f_1(x)) \neq 0$, *ou bien* $\mathrm{inv}_7(f_2(x)) \neq 0$.

Le résultat relatif à $\boldsymbol{Q}_7$ provient de ce que 7 est complètement ramifié dans K, et $f_1(x)$ et $f_2(x)$ doivent être des unités locales, tandis que $f_2(x) - f_1(x) = 1$. Mais les normes des unités locales sont congrues à ± 1 (mod. 7) et leur différence ne peut donc être égale à 1.

COROLLAIRE. — *L'ensemble $V(\boldsymbol{Q})$ est vide.*

En effet, il découle clairement de la proposition précédente que, pour tout adèle $(x_v) \in V(A)$, on a $\sum_v \mathrm{inv}_v(f_1(x)) \neq 0$ ou $\sum_v \mathrm{inv}_v(f_2(x)) \neq 0$.

On peut interpréter de la même façon les contre-exemples de Mordell [9] qui constituent plusieurs séries infinies.

L'exemple plus fin de Cassels et Guy [3] rentre aussi dans notre schéma général mais non sans quelques difficultés. Pour les détails, voir [7].

VARIÉTÉS ABÉLIENNES. — Soit V un espace homogène principal sur une variété abélienne V_0 et soit $b \in H^1(G, V_0(\bar{k}))$ sa classe de cohomologie, où $G = \mathrm{Gal}(\bar{k}/k)$. Si tous les $V(k_v)$ sont non vides, alors $b \in Ш(V_0)$.

Choisissons maintenant le sous-groupe B de $\mathrm{Br}(V)$. L'obstruction la plus économique est obtenue si l'ensemble $E = V(A) \bmod B$ est composé d'une seule classe, autrement dit si, pour tout $a \in B$, la spécialisation $a(x_v)$ ne dépend pas du choix de x_v dans $V(k_v)$. Pour cela, il suffit que $a \otimes k_v \in \mathrm{Br}_0(V \otimes k_v)$ pour tout v; dans ce cas, l'obstruction est alors l'homomorphisme $i\colon B \to \boldsymbol{Q}/\boldsymbol{Z}$ défini par

$$i(a) = \sum_v \mathrm{inv}_v(a(x_v)).$$

En particulier, le théorème 2 montre qu'on peut prendre pour B le groupe suivant:

$$B = \rho^{-1} \circ \varphi(Ш(\hat{V}_0)), \tag{2}$$

où $\rho\colon \mathrm{Br}(V) \to \mathrm{Br}(V)/\mathrm{Br}_0(V)$ est l'épimorphisme canonique.

Dans ces conditions, on a

6. THÉORÈME. — *Soit $a \in B$, $\rho(a) = \varphi(a')$, $a' \in Ш(\hat{V}_0)$, et soit $b \in Ш(V_0)$ la classe de l'espace V. On a alors*

$$i(a) = \langle b, a' \rangle \in \boldsymbol{Q}/\boldsymbol{Z},$$

où $\langle\, ,\rangle$ est la forme de Cassels-Tate $Ш(V_0) \times Ш(\hat{V}_0) \to \boldsymbol{Q}/\boldsymbol{Z}$.

La démonstration s'obtient par une simple comparaison de deux définitions (cf. la proposition 8 *c*) ci-dessous, qui contient l'idée centrale des calculs).

Remarques.

a) Regardons ce que l'on obtient si on construit l'obstruction à l'aide d'un sous-groupe plus grand que le groupe (2). Ceci a une raison d'être si l'obstruction précédente est nulle, ou, autrement dit, si (classe $V) \in Ш(V_0)$, avec les notations de Cassels [2]. Posons alors $B' = \rho^{-1} \circ \varphi(H^1(G, \hat{V}_0(\bar{k}))$. Il est évident que pour toute classe $X \in V(A) \bmod B'$, nous avons $B \in \mathrm{Ker}\, i_X$, où B est défini par (2). Chaque classe X définit donc un caractère

$$i'_X\colon B'/B = H^1(G, \hat{V}_0(\bar{k}))/Ш(\hat{V}_0) \to \boldsymbol{Q}/\boldsymbol{Z}.$$

Si, comme le suppose Cassels, $Ш$ est fini, alors $Ш(V_0) = \{0\}$ et $V \cong V_0$; l'ensemble $V_0(A)$ mod B' possède une structure de groupe naturelle. On peut alors montrer que i' fournit une dualité topologique

$$V_0(A) \bmod B' \times H^1(G, \hat{V}_0(\bar{k}))/Ш(\hat{V}_0) \to \boldsymbol{Q}/\boldsymbol{Z},$$

et donner une description plus transparente de la B'-équivalence.

Ceci constitue l'étape essentielle dans la construction d'une suite exacte duale à

$$0 \to H^1(G, \hat{V}_0(\bar{k}))/Ш(\hat{V}_0) \to \sum_v H^1(G_v, \hat{V}_0(k_v)) \to Б(\hat{V}_0) \to 0.$$

En fait, Cassels [2] considère une suite à 4 termes, avec $Ш(\hat{V}_0)$ à gauche, et il obtient la suite duale

$$0 \leftarrow Ш(V_0) \leftarrow \theta \leftarrow \prod_v V_0'(k_v) \leftarrow V_0(k)^{\sim} \leftarrow 0 \tag{3}$$

où $V_0'(k_v)$ est le quotient de $V_0(k_v)$ par sa composante neutre et $V_0(k)^{\sim}$ le complété de $V_0(k)$ pour la topologie induite.

b) Soit V_0 un tore et $\bar{V}$ sa fermeture projective lisse. Voskressensky a construit la suite exacte suivante ([14], théorème 6):

$$0 \leftarrow Ш(V_0) \leftarrow H^1(G, \operatorname{Pic}(\bar{V} \otimes \bar{k}) \leftarrow \prod_v V_0(k_v) \leftarrow V_0(k)^{\sim} \leftarrow 0. \tag{4}$$

L'analogie avec (3) est presque complète puisque, en raison du théorème 2, on a

$$H^1(G, \operatorname{Pic}(\bar{V} \otimes \bar{k})) \cong \operatorname{Br}_1(\bar{V})/\operatorname{Br}_0(\bar{V})$$

(dans (3), le groupe θ est effectivement dual de $\operatorname{Br}_1(V_0)/\operatorname{Br}_0(V_0) \ldots$).

c) Plusieurs propriétés de la forme de Cassels-Tate résultent directement de notre définition. Toutefois, l'additivité par rapport au premier argument (voir théorème 6) n'est pas évidente. C'est pourquoi nous allons reformuler la « composante locale » de notre construction de manière à rendre évidente l'existence d'un accouplement complétant les homomorphismes i_X.

Produit scalaire.

Soit k un corps parfait, V une variété sur k, $Z(V)$ le groupe des cycles de V de dimension zéro. Les points fermés $x \in V$ forment une base de ce groupe.

7. Définition. — *L'accouplement*

$$\operatorname{Br}(V) \times Z(V) \to \operatorname{Br}(k)$$

est défini par la formule

$$(a, \Sigma n_i(x_i)) = \Sigma n_i \operatorname{cor}_{k(x_i)/k} a(x_i) \tag{5}$$

pour $a \in \operatorname{Br}(V)$, $\Sigma n_i x_i \in Z(V)$, où cor est l'homomorphisme de corestriction

$$\operatorname{Br}(k(x_i)) \to \operatorname{Br}(k).$$

Cette définition a été proposée dans [8]. Lichtenbaum [6], et avant lui D. K. Faddeev [4], ont étudié une construction analogue lorsque V est une courbe ; dans le cas dim $V \geqslant 2$, on observe de nouveaux phénomènes qui sont intéressants.

Pour formuler les principales propriétés de l'accouplement ci-dessus, considérons la filtration

$$Z_1(V) \subset Z_a(V) \subset Z_0(V) \subset Z(V).$$

Le groupe $Z_0(V)$ est formé des cycles de degré zéro :

$$z = \Sigma n_i x_i \in Z_0(V) \Leftrightarrow \deg z = \Sigma n_i [k(x_i) : k] = 0.$$

Pour définir $Z_a(V)$, on utilise le fait que l'application canonique d'Albanese $\alpha : V \times V \to V_0$ induit l'homomorphisme « de sommation » $\beta : Z_0(V) \to V_0(k)$. Son noyau est $Z_a(V)$.

Enfin, $Z_1(V)$ est le groupe des cycles rationnellement équivalents à zéro. Il est engendré par les cycles de la forme $z(0) - z(\infty)$, où $\{ z(t), t \} \subset V \times \boldsymbol{P}^1$ est un système plat quelconque de cycles de V de dimension zéro, de base $\boldsymbol{P}^1$.

8. Proposition.

a) Pour tout $a \in \mathrm{Br}_0(V)$ *et tout* $z \in Z_0(V)$, *on a* $(a, z) = 0$.

b) Pour tout $a \in \mathrm{Br}(V)$ *et tout* $z \in Z_1(V)$, *on a* $(a, z) = 0$.

c) Soit $\varphi : H^1(G, \hat{V}_0(\bar{k})) \to \mathrm{Br}_1(V)/\mathrm{Br}_0(V)$ *et soit* $\rho : \mathrm{Br}_1(V) \to \mathrm{Br}_1(V)/\mathrm{Br}_0(V)$ *les applications canoniques. Si* $\rho(a) = \varphi(a')$, $z \in Z_0(V)$ *et si* $V(k)$ *n'est pas vide, on a*

$$(a, z) = (a', \beta(z))_T, \tag{6}$$

où $(\ , \ )_T$ *est l'accouplement de Tate* 13 : $H^1(G, \hat{V}_0(\bar{k})) \times V_0(k) \to \mathrm{Br}(k)$. *En particulier,* $\rho^{-1} \circ \varphi(H^1(G, V_0(\bar{k})))$ *et* $Z_a(V)$ *sont orthogonaux.*

(Il est probable que la condition « $V(k)$ est non vide » n'est pas indispensable).

De cette proposition découle immédiatement le théorème suivant :

9. Théorème. — *Le produit scalaire défini ci-dessus induit des accouplements*

$$\mathrm{Br}(V)/\mathrm{Br}(V_0) \times Z_0(V)/Z_1(V) \to \mathrm{Br}(k), \tag{7}$$

$$\mathrm{Br}'_1(V)/\mathrm{Br}_0(V) \times Z_0(V)/Z_1(V) \to \mathrm{Br}(k), \tag{8}$$

où $\mathrm{Br}'_1(V) = \rho^{-1} \circ \varphi(H^1(G, \hat{V}_0(\bar{k}))) \subset \mathrm{Br}_1(V)$;

$$\mathrm{Br}(V)/\mathrm{Br}'_1(V) \times Z_a(V)/Z_1(V) \to \mathrm{Br}(k). \tag{9}$$

Commentaires. — Il n'y a rien à dire de spécial sur l'accouplement (7) ; il est intervenu dans la construction de l'obstruction au principe de Hasse. L'accouplement (8) pourrait être considéré comme une « explication » de la construction de Tate, si celle-ci n'était pas déjà classique.

L'accouplement (9) est vraisemblablement nouveau. Les deux groupes qui y figurent ne peuvent être non triviaux que si dim $V \geqslant 2$, et ils ont encore été très peu étudiés (même pour les variétés abéliennes). Voilà ce que l'on sait à leur sujet :

Supposons pour simplifier que $H^1(G, NS(V \otimes \bar{k})) = 0$ (pour des V abéliennes et, plus généralement, pour des variétés sans torsion, cette condition peut être réalisée après extension finie du corps de base).

Alors $\mathrm{Br}'_1(V) = \mathrm{Br}_1(V)$ (théorème 2). D'après la définition de Br_1, le morphisme de projection $V \otimes \bar{k} \to V$ induit un plongement

$$\mathrm{Br}(V)/\mathrm{Br}_1(V) \hookrightarrow (\mathrm{Br}(V \otimes \bar{k}))^G,$$

où G agit sur $\mathrm{Br}(V \otimes \bar{k})$ par le deuxième facteur. D'après Grothendieck [5], il existe un isomorphisme canonique

$$\mathrm{Br}(V \otimes \bar{k}) = H^2(V, \mu_\infty)/(\boldsymbol{Q}/\boldsymbol{Z} \otimes NS(V \otimes \bar{k})),$$

où $H^2(V, \mu_\infty) = \varinjlim H^2(V, \mu_n)$. En particulier, $\mathrm{Br}(V \otimes \bar{k})$ est un groupe divisible de corang fini $B_2 - \rho$.

Selon une conjecture de Tate, le groupe $(\mathrm{Br}(V \otimes \bar{k}))^G$ doit être fini si $[k:\boldsymbol{Q}] < \infty$. On connaît peu de choses sur l'action de G sur $H^2(V, \mu_\infty)$ dans le cas des corps locaux. Lorsque $V = X \times Y$, où X et Y sont des courbes elliptiques, on peut construire, en utilisant la théorie de Serre [11], des exemples intéressants de V pour lesquels le corang de $(\mathrm{Br}(V \otimes \bar{k}))^G$ est non nul. Toutefois, j'ignore dans quelle mesure $\mathrm{Br}(V)/\mathrm{Br}_1(V)$ peut être différent de $(\mathrm{Br}(V \otimes \bar{k}))^G$.

Considérons maintenant le groupe $Z_a(V)/Z_1(V)$. Le seul résultat connu concernant ce groupe est le théorème suivant de Mumford [10]: *si $k = \boldsymbol{C}$ et* $\dim H^0(V, \Omega_V^2) > 0$, *alors $Z_a(V)/Z_1(V)$ est de dimension infinie.* Malheureusement, la méthode de Severi-Mumford ne donne presque pas de renseignements supplémentaires sur ce groupe; en particulier, j'ignore dans quelle mesure il peut être non trivial sur un corps dénombrable.

C'est pourquoi il est logique d'essayer d'utiliser l'accouplement (9) pour l'étude de ce groupe.

Il est à noter que les deux approches sont liées, d'une certaine façon, à l'existence de cycles transcendants de dimension deux sur V (par l'intermédiaire des inégalités $h^{2,0} > 0$ ou $B_2 - \rho > 0$). N'y a-t-il pas d'explication de ce fait?

Autre question: peut-on construire un élément infiniment divisible dans $Ш(V_0)$, où V_0 est une variété abélienne convenable, en utilisant l'obstruction sur $\mathrm{Br}(V)/\mathrm{Br}_1(V)$? En tout cas, la structure du noyau d'Albanese doit jouer un rôle dans l'arithmétique des variétés abéliennes.

10. Démonstration de la proposition 8

a) Soit $a \in \mathrm{Br}_0(V)$ l'image de $a' \in \mathrm{Br}(k)$. Alors, pour tout point fermé $x \in V$, $a(x)$ est l'image de $\mathrm{res}_{k/k(x)} a'$. On a donc

$$\mathrm{cor}_{k(x)/k}\, a(x) = [k(x): k] a$$

et par suite

$$(a, z) = \deg(z) \cdot a \quad \text{pour tout} \quad z \in Z(V).$$

b) Soit $C \subset V \times \boldsymbol{P}^1$ le graphe d'un système plat irréductible $z(t)$ de cycles de dimension zéro sur V. La compatibilité de la corestriction et de la spécialisation montre que pour tout élément $a \in \mathrm{Br}(V)$ et tout point $t \in \boldsymbol{P}^1(k)$, on a:

$$(a, z(t)) = (\mathrm{cor}_{C/\boldsymbol{P}^1}(p_1^*(a)\,|_C), t),$$

où $p_1 : V \times \boldsymbol{P}^1 \to V$ est la projection et l'homomorphisme $\mathrm{cor}_{C/\boldsymbol{P}^1} : \mathrm{Br}(C) \to \mathrm{Br}(\boldsymbol{P}^1)$ est induit par la corestriction habituelle aux points génériques. Mais

$$\mathrm{Br}(\boldsymbol{P}^1) = \mathrm{Br}_0(\boldsymbol{P}^1) = \mathrm{Br}(k),$$

et $(a, z(t))$ ne dépend donc pas de t.

c) La démonstration de la formule (6) repose sur une comparaison détaillée des définitions.

Puisque $V(k)$, par hypothèse, est non vide, il existe une application $\alpha_0 : V \to V_0$ telle que l'application d'Albanese $\alpha : V \times V \to V_0$ soit donnée par $\alpha(x, y) = \alpha_0(x) - \alpha_0(y)$. Identifions $Z(V)$ avec $Z(V \otimes \bar{k})^G$. Alors, l'application $\beta : Z_0(V) \to V(k)$ est donnée par la formule

$$\beta\Big(\sum_{x \in V(\bar{k})} n_x(x)\Big) = \Sigma n_x \alpha_0(x).$$

Soit $a' \in H^1(G, \hat{V}_0(\bar{k}))$; choisissons un cocycle $\{ a_s \}$ représentant a' dans une extension normale finie K/k où a' se décompose. Soit en outre :

$$z = \sum_{x \in V(\bar{k})} n_x(x) \in Z_0(V).$$

Nous garderons ces notations jusqu'à la fin de la démonstration.

Calcul de $(a', \beta(z))_T$.

Suivant la méthode de Tate [13], calculons d'abord $\delta a'$, où δ provient de la suite exacte (où S désigne l'homomorphisme « somme ») :

$$0 \to Z_a(\hat{V}_0 \otimes K) \to Z_0(\hat{V}_0 \otimes K) \xrightarrow{S} \hat{V}_0(K) \to 0.$$

Pour image inverse de a_s dans $Z_0(V_0 \otimes K)$, prenons le cycle $(a_s) - (0)$. La classe de cohomologie $\delta a'$ est alors représentée par le cocycle

$$\{ (sa_t) - (a_{st}) + (a_s) - (0) \} \in Z^2(G, Z_a(\hat{V}_0 \otimes K)).$$

Soit $D \subset \hat{V}_0 \times V$ un diviseur de Poincaré. Pour tout point géométrique $x \in \hat{V}_0(K)$, notons $D(x) \in \mathrm{Div}\,(V_0 \otimes K)$ sa fibre géométrique en x. Si $s, t \in G$, le diviseur

$$D(sa_t) - D(a_{st}) + D(a_s) - D(0) \tag{10}$$

est un diviseur principal d'après le théorème du carré. Soit $g_{s,t}$ la fonction rationnelle correspondante sur $V_0 \otimes K$.

Ici se terminent les opérations pour le premier terme a'.

Il reste encore à choisir une image inverse pour S du point $\beta(z)$. Nous prenons pour cela le cycle

$$\sum_{x \in V(\bar{k})} n_x(\alpha_0(x)) \in Z_0(V_0 \otimes \bar{k})^G.$$

Maintenant, par définition, la classe de cohomologie $(a', \beta(z))_T$ appartenant à $H^2(G, K^*)$ est représentée par le cocycle

$$\Big\{ \prod_{x \in V(\bar{k})} g_{s,t}(\alpha_0(x))^{n_x} \Big\} \in Z^2(G, K^*). \tag{11}$$

(Le diviseur de Poincaré D doit être choisi tel que $\mathrm{Supp}\,(\Sigma s D_t)$ ne contienne pas de points $\alpha_0(x)$ avec $n_x \neq 0$, ce que l'on peut toujours réaliser).

Calcul de (a, z).

Il faut d'abord calculer l'élément

$$\varphi(a') \in \mathrm{Br}_1(V)/\mathrm{Br}_0(V).$$

L'homomorphisme composé $\hat{V}_0(K) \to \mathrm{Pic}^0(V_0 \otimes K) \overset{\alpha_0^*}{\to} Pic^0(V \otimes K) \hookrightarrow \mathrm{Pic}\,(V \otimes K)$ transforme le cocycle $\{ a_s \}$ en

$$\{ \mathrm{Cl}_{V\otimes K}(\alpha_0^*(D(a_s))) \} \in Z^1(G, \mathrm{Pic}\,(V \otimes K)).$$

De plus (voir la démonstration du lemme 3), l'homomorphisme bord associé à la suite

$$0 \to K(\xi)^*/K^* \to \mathrm{Div}\,(V \otimes K) \to \mathrm{Pic}\,(V \otimes K) \to 0,$$

transforme ce cocycle en le cocycle $\{ f_{s,t} \bmod K^* \} \in Z^2(G, K(v)^*/K)$, où

$$\mathrm{div}\,(f_{s,t}) = \alpha_0^*(D(sa_t) - D(a_{st}) + D(a_s)). \tag{12}$$

La classe de ce cocycle est égale à l'image de $\varphi(a')$ dans $H^2(G, K(\xi)^*/K)$. La définition 7 montre clairement que (a, z) est représenté par le cocycle

$$\{ \prod_{x \in V(\bar{k})} f_{s,t}(x)^{n_x} \} \in Z^2(G, K^*). \tag{13}$$

Mais le diviseur D peut être choisi de telle sorte que $D(0) = 0$. On voit alors, en comparant les formules (10) et (12), que, après une normalisation convenable, on a

$$f_{s,t} = \alpha_0^*(g_{s,t}),$$

et donc

$$f_{s,t}(x) = g_{s,t}(\alpha_0(x)).$$

Ceci démontre l'égalité de (11) et (13) et termine la démonstration de la proposition 8.

BIBLIOGRAPHIE

[1] J. W. S. Cassels. — Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, *Journ. für die reine u. angew. Math.*, Bd. 211, H. 1/2 (1962), pp. 95-112.

[2] J. W. S. Cassels. — Arithmetic on curves of genus 1. VII. The dual exact sequence, *Journ. für die reine u. angew. Math.*, Bd. 216, H. 3/4 (1964), pp. 150-158.

[3] J. W. S. Cassels, M. J. T. Guy. — On the Hasse principle for cubic surfaces, *Mathematika*, 13 (1966), pp. 111-120.

[4] Д. К. Фаддеев. — К теории алгебр над полем алгебраических функций одной переменной, Вестник ЛГУ, № 7, сер. мат., в. 2 (1957), 45-51.

[5] A. Grothendieck. — Le groupe de Brauer, I, II, III, *Séminaire Bourbaki*, 290 (1965), 297 (1965), *IHES notes* (1966).

[6] S. Lichtenbaum. — Duality theorems for Curves over p-adic fiels, *Inventiones Math.*, vol. 7, f. 2 (1969), pp. 120-136.

[7] Ю. И. Манин. — Кубические формы : алгебра, геометрия, арифметика (в печати).

[8] —. — Кубические гиперповерхности III. Лупы Муфанг и эквивалентность Брауэра. Мат. сборник, т. 79, в. 2 (1969), 155-170.

[9] L. Mordell. — On the conjecture for the rational points on a cubic surface, *J. Lond. Math. Soc.*, 40 (1965), pp. 149-158.

[10] D. MUMFORD. — Rational equivalence of O-cycles on surfaces, *Journ. Math. Kyoto Univ.*, vol. 9, N. 2 (1969), pp. 195-204.

[11] J. P. SERRE. — *Abelian l-adic representations and elliptic curves*, New York, Benjamin, 1968.

[12] H. P. F. SWINNERTON-DYER. — Two special cubic surfaces, *Mathematika*, 9 (1962), pp. 54-56.

[13] J. TATE. — WC-groups over *p*-adic fields, *Seminaire Bourbaki*, exp. 156 (1957).

[14] В. Е. ВОСКРЕСЕНСКИЙ. — Бирациональные свойства линейных алгебраических групп, Известия АН СССР, сер. мат.

Steklov Mathematical Institute
Academy of Sciences of USSR
ul Vavilova 42,
Moscow V 333 (U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 413 à 417.

LE THÉORÈME DE TORELLI POUR LES SURFACES ALGÉBRIQUES DE TYPE $K3$

par I. R. SHAFAREVITCH

Ce qui suit est l'exposition d'un travail effectué en commun avec I. I. Pjatetckii-Shapiro. Nous étudions les surfaces algébriques sur le corps des nombres complexes qui possèdent une classe canonique nulle. Cette condition équivaut au fait que la première classe de Chern est égale à 0 ou encore au fait que le groupe structural du fibré tangent peut être réduit au groupe spécial linéaire.

Il est bien connu qu'il existe deux classes de telles surfaces. L'une d'entre elles est constituée par les variétés abéliennes de dimension 2. Les surfaces de l'autre classe sont simplement connexes. On les appelle surfaces de type $K3$.

Une variété abélienne est uniquement déterminée par les périodes de ses formes différentielles holomorphes de degré 1. Il est facile d'en déduire qu'elle est également déterminée par les périodes de sa forme différentielle holomorphe de degré 2. Sur une surface de type $K3$, il n'y a pas de forme holomorphe de degré 1, mais, en revanche, il existe une forme holomorphe de degré 2, unique à un facteur constant près. Nous examinerons dans quelle mesure les périodes de cette forme différentielle déterminent la surface. La question ne se pose de façon naturelle que pour les surfaces polarisées, i. e. munies d'une classe d'homologie de dimension 2 correspondant à une section hyperplane. Pour énoncer le résultat, il est nécessaire d'introduire quelques notions :

Comme on le sait (cf. par exemple [1], chap. IX), pour une surface X de type $K3$, le groupe $H_2(X, \mathbb{Z})$ est un $\mathbb{Z}$-module libre de rang 22 et l'indice d'intersection y détermine une structure de réseau pair unimodulaire euclidien de signature (3, 19). On sait que les réseaux euclidiens qui possèdent ces propriétés sont tous isomorphes. Fixons l'un d'eux, soit L, et un certain vecteur l de L. Nous appellerons surface distinguée de type $K3$ un triplet $(X, \xi, \varphi) = \tilde{X}$ où X est une surface de type $K3$, $\xi \in H_2(X, \mathbb{Z})$ une classe de sections hyperplanes pour un certain plongement projectif et $\varphi : H_2(X, \mathbb{Z}) \to L$ un isomorphisme de réseaux euclidiens tel que $\varphi(\xi) = l$.

Posons $\tilde{\Omega} = \mathrm{Hom}\,(L, \mathbb{C})$ et définissons dans cet espace un produit scalaire bilinéaire sur $\mathbb{C}$ qui prolonge celui donné sur L. Désignons par Ω le domaine de l'espace projectif de dimension 21 correspondant à $\tilde{\Omega}$, dont les points correspondent aux vecteurs $\omega \in \tilde{\Omega}$ tels que

$$\omega^2 = 0$$
$$\omega . \overline{\omega} > 0,$$

et par $\Omega(l)$ l'ensemble des $\omega \in \Omega$ tels que $\omega . l = 0$. L'ensemble $\Omega(l)$ se présente comme la réunion disjointe de deux variétés complexes dont chacune est isomorphe à un domaine borné symétrique du type IV de la classification de E. Cartan.

Comme on le montre dans [1], chapitre IX, à toute surface distinguée de type $K3$, on peut associer un point $\tau(\tilde{X}) \in \Omega(l)$. Pour cela, considérons une forme différentielle régulière ω sur X et, pour $\gamma \in H_2(X, \mathbb{Z})$, posons

$$f(\gamma) = \int_\gamma \omega.$$

Il est clair que $f \in \operatorname{Hom}(H_2(X, \mathbb{Z}), \mathbb{C})$ et que φ transforme f en $g \in \operatorname{Hom}(L, \mathbb{C}) = \tilde{\Omega}$. Puisque la forme ω est déterminée de manière unique à un facteur constant près, le point correspondant de l'espace projectif, dont on vérifie facilement qu'il appartient à $\Omega(l)$, est donc parfaitement déterminé. Ce point est noté $\tau(\tilde{X})$. On l'appelle périodes de la surface X et on appelle τ l'application des périodes.

Le résultat fondamental (théorème de Torelli pour les surfaces de type $K3$) affirme que la surface distinguée $\tilde{X}$ de type $K3$ est déterminée de manière unique par ses périodes, i.e. par le point $\tau(\tilde{X}) \in \Omega(l)$.

Voici le schéma de la démonstration de ce théorème. Nous nous appuierons sur le « théorème de Torelli local » pour les surfaces de type $K3$ démontré par G. N. Turina dans [1], chapitre IX. On construit une famille analytique $\mathscr{X} \to S$ de surfaces de type $K3$ dont toutes les fibres sont des surfaces distinguées, toutes les surfaces distinguées figurant (à isomorphisme près) parmi les fibres; cette famille est effectivement paramétrée par une base S de dimension 19. La construction repose sur la construction du schéma de Hilbert des surfaces de type $K3$ plongées dans un espace projectif et sur un passage au quotient selon le groupe projectif. Du résultat principal de [1], chapitre IX, résulte que l'application des périodes $\tau : S \to \Omega(l)$ est un isomorphisme local holomorphe de la base de notre famille dans $\Omega(l)$.

Nous construisons ci-dessous un ensemble partout dense $Z \subset \Omega(l)$ au-dessus duquel la représentation τ est bijective. Notre théorème découlera alors du résultat simple suivant:

Soit $f : \mathscr{U} \to V$ une application localement isomorphe de variétés analytiques. Supposons qu'il existe un ensemble $Z \subset V$, partout dense dans V, tel que $f^{-1}(z)$ soit réduit à un point pour tout point $z \in Z$. Alors f est un plongement.

Il reste à décrire la construction de l'ensemble $Z \subset \Omega(l)$ pour lequel on démontre d'abord le théorème de Torelli. Elle repose sur l'étude de certaines classes spéciales de surfaces du type $K3$.

Considérons une variété abélienne A de dimension 2 et son automorphisme θ: $\theta x = -x$, $x \in A$. Désignons par g le groupe composé de 1 et θ. L'espace quotient A/g est un espace complexe normal. Il possède 16 points doubles correspondant aux points d'ordre 2 de A. Chacun de ces points peut être désingularisé par une transformation quadratique; la variété ainsi obtenue est une surface de type $K3$, appelée surface de Kummer.

Si la variété abélienne A est réductible, c'est-à-dire contient une courbe elliptique, alors la surface de Kummer correspondante est dite spéciale.

Il se trouve qu'il est possible d'exprimer qu'une surface de type $K3$ est une surface de Kummer spéciale en termes du réseau euclidien $H_2(X, Z)$ et de l'application des périodes τ.

De manière précise, la structure de surface algébrique sur X particularise dans le groupe d'homologie $H_2(X, \mathbb{Z})$ un sous-réseau de cycles algébriques que nous désignerons par S. Le théorème de Lefschetz caractérise le réseau S en termes de $H_2(X, \mathbb{Z})$ et de la représentation des périodes τ : si $\widetilde{X} = (X, \varphi, \xi)$ est une surface distinguée, $\pi = \tau(\widetilde{X})$ est une forme linéaire complexe sur L déterminée à une proportionnalité près, et $S = \operatorname{Ker} \varphi^*(\pi)$. Ainsi, le réseau S est défini par les périodes de la surface distinguée $\widetilde{X}$.

Si A est une variété abélienne réductible et C une courbe elliptique contenue dans A, alors l'homomorphisme $A \to A/C$ définit une fibration en courbes elliptiques. Cette fibration définit un faisceau de courbes elliptiques sur la surface de Kummer spéciale X correspondante. Les classes des fibres d'un tel faisceau peuvent être décrites par leurs propriétés dans le réseau S. Cela donne un critère pour que X soit une surface de Kummer spéciale.

Le théorème de Torelli se démontre directement pour les surfaces de Kummer spéciales. Parmi les périodes de telles surfaces de Kummer figure l'ensemble partout dense dont nous avons besoin.

Indiquons quelques applications du théorème de Torelli. D'abord, il permet de décrire la « variété grossière des modules » des surfaces de type $K3$. Nous appellerons classe d'une telle surface le minimum des nombres $\frac{1}{2}\mathscr{D}^2$, où $\mathscr{D}$ est un diviseur effectif sur la surface et $\mathscr{D}^2 > 0$. Alors, la variété des modules M_k des surfaces de classe k est une variété algébrique $F - F_0$. Ici F est la compactification standard de l'espace $\Omega(l)/\Gamma$, quotient du domaine symétrique $\Omega(l)$ par son groupe discret d'automorphismes Γ, induit par les automorphismes du réseau L qui conservent un vecteur l, le vecteur l étant arbitraire de longueur $2k$. La sous-variété algébrique $F_0 \subset F$ se compose des images de la frontière de la compactification et du sous-ensemble défini par la condition $\omega . a = 0$, $a \in L$, $a . l = 0$, $a^2 = -2$.

Si $k = 2$, nous avons affaire aux surfaces de degré 4 dans $\mathbb{P}_3$. Dans ce cas, la variété M_2 est affine. Il est tout à fait vraisemblable qu'il en est toujours ainsi.

La variété M_k possède un modèle défini sur le corps $\mathbb{Q}$ et tel que, pour tout point $m \in M_k$, le corps $\mathbb{Q}(m)$ coïncide avec le « corps des modules » de la surface correspondante X au sens de Shimura [2]. En particulier, si X ne possède pas d'automorphisme $\neq 1$, alors $\mathbb{Q}(m)$ coïncide avec le corps de définition de cette surface.

Les autres applications sont liées à la structure du groupe des automorphismes de la surface de type $K3$. Soit S le groupe des classes de diviseurs d'une telle surface; on peut le considérer comme un réseau euclidien. Chaque vecteur $a \in S$ avec $a^2 = -2$ définit un automorphisme du réseau S :

$$x \mapsto x + (x . a) . a,$$

réflexion dans l'hyperplan orthogonal à a. Désignons par H le sous-groupe qu'ils engendrent dans le groupe de tous les automorphismes du réseau S ; il est clair que c'est un sous-groupe distingué. Il résulte facilement du théorème de Torelli que le groupe $\operatorname{Aut} S/H$, « à des groupes finis près », est isomorphe au groupe des automorphismes de la surface. Ici deux groupes G et G' sont dits isomorphes à des groupes finis près s'il existe des sous-groupes $G_1 \subset G$ et $G_1' \subset G'$ d'indices finis et des sous-groupes distingués finis $G_0 \subset G$, $G_0' \subset G_1'$ tels que $G_1/G_0 \simeq G_1'/G_0'$.

Par exemple, si le réseau S est de rang 2, il est déterminé par une forme quadratique indéfinie à deux variables $F(x, y)$. Le groupe des automorphismes de la surface X est infini si et seulement si la forme F ne représente ni 0 ni -2. Pour toute forme quadratique paire à deux variables indéfinie F, il existe une surface correspondante. Dans le travail [3], Severi a étudié le cas des surfaces du quatrième degré qui contiennent une courbe de degré 6 et de genre 2. Pour ces surfaces, la forme F est du type

$$4x^2 + 12xy + 2y^2,$$

et, en accord avec nos résultats, le groupe des automorphismes est infini. Comme dernière application, considérons les surfaces pour lesquelles le rang du groupe S est de valeur maximum possible 20. Nous les appellerons singulières. Le complémentaire orthogonal de S dans $H_2(X, \mathbb{Z})$ est le réseau défini positif des « cycles transcendants ». Il est facile de déduire du théorème de Torelli qu'une surface singulière est entièrement définie par le réseau T. Le réseau T est pair, c'est-à-dire que $t^2 \equiv 0$ (mod. 2) pour tout $t \in T$, et tout réseau pair défini positif correspond à une certaine surface singulière. La surface singulière est de Kummer si et seulement si $t^2 \equiv 0$ (mod. 4) pour tout $t \in T$.

Passons à certains problèmes soulevés par le théorème de Torelli. Si l'on compare cette situation à celle des variétés abéliennes de dimension 2, il est clair que, dans la théorie des surfaces de type $K3$, il manque un analogue à la notion d'isogénie. Il est facile de le définir dans le langage des périodes. Sur le domaine symétrique $\Omega(l)$ agit un groupe discret Γ dont les transformations correspondent aux différents isomorphismes $H_2(X, \mathbb{Z}) \to L$ qui transforment ξ en l. Des points équivalents correspondent à une même surface. Le groupe Γ est composé des points entiers d'un certain groupe algébrique G, $\Gamma = G(\mathbb{Z})$. Il est naturel d'appeler isogènes des surfaces auxquelles correspondent des points dans $\Omega(l)$ qui se déduisent l'un de l'autre par des transformations du groupe $G(\mathbb{Q})$. Donc le problème d'un équivalent algébrique de cette notion se pose.

Plus précisément, soit $g \in G(\mathbb{Q})$, x et $y \in \Omega(l)$, $y = gx$, et X et Y des surfaces distinguées telles que $\tau(x) = X$, $\tau(y) = Y$. La transformation g détermine un homomorphisme $H_2(X, \mathbb{Z}) \to H_2(Y, \mathbb{Z})$. Cet homomorphisme est-il donné par une certaine correspondance algébrique entre X et Y ? Telle est la formulation précise de notre problème. Une réponse négative à cette question réfuterait la conjecture de Hodge. Une réponse positive démontrerait la méromorphie et l'équation fonctionnelle des fonctions ζ des surfaces singulières de type $K3$ (et de beaucoup d'autres classes intéressantes). La recherche des surfaces de type $K3$ sur un corps fini est d'un grand intérêt. Quelle peut être la valeur minimale du rang du groupe S des classes de diviseurs sur de telles surfaces ? Si l'on admet la conjecture de Tate, il est facile de montrer qu'elle est $\geqslant 2$. Nous ne savons pas si cette valeur peut être atteinte. Quelles sont les surfaces qui correspondent à la valeur maximale 22 de ce rang ? Sont-elles toutes des surfaces de Kummer ?

En conclusion mentionnons le problème extrêmement intéressant de la généralisation de ces considérations aux variétés algébriques de dimension quelconque et de classe canonique nulle.

BIBLIOGRAPHIE

[1] « Алгебраические поверхности ». Труды Математического Института им. В. А. Стеклова, т. 75. Москва 1965.

[2] G. SHIMURA. — « Number fields and zeta functions associated with discontinuous groups and algebraic varieties ». Труды Международного Конгресса Математиков. Москва 1966, стр. 290-299.

[3] F. SEVERI. « Complementi alla teoria della base per la totalita delle curve di una superficie algebrica ». Rendiconti del circolo matematico di Palermo. T. 30, 1910, 265-288.

Steklov Mathematical Institute
Academy of Sciences of USSR
ul Vavilova 42,
Moscow V 333
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 419 à 423.

B_5 - GÉOMÉTRIE ALGÉBRIQUE

CONSTRUCTION TECHNIQUES FOR ALGEBRAIC SPACES

by M. ARTIN

This report may be viewed as a continuation of the discussion of the etale topology of [1], beginning with a partial answer to a question raised there. The idea here is, basically, to combine a theorem on the existence of algebraic functions, and known methods, with the notion of algebraic space [9, 12].

§ 1. Approximation of formal solutions of polynomial equations by algebraic ones.

Let R be a field or a discrete valuation ring such that the field of fractions $\hat{K}$ of $\hat{R}$ is separable over $K = \text{fract}(R)$, and let p denote the maximal ideal of R. We consider a finite set $f = f_1, \ldots, f_r \in R[x, y]$ of polynomials in the variables $x = x_1, \ldots, x_m$; $y = y_1, \ldots, y_n$.

THEOREM (1.1). — Let c be an integer. Given elements $\bar{y} = \bar{y}_1, \ldots, \bar{y}_n \in \hat{R}[[x]]$ with $f(x, \bar{y}) = 0$, there are elements $y \in \hat{R}[[x]]$ with $y \equiv \bar{y}$ (modulo $(p, x)^c$) which are *algebraic* over $R[x]$, such that $f(x, y) = 0$.

This result was proved by Greenberg [7] in case $m = 0$ (no x), and in general in [3]. There are examples showing that some hypothesis on R is necessary [7].

A variant of this theorem would be the following:

CONJECTURE (1.2). — Let c be an integer. There is an integer $N = N(c)$ such that if $f(x, \bar{y}) \equiv 0$ (mod $(p, x)^N$), there are elements $y \equiv \bar{y}$ (mod $(p, x)^c$) with $f(x, y) = 0$.

Of course, y could be taken algebraic over $R[x]$, by Theorem (1.1). This conjecture has been proved when $m = 0$ [7] or if R is a field [3]. In the latter case, it can moreover be shown that N depends only on the degrees of the f_i and on the number of variables (and not on R). It would be very interesting to have estimates on $N(c)$ for a given system of equations $f = 0$. When $m = 0$, P. Cohen (unpublished) has shown that N is a linear function of c.

One consequence of (1.2) is that a system of equations having an approximate solution (mod $(p, x)^c$) for every c has an actual solution. Interestingly enough, this is easy to prove if the residue field is finite or algebraically closed and uncountable, but does not seem trivial in general.

Here is a more general version of (1.1).

Conjecture (1.3). — Let A be an excellent [6] henselian local ring, let

$$f = f_1, \dots, f_n \in A[Y_1, \dots, Y_n],$$

and let $\bar{y} \in \hat{A}$ be elements such that $f(\bar{y}) = 0$. For every c, there exist $y \in A$ with $y \equiv \bar{y} \pmod{\mathfrak{m}^c}$ and $f(y) = 0$.

From (1.1), one can show.

Corollary (1.4). — This conjecture is true if A is the henselization of an R-algebra of finite type.

An important further case of this conjecture would be that A is the henselization of a polynomial ring over a complete local ring, say of $R[[x]][x']$, where $x = x_1, \dots, x_m$; $x' = x'_1, \dots, x'_m$. If R is a field, then the case that $m = 1$ follows from (1.1). I do not see how to handle $m = 2$.

§ 2. Existence of deformations.

Using theorem (1.1), one can prove the existence of universal deformations of certain structures. Since our results are all local for the etale topology, we may as well work with henselian rings: Let R be a discrete valuation ring as in section 1 or an algebra of finite type over such a ring, with a chosen residue field k. Denote by C the category of henselian R-algebras with residue field k. We consider functors

$$F : C \to (\text{sets}) \tag{2.1}$$

such that $F(k)$ consists of one element. Let $\bar{A} \in C$ be a complete local ring. A *formal element* ξ of $F(\bar{A})$ is a compatible sequence of elements $\xi_n \in F(\bar{A}/\mathfrak{m}^{n+1})$ for every n. Such an element is called *formally versal* (resp. universal) if given a ring $B' \in C$ of finite length, every diagram of solid arrows

(2.2)
$$\begin{tikzcd} & B \arrow[d] \\ \bar{A} \arrow[ur, dotted] \arrow[r] & B' \end{tikzcd} \qquad \text{sending} \qquad \begin{tikzcd} & \eta \arrow[d, mapsto] \\ \xi \arrow[ur, dotted, mapsto] \arrow[r, mapsto] & \eta' \end{tikzcd},$$

where B' is a quotient of R and $\xi = \hat{\xi}$, can be completed with a dotted arrow (resp. with a unique dotted arrow). Schlessinger [16] gives the following criterion for the existence of a formal versal element: Let $A' \to A$ be a surjective map in C whose kernel is of dimension 1 over k, and let $B \to A$ be another map.

Theorem (2.3) (Schlessinger). — F admits a formal versal deformation if

(1) The map

$$F(A' \times_A B) \to F(A') \times_{F(A)} F(B)$$

is surjective whenever A, A', B are finite dimensional over k, and is bijective when moreover $A = k$, $A' = k[t]/(t^2)$.

(2) $F(k[t]/(t^2))$ is a finite dimensional k-vector space.

If $\xi \in F(A)$, where A is essentially of finite type over R, i. e., is the henselization of an R-algebra of finite type, then we call ξ an *algebraic* element. An algebraic element is *(uni)versal* if every diagram (2.2) can be completed, where now $B \in C$ is arbitrary.

In addition, we will call ξ *weakly* versal if the associated formal element is formally versal, and if the map Hom $(A, B) \xrightarrow{\xi} F(B)$ is surjective for every B, i. e., if (2.2) holds when $B' = k$.

THEOREM (2.4). — Suppose F admits a formal versal element $\hat{\xi} \in F(\overline{A})$, and that F commutes with filtering direct limits in C.

(*i*) If $\hat{\xi}$ is represented by an actual element $\overline{\xi} \in F(\hat{A})$, then it is represented by an algebraic element $\xi \in F(A)$ for some A essentially of finite type.

(*ii*) If F satisfies (*i*) and condition (2.5) for every complete local ring $B \in C$, then ξ is weakly versal.

(*iii*) If in addition F satisfies condition (2.3) (1) when A, A', B are essentially of finite type, and condition (2.5) below for every B, then ξ is versal.

CONDITION (2.5). — Let $\xi, \eta \in F(B)$. If ξ, η induce the same element in $F(B/\mathfrak{m}^n)$ for every n, then $\xi = \eta$.

I do not know an example of a weakly versal element which is not versal. They are certainly pathological if they exist. In any case, if in (*ii*) the element $\hat{\xi}$ is formally universal of if k is a finite field, then ξ is (uni)versal.

The formal nature of the hypotheses of (*i*) is not clear to me. In the complex analytic analogue, the substitution of a complete local ring $\overline{A}$ into F would not seem to make much sense. This suggests that the conditions on direct and inverse limits might be combined into a single one. But, techniques don't seem available to handle such a condition.

Theorem (2.4) has been applied successfully to various functors [4] [13]. One important case which is not yet settled is that of deformations of isolated singularities. The existence of algebraic deformations was proved by Deligne (unpublished) for complete intersections, and the analogous analytic problem has been settled by Kas-Schlessinger (unpublished), and Tiurina [17].

§ 3. Application to global constructions.

The natural global context for the results of section 2 is that of *algebraic space* [9], or, more generally, of algebraic stack [5]. An algebraic space X may be defined as a quotient $X = U/R$ of a sum of affine schemes U by an equivalence relation $R \subset U \times U$ which is etale over U. (For a precise definition, see Knutson [9], Moisezon [12]). Algebraic spaces are more general objects than schemes, but behave in a similar way.

Here is the basic existence theorem. Let S be a scheme of finite type over R (cf. § 1), and let

$$F : (\text{schemes}/S)^0 \to (\text{sets})$$

be a functor. When $X = \operatorname{Spec} A$ is affine, we write $F(A) = F(X)$.

THEOREM (3.1). — F is represented by an algebraic space locally of finite type over S if and only if

(0) F is a sheaf for the etale topology.

(1) F is locally of finite presentation, i. e., $F(\varinjlim A_i) = \varinjlim F(A_i)$ for every filtering system of $\mathcal{O}_S$-algebras.

(2) Let X be of finite type over S and $\xi, \eta \in F(X)$. The condition $\xi = \eta$ is represented by a closed subscheme of X.

(3) F is effectively pro-representable ([8], [4]).

(4) If $\xi \in F(U)$, where U is of finite type over S, and if the corresponding map $U \to F$ is formally etale at a point $u \in U$ of finite type, then it is formally etale at every point of finite type in a neighborhood of u.

These conditions follow the general pattern introduced by Grothendieck [13, 14]. Condition (4) is rather technical and is explained at length in [4]. The pro-representability (3) can be replaced by

(3.2) Let $\xi_0 \in F(k_0)$, where k_0 is an $\mathcal{O}_S$-field of finite type. There is a complete local ring $\bar{A}$ and an element $\bar{\xi} \in F(\bar{A})$ such that the map Spec $\bar{A} \to F$ is formally etale at the closed point of Spec $\bar{A}$, and that ξ_0 lifts to a map Spec $k'_0 \to$ Spec $\bar{A}$ for some separable extension k'_0 of k_0.

If the residue fields of finite type of S are perfect, this condition can be expressed in terms of Schlessinger's criterion (2.3). Otherwise one has to take into account inseparable field extensions (Levelt [10], [4]).

The above theorem can be used to prove representability of Hilbert and Picard functors [4], [13] and the existence of modifications of algebraic spaces [4]. An analogous result can be proved for *algebraic stacks* (cf. Deligne and Mumford [5]), viz.

THEOREM (3.2). — Let F be a category fibred in groupoids over (schemes/S). Then F is an algebraic stack locally of finite type over S if and only if

(0) F is a stack for the etale topology.

(1) F is locally of finite presentation.

(2) Let ξ, η be 1-morphisms from X to F. Then Isom (x, ξ, η) is an algebraic space locally of finite type over S.

(3) Condition (3.2) holds for 1-morphisms ξ_0: Spec $k_0 \to F$.

(4) Condition (3.1) (4) holds for 1-morphisms $U \to F$.

BIBLIOGRAPHY

[1] M. ARTIN. — The etale topology of schemes, *Proceedings of the International Congress*, Moscow (1966), pp. 44-56.

[2] —. — *The implicit function theorem in algebraic geometry*, *Algebraic Geometry*, Papers presented at the Bombay Colloquium, Oxford, Bombay (1969), pp. 13-34.

[3] —. — Algebraic approximation of structures over complete local rings, *Pub. Math. I. H. E. S.*, No. 36 (1969), pp. 23-58.

[4] —. — Algebraization of formal moduli, in *A Collection of Mathematical Papers in Honor of K. Kodaira*, University of Tokyo Press, 1969, and *Ann. of Math.*, 99 (1970), pp. 88-135.

[5] P. DELIGNE and D. MUMFORD. — The irreducibility of the space of curves of a given genus, *Pub. Math. I. H. E. S.*, No. 36 (1969), pp. 75-109.

[6] J. Dieudonné and A. Grothendieck. — Éléments de géométrie algébrique, *Pub. Math. I.H.E.S.* (1960-1968).
[7] M. Greenberg. — Rational points in henselian discrete valuation rings, *Pub. Math. I. H. E. S.*, No. 23 (1964).
[8] A. Grothendieck. — Fondements de géométrie algébrique, extrait du Séminaire Bourbaki (1957-1962) (mimeographed notes).
[9] D. Knutson. — Algebraic spaces, *Springer Lecture Notes* (to appear).
[10] A. H. M. Levelt. — Foncteurs exacts à gauche, *Inventiones Math.*, 8 (1969), pp. 114-140.
[11] Б. Г. Мойшезон. — Теоремы разрешения для компактных комплексных пространств с достаточно большим полем мероморфных функций, Изв. АН СССР, сер. мат., 31 (1967), pp. 1385-1414.
[12] —. — Теорема Кастельнуово-Энриквеса о стягивании для произвольной размерности, Изв. АН СССР, сер. мат., 33 (1969), pp. 974-1025.
[13] J. P. Murre. — On contravariant functors from the category of preschemes over a field into the category of abelian groups, *Pub. Math. I. H. E. S.*, No. 23 (1964).
[14] —. — Representation of unramified functors, Applications, Séminaire Bourbaki, 17 (1964-1965), No. 294 (mimeographed notes).
[15] F. Oort. — Hensel's lemma and rational points over local rings, *Symp. Math. Inst. Naz. di Alta Mat.*, 3 (1970), pp. 217-232.
[16] M. Schlessinger. — Functors of Artin rings, *Trans. Amer. Soc.*, 130 (1968), pp. 205-222.
[17] Г. Н. Тюрина. — Локально полууниверсальные плоские деформации изолированных особенностей комплексных пространств, Нзв. Акад. СССР, сер. мат., 33 (1969), pp. 1026-1058.

M. I. T.
Department of Mathematics,
Cambridge, Mass. 02139
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 425 à 430.

THÉORIE DE HODGE I

par PIERRE DELIGNE

On se propose de donner un dictionnaire heuristique entre énoncés en cohomologie l-adique et énoncés en théorie de Hodge. Ce dictionnaire a notamment pour sources [3] et la théorie conjecturale des motifs de Grothendieck [2]. Jusqu'ici, il a surtout servi à formuler, en théorie de Hodge, des conjectures, et il en a parfois suggéré une démonstration.

DÉFINITION 1.1. — *Une* structure de Hodge mixte H *consiste en*

(*a*) *Un $\mathbb{Z}$-module de type fini $H_{\mathbb{Z}}$ (le* « réseau entier »);

(*b*) *Une filtration croissance finie W sur $H_{\mathbb{Q}} = H_{\mathbb{Z}} \otimes \mathbb{Q}$ (la* « filtration par le poids »);

(*c*) *Une filtration décroissante finie F sur $H_{\mathbb{C}} = H_{\mathbb{Z}} \otimes \mathbb{C}$ (la* « filtration de Hodge »).

Ces données sont soumises à l'axiome:

Il existe sur $\mathrm{Gr}_W(H_{\mathbb{C}})$ une (unique) bigraduation par des sous-espaces $H^{p,q}$ telle que

(*i*) $\mathrm{Gr}_W^n(H_{\mathbb{C}}) = \bigoplus_{p+q=n} H^{p,q}$

(*ii*) *la filtration F induit sur $\mathrm{Gr}_W(H_{\mathbb{C}})$ la filtration*

$$\mathrm{Gr}_W(F)^p = \bigoplus_{p' \geq p} H^{p',q'}$$

(*iii*) $\overline{H^{pq}} = H^{qp}$.

Un *morphisme* $f : H \to H'$ est un homomorphisme $f_{\mathbb{Z}} : H_{\mathbb{Z}} \to H'_{\mathbb{Z}}$ tel que $f_{\mathbb{Q}} : H_{\mathbb{Q}} \to H'_{\mathbb{Q}}$ et $f_{\mathbb{C}} : H_{\mathbb{C}} \to H'_{\mathbb{C}}$ soient respectivement compatibles aux filtrations W et F.

Les *nombres de Hodge* de H sont les entiers

$$h^{pq} = \dim H^{pq} = h^{qp}. \tag{1.2}$$

On dit que H est pure de *poids n* si $h^{pq} = 0$ pour $p + q \neq n$ (i. e. si $\mathrm{Gr}_W^i(H) = 0$ pour $i \neq n$). On dit encore que H est une *structure de Hodge de poids n*.

La *structure de Hodge de Tate* $\mathbb{Z}(1)$ est la structure de Hodge de poids -2, purement de type $(-1, -1)$, pour laquelle $\mathbb{Z}(1)_{\mathbb{C}} = \mathbb{C}$ et $\mathbb{Z}(1)_{\mathbb{Z}} = 2\pi i\mathbb{Z} = \mathrm{Ker}(\exp : \mathbb{C} \to \mathbb{C}^*) \subset \mathbb{C}$. On pose $\mathbb{Z}(n) = \mathbb{Z}(1)^{\otimes n}$.

On peut montrer que les structures de Hodge mixtes forment une catégorie abélienne. Si $f : H \to H'$ est un morphisme, alors $f_{\mathbb{Q}}$ et $f_{\mathbb{C}}$ sont strictement compatibles aux filtrations W et F ([1], 2.3.5).

2. Soient A un anneau normal intègre de type fini sur $\mathbb{Z}$, K son corps des fractions

et $\overline{K}$ une clôture algébrique de K. Soit K_{nr} la plus grande sous-extension de $\overline{K}$ non ramifiée en chaque idéal premier de A. On sait que, ou on pose

$$\pi_1(\mathrm{Spec}(A), \overline{K}) = \mathrm{Gal}(K_{nr}/K).$$

Pour chaque point fermé x de $\mathrm{Spec}(A)$, défini par un idéal maximal m_x de A, le corps résiduel $k_x = A/m_x$ est fini; le point x définit une classe de conjugaison de « substitutions de Frobenius » $\varphi_x \in \pi_1(\mathrm{Spec}(A), \overline{K})$. On pose $q_x = \# k_x$ et $F_x = \varphi_x^{-1}$.

Soient K un corps de type fini sur le corps premier de caractéristique p, $\overline{K}$ une clôture algébrique de K, l un nombre premier $\neq p$ et H un $\mathbb{Z}_l$- (ou un $\mathbb{Q}_l$-) module de type fini muni d'une action continue ρ de $\mathrm{Gal}(\overline{K}/K)$. On supposera toujours par la suite qu'il existe A comme plus haut, avec l inversible dans A, tel que ρ se factorise par $\pi_1(\mathrm{Spec}(A), \overline{K}) = \mathrm{Gal}(K_{nr}/K)$. On dira que H est *pur de poids n* si pour tout point fermé x d'un ouvert non vide de $\mathrm{Spec}(A)$, les valeurs propres α de F_x agissant sur H sont des entiers algébriques dont tous les conjugués complexes sont de valeur absolue $|\alpha| = q_x^{n/2}$.

PRINCIPE 2.1. — *Si le module galoisien H « provient de la géométrie algébrique », il existe sur $H_{\mathbb{Q}_l} = H \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ une (unique) filtration croissante W (la* « filtration par le poids »*), invariante par Galois, telle que $\mathrm{Gr}_n^W(H)$ soit pur de poids n.*

On peut penser que $\mathrm{Gr}_n^W(H)$ est de plus semi-simple.

Lorsqu'on dispose de la résolution des singularités, on peut souvent donner de W une définition conjecturale, dont la correction résulte des conjectures de Weil [5] (cf. 6).

Soit μ le sous-groupe de $\overline{K}^*$ formé des racines de l'unité. Le *module de Tate* $\mathbb{Z}_l(1)$, défini par

$$\mathbb{Z}_l(1) = \mathrm{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, \mu)$$

est pur de poids -2. On pose $\mathbb{Z}_l(n) = \mathbb{Z}_l(1)^{\otimes n}$.

Il est trivial que tout morphisme $f: H \to H'$ est strictement compatible à la filtration par le poids.

Le principe 2.1 concorde avec le fait que toute extension de $\mathbb{G}_m$ (« poids -2 ») par une variété abélienne (« poids $-1 > -2$ ») est triviale.

3. TRADUCTION. — *Les modules galoisiens qui apparaissent en cohomologie l-adique ont pour analogue, sur $\mathbb{C}$, les structures de Hodge mixte. On a de plus le dictionnaire*

module pur de poids n	structure de Hodge de poids n
filtration par le poids	filtration par le poids
homomorphisme compatible à Galois	morphisme
module de Tate $\mathbb{Z}_l(1)$	structure de Hodge de Tate $\mathbb{Z}(1)$

4. Soit X une variété algébrique complexe (= schéma de type fini sur $\mathbb{C}$, qu'on supposera séparé). Il existe un sous-corps K de $\mathbb{C}$, de type fini sur $\mathbb{Q}$ tel que X puisse être défini sur K (i. e. provienne par extension des scalaires de K à $\mathbb{C}$ d'un K-schéma X'). Soit $\overline{K}$ la fermeture algébrique de K dans $\mathbb{C}$. Le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ agit alors sur les groupes de cohomologie l-adique $H^*(X, \mathbb{Z}_l)$; on a

$$H^*(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_l = H^*(X, \mathbb{Z}_l) = H^*(X'_{\overline{K}}, \mathbb{Z}_l).$$

D'après 3, il y a lieu de s'attendre à ce que les groupes de cohomologie $H^n(X(\mathbb{C}), \mathbb{Z})$ portent des structures de Hodge mixtes naturelles. C'est ce qu'on peut prouver (voir [1], 3.2.5, pour le cas où X est lisse ; la démonstration est algébrique, à partir de la théorie de Hodge classique [6]). Pour X projectif et lisse, les conjectures de Weil impliquent que $H^n(X, \mathbb{Z}_l)$ est pur de poids n, tandis que la théorie de Hodge classique munit $H^n(X, \mathbb{Z})$ d'une structure de Hodge de poids n. Pour tout morphisme $f : X \to Y$ et pour K assez grand, $f^* : H^*(Y, \mathbb{Z}_l) \to H^*(X, \mathbb{Z}_l)$ commute à Galois (par transport de structure); de même, $f^* : H^*(Y, \mathbb{Z}) \to H^*(X, \mathbb{Z})$ est un morphisme de structures de Hodge mixte. Pour X lisse, la classe de cohomologie dans $H^{2n}(X, \mathbb{Z}_l(n))$ d'un cycle algébrique de codimension n, Z, défini sur K, est invariante par Galois, i. e. définit

$$c(Z) \in \mathrm{Hom}_{\mathrm{Gal}}(\mathbb{Z}_l(-n), H^{2n}(X, \mathbb{Z}_l)).$$

De même, la classe de cohomologie $c(Z) \in H^{2n}(X(\mathbb{C}), \mathbb{Z})$ est purement de type (n, n), i. e. correspond à

$$c(Z) \in \mathrm{Hom}_{H.M.}(\mathbb{Z}(-n), H^{2n}(X(\mathbb{C}), \mathbb{Z})).$$

5. Si $f : H \to H'$ est un morphisme, compatible à Galois, entre $\mathbb{Q}_l$-vectoriels de poids différents, on a $f = 0$. De même, si $f : H \to H'$ est un morphisme de structures de Hodge mixte pures de poids différents, alors f est de torsion. Une remarque plus utile est la

SCHOLIE 5.1. — *Soient H et H' des structures de Hodge de poids n et n', avec $n > n'$. Soit $f : H_{\mathbb{Q}} \to H'_{\mathbb{Q}}$ un homomorphisme tel que $f : H_{\mathbb{C}} \to H'_{\mathbb{C}}$ respecte F. Alors $f = 0$.*

6. Soient X une variété projective et lisse sur $\mathbb{C}$, $D = \sum_1^n D_i$ un diviseur à croisements normaux dans X, somme de diviseurs lisses, et j l'inclusion dans X de $U = X - D$. Pour $Q \subset [1, n]$, on pose $D_Q = \bigcap_{i \in Q} D_i$.

En cohomologie l-adique, on a canoniquement

(6.1) $$R^q j_* \mathbb{Z}_l = \bigoplus_{\# Q = q} \mathbb{Z}_l(-q)_{D_Q},$$

et la suite spectrale de Leray pour j s'écrit

(6.2) $$E_2^{pq} = \bigoplus_{\# Q = q} H^p(D_Q, \mathbb{Q}_l) \otimes \mathbb{Z}_l(-q) \Rightarrow H^{p+q}(U, \mathbb{Q}_l).$$

D'après les conjectures de Weil [5], $H^p(D_Q, \mathbb{Q}_l)$ est pur de poids p, de sorte que E_2^{pq} est pur de poids $p + 2q$. En tant que quotient d'un sous-objet de E_2^{pq}, E_r^{pq} aussi est pur de poids $p + 2q$. D'après 5, $d_r = 0$ pour $r \geq 3$, car les poids $p + 2q$ et $p + 2q - r + 2$ de E_r^{pq} et $E_r^{p+r, q-r+1}$ sont différents. On a donc $E_3^{pq} = E_\infty^{pq}$. A une renumérotation près, la filtration par le poids de $H^*(U, \mathbb{Q}_l)$ est l'aboutissement de (6.2)

(6.3) $$\mathrm{Gr}_n^W(H^k(U, \mathbb{Q}_l)) = E_3^{2k-n, n-k}$$

7. En cohomologie entière, pour la topologie usuelle, la suite spectrale de Leray pour j s'écrit

(7.1) $$'E_2^{pq} = \bigoplus_{\# Q = q} H^p(D_Q, \mathbb{Z}) \Rightarrow H^{p+q}(U, \mathbb{Z}).$$

Puisque chaque D_Q est une variété projective non singulière, $'E_2^{pq}$ est muni d'une structure de Hodge de poids p. On pose $E_2^{pq} = 'E_2^{pq} \otimes \mathbb{Z}(-q)$ (structure de Hodge de poids $p + 2q$). Comme groupe abélien, $E_2^{pq} = 'E_2^{pq}$; il y a intérêt à considérer (7.1) comme une suite spectrale de terme initial E_2^{pq}. D'après 3, il faut s'attendre à ce que $d_2 : E_2^{pq} \to E_2^{p+2,q-1}$ soit un morphisme de structure de Hodge. On le prouve en interprétant d_2 comme un morphisme de Gysin. Dès lors, E_3^{pq} est muni d'une structure de Hodge de poids $p + 2q$. D'après 3, on s'attend à ce que, *modulo torsion*, la suite spectrale (6.4) dégénère au terme E_3 ($E_3 = E_\infty$), et à ce que la nullité des d_r ($r \geq 3$) soit une application de 5.1. Ce programme est mené à bien dans [1] 3.2. On y *définit* la filtration par le poids de $H^*(U, \mathbb{Q})$ comme aboutissement de (7.1), à la renumérotation (6.3) près.

En fait, pour munir des groupes de cohomologie H^* d'une structure de Hodge mixte, le point clef a toujours été jusqu'ici de trouver une suite spectrale E d'aboutissement H^* telle que l'analogue l-adique de E_2^{pq} soit conjecturalement pur (de poids $p + 2q$); E_2^{pq} doit alors porter une structure de Hodge naturelle (de poids $p + 2q$), et la filtration W est l'aboutissement de E.

8. Soit $\operatorname{Spec}(V)$ le spectre d'un anneau de valuation discrète hensélien (un *trait hensélien*) de corps de fractions K et de corps résiduel k de type fini sur le corps premier de caractéristique p. Soient $\overline{K}$ une clôture algébrique de K et H un vectoriel de dimension finie sur $\mathbb{Q}_l$ ($l \neq p$), sur lequel $\operatorname{Gal}(\overline{K}/K)$ agit continûment. D'après Grothendieck, on sait ([4], appendice) qu'un sous-groupe d'indice fini du groupe d'inertie I agit de façon unipotente. Remplaçant V par une extension finie, on se ramène au cas où l'action de I tout entier est unipotente (cas *semi-stable*); elle se factorise alors le plus grand pro-l-groupe I_l quotient de I, canoniquement isomorphe à $\mathbb{Z}_l(1)$.

Principe 8.1. — *Dans le cas semi-stable, si le module galoisien H « provient de la géométrie algébrique », il existe une (unique) filtration croissante W de H (la* « filtration par le poids ») *telle que I agisse trivialement sur* $\operatorname{Gr}_n^W(H)$ *et que* $\operatorname{Gr}_n^W(H)$, *en tant que module galoisien sous* $\operatorname{Gal}(\bar{k}/k) \simeq \operatorname{Gal}(\overline{K}/K)/I$, *soit pur de poids n.*

On comparera à 2.1 et à l'appendice de [4].

Lorsqu'on dispose de la résolution des singularités, on peut parfois donner de W une définition conjecturale, dont la validité résulte des conjectures de Weil. A l'aide de la résolution et de Weil, il est souvent facile de montrer qu'en tout cas H se dévisse en modules galoisiens (sous $\operatorname{Gal}(\bar{k}/k)$) purs.

Supposons H semi-stable. Pour $T \in I_l$, on définit $\log T$ comme la somme *finie* $-\sum_{n>0} (Id - T)^n/n$. L'application $(T, x) \to \log T(x)$ s'identifie à un homomorphisme

$$M: \quad \mathbb{Z}_l(1) \otimes H \to H. \tag{8.2}$$

Puisque $\mathbb{Z}_l(1)$ est de poids -2, on a nécessairement (cf. 5)

$$M(\mathbb{Z}_l(1) \otimes W_n(H)) \subset W_{n-2}(H) \tag{8.3}$$

et M induit

$$\operatorname{Gr}(M): \quad \mathbb{Z}_l(1) \otimes \operatorname{Gr}_n^W(H) \to \operatorname{Gr}_{n-2}^W(H). \tag{8.4}$$

8.5. Si X est une variété projective non singulière sur un corps algébriquement clos k_0, on définit

$$L:\quad \mathbb{Z}_l(-1)\otimes H^*(X,\mathbb{Z}_l)\to H^*(X,\mathbb{Z}_l)$$

comme étant le cup-produit avec la classe de cohomologie d'une section hyperplane. On notera une analogie formelle entre L et M ; de même que M est défini par une action de $\mathbb{Z}_l(1)$, on peut regarder L comme défini par une action de $\mathbb{Z}_l(-1)$; L augmente le degré de 2, et $\operatorname{Gr} M$ (8.4) le diminue de 2.

9. Soient D le disque unité, $D^* = D - \{0\}$ et X

$$\begin{tikzcd} X \arrow[rr, hook] \arrow[dr, "f"'] & & \mathbb{P}^r(\mathbb{C})\times D \arrow[dl, "\mathrm{pr}_2"] \\ & D & \end{tikzcd}$$

une famille de variétés projectives paramétrée par D, avec f propre et $f \mid D^*$ lisse. Gardons les notations de 8, et rappelons que dans l'analogie entre trait hensélien et petit voisinage de 0 dans la droite complexe on a le dictionnaire suivant (noter que le spectre de l'anneau des germes de fonctions holomorphes en 0 est un trait hensélien):

9.1.

D	$\operatorname{Spec}(V)$
D^*	$\operatorname{Spec}(K)$
un revêtement universel $\tilde{D}^*$ de D^*	$\operatorname{Spec}(\bar{K})$
groupe fondamental $\pi_1(D^*)$	groupe d'inertie I
(avec $\pi_1(D^*) = \mathbb{Z} \simeq \mathbb{Z}(1)_{\mathbb{Z}}$)	(avec $I_l = \mathbb{Z}_l(1)$)
X	schéma projectif X sur $\operatorname{Spec}(V)$
$X^* = f^{-1}(D^*)$	X_K
$\tilde{X} = X\times_D \tilde{D}^*$	$X_{\bar{K}}$
système local $R^if_*\mathbb{Z} \mid D^*$	module galoisien $H^i(X_{\bar{K}},\mathbb{Z}_l)$
$H^i(\tilde{X},\mathbb{Z})$	$H^i(X_{\bar{K}},\mathbb{Z}_l)$

On notera que $\tilde{X}$ est homotopiquement équivalent à chacune des fibres $X_t = f^{-1}(t)$ $(t\in D^*)$: $H^i(X_{\bar{K}},\mathbb{Z}_l)$ a encore pour analogue $H^i(X_t,\mathbb{Z})$ et à l'action de I correspond la transformation de monodromie T.

Ici encore, on sait qu'un sous-groupe d'indice fini de $\pi_1(D^*)$ agit de façon unipotente sur $H^i(\tilde{X},\mathbb{Q}) = H^i(X_t,\mathbb{Q})$. Plaçons-nous dans le cas semi-stable où $\pi_1(D^*)$ tout entier agit de façon unipotente (ceci revient à remplacer D par un revêtement fini), et soit T l'action du générateur canonique de $\pi_1(D^*)$.

Par 3 et 8, on s'attend à ce que $H^i(\tilde{X},\mathbb{Q}) \simeq H^i(X_t,\mathbb{Q})$ soit muni d'une filtration croissante W, que $\operatorname{Gr}_n^W(H^i(\tilde{X},\mathbb{Q}))$ soit muni d'une structure de Hodge de poids n, que $\log T(W_n)\subset W_{n-2}$ et que $\log T$ induise un morphisme de structures de Hodge

$$M_n:\quad \mathbb{Z}(-1)\otimes \operatorname{Gr}_n^W(H^i)\to \operatorname{Gr}_{n-2}^W(H^i).$$

On aimerait de plus que (8.2), et non seulement (8.3) et (8.4), aient un analogue.

On parvient en fait à définir, pour chaque vecteur u de l'espace tangent à D en $\{0\}$, une structure de Hodge mixte $\mathscr{H}_u$ sur $H^i(\tilde{X},\mathbb{Z})$. La filtration W et les structures de Hodge sur les $\operatorname{Gr}_n^W(H^i)$ sont indépendantes de u, et la dépendance en u de $\mathscr{H}_u$ s'exprime simplement en terme de T. En analogie avec (8.2), on trouve que, quel que soit u, log T induit un homomorphisme de structures de Hodge mixtes

$$M: \quad \mathbb{Z}(1) \otimes H^i(\tilde{X}, \mathbb{Z}) \to H^i(\tilde{X}, \mathbb{Z}).$$

Enfin, l'analogie 8.5 n'est pas trompeuse (mais ici, le fait que $f \mid D^*$ soit supposé propre et lisse est sans doute essentiel). On prouve que

$$(\log T)^k: \quad \mathrm{Gr}^W_{n+k}(H^n(\tilde{X}, \mathbb{Q})) \to \mathrm{Gr}^W_{n-k}(H^n(\tilde{X}, \mathbb{Q}))$$

est un isomorphisme pour tout k (cf. [6], IV 6, cor. au th. 5). Ceci caractérise la filtration W. Jusqu'ici, on ne dispose d'un analogue du théorème de positivité de Hodge (cf. [6], IV 7, cor. au th. 7) que dans des cas très particuliers. On espère que les structures mixtes $\mathscr{H}_u$ déterminent le comportement asymptotique, pour $t \to 0$, de la famille de structures pures $H^i(X_t, \mathbb{Z})$ $(t \in D^*)$.

BIBLIOGRAPHIE

[1] P. Deligne. — Théorie de Hodge, à paraître aux *Publ. Math. I. H. E. S.*, 40.

[2] M. Demazure. — Motifs des variétés algébriques, *Sém. Bourbaki* (1969-1970), exp. 365.

[3] J.-P. Serre. — Analogues kählériens de certaines conjectures de Weil, *Ann. of Math.*, 71, 2 (1960), pp. 392-394.

[4] — and J. Tate. — Good reduction of abelian varieties, *Ann. of Math.*, 88, 3 (1968), pp. 492-517.

[5] A. Weil. — Number of solutions of equations in finite fields, *Bull. Amer. math. Soc.*, 55 (1949), pp. 497-508.

[6] —. — Introduction à l'étude des variétés kählériennes, *Act. Sci. et Ind.*, 1267, Hermann (1958).

I. H. E. S.
35, route de Chartres,
91-Bures-sur-Yvette
(France)

Actes, Congrès intern. math., 1970. Tome 1, p. 431 à 436.

GROUPES DE BARSOTTI-TATE ET CRISTAUX

par A. GROTHENDIECK

Dans la suite, p désigne un nombre premier fixé. Nous nous proposons d'exposer l'esquisse d'une généralisation de la théorie de Dieudonné [4] des groupes formels sur un corps parfait de car. p, au cas « des groupes de Barsotti-Tate » (« groupes p-divisibles » dans la terminologie de Tate [5]) sur un schéma de base S sur lequel p est nilpotent. Un exposé plus détaillé se trouvera dans des notes développant un cours que j'ai donné sur ce sujet en juillet 1970 au Séminaire de Mathématique Supérieure de l'Université de Montréal, cf. aussi [7].

1. Généralités.

Si S est un schéma, on identifie les schémas X sur S aux faisceaux (fppf) [2] qu'ils représentent. Les (faisceaux en) groupes sur S sont supposés commutatifs. Un groupe G sur S est appelé un *groupe de Barsotti-Tate sur* S (ou p-groupe de BT sur S, si on veut spécifier p), s'il satisfait aux conditions suivantes:

a) $p.G = G$, i. e. G est p-divisible.

b) G est de p-torsion, i. e. $G = \varinjlim\limits_{n} {}_{p^n}G$.

c) Les groupes $G(n) = {}_{p^n}G \overset{(\text{def})}{=\!=} \operatorname{Ker}(p^n.\mathrm{id}_G)$ sont (représentables par des S-schémas) finis localement libres.

En fait, il suffit (moyennant *a*) et *b*)) de supposer que $G(1) = {}_pG$ soit fini localement libre, pour que les $G(n)$ le soient comme extensions multiples de groupes isomorphes à $G(1)$. Notons que $G(1)$ est de rang de la forme p^d, où d est une fonction sur S localement constante à valeurs dans les entiers naturels, et que pour tout n, $G(n)$ est alors de rang p^{dn}. L'entier d s'appelle le *rang* ou la *hauteur* du groupe de Barsotti-Tate G. Remarquons qu'une extension de deux groupes de BT est un groupe de BT, et que le rang se comporte additivement pour les extensions. Notons aussi que l'image inverse par un changement de base $S' \to S$ d'un groupe de BT est un groupe de BT.

Lorsque p est premier aux caractéristiques résiduelles de S, la catégorie des groupes de BT sur S est équivalente à la catégorie des faisceaux p-adiques libres constants tordus sur S [3], en associant à G le faisceau p-adique

$$T_p(G) = \text{« } \varprojlim \text{ » } G(n),$$

le morphisme de transition $G(n') \to G(n)$ étant induit par la multiplication par $p^{n'-n}$ (pour $n' \geqslant n$). Si S est connexe et muni d'un point géométrique s, la catégorie en question est donc équivalente à celle des représentations linéaires continues du groupe fondamental $\pi = \pi_1(S, s)$ dans des $\mathbb{Z}_p$-modules libres de type fini.

Lorsque A est un schéma abélien sur S, son sous-groupe de p-torsion maximal

$$_{p^\infty}A = \varinjlim_n {}_{p^n}A$$

est un groupe de BT, de rang égal à $2d$, ou d est la dimension relative de A. Les propriétés de A ont tendance à se réfléter de facon très fidèle dans celles du groupe de BT associé, ce qui est une des raisons principales de l'intérêt des groupes de BT. Signalons à ce propos le

Théorème de Serre-Tate [6] [7]. — *Supposons que p soit localement nilpotent sur S* (i. e. *les car. residuelles de S sont egales a p) et soit S' un voisinage infinitésimal de S. Alors, pour tout schéma abelien A sur S, les prolongements A' de A à S'* « *correspondent exactement* » *aux prolongements du groupe de BT G associe à A en un groupe de BT G' sur S'.*

En fait, on obtient une équivalence entre la catégorie des schémas abéliens A' sur S', et la catégorie des triples (G', A, ϕ) d'un groupe de BT G' sur S', d'un schéma abélien A sur S, et d'un isomorphisme $\phi : G' \mid S \simeq {}_{p^\infty}A$.

2. Groupe formel associé à un groupe de *BT*.

Si G est un faisceau sur S muni d'une section e, on définit de façon évidente le voisinage infinitésimal d'ordre n de cette section dans G, $\mathrm{Inf}^n(G, e)$, et le voisinage infinitésimal d'ordre infini

$$\overline{G} = \mathrm{Inf}^\infty(G, e) = \varinjlim \mathrm{Inf}^n(G, e).$$

Lorsque G est un groupe de BT sur S et que p est localement nilpotent sur S, on prouve que $\overline{G}$ est un *groupe de Lie formel*, qu'on appelle le *groupe formel associé au groupe de BT G.* Sa formation est fonctorielle en G et commute au changement de base. Lorsque S est réduit à un point, $\overline{G}$ lui-même est un groupe de BT, et G est une extension d'un groupe de BT $G/\overline{G}$ ind-étale par le groupe de BT ind-infinitésimal $\overline{G}$. La catégorie des groupes de BT ind-infinitésimaux n'est alors autre que celle des groupes de Lie formels qui sont p-divisibles, i. e. ou la multiplication par p est une isogénie [5].

3. Théorie de Dieudonné.

Nous supposons maintenant p localement nilpotent sur S. Pour la notion de « cristal en modules localement libre » sur S, nous renvoyons à [1]; nous considérons ici S comme un schéma sur $\mathbb{Z}_p$, l'idéal $p\mathbb{Z}_p$ de $\mathbb{Z}_p$ étant muni de ses structures de puissances divisées. La théorie de Dieudonné généralisée consiste en la définition d'un « *foncteur de Dieudonné* ».

$$\mathbb{D} : BT(S)^0 \to \text{Crismodloclib}(S),$$

ou $BT(S)$ désigne la catégorie des groupes de BT sur S. Ce foncteur est compatible avec les changements de base. On peut le construire par deux procédés assez distincts en apparence (méthode de l'exponentielle, et méthode des $\natural$-extensions), dont la description dépasse le cadre de cette note. La première méthode a l'avantage de se prêter directement à la théorie des extensions infinitésimales de groupes de BT du paragraphe suivant; la deuxième, de permettre une comparaison assez directe de ce foncteur et le foncteur défini classiquement par Dieudonné, dans le cas où S est le spectre d'un corps parfait: dans ce cas, on trouve un isomorphisme canonique entre ce dernier, et le foncteur que nous construisons.

Lorsque S est de caractéristique p, on dispose des morphismes de Frobenius et de Verschiebung (décalage):

$$G \underset{V_G}{\overset{F_G}{\rightleftarrows}} G^{(p/S)},$$

d'où, en transformant par le foncteur de Dieudonné $\mathbb{D}$, des morphismes

$$M \underset{V_M}{\overset{F_M}{\rightleftarrows}} M^{(p/S)}, \qquad M = D(G),$$

satisfaisant les conditions habituelles

$$F_M V_M = p.\mathrm{id}_M, \qquad V_M F_M = p.\mathrm{id}_{M^{(p/s)}}.$$

Un cristal M muni de morphisme F_M, V_M satisfaisant aux conditions précédentes sera appelé un *cristal de Dieudonné.* Ainsi, la théorie de Dieudonné généralisée nous fournit un foncteur contravariant de la catégorie des groupes de Barsotti-Tate sur S dans celle des cristaux de Dieudonné, compatible aux changements de base. Lorsque S est le spectre d'un corps parfait, la théorie de Dieudonné classique nous apprend que c'est une équivalence de catégorie. Dans le cas général, on peut espérer que ce foncteur soit pleinement fidèle.

On peut d'ailleurs donner une description conjecturale assez simple de l'image essentielle de ce foncteur, que nous n'expliciterons pas ici.

4. Filtration du cristal de Dieudonné et déformations de groupes de BT.

Nous supposons toujours p localement nilpotent. Avec la construction du cristal de Dieudonné $\mathbb{D}(G)$ d'un groupe de BT G, on trouve en même temps une filtration canonique du module localement libre $\mathbb{D}(G)_S$ sur S par un sous-module localement facteur direct Fil $(\mathbb{D}(G)_S)$. De façon précise, on trouve une suite exacte canonique

$$0 \to \underline{\omega}_G \to \mathbb{D}(G)_S \to \check{\underline{\omega}}_{G^*} \to 0,$$

où $\underline{\omega}_G$ est le faisceau localement libre sur S des 1-formes différentielles le long de la section unité du groupe de Lie formel $\overline{G}$ associé à G (n° 2), et $G^* = \varinjlim G(n)^*$ désigne le groupe de BT *dual* de G (pour la dualité de Cartier), enfin $\check{}$ désigne le module dual. La suite exacte envisagée est fonctorielle en G, et commute aux changements de base.

Soit maintenant S' un épaississement à puissances divisées de S, et supposons que, ou bien les puissances divisées envisagées sont nilpotentes, ou bien que les fibres de G sont connexes, ou qu'il en soit ainsi de celles de G^* (i. e. $G(1)$ est unipotent). Considérons le module localement libre $\mathbb{D}(G)_{S'}$ sur S'. Pour tout prolongement G' de G en un groupe de BT sur S, $\mathbb{D}(G)_{S'}$ peut s'identifier à $\mathbb{D}(G')_S$, et à ce titre il est muni d'une filtration par un sous-module localement facteur direct Fil $\mathbb{D}(G')$, qui prolonge la filtration Fil $\mathbb{D}(G)$ dont on dispose déjà sur $\mathbb{D}(G)_S$. Ceci dit, on trouve que les prolongements de G en un groupe de BT G' sur S' « correspondent exactement » aux prolongements de la filtration qu'on a sur $\mathbb{D}(G)_S$ en une filtration de $\mathbb{D}(G)_{S'}$ par un sous-module localement facteur direct. Plus précisément, on trouve une équivalence entre la catégorie des groupes de BT G' sur S' (resp. ceux à fibres connexes, resp. ceux à fibres ind-unipotentes) avec la catégorie des couples (G, Fil), où G est un groupe de BT sur G (resp. un groupe de BT à fibres connexes, resp. à fibres und-unipotentes), et où Fil est une filtration de $\mathbb{D}(G)_{S'}$ par un sous-module localement facteur direct, prolongeant la filtration canonique de $\mathbb{D}(G)_S$.

Remarques.

1. Sans hypothèse sur les puissances divisées envisagées ou sur les fibres de G, on a en tous cas un foncteur

$$G' \mapsto (G, \mathrm{Fil}),$$

mais même si G est la somme du groupe constant $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ et de son groupe de BT dual ${}_{p^\infty}\boldsymbol{G}_m$, il n'est plus vrai (si les puiss. div. ne sont pas nilpotentes) qu'un prolongement de G soit connu quand on connait le prolongement correspondant d'une filtration. Ceci est lié au fait que le logarithme sur $1 + J$ (J l'idéal d'augmentation) n'est plus nécessairement injectif.

2. Soit toujours S un schéma où p soit localement nilpotent, et soit $S_0 \hookrightarrow S$ le sous-schéma Var (p) défini par l'annulation de p. Alors S est un épaississement à puissances divisées de S, et si $p \neq 2$, il est à puissances divisées (localement) nilpotentes. On peut donc appliquer la théorie de déformations précédentes, pour expliciter les groupes de BT sur S en termes de groupes de BT sur le schéma S_0 de car. p, et du prolongement d'une filtration, à condition, si $p = 2$, de se borner aux groupes de BT à fibres connexes ou ind-unipotentes. *Si* la théorie de Dieudonné du n° 3 fournit une description complète de la catégorie des groupes de BT sur S_0 en termes cristallins (ce qui pour l'instant reste conjectural), on en déduit donc une description de la catégorie des groupes de BT sur S en termes purement « cristallins », avec toutefois le grain de sel habituel pour $p = 2$.

5. Groupes de BT à isogénie près.

La catégorie des groupes de BT « à isogénie près » sur S est par définition la catégorie dont les objects sont les groupes de BT sur S, et ou $\mathrm{Hom}_{\mathrm{isog}}(G, G')$ est défini comme $\mathrm{Hom}(G, G') \otimes_{\mathbb{Z}} \mathbb{Q}$. Si p est localement nilpotent sur S, on trouve donc un foncteur de la catégorie des groupes de BT sur S à isogénie près, dans celle des cristaux sur S à isogénie près. Lorsque S' est un voisinage infinitésimal de S, l'idéal d'épaississement étant annulé par une puissance de p, on trouve que le foncteur restriction induit une *équivalence* de la catégorie des groupes de BT à isogénie près sur S', avec la catégorie analogue pour S: ainsi, la théorie des déformations infinitésimales à isogénie près est triviale.

Par un passage à la limite facile, on déduit des résultats du paragraphe précédent le résultat qui suit.

Soit A un anneau séparé et complet pour la topologie p-adique, $A_n = A/p^{n+1}A$.

Pour tout groupe de BT G_0 sur $S_0 = \mathrm{Spec}\,(A_0)$, on définit par passage à la limite sur les $D(G_0)_{A_n}$ un A-module de type fini localement libre $M = \mathbb{D}(G_0)$, et si G_0 est prolongé en G sur A, M est muni d'une filtration par un sous-module facteur direct $M' = \mathrm{Fil}\, M \subset M$. Localisant par rapport à p, on trouve un A_p-module localement libre M_p, muni d'un facteur direct Fil M_p. On trouve ainsi un foncteur $G_0 \to \mathbb{D}(G_0)_p$ de la catégorie des groupes de BT à isogénie près sur A_0, dans la catégorie des modules localement libres sur A_p, et un foncteur $G \mapsto (G_0, \mathrm{Fil})$ de la catégorie des groupes de BT à isogénie près G sur S, dans la catégorie des couples (G_0, Fil) d'un groupe de BT à isogénie près G_0 sur S_0, et d'un sous-module facteur direct Fil $\mathbb{D}(G_0)_p$. *Ce dernier foncteur est pleinement fidèle.*

Considérons notamment le cas où A est un anneau de valuation discrète complet à corps résiduel k parfait de car. p, et à corps des fractions K de caractéristique nulle. On trouve qu'un groupe de BT G sur A est connu à isogénie près, quand on connait *a*) le groupe de BT $G_0 = G \otimes_A k$ sur k à isogénie près, ou ce qui revient au même, son espace de Dieudonné $E = D(G_0)_W \otimes_W L$ (ou L est le corps des fractions de l'anneau des vecteurs de Witt sur k), muni de F_E et V_E, et *b*) la filtration correspondante de $D(G_0)_p = E \otimes_L K$.

Remarques. — Le résultat qui précède soulève de nombreuses questions auxquelles je ne sais répondre :

1. Quelles sont les filtrations sur $E \otimes_L K$ qu'on peut obtenir par un groupe de BT à isogénie près sur A ? Forment-elles un ouvert de Zariski d'une grassmanienne ?

2. Comment peut-on expliciter G, et plus particulièrement sa fibre générique G_K (qu'on peut interpréter comme un vectoriel de dimension finie sur $\mathbb{Q}_p$ sur lequel Gal $(\overline{K}/K)$ opère), en termes du couple $(E, \mathrm{Fil} \subset E \otimes_L K)$, ou E est un L-vectoriel muni de F_E et V_E ?

3. Quels sont les modules galoisiens qu'on trouve à l'aide de groupes de BT à isogénie près G sur A ? Comment, à l'aide d'un tel module galoisien, peut-on reconstituer plus ou moins algébriquement le couple (E, Fil) ? (Cette question se pose à cause du théorème de Tate [5], qui nous dit que G est connu quand on connait le module galoisien associé.)

Enfin, pour traiter la cohomologie cristalline et ses relations avec la cohomologie p-adique, il y a lieu de se poser des questions analogues, où les cristaux de Dieudonné avec filtrations à 2 crans sont remplacés par des cristaux avec un morphisme de Frobenius et des filtrations finies de longueur quelconque (la cohomologie en dimension n donnant lieu à des filtrations à $n + 1$ crans). De plus, il y a lieu de ne pas se restreindre au cas des bases de dimension 1, et de revenir au cas des anneaux A supposés simplement séparés et complets pour la topologie p-adique.

BIBLIOGRAPHIE

[1] P. Berthelot. — Cohomologie cristalline des schémas, *Notes aux C. R.*, du 18-8-, 1-9 et 8-9-1969.

[2] M. Demazure. — In S. G. A. 3 IV (Springer *Lecture Notes*, No. 151).

[3] P. Jouanolou. — In S. G. A. 5 VI *(Institut des Hautes Études Scientifiques)*.

[4] U. I. MANIN. — Théorie des groupes commutatifs formels sur des corps de car. finie, *Uspechi Mat. Nauk* (en russe), 18 (1963), pp. 3-90.

[5] J. TATE. — p-divisible groups in local fields, *Proceedings of a Conference held at Driebergen* (The Netherlands) in 1966, Springer (Berlin), 1967.

[6] Séminaire de J. TATE au Collège de France en 1968 (écrire à TATE, Dep. of Math., 2 Divinity Avenue, Cambridge, Mass., U. S. A).

[7] W. MESSING. — The crystals associated to BARSOTTI-TATE groups, thèse, Princeton (1971).

(Collège de France,
11, Place Marcelin-Berthelot,
Paris 5e
France).

Actes, Congrès intern. math., 1970. Tome 1, p. 437 à 443.

THE REGULARITY THEOREM IN ALGEBRAIC GEOMETRY

by Nicholas M. KATZ

I. Introduction.

A basic finiteness theorem for families of algebraic varieties is that the Picard-Fuchs differential equations have only regular (in the sense of Fuchs) singular points. The theorem was proved analytically by P. A. Griffiths [3], then by P. Deligne, both of whom used Hironaka's resolution of singularities [5] to be able to estimate the growths of solutions.

Just recently, Deligne and the speaker independently found a purely algebro-geometric proof, which makes the theorem a simple corollary of resolution. The method also leads to a direct proof of the monodromy theorem.

II. The notion of regular singular points [1].

Let U be a smooth $\mathbb{C}$-scheme. An algebraic differential equation on U is by definition a pair (M, ∇) consisting of a coherent sheaf M on U with an integrable connection (the existence of ∇ implies that M is, in fact, locally free). We will view ∇ as a homomorphism of abelian sheaves

$$(2.1) \qquad \nabla : M \to \Omega^1_U \otimes_{\mathcal{O}_U} M$$

(writing Ω^1_U for $\Omega^1_{U/\mathbb{C}}$) which satisfies the usual product rule and which extends to define a structure of *complex* on $\Omega^{\cdot}_U \otimes_{\mathcal{O}_U} M$, the " absolute de Rham complex " of (M, ∇).

Now let S be a proper and smooth $\mathbb{C}$-scheme, $D = \cup D_i$ a union of connected smooth divisors in S with normal crossings, such that $U \xrightarrow{\sim} S - D$, which we will refer to as a *compactification* of U. Let $Der_D(S/\mathbb{C})$ denote the (locally free) sheaf on S of derivations which preserve the ideal sheaf of each branch D_i of D. The sheaf of differentials on S with logarithmic singularities along D is defined by

$$(2.2) \qquad \begin{aligned} \Omega^1_S (\log D) &\overset{\text{def'n}}{=\!=} \mathcal{H}om_{\mathcal{O}_S}(Der_D(S/\mathbb{C}), \mathcal{O}_S) \\ \Omega^p_S (\log D) &= \Lambda^p_{\mathcal{O}_S} \Omega^1_S (\log D) \end{aligned}$$

It is immediate that $\Omega^{\cdot}_S (\log D)$ is a subcomplex of $i_* \Omega^{\cdot}_U$ ($i : U \hookrightarrow S$ denoting the inclusion).

Following Fuchs and Deligne, we say that an algebraic differential equation (M, ∇) on U has regular singular points if, for *every* compactification $U = S - D$ as above (by Hironaka [5], such compactifications exist!), there exists a pair $(\overline{M}, \overline{\nabla})$ consisting of a locally free sheaf $\overline{M}$ on S which prolongs M and a homomorphism $\overline{\nabla}$ of abelian sheaves

$$\overline{\nabla}: \quad \overline{M} \rightarrow \Omega^1_S (\log D) \otimes_{\mathcal{O}_S} \overline{M} \tag{2.3}$$

which prolongs ∇.

III. **Remarks on the definition.**

(3.1) It is rather forbidding in appearance, but is certainly satisfied by ($\mathcal{O}_U$, d = exterior differentiation).

(3.2) A consideration of the local monodromy around D shows that the underlying *analytic* differential equation (M^{an}, ∇^{an}) always admits an *analytic* extension ($\overline{M^{an}}$, $\overline{\nabla^{an}}$) as above, which, by GAGA, is uniquely *algebrifiable*. Restricting this algebraic data to U, we get a second algebraic differential equation (M', ∇') on U, which depends *only* and *functorially* on (M, ∇), and an isomorphism of (M^{an}, ∇^{an}) with (M'^{an}, ∇'^{an}). The condition that (M, ∇) have regular singular points is that the above isomorphism come from an isomorphism of (M, ∇) and (M', ∇').

(3.3) It follows easily from (3.2) that (M, ∇) has regular singular points if and only if for every morphism $f : V \rightarrow U$ with V a smooth *curve*, the inverse image $f^*(M, \nabla)$ on V has regular singular points.

(3.4) If U is a connected smooth curve, and $U = S - D$ its canonical compactification, (M, ∇) has regular singular points if there exists an extension ($\overline{M}$, $\overline{\nabla}$) as above with $\overline{M}$ *coherent* ($\overline{M}$/torsion is a locally free extension to which $\overline{\nabla}$ passes over).

(3.5) Combining (3.3) and (3.4), it follows that (M, ∇) has regular singular points if for *one* compactification $U = S - D$ there exists an extension ($\overline{M}$, $\overline{\nabla}$) as above with $\overline{M}$ coherent

IV. **Relative de Rham cohomology** [7].

Let $f : U \rightarrow V$ be a proper and smooth morphism of smooth $\mathbb{C}$-schemes, and (M, ∇) an algebraic differential equation on U. Composing ∇ with the projection $\Omega^1_U \otimes_{\mathcal{O}_U} M \rightarrow \Omega^1_{U/V} \otimes_{\mathcal{O}_U} M$, we obtain an integrable V-connection, still noted,

$$\nabla: \quad M \rightarrow \Omega^1_{U/V} \otimes_{\mathcal{O}_U} M \tag{4.1}$$

which extends to provide a structure of complex to $\Omega^{\cdot}_{U/V} \otimes_{\mathcal{O}_U} M$, the " relative de Rham complex of (M, ∇) ". The relative de Rham cohomology sheaves on V of (M, ∇) are defined by

$$H^q_{DR}(U/V, (M, \nabla)) = \mathbb{R}^q f_* (\Omega^{\cdot}_{U/V} \otimes_{\mathcal{O}_U} M) \tag{4.2}$$

These sheaves are coherent, as f is proper, and are endowed with an integrable connection, whose construction we now recall.

Filter the absolute de Rham complex of (M, ∇) by the subcomplexes

$$(4.3)\quad F^i = F^i(\Omega^{\cdot}_U \otimes_{\mathcal{O}_U} M) = \text{image}: f^*(\Omega^i_V) \otimes_{\mathcal{O}_U} \Omega^{\cdot - i}_U \otimes_{\mathcal{O}_U} M \to \Omega^{\cdot}_U \otimes_{\mathcal{O}_U} M.$$

The associated graded objects are given by

$$(4.4)\qquad gr^i = F^i/F^{i+1} = f^*(\Omega^i_V) \otimes_{\mathcal{O}_U} (\Omega^{\cdot - i}_{U/V} \otimes_{\mathcal{O}_U} M)$$

The integrable connection sought on $H^q_{DR}(U/V, (M, \nabla))$ is the differential $d_1^{0,q}$ in the spectral sequence of the filtered complex $\Omega^{\cdot}_U \otimes_{\mathcal{O}_U} M$ and the functor $\mathbb{R}^0 f_*$, or, in more down to earth terms, it is the coboundary map δ_q, in the long cohomology sequence of the $\mathbb{R}^q f_*$ arising from the short exact sequence $0 \to gr^1 \to F^0/F^2 \to gr^0 \to 0$. Remember that, by (4.4), we have

$$(4.5)\qquad \begin{cases} \mathbb{R}^q f_*(gr^0) = H^q_{DR}(U/V, (M, \nabla)) \\ \mathbb{R}^{q+1} f_*(gr^1) = \Omega^1_V \otimes_{\mathcal{O}_V} H^q_{DR}(U/V, (M, \nabla)). \end{cases}$$

(4.6) Thus $(H^q_{DR}(U/V, (M, \nabla)), \delta_q)$ is an algebraic differential equation on V. In particular, $H^q_{DR}(U/V, (M, \nabla))$ is locally free; this being so for all q, it follows that *the formation of the* $H^q_{DR}(U/V, (M, \nabla))$ *is compatible with arbitrary change of base.*

We remark that in the case $(M, \nabla) = (\mathcal{O}_U, d)$, the connection just constructed on $H_{DR}(U/V) \overset{\text{defn}}{=\!=} \mathbb{R} f_*(\Omega^{\cdot}_{U/V})$ is the *Gauss-Manin connection*, and the resulting algebraic differential equation is classically called the *Picard-Fuchs equation.*

V. The regularity theorem.

THEOREM. — *Assumptions as in IV, if (M, ∇) has regular singular points, then the algebraic differential equations $(H^q_{DR}(U/V, (M, \nabla)), \delta_q)$ on V have regular singular points.*

Proof. — Combining (3.4) and (4.6), it suffices to treat the case in which V is a smooth connected curve. Let T be the complete non singular model of the function field of V, so that $V = T - Y$, Y a finite set of points of T, is the canonical compactification of V. By Hironaka [5], we can " compactify " the morphism $f: U \to V$ into a morphism $\pi: S \to T$, so as to have a cartesian diagram

$$(5.1)\qquad \begin{array}{ccc} U & \hookrightarrow & S. \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \pi} \\ V & \hookrightarrow & T \end{array}$$

in which $D \overset{\text{defn}}{=\!=} \{\pi^{-1}(Y)\}^{\text{red.}}$ is a union of connected smooth divisors in S which cross normally, and $U = S - D$ is a *compactification* of U in the sense of II.

Notice that $\pi^*(\Omega^1_T (\log Y))$ is a subsheaf of $\Omega^1_S (\log D))$. We define the (locally free) sheaf of relative differentials with logarithmic singularities along D by

$$(5.2)\qquad \begin{cases} \Omega^1_{S/T} (\log D) \overset{\text{defn}}{=\!=} \Omega^1_S (\log D)/\pi^*(\Omega^1_T (\log Y)) \\ \Omega^p_{S/T} (\log D) = \Lambda^p_{\mathcal{O}_S} \Omega^1_{S/T} (\log D) \end{cases}$$

The *complex* $\Omega^{\cdot}_{S/T}$ (log D) on S is a prolongation of $\Omega^{\cdot}_{U/V}$, and fits into a short exact sequence of complexes

(5.3) $0 \to \pi^*(\Omega^1_T\,(\log Y) \otimes_{\mathcal{O}_S} \Omega^{\cdot-1}_{S/T}\,(\log D) \to \Omega^{\cdot}_S\,(\log D) \to \Omega^{\cdot}_{S/T}\,(\log D) \to 0$

Now let $(\overline{M}, \overline{\nabla})$ be an extension of (M, ∇) to S, with $\overline{M}$ locally free and $\overline{\nabla}: \overline{M} \to \Omega^1_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}$ a prolongation of ∇, and consider the complex deduced from $\overline{\nabla}$,

(5.4) $$\Omega^{\cdot}_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}$$

which is a prolongation of $\Omega^{\cdot}_U \otimes_{\mathcal{O}_U} M$.

Filter $\Omega^{\cdot}_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}$ by the subcomplexes

(5.5) $F^i = \text{image } \pi^*(\Omega^i_T\,(\log Y) \otimes_{\mathcal{O}_S} \Omega^{\cdot-i}_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M} \to \Omega^{\cdot}_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}$

The associated graded objects are given by

(5.6) $$gr^i = F^i/F^{i+1} = \pi^*(\Omega^i_T\,(\log Y)) \otimes_{\mathcal{O}_S} (\Omega^{\cdot-i}_{S/T}\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}).$$

In particular, gr^0 is a prolongation of the relative de Rham complex $\Omega_{U/V} \otimes M$ of (M, ∇).

We define the coherent sheaves on T.

(5.7) $$H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})) \stackrel{\text{defn}}{=\!=} \mathbb{R}^q\pi_*(\Omega^{\cdot}_{S/T}\,(\log D) \otimes_{\mathcal{O}_S} M)$$

which are prolongations of the locally free sheaves $H^q_{DR}(U/V, (M, \nabla))$ on V. The extensions of δ_q to homomorphisms of abelian sheaves

(5.8) $$\overline{\delta}_q:\ H^q(S/T, (\overline{M}, \overline{\nabla})) \to \Omega^1_T\,(\log Y) \otimes_{\mathcal{O}_T} H^q_{DR}(S/T, (\overline{M}, \overline{\nabla}))$$

are provided by the coboundary maps of the long cohomology sequence of the $\mathbb{R}^q\pi_*$ arising from the short exact sequence $0 \to gr^1 \to F^0/F^2 \to gr^0 \to 0$

Remember that, by (5.6), we have

(5.9) $$\begin{cases} \mathbb{R}^q\pi_*(gr^0) = H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})) \\ \mathbb{R}^{q+1}\pi_*(gr^1) = \Omega^1_T\,(\log Y) \otimes_{\mathcal{O}_T} H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})). \end{cases}$$

Thus the $(H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})), \overline{\delta}_q)$ provide the desired extensions of the

$$(H^q_{DR}(U/V, (M, \nabla)), \delta_q).$$ QED.

VI. The exponents.

Notations as in II, let $(\overline{M}, \overline{\nabla})$ be an algebraic differential equation on S with logarithmic singularities along D. For each branch D_i of D, we denote by $\overline{M}(D_i)$ the locally free sheaf $\mathcal{O}_{D_i} \otimes_{\mathcal{O}_S} \overline{M}$ on D_i. Composing $\overline{\nabla}$ with the map " residue along D_i "

(6.1) $$\Omega^1_S\,(\log D) \otimes_{\mathcal{O}_S} \overline{M} \xrightarrow{\text{"residue along } D_i\text{"} \otimes 1} \mathcal{O}_{D_i} \otimes_{\mathcal{O}_S} \overline{M} = \overline{M}(D_i)$$

we obtain an ($\mathcal{O}_{D_i}$-linear) endomorphism L_i of $\overline{M}(D_i)$. As D_i is proper, the characteristic polynomial of L_i, $P_i(X) = \det(XI - L_i; \overline{M}(D_i))$ lies in $\mathbb{C}[X]$. Classically, P_i is called the *indicial polynomial* of $(\overline{M}, \overline{\nabla})$ around D_i, and its roots are called *exponents* of $(\overline{M}, \overline{\nabla})$ around D_i. The numbers $\exp(2\pi i\varepsilon)$, ε an exponent, are the proper values of the local monodromy transformation " turning once around D_i " of the space of local holomorphic horizontal sections of $(\overline{M}, \overline{\nabla}) \mid S - D$; thus the exponents, which *depend* on $(\overline{M}, \overline{\nabla})$, are determined modulo $\mathbb{Z}$ by $(\overline{M}, \overline{\nabla}) \mid S - D$.

VII. The Monodromy theorem.

THEOREM. — *Let V be a smooth connected curve, T its canonical compactification, $f: U \to V$ a proper and smooth morphism, and $\pi: S \to T$ a compactification of f as in* (5.1). *Let $(\overline{M}, \overline{\nabla})$ be an algebraic differential equation on U, and $(\overline{M}, \overline{\nabla})$ an extension to S as in* (2.1). *Denote by $P_i(X)$ the indicial polynomial of $(\overline{M}, \overline{\nabla})$ around D_i.*

Let $y \in T - V$, and $\pi^{-1}(y) = \Sigma_{i=1}^r a_i D_i$ its scheme-theoretic fibre. Then the indicial polynomial at y of $(H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})), \overline{\delta}_q)$ divides a power of

$$\prod_{i=1}^{r} \prod_{j_i=0}^{a_i-1} P_i(a_i X - j_i)$$

Proof. — The question being local around y, let us base-change the entire situation by the inclusion $\operatorname{Spec}(\mathcal{O}_{T,y}) \to T$, but for simplicity keep the same notations (so T henceforth means $\operatorname{Spec}(\mathcal{O}_{T,y})$, etc.). We must now adopt the dual view of the " connection with logarithmic singularities " $\overline{\nabla}$ as an *action* of $Der_D(S/C)$ on $\overline{M}$ satisfying the usual rules [8], and similarly of $\overline{\delta}_q$ as an action of $\mathrm{Der}_y(T/C)$ on $H^q_{DR}(S/T, (\overline{M}, \overline{\nabla}))$. Let t be a uniformizing parameter at y. Then the indicial polynomial at y of $(H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})), \overline{\delta}_q)$ is just the characteristic polynomial of the endomorphism $\overline{\delta}_q\left(t\dfrac{d}{dt}\right)$ of $H^q_{DR}(S/T, (\overline{M}, \overline{\nabla}))(y)$. We will show that

$$\left[\prod_{i=1}^{r} \prod_{j_i=0}^{a_i-1} P_i\left(a_i\overline{\delta}_q\left(t\frac{d}{dt}\right) - j_i\right)\right]^{q+1} [H^q_{DR}(S/T, (\overline{M}, \overline{\nabla}))] \subset tH^q_{DR}(S/T, (\overline{M}, \overline{\nabla})) \tag{7.1}$$

To do this we will use the explicit formulas of [8] for $\overline{\delta}_q\left(t\dfrac{d}{dt}\right)$. Let $\underline{U}$ be a covering of S by affine open sets $U_1, U_2, \ldots$ which is sufficiently fine, in the sense that each U_ν admits coordinates $x_1, \ldots, x_n$, in terms of which D_i is defined by the equation $x_i = 0$ (or by the equation $1 = 0$, if D_i does not meet U_ν), and in terms of which $t = \Pi_{i=1}^r x_i^{b_i}$, with $b_i = 0$ or a_i. Let $C^{\cdot\cdot}$ denote the Cech bicomplex of quasi-coherent T-modules $C^{\cdot}(\underline{U}, \Omega^{\cdot}_{S/T}(\log D) \otimes_{\mathcal{O}_S} \overline{M})$, whose (total) cohomology objects are just the

$$H^q_{DR}(S/T, (\overline{M}, \overline{\nabla})).$$

According to [8], we may construct an action σ of $t\dfrac{d}{dt}$ on the underlying sheaf of $C^{\cdot\cdot}$ (i. e., for $h \in \mathcal{O}_{T,y}$ and $c \in C^{\cdot\cdot}$, $\sigma(hc) = t\dfrac{dh}{dt}c + h\sigma(c)$) which commutes with the total coboundary of $C^{\cdot\cdot}$ and induces $\overline{\delta}_q\left(t\dfrac{d}{dt}\right)$ upon passage to cohomology. Indeed, if we choose for each open set U_ν of the covering an element $d_\nu \in \Gamma(U_\nu, \mathrm{Der}_D(S/C))$ which prolongs $t\frac{d}{dt}$, there is a σ as above which preserves the filtration F^q of $C^{\cdot\cdot}$ by the first degree, and which on $gr^q_F C^{\cdot\cdot} = C^{q,\cdot}$ is just the Lie derivative $\mathrm{Lie}(\overline{\nabla}(d_{v_0}))$ on

$$\Gamma(U_{v_0} \cap \ldots \cap U_{v_q}, \Omega^{\cdot}_{S/T}(\log D) \otimes_{\mathcal{O}_S} \overline{M}),$$

for $v_0 < \ldots < v_q$.

For each branch D_i of D, we denote by σ_i the action of $t\frac{d}{dt}$ on $C^{\cdot\cdot}$ corresponding the choices of liftings of $t\frac{d}{dt}$ to an element $d_v^{(i)} \in \Gamma(U_v, Der_D(S/C))$ given by

$$(7.2) \quad d_v^{(i)} = \begin{cases} \dfrac{1}{a_i} x_i \dfrac{\partial}{\partial x_i} & \text{if } D_i \text{ meets } U_v \\ \dfrac{1}{a_j} x_j \dfrac{\partial}{\partial x_j} & \text{if } D_i \text{ does not meet } U_v, \text{ and } j \text{ is the least integer such that } D_j \text{ meets } U_v \end{cases}$$

We define

$$(7.3) \qquad \begin{cases} \mathscr{L}_i = \prod_{j_i=0}^{a_i-1} P_i(a_i\sigma_i - j_i) & \text{for} \quad i = 1, \ldots, r \\ \mathscr{L} = \mathscr{L}_1 \ldots \mathscr{L}_r \end{cases}$$

The product rule assures that $\mathscr{L}(tF^q) \subset tF^q$, so that to conclude the proof we need only show that $\mathscr{L}(F^q) \subset tF^q + F^{q+1}$, or equivalently, that $\mathscr{L}(gr^q_F C^{\cdot\cdot}) \subset t gr^q_F C^{\cdot\cdot}$. But this last is a " local " statement, namely that over $U_{v_0} \cap \ldots \cap U_{v_q}$, $v_0 < \ldots < v_q$, we have

$$(7.4) \quad \prod_{i=1}^{r} \prod_{j_i=0}^{a_i-1} P_i\,(\mathrm{Lie}\,(a_i\overline{\nabla}(d_{v_0}^{(i)})) - j_i)[\Omega^{\cdot}_{S/T}\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}] \subset t\Omega^{\cdot}_{S/T}\,(\log D) \otimes_{\mathcal{O}_S} \overline{M}$$

or, what is equivalent, that over U_{v_0} we have

$$(7.5) \qquad \prod_{i=1}^{r} \prod_{j_i=0}^{a_i-1} P_i(a_i\overline{\nabla}(d_{v_0}^{(i)}) - j_i)\overline{M} \subset t\overline{M};$$

Since the various lifting $d_{v_0}^{(i)}$ of $t\frac{d}{dt}$ to U_{v_0} were so chosen as to mutually commute, the $\overline{\nabla}(d_{v_0}^{(i)})$ mutually commute (integrability), so we may rearrange the product and " absorb " those P_i corresponding to D_i which do not meet U_{v_0}. Thus we may assume that all the D_i meet U_{v_0}, $t = x_1^{a_1} \ldots x_r^{a_r}$, and $a_i d_{v_0}^{(i)} = x_i \frac{\partial}{\partial x_i}$. Since P_i is a polynomial with constant coefficients and $\overline{\nabla}\left(x_i \frac{\partial}{\partial x_i}\right)$ is x_j-linear for $j \neq i$, it suffices to show that, for $i = 1, \ldots, r$, we have

$$(7.6) \qquad \prod_{j_i=0}^{a_i-1} P_i\left(\overline{\nabla}\left(x_i \frac{\partial}{\partial x_i}\right) - j_i\right)(\overline{M}) \subset x_i^{a_i}\overline{M} \quad \text{over} \quad U_{v_0}.$$

Recalling that the endomorphism L_i of $\overline{M}(D_i)$ is deduced from $\nabla\left(x_i \frac{\partial}{\partial x_i}\right)$ over U_{v_0} by reduction modulo (x_i), we have, by definition of P_i,

$$P_i\left(\nabla\left(x_i \frac{\partial}{\partial x_i}\right)\right)(\overline{M}) \subset x_i\overline{M} \quad \text{over} \quad U_{v_0} \tag{7.7}$$

Combining this with the commutation formula

$$P_i\left(\nabla\left(x_i \frac{\partial}{\partial x_i}\right) - j\right) \circ x_i^j = x_i^j P_i\left(\nabla\left(x_i \frac{\partial}{\partial x^i}\right)\right) \tag{7.8}$$

the desired formula (7.6) (and hence the theorem) follows by induction on a_i. QED.

REFERENCES

[1] P. Deligne. — Équations différentielles à points singuliers réguliers, Springer-Verlag, *Lecture Notes in Mathematics* (1970).

[2] L. Fuchs. — Zur Theorie der linearen Differentialgleichungen mit veränderlichen Koeffizienten, *J. für reine und angewandte Mathematik*, 66 (1866), pp. 121-160; 68 (1868), pp. 354-385.

[3] P. Griffiths. — Monodromy of Homology and Periods of Integrals on Algebraic Manifolds, Notes available from Princeton University (1968).

[4] —. — Periods of Integrals on Algebraic Manifolds; summary of Main Results and Discussion of Open Problems, *B. A. M. S.*, 75, 2 (1970), pp. 228-296.

[5] H. Hironaka. — Resolution of Singularities of an Algebraic Variety over a field of characteristic zero, I, II, *Ann. of Math.*, 79 (1964), pp. 109-326.

[6] A. Landman. — On the Picard-Lefschetz transformation, Ph. D. Berkeley thesis (1966).

[7] J. Manin. — Moduli Fuchsiani, *Annali Scuola Norm. Sup. Pisa*, Ser. III, 19 (1965), pp. 113-126.

[8] T. Oda and N. Katz. — On the differentiation of De Rham cohomology classes with respect to parameters, *J. Math. Kyoto Univ.*, 8, 2 (1968), pp. 199-213.

Princeton University
Department of Mathematics,
Fine Hall
Princeton, New Jersey 08540
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 445 à 449.

FINITENESS THEOREMS FOR ALGEBRAIC CYCLES

by STEVEN L. KLEIMAN (1)

Fix an algebraically closed ground field k and consider non-singular projective varieties X, Y irreducible of dimension n, m. Let $C^r(X)$ denote the group of cycles of codimension r. An equivalence relation $\sim$ is called *adequate* if the quotient $\bigoplus_r (C^r(X)/\sim)$ becomes a ring under intersection product which behaves functorially under f_* and f^* for maps $f: Y \to X$. We seek to filter $C^r(X)$ by means of adequate equivalence relations so that the successive quotients are free groups of finite rank, finite groups or continuous systems of finite dimension. Since Samuel [13] spoke on this problem at the International Congress in 1958, some of the questions he raised have been answered, new questions have captured our attention and our techniques have greatly matured.

Let $C^r_{\mathrm{alg}}(X)$ denote the subgroup of cycles algebraically equivalent to 0 (resp. $C^r_{\mathrm{rat}}(X)$ the cycles rationally equivalent to 0), i. e., those cycles which deform to 0 in an algebraic family $\{ Z(t) \}$ defined by a cycle $Z \in C^r(T \times X)$ parametrized by an irreducible non-singular variety T (resp. by $T = \mathbb{P}^1$) (2). We first seek the finest adequate relation $\sim$ such that $(C^r_{\mathrm{alg}}(X)/\sim)$ is continuous of finite dimension in one of the usual senses explained below.

A family F of cycle classes is said to be *limited* by an algebraic family $\{ Z(t) \}$ if every class is represented by some cycle $Z(t)$. This notion is rather crude because two different cycles may represent the same class.

On a surface X with $p_g > 0$, the residue classes $(C^2_{\mathrm{alg}}(X)/\mathrm{rat})$ do not form a limited family (cf. Mumford [11]). Consequently, on the Kummer surface of the self-product of an elliptic curve, the points rationally equivalent to a given point do not form a closed set (cf. [13], § 4.2).

In a more refined condition on $\sim$, we require $(C^r_{\mathrm{alg}}(X)/\sim)$ to correspond to the k-points of a variety A in such a way that the natural map $w: C^r_{\mathrm{alg}}(X) \to A(k)$ turn algebraic families $\{ Z(t) \mid t \in T(k) \}$ into T-points of A; precisely, a morphism

(1) Much of this report is the fruit of meditation on some of the work and comments of David LIEBERMAN; *I* am personally indebted to him for pointing out the consequences of Mumford's work, for explaining his own work, Griffiths' insight and Grothendieck's construction, and for giving birth with me to the simple proof that numerical and homological equivalence coincide on a complex abelian variety.

(2) Algebraic equivalence is an adequate relation, and rational equivalence is the finest adequate relation (cf. [13], § 2). Unfortunately, in the literature there is not yet a satisfactory account of rational equivalence, especially of the « moving lemma ».

$B(Z, w): T \to A$ must exist which carries t to $w(Z(t))$. Now, these T-points form an additive group, and any algebraic family parametrized by an open subset of a non-singular curve T extends over all of T (the condition of the valuative criterion of completeness); hence, we also require A to be an abelian variety and w a group homomorphism. Such w are called *rational homomorphisms.* The " image " of w is an abelian subvariety because any Z in $C^r_{\mathrm{alg}}(X)$ can be deformed to 0 in a family parametrized by an abelian variety; so we may take w surjective.

A cycle is *abelian* (cf. [13]) if it lies in the kernel of every rational homomorphism w. Abelian equivalence is adequate because every $Z \in (C^s(Y \times X)/\mathrm{alg})$ determines a well-defined rational homomorphism $w(Z(.))$ on $C^{(r-s+m)}_{\mathrm{alg}}(Y)$. We seek one rational homomorphism w whose kernel is precisely the abelian cycles, in other terms, the universal surjective w. If such a w exists, then $(C^r_{\mathrm{alg}}(X)/\mathrm{Abl})$ is limited.

In fact, given any surjective rational homomorphism $w: C^r_{\mathrm{alg}}(X) \to A(k)$, there exists an abelian variety T and a class $Z \in (C^r(T \times X)/\mathrm{rat})$ such that $B(Z, w): T \to A$ is an isogeny. For, take such a pair (T, Z) where $B(Z, w)$ has finite kernel and assume $\dim(T)$ is maximal. Suppose there is a cycle in $C^r_{\mathrm{alg}}(X)$ whose image under w does not lie in the image of $B(Z, w)$, and take a family $W(j)$ parametrized by an abelian variety J which deforms this cycle to 0. Construct a maximal abelian subvariety T' of TxJ containing $Tx0$, with $(T' \cap \mathrm{Ker}\,(B(Z \times J + T \times W, w)))$ finite. Then

$$\dim(T) < \dim(T'),$$

a contradiction.

A homomorphism $w : C^r_{\mathrm{alg}}(X) \to A(k)$ is *P-rational* (3) if A is a Picard variety $\mathrm{Pic}^0(Y)$ and w is $Z(.) : C^r_{\mathrm{alg}}(X) \to (C^1_{\mathrm{alg}}(Y)/\mathrm{rat}) = A(k)$ where $Z \in (C^{n-r+1}(X \times Y)/\mathrm{alg})$. For example, the natural homomorphism v: $C^1_{\mathrm{alg}}(X) \to \mathrm{Pic}^0(X)(k)$ is defined by the diagonal class on $X \times X$, and v: $C^n_{\mathrm{alg}}(X) \to \mathrm{Alb}\,(X)(k)$, by the Poincaré class π_X on $X \times \mathrm{Pic}^0(X)$; in both examples v is the universal surjective rational homomorphism, and in the first, $\mathrm{Ker}\,(v)$ is $C^1_{\mathrm{rat}}(X)$.

The P-rational homomorphism w is rational. For, if $W \in (C^r(T \times X)/\mathrm{alg})$, then $(Z \circ W)(t)$ represents $B(W, w)(t)$. However, $(Z \circ W) \in (C^1(T \times Y)/\mathrm{rat})$, so there is a morphism $f : T \to \mathrm{Pic}^0(Y)$ such that $Z \circ W = f^*\pi_Y$. A cycle is *Picard equivalent* to 0 if it lies in the kernel of every P-rational homomorphism; Picard equivalence is clearly adequate and coarser than abelian equivalence (One might boldly hope they coincide!).

Abelian (resp. Picard) equivalence $\sim$ would define continuous finiteness in the most refined sense if there existed an abelian variety A and a class $\pi \in (C^r(A \times X)/\sim)$ such that $\pi(.) : A(k) \to (C^r_{\mathrm{alg}}(X)/\sim)$ is bijective. Then (cf. [7], § 2), $w = \pi(.)^{-1}$ is rational (resp. P-rational) and universal (4), and any family $\{ Z(t) \in (C^r_{\mathrm{alg}}(X)/\sim) \}$ parameterized by a variety T, is the pull-black of $\{ \pi(a) \}$ under a map $f : T \to A$ and $f = B(Z, w)$.

It is an (unrecorded, 1964) observation of Grothendieck that $(C^r_{\mathrm{alg}}(X)/\mathrm{Pic})$ is limited

(3) It amounts to the same to consider compositions $C^r_{\mathrm{alg}}(X) \xrightarrow{W(\cdot)} (C^a_{\mathrm{alg}}(A)/\mathrm{Abl}) \xrightarrow{S} A(k)$ where $W \in (C^{n-r+a}(X \times A)/\mathrm{alg})$, A is an abelian variety of dimension a and S is the canonical sum map: given W, take $Y = \mathrm{Pic}^0(A)$; given Y, replace $A = \mathrm{Pic}^0(Y)$ by the jacobian of a general 1-dimensional linear space section of Y.

(4) Notice w can be obtained by melding the various rational (resp. P-rational) maps on $C^r_{\mathrm{alg}}(X)$ which distinguish from 0 those cycles not ~ 0.

by a family $\{\pi^r(p)\}$ (defined up to Picard equivalence) parametrized by an abelian variety $P^r(X)$ ([5]). For, given a P-rational homomorphism $w\colon C^r_{\mathrm{alg}}(X) \to A(k)$, construct (as above) an abelian variety P and a class $\pi \in (C^r(P \times X)/\mathrm{Pic})$ such that $f = B(\pi, w)$ is an isogeny from P to $A = \mathrm{Pic}^0(Y)$ and consider the commutative diagram of correspondences (where Z defines w):

$$\begin{array}{ccc} H^{(2n-2r+1)}(X) & \xleftarrow{{}^tZ(\cdot)} & H^{(2m-1)}(Y) \\ \big\downarrow {\scriptstyle {}^t\pi(\cdot)} & & \big\downarrow {\scriptstyle \pi_Y(\cdot)} \\ H^1(P) & \xleftarrow{\quad f^* \quad} & H^1(A) \end{array}$$

Since $\pi_Y(\,.\,)$ and f^* are isomorphisms (cf. [6], § 2, Appendix), $\dim(A) < \dim(H^{(2n-2r+1)}(X))$ and the process of melding the (w, A) is bound to finish.

Over the complexes, we also have (cf. Weil [14] and Lieberman [7]) the Weil-jacobian $J^r(X) = H^{2r-1}(X, \mathbb{R})/\mathrm{Im}\,(H^{2r-1}(X, \mathbb{Z}))$ and the Weil homomorphism

$$w\colon\ C^r_{\mathrm{hom}}(X) \to J^r(X)$$

where $C^r_{\mathrm{hom}}(X)$ denotes the group of cycles homologically equivalent to 0, the kernel of the cycle map $C^r(X) \to H^{2r}(X, \mathbb{R})$. The torus $J^r(X)$ has a structure of an abelian variety (that does not vary analytically) and $w \mid C^r_{\mathrm{alg}}(X)$ is a rational homomorphism; so $J^r_a(X) = w(C^r_{\mathrm{alg}}(X))$ is an abelian subvariety. Weil equivalence, defined by $\mathrm{Ker}\,(w)$, is adequate, finer than Picard equivalence and coarser than abelian equivalence. If homological and torsion ([6]) equivalence coincide on $A \times X$ for all abelian varieties A, then Weil and abelian equivalence coincide; if homological and numerical ([6]) equivalence coincide on $X \times J^r_a(X)$, then Weil and Picard equivalence coincide on X and $J^r_a(X)$ and $J^{n-r+1}_a(X)$ are dual abelian varieties. Now, $J^r_a(X)$ is contained in the largest complex torus in $\mathrm{Im}\,(H^{r-1,r}(X) \to J^r)$, but $w(C^r_{\mathrm{hom}}(X))$ is not; this observation led Griffiths [2] to his celebrated example (valid in any characteristic, cf. Katz [4]) of a 1-cycle on a 3-fold which is homologous to 0, but not torsion equivalent to 0.

It is generally conjectured that homological and numerical equivalence coincide on all X (in every characteristic). If there is a surjective map $f : Y \to X$, then the conjecture holds for X if it does for Y; in fact, for any adequate equivalence relation $\sim$ and any cycle Z on X, if $f^*Z \sim 0$ then $dZ \sim 0$ where d is the degree over X of an n-dimensional linear space section of Y (in view of the projection formula). If X is an abelian variety and C a 1-dimensional linear space section, then there are canonical surjections $\mathrm{Jac}\,(C) \to X$ and $C^{\times g} \to \mathrm{Jac}\,(C)$ for $g \gg 0$. Thus, to verify the conjecture for an abelian variety, we need only verify it for a product of curves, where it is obvious in characteristic 0. In fact, the conjecture follows from Grothendieck's two standard conjectures (cf. [5]): the Hodge index theorem for algebraic cycles (known in positive

([5]) If $X \mapsto H(X)$ denotes a Weil cohomology such as l-adic cohomology, then

$$\dim\,(P^r(X)) \leq \dim\,(H^{2r-1}(X));$$

in fact, $H(P^r(X))$ is a certain subspace of $H^{(2n-2r+1)}(X)$. Further, ${}^t\pi^{(n-r+1)} \circ \pi^r$ defines a surjection $P^r(X) \to \mathrm{Pic}^0(P^{(n-r+1)}(X))$, which has finite kernel by symmetry. Also, $P^1(X) = \mathrm{Pic}^0(X)$ and $P^n(X) = \mathrm{Alb}\,(X)$. This theory ought to be further explored.

([6]) A cycle is torsion (or τ —) equivalent to 0 if some (nonzero) multiple is algebraically equivalent to 0. Numerical equivalence is defined to render the intersection pairing nonsingular and is clearly the coarsest nontrivial adequate relation.

characteristic only for surfaces) and the algebricity of the cycle defining the $*$-operator (7).

The group $(C^r(X)/\text{alg})$ is countable and invariant under extension of the ground field after the theory of Chow coordinates; hence, we expect discrete finiteness here. In fact, the group $(C^r(X)/\text{num})$ is free of finite rank (8). A finer study (apparently a difficult study) of Chow coordinates might bound the number of maximal algebraic families of positive r-cycles of degree d by a polynomial in d. This bound would easily imply that $(C^r(X)/\tau)$ has finite rank. For $r = 1$, such a polynomial bound exists *a fortiori* because $(C^1(X)/\text{alg})$ has finite type (Néron-Severi theorem [12]) and distinct maximal families sufficiently close numerically to a polarization represent distinct cycle classes modulo algebraic equivalence.

For $r = 1$, the entire above theory is virtually satisfactory even within the sharper, richer context of schemes (cf. Grothendieck [3]) or better, algebraic spaces (cf. Artin [1]). The Picard space has well been constructed by methods which are moreover logically independent of any finiteness theorem. The finiteness theorems may then be stated in terms of limited families of invertible sheaves (generalizing divisor classes modulo rational equivalence). The key result (cf. [5], (3.13)) is: let X be a projective scheme over a noetherian base with geometrically integral fibers of dimension n and F a family of invertible sheaves L on these fibers. Then the following conditions are equivalent: (*i*) F is limited (9); (*ii*) There exists an integer A independent of L such that $A > |a_1|, -a_2$ where $\chi(L(x)) = \Sigma_{i=0}^{n} a_i \binom{x+i}{i}$ is the Hilbert polynomial; (*iii*) There exists an integer N independent of L such that $N > |\langle D \cdot H^{n-1} \rangle|$ and $N > -\langle D^2 \cdot H^{n-2} \rangle$ where $D = c_1(L)$ and $H = c_1(\mathcal{O}(1))$; (*iv*) There exists an integer N independent of L such that $L(N)$ and $L^{-1}(N)$ are ample. This theorem implies in particular (Matsusaka's result [9]) that numerical and torsion equivalence of divisors coincide and that $(C^1_\tau(X)/\text{alg})$ is finite. The proof of the theorem is achieved through development of a technique introduced in this connection by Mumford [10], and it does not rest on the traditional theory of Chow coordinates but rather gives the finiteness of the Hilbert and Chow schemes as corollaries.

REFERENCES

[1] M. Artin. — *Algebrization of formal moduli I*, Kodaira volume, Univ. Tokyo Press, Princeton Univ. Press (1969).

[2] P. Griffiths. — On the Periods of Certain Rational Integrals III, *Annals of Math.* (1969).

[3] A. Grothendieck. — FGA-Fondements de la géométrie algébrique, Extraits du *Séminaire Bourbaki* (1957-1962).

(7) The family of varieties with algebraic $*$-operators is stable under product, smooth hyperplane section and specialization and it contains curves (obvious), surfaces (Hodge-Grothendieck), abelian varieties (Lieberman [8]) and the usual rational varieties with cellular decompositions (Grothendieck).

(8) This theorem is a formal consequence of the deep theorem of existence of a Weil cohomology such as l-adic cohomology (cf. [6], (3.5)).

(9) Equivalently, the corresponding subset of the Picard scheme is quasi-compact.

[4] N. KATZ. — *Le théorème de Griffiths*, Exposé XX, SGA 7, I. H. E. S.
[5] S. KLEIMAN. — *Les théorèmes de finitude pour le foncteur de Picard*, Exposé XIII, SGA 6, I. H. E. S.
[6] —. — Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, North Holland (1968).
[7] D. LIEBERMAN. — Higher Picard varieties, *Amer. J. Math.* (1969).
[8] —. — Numerical and homological equivalence, *Amer. J. Math.* (1969).
[9] T. MATSUSAKA. — The criteria for algebraic equivalence and the torsion group, *Amer. J. Math.* (1957).
[10] D. MUMFORD. — *Lectures on curves on surfaces*, Princeton « Orange Series » (1966).
[11] —. — Rational equivalence of O-cycles on surfaces, *J. Math. Kyoto Univ.* (1969).
[12] A. NÉRON. — Problèmes arithmétiques, *Bull. Soc. Math.* (1952).
[13] P. SAMUEL. — Relations d'équivalence en géométrie algébrique, *Proc. Internat. Congress of Math.*, Cambridge, England (1958).
[14] A. WEIL. — On Picard varieties, *Amer. J. Math.* (1952).

Massachusetts Institute
of Technology
Cambridge,
Massachusetts 02139
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 451 à 456.

ONE DIMENSIONAL FORMAL COHOMOLOGY

by P. MONSKY

Let V be a variety over a field k. When $k = \mathbb{C}$, the cohomology groups of the analytic space attached to V are useful in the study of V. For arbitrary k it is natural to look for a purely algebraic substitute for these groups. Suppose for example that V is non-singular and affine. Let Ω^i be the sheaf of i-forms on V, $d: \Omega^i \to \Omega^{i+1}$ be exterior differentiation and $H^{\cdot}_{DR}(V)$ the homology of the complex $\Gamma(\Omega^0) \xrightarrow{d} \Gamma(\Omega^1) \xrightarrow{d} \ldots$ More generally if V is an arbitrary non-singular variety take $H^{\cdot}_{DR}(V)$ to be the hypercohomology of the complex of sheaves $\Omega^0 \xrightarrow{d} \Omega^1 \xrightarrow{d} \ldots$ $H^{\cdot}_{DR}(V)$ is known as the " De Rham cohomology " of V. When $k = \mathbb{C}$ Grothendieck has shown that

$$H^{\cdot}_{DR}(V) \approx H^{\cdot}(V_{\text{anal}}; \mathbb{C})$$

(see [1]). When k has characteristic 0, $V \mapsto H^{\cdot}_{DR}(V)$ is a good cohomology theory for non-singular varieties. But in characteristic $p > 0$, De Rham cohomology goes wrong. For example, when V is the affine line, $H^0_{DR}(V)$ and $H^1_{DR}(V)$ may be identified with the kernel and cokernel of the map $\dfrac{d}{dT}: k[T] \to k[T]$, spaces which are far too large. And pathology occurs even when V is complete.

Even so it appears likely that there is a satisfactory cohomology theory of De Rham type for varieties in characteristic p. The coefficient field however must be taken to be a complete discretely valued field of characteristic 0 with residue class field k rather than k itself. Indeed work done by Dwork and Katz, by Lubkin and by Washnitzer and me all seem to reflect aspects of a single underlying " p-adic " cohomology theory. Though this theory is far less developed than De Rham cohomology in characteristic 0 or the l-adic cohomology of Grothendieck and Artin, it is quite promising. In this talk I'll describe the approach taken by Washnitzer and me and then discuss some recent work of mine on H^1.

1

Let $(R, (\pi))$ be a complete mixed characteristic discrete valuation ring, $k = R/(\pi)$, and $K = R \bigotimes_{Z} Q$. If $\overline{A}$ is a finitely generated smooth k-algebra we shall define certain " formal cohomology groups " $H^i(\overline{A}; K)$ attached to the non-singular variety Spec $\overline{A}$; the $H^i(\overline{A}; K)$ will be vector spaces over K.

The definition makes use of a certain class of R-algebras; the " w. c. f. g. algebras ". An R-algebra A is said to be weakly complete if $\cap\, \pi^i A = (0)$, and every sum

$$\sum_0^{\infty} \pi^i p_i(a_1, \ldots, a_m)$$

with $a_i \in A$, $p_i \in R[X_1, \ldots, X_m]$ and $\deg p_i/(i+1)$ bounded above converges to an element of A in the π-adic topology. If A is an R-algebra let $\hat{A}$ be the completion of A with respect to the ideal (π) and $A^\dagger$ be the smallest weakly complete subalgebra of $\hat{A}$ containing A. $A^\dagger$ is known as the weak completion of A. The weak completion of $R[X_1, \ldots, X_m]$ may be identified with a ring of restricted power series over R. By a w. c. f. g. algebra we mean an R-algebra which is a homomorphic image of $R[X_1, \ldots, X_m]^\dagger$ for some m. If A is w. c. f. g. it is weakly complete, and $A/\pi^j A$ is a finitely generated R/π^j algebra for all j. One may develop a theory of differential forms on a w. c. f. g. algebra A. Namely, let $\Omega^{\cdot}_{A/R}$ be a free exterior algebra on $\Omega^1_{A/R}$, and $D^{\cdot}(A) = \Omega^{\cdot}_{A/R}/\cap\, \pi^j \Omega^{\cdot}_{A/R}$. Then the $D^i(A)$ are finite A modules and one may define a degree 1 exterior differentiation d on $D^{\cdot}(A)$. Let $H^{\cdot}(A)$ be the homology of the complex $D^0(A) \xrightarrow{d} D^1(A) \xrightarrow{d} \ldots$

Suppose $\bar{A}$ is finitely generated and smooth over k. By a weak formalization of $\bar{A}$ we mean an R-flat w. c. f. g. algebra A together with an isomorphism $A/\pi A \xrightarrow{\approx} \bar{A}$. Under a mild restriction on $\bar{A}$, which I'll ignore in this talk, such an A exists and is unique up to (non-canonical) isomorphism. If $\bar{A}$ and $\bar{B}$ have A and B as weak formalizations then any k-algebra map $\bar{f} : \bar{A} \to \bar{B}$ lifts to an R-algebra map $f : A \to B$ and any two liftings induce the same map $H^{\cdot}(A) \otimes Q \to H^{\cdot}(B) \otimes Q$. Thus the assignment $\bar{A} \mapsto H^{\cdot}(\bar{A}; K) = H^{\cdot}(A) \otimes Q$ is functorial. For full details, see [3].

Calculation of $H(\bar{A}; K)$ is difficult in general but there are scattered results. H^0 for example is easily handled; if $\bar{A}$ is the coordinate ring of an absolutely irreducible affine variety then $H^0(\bar{A}; K) = K$. H^1 is amenable to attack; I'll talk about this later. One case in which all of $H^{\cdot}(\bar{A}; K)$ may be computed is when $\bar{A}$ is the coordinate ring of the complement of a non-singular hypersurface in n-dimensional projective space. Then, $H^i(\bar{A}; K) = 0$ for $1 \le i \le n-1$, while $H^n(\bar{A}; K)$ is finite dimensional and coincides with a space introduced by Dwork in his study of the zeta-function of a hypersurface.

We come now to the question of " globalization ". If U is a non-singular affine variety over k set $H^i(U; K) = H^i(\Gamma(U); K)$. $U \mapsto H^i(U; K)$ are contravariant functors and one hopes to extend these functors to all non-singular varieties, affine or not. This seems to be hard; the trouble is that global liftings, even in a formal sense, need not exist.

One approach, satisfactory for H^1, is the following. $U \mapsto H^j(U; K)$ defines a pre-sheaf on the affine open sets of our given non-singular variety V; let $\mathscr{H}^j$ be the associated sheaf. In some cases the $\mathscr{H}^j$ may be used to give a satisfactory definition of $H^i(V; K)$. For example $U \mapsto H^1(U; K)$ is actually a sheaf and we set $H^1(V; K) = \Gamma(V, \mathscr{H}^1)$. There is no obvious way of defining $H^2(V; K)$; however $H^1(V, \mathscr{H}^1)$ and $\Gamma(V, \mathscr{H}^2)$ should be thought of as the algebraic and transcendental parts of $H^2(V; K)$. For $i > 2$ this approach to globalization breaks down; Lubkin and Washnitzer have proposed methods that may resolve the problem.

2

For the rest of this talk we'll be concerned with H^1, and shall assume for simplicity that k is algebraically closed. Let $\bar{V}$ and $\bar{W}$ denote non-singular varieties over k. Our main results are the following:

(1) $H^1(\overline{V}; K)$ is finite dimensional.

(2) If $\overline{V}$ and $\overline{W}$ are irreducible, then $H^1(\overline{V} \times \overline{W}; K) \approx H^1(\overline{V}; K) \oplus H^1(\overline{W}; K)$.

(3) Let $\varphi : \overline{V} \to \overline{W}$ be a morphism with dense image. Then

$$\varphi^* : \quad H^1(\overline{W}; K) \to H^1(\overline{V}; K)$$

is injective.

(4) Suppose there is a scheme V, smooth and projective over R such that $V \underset{R}{\times} k \approx \overline{V}$. Let V' be the variety $V \underset{R}{\times} K$. Then $H^1(\overline{V}; K) \approx H^1_{DR}(V')$. If $\mathrm{Alb}(\overline{V})$ is the Albanese variety of $\overline{V}$, then $\dim H^1(V; K) = 2 \cdot \dim \mathrm{Alb}(\overline{V})$.

(5) Suppose $\overline{V}$ is complete and non-singular in codimension 1 and $\overline{W}$ is the set of regular points of $\overline{V}$. Then, $\dim H^1(\overline{W}; K) \geqq 2 \cdot \dim \mathrm{Alb}(\overline{V})$.

(1) and (2) are difficult; I'll discuss the proof of (1) later. (3) reduces easily to the case when $\overline{V}$ is a dense open subset of $\overline{W}$; this is handled by Meredith in his thesis. The first part of (4) comes directly from a comparison theorem proved by Meredith in [2], relating the cohomology of a coherent sheaf on $\mathbb{P}^n(R)$ to the cohomology of the " weak completion " of the sheaf. To prove the second part let $\mathrm{Alb}(V')$ be the Albanese variety of V'. Since K has characteristic 0, the Hodge spectral sequence for V' degenerates and $\dim H^1_{DR}(V') = h^{0,1}(V') + h^{1,0}(V')$. As we're in characteristic 0, $h^{0,1}(V') = h^{1,0}(V') = \dim \mathrm{Alb}(V') = \dim \mathrm{Alb}(\overline{V})$, completing the proof. Turning to (5), let $\varphi : \overline{W} \to \mathrm{Alb}(\overline{V})$ be the obvious map. The image of φ generates $\mathrm{Alb}(\overline{V})$; some formalism using (2) and (3) shows that $\varphi^* : H^1(\mathrm{Alb}(\overline{V}); K) \to H^1(\overline{W}; K)$ is injective. Now Mumford has shown that all Abelian varieties are liftable. So by (4),

$$\dim H^1(\overline{W}; K) \geq \dim H^1(\mathrm{Alb}(\overline{V}); K) = 2 \cdot \dim \mathrm{Alb}(\overline{V}).$$

It seems likely that equality always holds in (5); i. e. that φ^* is actually bijective. The analogous result for De Rham cohomology in characteristic 0 follows easily from the analytic definition of the Albanese.

3

In this section and the next we'll sketch a proof of the finite dimensionality of $H^1(\overline{V}; K)$, assuming k algebraically closed for simplicity. First we describe two of the basic tools; the Gysin sequence and the differentiation of cohomology classes with respect to parameters (i. e. the Gauss-Manin-Grothendieck-Katz-Oda connection).

Let $\mathcal{O}$ be a base ring and A be a finitely generated $\mathcal{O}$ algebra. Suppose $t \in A$ is not a zero-divisor, and that A and $A/(t)$ are smooth over $\mathcal{O}$. Let $H^{\cdot}_Q(A/\mathcal{O})$, or more briefly $H^{\cdot}_Q(A)$, be the homology of the complex $\Omega^{\cdot}_{A/\mathcal{O}} \otimes Q$. Define $H^{\cdot}_Q(A_t)$ and $H^{\cdot}_Q(A/(t))$ similarly. Then there is a long exact Gysin sequence:

$$\to H^{i-2}_Q(A/(t)) \to H^i_Q(A) \to H^i_Q(A_t) \to H^{i-1}_Q(A/(t)) \to$$

Suppose next that A is finitely generated and smooth over $\mathcal{O}$. Then the derivations of $\mathcal{O}$ operate on the homology $H^{\cdot}(A)$ of $\Omega^{\cdot}_{A/\mathcal{O}}$. More precisely, each $\Delta : \mathcal{O} \to \mathcal{O}$ induces an operator $\Delta_* : H^{\cdot}(A) \to H^{\cdot}(A)$ such that $\Delta_*(b\alpha) = \Delta b \cdot \alpha + b \cdot \Delta_*(\alpha)$ for all $b \in \mathcal{O}$. The operators Δ_* commute with all mappings of finitely generated smooth $\mathcal{O}$-algebras, and with the maps in the Gysin sequence.

We begin the proof that $H^1(\bar{V}; K)$ is finite dimensional. One may assume that $\bar{V}$ is affine and irreducible. Let k'' be the function field of $\bar{V}$. It proves sufficient to show the finite dimensionality of H^1 for any one particular affine model of k''/k. Also we are free to replace k'' by any finite extension. We argue by induction on $r = \text{t.d.}\, k''/k$. $r = 0$ is trivial; for the rest of this section assume that $r = 1$.

Let $f(X, Y) = 0$ be an affine plane model of k''/k of degree n having d ordinary double points. We may assume that the coefficient of Y^n in f is 1, and that f has n distinct points at infinity. There is a plane curve $g(X, Y) = 0$ of degree m which passes through all the double points of f and has $mn - 2d$ additional simple intersections with f, none of them at infinity. $\bar{A} = (k[X, Y]/f)_g$ is a non-singular affine model of k''/k; we'll show directly that $H^1(\bar{A}; K)$ is finite dimensional.

Using arguments from Severi [5], and the completeness of R we can find an $F \in R[X, Y]$ of degree n lifting f and having d ordinary double points. We can further construct a G in $R[X, Y]$ of degree m lifting g and passing through the double points of F. Let $A_0 = (R[X, Y]/F)_G$ and A be the weak completion of A_0. A is a weak formalization of $\bar{A}$. $H_Q^{\cdot}(A_0)$ and $H_Q^{\cdot}(A)$ will denote the homology of the complexes $\Omega^{\cdot}_{A_0/R} \otimes Q$ and $D^{\cdot}(A) \otimes Q$. It suffices to show that $H_Q^1(A_0)$ is finite dimensional and that

$$H_Q^1(A_0) \to H_Q^1(A)$$

is onto.

Denote the images of X and Y in A_0 by x and y and set $u = G(x, y)^{-1}$. $A_0 = R[x, y, u]$, and dx and dy generate $\Omega^1_{A_0/R}$. Since $F(x, y) = 0$, $\Omega^1_{A_0/R}$ is spanned as an R-module by the forms $u^i \chi^j \omega$ where ω runs through the finite set

$$\{ dx, dy, ydx, ydy, \ldots, y^{n-1}dx, y^{n-1}dy \}.$$

Let p be the characteristic of k and $\lambda(s) = [\log_p(s + 1)]$ for $s \geq 0$. One sees easily that it suffices to prove the following:

Let $\omega \in \Omega^1_{A_0/R}$. Then there is an integer s, a constant c, and a finite R-module M of 1-forms such that for all i and $j \geq 0$ we have $p^{s+\lambda(i+j)} u^i x^j \omega = dh_{ij}(x, y, u) + \omega_{ij}$ where h_{ij} has coefficients in R and degree $\leq c(i + j + 1)$, and $\omega_{ij} \in M$.

So what we need is a method for studying all the $u^i x^j \omega$ simultaneously. This is done by the following trick. Introduce indeterminates T_1 and T_2. Then

$$\theta = \omega/(1 - T_1 u)(1 - T_2 x)$$

is a 1-form which carries information about all the $u^i x^j \omega$; information which may be extracted by expanding θ in powers of T_1 and T_2.

More precisely, let $\mathcal{O}$ be the localization of $R[[T_1, T_2]]$ with respect to the powers of $T_1 T_2$. By analyzing the intersections of $F(X, Y) = 0$ with the curves $G(X, Y) = T_1$ and $X = T_2^{-1}$ one may show that $A_0 \underset{R}{\otimes} \mathcal{O}/(1 - T_1 u)(1 - T_2 x)$ is isomorphic as $\mathcal{O}$ algebra with $\mathcal{O}^{mn+n}$. Thus both $A_0 \otimes \mathcal{O}$ and $A_0 \otimes \mathcal{O}/(1 - T_1 u)(1 - T_2 x)$ are smooth over $\mathcal{O}$ and we have a Gysin sequence. Let $\mathcal{O}'$ be the localization of $A_0 \otimes \mathcal{O}$ with respect to the powers of $(1 - T_1 u)(1 - T_2 x)$. The Gysin sequence in this situation is just the short exact sequence:

$$0 \to H_Q^1(A_0/R) \otimes \mathcal{O} \xrightarrow{i} H_Q^1(\mathcal{O}'/\mathcal{O}) \xrightarrow{j} \mathcal{O}^{mn+n} \otimes Q \to 0$$

Now $\theta = \omega/(1 - T_1 u)(1 - T_2 x)$ may be interpreted as an element of $\Omega^1_{\mathcal{O}'/\mathcal{O}}$; we shall use the above exact sequence to get information about θ.

Any θ in $\Omega^1_{\mathcal{O}'/\mathcal{O}} \otimes Q$ may be " expanded " as $\Sigma L_{ij}(\theta) T_1{}^i T_2{}^j$ where the $L_{ij}(\theta)$ are in $\Omega^1_{A_0/R} \otimes Q$. Consider the following 2 conditions on θ:

(*a*) There exists an integer s, a constant c, and a finite R-module M of 1-forms such that for all i and j we have $p^s L_{ij}(\theta) = dh_{ij}(x, y, u) + \omega_{ij}$ where h_{ij} has coefficients in R and degree $\leq c(|i| + |j| + 1)$, and all $\omega_{ij} \in M$.

(*b*) There exists an integer s, a constant c, and a finite R-module M of 1-forms such that for all i and j we have $p^{s+\lambda(|i|+|j|)} L_{ij}(\theta) = dh_{ij}(x, y, u) + \omega_{ij}$ where h_{ij} has coefficients in R and degree $\leq c(|i| + |j| + 1)$, and all $\omega_{ij} \in M$.

Note first that every exact θ and every θ in $\Omega^1_{A_0/R}$ satisfies (*a*). Since an $\mathcal{O} \otimes Q$ linear combination of forms satisfying (*a*) also satisfies (*a*), we find that (*a*) holds for every θ which represents an element of $H^1_Q(\mathcal{O}'/\mathcal{O})$ that lies in the image of i. Let θ_k be elements of $\Omega^1_{\mathcal{O}'/\mathcal{O}} \otimes Q$ whose images under j are the basic idempotents in $\mathcal{O}^{mn+n} \otimes Q$. We show that the θ_k satisfy (*b*). Observe that the derivations $\dfrac{\partial}{\partial T_1}$ and $\dfrac{\partial}{\partial T_2}$ of $\mathcal{O}$ operate on $H^1_Q(\mathcal{O}'/\mathcal{O})$ and that $j\left(\dfrac{\partial \theta_k}{\partial T_1}\right) = \dfrac{\partial}{\partial T_1} j(\theta_k) = 0$. So $\partial\theta_k/\partial T_1$ represents an element in the image of i, and the same is true of $\partial\theta_k/\partial T_2$. When $i \neq 0$, $L_{ij}(\theta_k) = \dfrac{1}{i} L_{i-1,j}\left(\dfrac{\partial \theta_k}{\partial T_1}\right)$; when $j \neq 0$, $L_{ij}(\theta_k) = \dfrac{1}{j} L_{i,j-1}\left(\dfrac{\partial \theta_k}{\partial T_2}\right)$. Since (*a*) holds for $\dfrac{\partial \theta_k}{\partial T_1}$ and $\dfrac{\partial \theta_k}{\partial T_2}$, an easy calculation shows that (*b*) holds for θ_k. But an $\mathcal{O} \otimes Q$ linear combination of forms satisfying (*b*) also satisfies (*b*). Thus (*b*) holds for all θ, and taking $\theta = \omega/(1 - T_1 u)(1 - T_2 x)$ with ω in $\Omega^1_{A_0/R}$ we get the desired estimates.

4

If t. d. $k''/k > 1$ things are more complicated. We choose k' so that $k \subset k' \subset k''$, t. d. $k''/k' = 1$ and k''/k' admits an absolutely irreducible absolutely non-singular projective model. By taking a suitable plane projection of this model and extending k' and k'' finitely if necessary we can find f and g in $k'[X, Y]$ as in the last section, f being an affine plane model of k''/k' with d ordinary double points. Take $\bar{B}$ to be a finitely generated smooth k-algebra with quotient field k', containing the coefficients of f and g and $\bar{A}$ to be $(\bar{B}[X, Y]/f)_g$. The generic fibre of the map

$$\bar{\varphi}: \operatorname{Spec} \bar{A} \to \operatorname{Spec} \bar{B}$$

is a projective plane curve with d ordinary double points from which the double points and $mn + n - 2d$ additional points have been removed. Replacing $\bar{B}$ by a localization we may assume that every fibre of $\bar{\varphi}$ looks like this.

If B is a weak formalization of $\bar{B}$ then $\bar{\varphi}$ may be lifted to a good family of curves over Spec B. More precisely one can find F and G in $B[X, Y]$ lifting f and g such that every fibre of the map φ: Spec $(B[X, Y]/F)_G \to$ Spec B has the description just given. Again this is done using ideas from Severi and a form of Hensel's lemma for weakly complete algebras. Let $A_0 = (B[X, Y]/F)_G$ and A be the weak completion of A_0; A is a weak formalization of $\bar{A}$. Set $D^{\cdot}(A/B) = \Omega^{\cdot}(A/B)/\cap \pi^j\Omega^{\cdot}(A/B)$. The $D^i(A/B)$ are finite A modules and $D^i(A/B) = 0$ for $i > 1$.

One shows directly that $H^0(D^{\cdot}(A/B)) = B$ and deduces from this an exact sequence:

$$0 \to H^1_Q(B) \to H^1_Q(A) \xrightarrow{\sigma} H^1(D^{\cdot}(A/B) \otimes Q)$$

Since $H^1_Q(B) = H^1(\bar{B}; K)$ is finite dimensional by the induction assumption, it suffices to show that the image of σ is finite dimensional over K. Now the R-linear derivations of B may be shown to act on $H^1(D^{\cdot}(A/B) \otimes Q)$, and image σ is annihilated by all the Δ_*. So it's enough to show that the intersection of the kernels of the Δ_* is finite-dimensional over K.

By a generalization of the argument sketched in the last section one shows that $H^1(D^{\cdot}(A/B) \otimes Q)$ is a finite projective $B \otimes Q$ module. The finite dimensionality of $\cap \ker \Delta_*$ is then a straightforward argument with formal differential equations. Full details will appear in [4].

REFERENCES

[1] A. Grothendieck. — On the De Rham cohomology of algebraic varieties, *Pub. Math.*, I. H. E. S., Paris, 29 (1966).

[2] D. Meredith. — Weak formal preschemes and the Monsky-Washnitzer cohomology groups, Brandeis Univ. thesis (1969).

[3] P. Monsky and G. Washnitzer. — Formal cohomology I, *Ann. of Math.*, 88 (1968), pp. 181-217.

[4] P. Monsky. — Formal cohomology IV, to appear.

[5] F. Severi. — *Vorlesungen über algebraische geometrie*, pp. 316-317.

Brandeis University
Department of Mathematics,
Waltham,
Massachusetts 02154
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 457 à 465.

THE STRUCTURE OF THE MODULI SPACES OF CURVES AND ABELIAN VARIETIES

by DAVID MUMFORD

§ 1. The purpose of this talk is to collect together what seem to me to be the most basic moduli spaces (for curves and abelian varieties) and to indicate some of their most important interrelations and the key features of their internal structure, in particular those that come from the theta functions. We start with abelian varieties. Fix an integer $g \geqslant 1$. To classify g-dimensional abelian varieties, the natural moduli spaces are:

$$\mathscr{A}^{(n)} = \left\{ \begin{array}{l} \text{moduli space of pairs } (X, \lambda),\ X \text{ a } g\text{-dimensional} \\ \text{abelian variety, } \lambda: X \to \hat{X} \text{ a polarization such} \\ \text{that } \deg(\lambda) = n^2 \end{array} \right\}$$

Here and below when we talk of a moduli space, we mean a coarse moduli space in the sense of [11], p. 99 and in all cases these moduli spaces will actually exist as schemes of finite type over Spec ($\mathbf{Z}$). This can be proven by the methods of [11], Ch. 7, for instance, which also shows that all the moduli spaces used are quasi-projective at least over every open set Spec $\mathbf{Z}\left[\frac{1}{p}\right]$.

The local structure of $\mathscr{A}^{(n)}$ seems quite difficult to work out at some points. However, for every sequence $\delta_1, \ldots, \delta_g$ such that $\delta_1 \mid \ldots \mid \delta_g$, $\prod_{i=1}^{g} \delta_i = n$, let

$$\mathscr{A}^{(\delta)} = \left\{ \begin{array}{l} \text{the open subscheme of } \mathscr{A}^{(n)} \text{ of pairs } (X, \lambda) \\ \text{such that} \\ \qquad \ker(\lambda) \cong \prod_1^g \mathbf{Z}/\delta_i\mathbf{Z} \times \prod_1^g \mu_{\delta_i} \end{array} \right\}$$

The $\mathscr{A}^{(\delta)}$'s are disjoint and exhaust all of $\mathscr{A}^{(n)}$ except for (X, λ)'s such that char$|$n and ker (λ) contains a subgroup isomorphic to α_p. The local structure of $\mathscr{A}^{(\delta)}$ is not hard to work out (using results of Serre-Tate [20], and Grothendieck and myself on the formal deformation theory of abelian varieties and p-divisible groups, see Oort [17]). In particular all components of $\mathscr{A}^{(\delta)}$ dominate Spec ($\mathbf{Z}$). Now I have proven that for all n and all p, the open subset of $\mathscr{A}^{(n)} \times$ Spec $\mathbf{Z}/p\mathbf{Z}$ of (X, λ)'s such that X is ordinary (*) is *dense* (cf. [14] for a sketch of the proof). Therefore $\bigcup_\delta \mathscr{A}^{(\delta)}$ is dense in $\mathscr{A}^{(n)}$. Since $\mathscr{A}^{(\delta)} \times$ Spec ($\mathbf{C}$) is irreducible (see below), it follows that the components of $\mathscr{A}^{(n)}$ are the closures $\overline{\mathscr{A}}^{(\delta)}$ of the $\mathscr{A}^{(\delta)}$ and that all of them dominate Spec ($\mathbf{Z}$). It is *not*

(*) i. e. has the maximal number p^g of points of order p.

known, however, whether the geometric fibres of $\mathscr{A}^{(\delta)}$ over finite primes are irreducible or not.

Now these various schemes $\mathscr{A}^{(n)}$ are all related by the isogeny correspondences:

$$Z_{n_1,n_2,k} = \left\{ (X, \lambda)\varepsilon\mathscr{A}^{(n_1)}, (Y, \mu)\varepsilon\mathscr{A}^{(n_2)} \;\middle|\; \begin{array}{l} \exists \text{ an isogeny } \pi : X \to Y \\ \text{of degree } k \text{ such that} \\ n_1{}^2\hat{\pi}\circ\mu\circ\pi = (kn_2)^2\lambda \end{array} \right\}$$

To uniformize all of these, one introduces a second more convenient sequence of moduli spaces. Firstly, over the base scheme $Z[\zeta_n]$, ζ_n a primitive n-th root of 1, let

$$\mathscr{A}_n^* = \left\{ \begin{array}{l} \text{moduli space of triples } (X, \lambda, \alpha),\ X \text{ a } g\text{-dimensional} \\ \text{abelian variety, } \lambda : X \xrightarrow{\approx} \hat{X} \text{ a principal polarization,} \\ \text{and } \alpha : X_n \xrightarrow{\sim} (Z/nZ)^g \times \mu_n^g \text{ a symplectic isomorphism} \end{array} \right\}$$

These spaces are normal and irreducible and form a tower with respect to the natural quasi-finite morphisms $\mathscr{A}_{nm}^* \to \mathscr{A}_n^*$ given by $(X, \lambda, \alpha) \mapsto (X, \lambda, \operatorname{res}_{X_n}\alpha)$. Secondly, we enlarge these schemes somewhat by letting $\mathscr{A}_n$ be the normalization of $\mathscr{A}_1$ in the field of rational functions $Q(\mathscr{A}_n^*, \zeta_n)$. Then $\mathscr{A}_n$ is a normal irreducible scheme in which $\mathscr{A}_n^*$ is an open subscheme, and the $\mathscr{A}_n$'s form a tower with respect to finite morphisms $\mathscr{A}_{nm} \to \mathscr{A}_n$. Note that $\mathscr{A}_n = \mathscr{A}_n^*$ except over primes dividing n. Moreover, if $n \geqslant 3$, $\mathscr{A}_n$ is smooth over Z except at non-ordinary abelian schemes in characteristics dividing n. Next, we can uniformize very nearly all of $\mathscr{A}^{(\delta)}$ by the natural morphism:

$$\begin{gathered} \mathscr{A}_{\delta_g}^* \to \mathscr{A}^{(\delta)} \\ (X, \lambda, \alpha) \mapsto (Y, \mu) \end{gathered}$$

where Y is the etale covering of X defined by requiring its dual to be the quotient:

$$\hat{Y} = \hat{X}/\alpha^{-1}[(0) \times \Pi\mu_{\delta_i}],$$

and μ is the polarization on Y induced by λ. In the tower $\{ \mathscr{A}_n \}$ one now has the Hecke ring of correspondences instead of the isogeny correspondences. These come essentially from 2 types of morphisms:

(*a*) $Q(\mathscr{A}_n, \zeta_n)$ is a Galois extension of $Q(\mathscr{A}_1, \zeta_n)$ with Galois group $\mathrm{Sp}(2g, Z/nZ)$, hence $\mathrm{Sp}(2g, Z/nZ)$ acts as a group of automorphisms of $\mathscr{A}_n$;

(*b*) the morphism

$$\begin{gathered} \mathscr{A}_n^* \to \mathscr{A}_1 \\ (X, \lambda, \alpha) \mapsto (Y, \mu) \end{gathered}$$

(where $Y = X/\alpha^{-1}[(Z/nZ)^g \times (0)]$, and if $\pi : X \to Y$ is the natural map, then $\mu : Y \xrightarrow{\sim} \hat{Y}$ is determined by the requirement $\hat{\pi}\circ\mu\circ\pi = n\lambda$). For a discussion on Hecke operators in the classical case, see Shimura [21]. The picture is even clearer when you pass to an inverse limit: e. g. for all n,

$$\varprojlim_k \mathscr{A}_{n^k} \times \operatorname{Spec} R_n$$

where

$$R_n = Z\left[\frac{1}{n}, \zeta_n, \zeta_{n^2}, \ldots\right]$$

exists as a scheme and $\prod_{p|n} \mathrm{Sp}(2g, Q_p)$ acts on it (See [12], § 9 for the case $n = 2$).

Over the complex ground field, these moduli spaces have well-known analytic uniformizations coming from the theory of Siegel modular forms:

$$\begin{aligned}
\mathscr{A}^{(n)} \times \operatorname{Spec}(C) &= \coprod_{\delta} \mathscr{A}^{(\delta)} \times \operatorname{Spec}(C) \\
\mathscr{A}^{(\delta)} \times \operatorname{Spec}(C) &= \mathfrak{H}/\Gamma_{\delta} \\
\mathscr{A}_n \times \operatorname{Spec}(C) &= \mathscr{A}_n^* \times \operatorname{Spec}(C) = \mathfrak{H}/\Gamma(n)
\end{aligned}$$

where

$$\mathfrak{H} = \text{Siegel upper } \frac{1}{2} - \text{plane} = \left\{ Z \;\middle|\; \begin{array}{l} Z = g \times g \text{ complex matrix} \\ {}^tZ = Z,\ \operatorname{Im} Z > 0 \end{array} \right\}$$

$$\begin{aligned}
\Gamma(n) &= \{ A \in \operatorname{Sp}(2g, Z)/(\pm I) \mid A = I_{2g} \bmod n \} \\
\Gamma_{\delta} &= \{ A \in GL(2g, Z)/(\pm I) \mid {}^tA . J_{\delta} . A = J_{\delta} \},
\end{aligned}$$

where

$$J_{\delta} = \left(\begin{array}{c|c} 0 & \begin{matrix} \delta_1 & & \\ & \ddots & \\ & & \delta_g \end{matrix} \\ \hline \begin{matrix} -\delta_1 & & \\ & \ddots & \\ & & -\delta_g \end{matrix} & 0 \end{array} \right)$$

Thus $\mathfrak{H}$ is the analytic " inverse limit " of the $\mathscr{A}_n$'s over Spec C. All the irreducibility assertions made so far are proven by these analytic uniformizations.

$$\begin{tikzcd}
\vdots \arrow[d] & & & \\
\mathscr{A}_n \arrow[d] \arrow[r, phantom, "\supset"] & \mathscr{A}_n^* \arrow[dr] \arrow[ddr] & & \\
\vdots \arrow[d] & & \mathscr{A}^{(\delta)} \arrow[r, phantom, "\subset"] & \mathscr{A}^{(n)} \\
\mathscr{A}_1 & & \mathscr{A}^{(\delta')} \arrow[ur, phantom, "\subset"] &
\end{tikzcd}$$

Summary of moduli spaces.

§ 2. The next point is that there is a moduli space intermediate in the tower between $\mathscr{A}_n^*$ and $\mathscr{A}_{2n}^*$ on which there are *canonical coordinates.* Following Igusa, we christen this $\mathscr{A}_{n,2n}^*$ and it is defined as follows in char. $\neq 2$:

$$\mathscr{A}_{n,2n}^* = \left\{ \begin{array}{l} \text{moduli space of triples } (X, L, \alpha),\ X \text{ an abelian} \\ \text{variety of dimension } g,\ L \text{ an ample symmetric} \\ \text{invertible sheaf, } \alpha \text{ a symmetric isomorphism:} \\ \qquad \alpha : \mathscr{G}(L) \xrightarrow{\sim} G_m \times (Z/nZ)^g \times \mu_n^g \\ \text{such that} \\ \quad i) \text{ if } n \text{ even, } e_*^L \equiv 1 \text{ on } X_2, \\ \quad ii) \text{ if } n \text{ odd, } e_*^L \text{ takes the value } +1 \text{ more often} \\ \text{than the value } -1. \end{array} \right\}$$

For definitions of $\mathscr{G}(L)$, e_*^L, etc., see [12], § 1, 2 and [15], § 23. There is an obvious map

$$\begin{aligned} \mathscr{A}^*_{n,2n} &\to \mathscr{A}^*_n \\ (X, L, \alpha) &\mapsto \left(X, \frac{1}{n}\varphi_L, \overline{\alpha}\right) \end{aligned}$$

where $\overline{\alpha}$ is the induced map from $\mathscr{G}(L)/G_m \cong X_n$ to $(Z/nZ)^g \times \mu_n^g$. There is a not so obvious map $\mathscr{A}^*_{2n} \times \operatorname{Spec} Z\left[\frac{1}{2}\right] \to \mathscr{A}^*_{n,2n}$ (see [12], § 2). Over C, $\mathscr{A}^*_{n,2n}$ is simply the quotient $\mathfrak{H}/\Gamma(n, 2n)$, where $\Gamma(n, 2n)$ is the subgroup between $\Gamma(n)$ and $\Gamma(2n)$ described by Igusa [9]. Canonical coordinates on $\mathscr{A}^*_{n,2n}$ (where $n \geqslant 2$) are defined as follows:

i) $\mathscr{G}(L)$ and hence $G_m \times (Z/nZ)^g \times \mu_n^g$ acts on $H^0(X, L)$. Write this action as $U_{(\lambda,a,b)}: H^0(X, L) \to H^0(X, L)$,

ii) there is a section $\sigma \in H^0(X, L)$ unique up to scalars such that $U_{(1,0,c)}\sigma = \sigma$, all $c \in \mu_n^g$,

iii) let $\sigma \to \sigma(0)$ denote evaluation of sections at $0 \in X$. We obtain a function:

$$\begin{aligned} (Z/nZ)^g &\to K \\ \alpha &\mapsto (U_{(1,\alpha,0)}\sigma)(0) \end{aligned}$$

unique up to multiplication by a constant, which is never identically zero.

iv) If $N = n^g - 1$, and the homogeneous coordinates of P_N are put in one-one correspondence with the elements of $(Z/nZ)^g$, this defines a morphism:

$$\Theta : \mathscr{A}^*_{n,2n} \to P_N$$

THEOREM. — If $n \geqslant 4$, Θ is an immersion.

This theorem was proven over C for various n's by Baily [4] and Igusa [9]; in the general case, all the essentials for the proof are in [13]. Over C, Θ is the morphism defined by

$$Z \mapsto \left(\ldots, \theta_{nZ}\begin{bmatrix} 0 \\ \alpha/n \end{bmatrix}(0), \ldots\right)_{\alpha \in (Z/nZ)^g}$$

where $Z \in \mathfrak{H}$, and θ is Riemann's theta function. If $8 \mid n$, one can even find a finite set of homogeneous quartic polynominals—Riemann's theta relations—such that the image of Θ is an open part of the subscheme of P_N defined by these quartics (see [12], § 6).

Even in the char. p case, it is possible to reformulate these canonical coordinates as values of a type of theta function. These theta functions are not functions on the universal covering space of X, but rather on the Tate group.

If p = char. of ground field,

$V(X)$ = group of sequences $\{x_i\}$, $i \geqslant 1$ but $p \nmid i$, where $x_i \in X$, $nx_{in} = x_i$ and x_1 has finite order k prime to p.

Let $T(X) = \{(x_i) \in V(X)$ such that $x_1 = 0\}$.

We get an exact sequence:

$$0 \to T(X) \to V(X) \to (\text{torsion on } X \text{ prime to } p) \to 0$$

We use the result:

THEOREM. — Let L be an ample symmetric invertible sheaf of degree 1 on an abelian variety X of char. p. If $p \nmid 2n$, then for all $x \in X_n$ for every choice of a point $y \in X$ such that $2ny = x$, there is a canonical isomorphism:

$$L \otimes_{\mathcal{O}_X} k(x) \cong L \otimes_{\mathcal{O}_X} k(0)$$

COROLLARY. — If $\sigma \in \Gamma(L)$, then evaluating σ via the above isomorphisms defines a function

$$\theta: V(X) \to L \otimes_{\mathcal{O}_X} k(0) \cong k$$

such that if $x \in \frac{1}{n} T(X)$, then $\theta(x + y) = \theta(x)$ if $y \in 2nT(X)$.

In fact the functions that we obtain in this way have the following properties:

a) $$\theta(x + a) = e_*\left(\frac{a}{2}\right)e\left(\frac{a}{2}, x\right)\theta(x), \; x \in V(X), \; a \in T(X)$$

where

$$e_*: \frac{1}{2} T(X) \to \{\pm 1\} \qquad \text{and} \qquad e: V(X) \times V(X) \to k^*$$

are the functions induced by e_*^L and e_n on $V(X)$.

b) $\theta(-x) = \pm\,\theta(x)$, the sign depending on the Arf invariant of e_*^L.

c) $$\prod_{i=1}^{4} \theta(x_i) = 2^{-g} \sum_{\eta \in \frac{1}{2}T(X)/T(X)} e(y, \eta)(\prod_{i=1}^{4} \theta(x_i + y + \eta)),$$

where

$$y = -\frac{1}{2}\Sigma x_i$$

d) $$\forall x \in V(X), \qquad \exists \eta \in \frac{1}{2} T(X) \qquad \text{such that} \qquad \theta(x + \eta) \neq 0.$$

e) Up to an elementary linear transformation whose coefficients are roots of 1, the set of values of θ on $\frac{1}{n} T(X)$ is equal to the set of values of the canonical coordinates Θ on the triple (X, L^{n^2}, α) (for any symmetric α).

f) Over $\mathbf{C}$, if Z is a period matrix for X, θ is essentially the function $a \mapsto \theta_Z[a](0)$, $a \in \mathbf{Q}^{2g}$.

g) Moreover, if we restrict the domain to $V_2(X)$, this 2-adic Tate group, all functions $\psi: V_2(X) \to k$ satisfying *a)*, *b)*, *c)* and *d)* arise from a unique principally polarized abelian variety.

(Cf. [12], § 8 through § 12).

§ 3. We turn next to curves. Fix $g \geqslant 2$. Let

$$\mathcal{M} = \left\{ \begin{array}{c} \text{moduli space of non-singular} \\ \text{complete curves } C \text{ of genus } g \end{array} \right\}$$

$\mathcal{M}$ is not only irreducible, but it has irreducible geometric fibres over Spec ($\mathbf{Z}$), cf. [5]. This is proven by introducing a compacification $\overline{\mathcal{M}}$ of $\mathcal{M}$, where

$$\overline{\mathcal{M}} = \left\{ \begin{array}{l} \text{moduli space of stable complete curves } C \\ \text{such that } \dim H^1(o_C) = g \end{array} \right\}$$

and where a *stable curve* is one with at most ordinary double points and such that every non-singular rational component has at least 3 double points on it.

$\overline{\mathcal{M}}$ has recently been proven by F. Knudsen, Seshadri and my self to be a scheme projective over $\mathbf{Z}$

Define:

$$\begin{aligned} t: \mathcal{M} &\to \mathcal{A}_1 \\ C &\mapsto (\mathrm{Pic}^0\,(C), \lambda) \end{aligned}$$

where λ is the theta polarization, viz: fixing a base point x_0 on C, we obtain a morphism:

$$\begin{aligned} \phi: C &\to \mathrm{Pic}^0\, C \\ x &\mapsto \text{class of } o_C(x - x_0) \end{aligned}$$

hence

$$\widehat{\mathrm{Pic}^0}\, C = \mathrm{Pic}^0\,(\mathrm{Pic}^0\, C) \overset{\phi^*}{\to} \mathrm{Pic}^0\,(C)$$

and $\lambda = -(\phi^*)^{-1}$.

According to Torelli's theorem (cf. [1], [10]), t is injective on geometric points. Its image however is not closed since t extends to a morphism on $\tilde{\mathcal{M}}$:

$$\left\{ \begin{array}{l} \text{Stable curves made from} \\ \text{non-singular components} \\ \text{connected together like a} \\ \text{tree} \end{array} \right\} = \begin{tikzcd} \overline{\mathcal{M}} \\ \tilde{\mathcal{M}} \arrow[u, phantom, "\cup"] \arrow[dr, dashed, "\tilde{t}"] \\ \mathcal{M} \arrow[u, phantom, "\cup"] \arrow[r, "t"'] & \mathcal{A}_1 \end{tikzcd}$$

and $\tilde{t}$ can be shown to be a proper morphism taking each stable curve C in $\tilde{\mathcal{M}}$ to $\mathrm{Pic}^0\, C$ with a suitable polarization (cf. Hoyt [8]). Let $\mathcal{T} = \overline{t(\mathcal{M})} = \tilde{t}(\tilde{\mathcal{M}})$: this is called the *Torelli locus.* A famous classical problem is to describe $\mathcal{T}$, or its inverse image in some $\mathcal{A}_n$, by explicit equations, e. g. polynomials in the theta-nulls. Partial results on this were obtained in characteristic zero by Riemann [18], Schottky, and Schottky-Jung [19]. Their results have been rigorously established recently by Farkas and Rauch [6], and some interesting generalizations have been given by Fay [7]. A completely different approach to this problem is given in the beautiful paper of Andreotti and Mayer [2]. I want to finish by sketching the key point in Schottky's theory and stating a theorem on what his equations do characterize. We assume char. $\neq 2$.

Let $\Pi: \hat{C} \to C$ be an etale double covering, and let $\iota: \hat{C} \to \hat{C}$ be the corresponding involution. If g = genus of C, then $2g - 1$ = genus of $\hat{C}$. The Jacobians $J = \mathrm{Pic}^0\, C$, $\hat{J} = \mathrm{Pic}^0\, \hat{C}$ are related by 2 homeomorphisms:

$$\hat{J} \underset{\Pi^*}{\overset{Nm}{\rightleftarrows}} J$$

such that $Nm \circ \Pi^* = 2_J$. ι acts on $\hat{J}$ also. Define:

$$P = \text{locus of points } \{\, \iota x - x \,\} \text{ in } \hat{J}.$$

We get isogenies:

$$\hat{J} \underset{\alpha}{\overset{\beta}{\rightleftarrows}} J \times P$$

$$\alpha(x, y) = \Pi^* x + y$$
$$\beta(z) = (Nmz,\ z - \iota z)$$

such that $\alpha \circ \beta = \beta \circ \alpha =$ mult. by 2. Next fix γ, a division class on C such that $2\gamma \equiv K_C$, the canonical divisor class, and such that dim $H^0(o(\gamma))$ is even (cf. [16] for this). We get symmetric divisors:

$$\Theta = \{\text{ locus of div. classes } \sum_1^{g-1} P_i - \gamma \} \subset J$$

$$\hat{\Theta} = \{\text{ locus of div. classes } \sum_1^{2g-2} P_i - \Pi^*\gamma \} \subset \hat{J}$$

representing the standard polarizations of J and $\hat{J}$.

LEMMA

a) $\Pi^{*-1}(\hat{\Theta}) = \Theta + \Theta_\kappa$, where $\{0, \kappa\} = \operatorname{Ker}(\Pi^*)$.

b) $\exists$ a symmetric divisor Ξ on P such that $\hat{\Theta}.P = 2\Xi$.

c) $\alpha^{-1}(\hat{\Theta}) \equiv \Theta \times P + \Theta_\kappa \times P + 2J \times \Xi$.

In particular, Ξ has degree 1 and defines a principal polarization on P. Abstractly put now we have a situation with.

i) 3 abelian varieties X, Y, Z of dimensions g, $g - 1$, $2g - 1$ resp.,

ii) 3 ample degree 1 symmetric divisors $\Theta_X \subset X$, $\Theta_Y \subset Y$, $\Theta_Z \subset Z$, which define as in § 2 theta-functions θ_X on $V(X)$, θ_Y on $V(Y)$ and θ_Z on $V(Z)$,

iii) isogenies $Z \underset{\alpha}{\overset{\beta}{\rightleftarrows}} X \times Y$ such that $\alpha \circ \beta = \beta \circ \alpha =$ mult. by 2. In such a case, $Z \cong X \times Y/H$, where H is a so-called Göpel group, and $V(Z) \cong V(X) \times V(Y)$. Moreover θ_Z can be computed from θ_X and θ_Y by one of the basic theta formulas. But then the lemma, esp. part *a)*, implies non-trivial identities on θ_X and θ_Y. In fact, it follows that for a suitable $\eta \in \frac{1}{2} T(X)$ with image κ in X and a suitable homeomorphism:

$$\varphi : \left\{ x \in \frac{1}{2} T(X) \mid e(x, \eta) = 1 \right\} \to \frac{1}{2} T(Y)$$

$$(*) \qquad \begin{cases} \dfrac{\theta_X(x).\theta_X(x+\eta)}{\theta_Y(\varphi x)^2} = \dfrac{\theta_X(y).\theta_X(y+\eta)}{\theta_Y(\varphi y)^2} \\ \text{all} \qquad x, y \in \frac{1}{2} T(X) \\ \text{with} \quad e(x, \eta) = e(y, \eta) = 1 \end{cases}$$

If we globalize this set-up, we get the following moduli situation: $\mathscr{M}_*$ is to be the normalization of $\mathscr{M}$ is a suitable finite algebraic extension of its function field such that for every point of $\mathscr{M}_*$ there is given rationally not only a curve C of genus g, but

(a) a (4,8)-structure on J (i. e. a point of $\mathscr{A}_{(4,8)}$ lying over J in $\mathscr{A}_1$), (b) a double covering $\Pi : \hat{C} \to C$, (c) a (4,8)-structure on P (cf. [5], pp. 104-108 for a precise discussion of such " non-abelian levels "). Thus, if we let $\mathscr{A}$'s (resp. $\mathscr{B}$'s) represent moduli spaces for abelian varieties of dim. g (resp. dim. $g - 1$), we have morphisms:

$$\begin{tikzcd} & \mathscr{A}_{4,8} \\ \mathscr{M}^* \arrow[ur, "t_*"] \arrow[dr, "s_*"'] & \\ & \mathscr{B}_{4,8} \end{tikzcd}$$

and since θ_J on $\frac{1}{2}T(J)$ $\left(\text{resp. } \theta_P \text{ on } \frac{1}{2}T(P)\right)$ are coordinates on $\mathscr{A}_{4,8}$ (resp. $\mathscr{B}_{4,8}$), the identities (*) define a locus $\mathscr{C} \subset \mathscr{A}_{4,8} \times \mathscr{B}_{4,8}$ (the η and φ must be independent of the curve you start with). We find:

THEOREM. — Im (t_*, s_*) is an open subset of one of the components of locus $\mathscr{C}$ of solutions of the Schottky-Jung identites (*) inside the moduli space $\mathscr{A}_{4,8} \times \mathscr{B}_{4,8}$.

REFERENCES

[1] A. ANDREOTTI. — On a theorem of Torelli, *Am. J. Math.*, 80 (1958).

[2] — and A. MAYER. — On period relations for abelian integrals on algebraic curves, *Annali di Scuolo Norm. di Pisa* (1967).

[3] M. ARTIN. — The implicit function theorem in algebraic geometry, in *Algebraic Geometry*, Oxford Univ. Press (1969).

[4] W. BAILY. — On the moduli of abelian varieties with multiplications, *J. Math. Soc. Japan*, 15 (1963).

[5] P. DELIGNE and D. MUMFORD. — The irreducibility of the space of curves of given genus, *Pub. I. H. E. S.*, 36 (1969).

[6] H. FARKAS and RAUCH. — Two kinds of theta constants and period relations on a Riemann Surface, *Proc. Nat. Acad. U. S.*, 62 (1969).

[7] J. FAY. — *Special moduli and theta relations*, Ph. D. Thesis, Harvard (1970).

[8] W. HOYT. — On products and algebraic families of jacobian varieties, *Annals of Math.*, 77 (1963).

[9] J. I. IGUSA. — On the graded ring of theta-constants, *Am. J. Math.*, 86 (1964) and 88 (1966).

[10] T. MATSUSAKA. — On a theorem of Torelli, *Am. J. Math.*, 80 (1958).

[11] D. MUMFORD. — *Geometric Invariant theory*, Springer-Verlag, Heidelberg (1965).

[12] —. — On the equations defining abelian varieties, *Inv. Math.*, Part I: vol. 1 (1966), Parts II and III: vol. 3 (1967).

[13] —. — Varieties defined by quadratic equations, in Questioni sulle varieta algebriche, *Corsi dal C. I. M. E.*, 1969, Edizioni Cremonese, Roma.

[14] —. — *Bi-extensions of formal groups, in Algebraic Geometry*, Oxford Univ. Press (1969).

[15] —. — *Abelian varieties*, Oxford Univ. Press (1970).

[16] —. — Theta characteristics of an algebraic curve, to appear in *Annales de l'École Normale Supérieure* (1971).
[17] F. OORT. — Finite group schemes, local moduli for abelian varieties and lifting problems, to appear in *Proc. Nordic Summer school of 1970*, Wolters-Noordhoff, Groningen.
[18] B. RIEMANN. — *Collected works*, Nachtrag IV, Dover edition (1953).
[19] F. SCHOTTKY and H. JUNG. — Neue Sätze über symmetralfunctionen und die Abelschen funktionen der Riemann'sche theorie, *Sitzungber, Berlin Akad. Wissensch.*, vol. I (1909).
[20] J. P. SERRE and J. TATE. — *Proc. of seminar on formal groups at Woods Hole Summer Institute* (1964), mimeographed notes.
[21] G. SHIMURA. — Moduli of abelian varieties and number theory, in algebraic groups and discontinuous subgroups, *Am. Math. Soc.* (1966).

Harvard University,
Department of Mathematics,
2, Divinity Avenue,
Cambridge, Mass. 02138
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 467 à 471.

QUELQUES CONJECTURES DE FINITUDE EN GÉOMÉTRIE DIOPHANTIENNE

par A. N. PARŠIN

Suivant une tradition établie, j'aimerais examiner une série de conjectures relatives à l'arithmétique des courbes et des variétés abéliennes. Dans ce domaine, Chafarevitch a formulé au Congrès de Stockholm [13], il y a huit ans, deux conjectures fondamentales. Elles concernent la situation suivante.

Soit K un corps de nombres de degré fini sur $\underline{Q}$ ou un corps de fonctions algébriques d'une variable; dans ce dernier cas, nous désignerons par k le corps des constantes. Nous étudierons les schémas projectifs lisses X géométriquement irréductibles sur K. Si v est une place du corps K, alors X a bonne réduction en v si v n'est pas archimédienne et s'il existe sur Spec O_v (O_v est l'anneau local de la place v) un schéma lisse propre de fibre générique X, et a mauvaise réduction dans le cas contraire. Nous désignerons par S l'ensemble fini des places du corps K ou X a mauvaise réduction et ces notations seront utilisées dans toute la suite. Enfin, soit $k(v)$ le corps résiduel de l'anneau local O_v.

CONJECTURE C1. — Il existe seulement un nombre fini, à K isomorphismes près, de courbes sur K de genre $g \geqslant 1$ donné et d'ensemble S donné (si $g = 1$, on suppose qu'il y a une K-place sur les courbes et si K est un corps de fonctions il est nécessaire de se limiter à des courbes non constantes).

La courbe X est dite constante si elle est de la forme $Y \otimes L$ sur une extension finie L du corps K, ou Y, est définie sur le corps des constantes du corps L.

CONJECTURE C2. — Soit $K = \underline{Q}$ ou $k(x)$. Toute courbe sur K de genre $g \geqslant 1$ dont l'ensemble S est vide est constante.

En particulier, dans le cas arithmétique $K = \underline{Q}$, il n'existe pas de telle courbe. Cette conjecture est donc analogue aux classiques théorèmes de Hermite et Minkowski en théorie des nombres.

La conjecture C1 est en liaison avec la conjecture suivante de Mordell.

CONJECTURE M ([5], [7]). — Si X est une courbe non constante de genre $g > 1$ sur K, alors l'ensemble $X(K)$ est fini.

Si K est un corps de fonctions dont le corps des constantes est fini, il existe des courbes constantes sur K pour lesquelles la conjecture M est en défaut.

THÉORÈME 1. — La conjecture C1 entraine la conjecture M.

La démonstration repose sur l'argument suivant : si X/K est une courbe de genre

$g \geqslant 1$ et $P \in X(K)$, alors on peut construire des courbes X_P, définies sur des corps K_P, dont le degré et le genre sur K ne dépendent pas de P. Ces courbes sont des revêtements de la courbe X ramifiés seulement en P et les corps K_P sont ramifiés sur K seulement sur l'ensemble S relatif à la courbe X. Enfin, les courbes X_P possèdent la propriété suivante : si π est la projection canonique de l'ensemble des places du corps K_P dans l'ensemble des places du corps K, alors X_P a une bonne réduction en dehors de $\pi^{-1}(S)$.

Cette construction généralise un résultat connu de Kodaira [4]. L'étude des courbes X_P, $P \in X(K)$, montre, en utilisant $C1$, qu'il n'y a, à isomorphisme près sur le corps de définition, qu'un nombre fini de telles courbes (et aussi un nombre fini de corps K_P). Pour $g > 1$, on en déduit la finitude de l'ensemble $X(K)$ puisque, pour une courbe, il n'y a qu'un nombre fini de morphismes sur une courbe de genre $g > 1$.

La conjecture M a été démontrée pour un corps de fonctions par Yu. V. Manin [6] et H. Grauert [2]. Nous donnons une autre démonstration dans [9], en utilisant le fait que si $\tilde{X}_P$ est le modèle minimal de la courbe X_P, alors la hauteur du point $P \in X(K)$ relativement au faisceau Ω_X^1 est bornée par l'indice de self-intersection d'une classe canonique sur la surface $\tilde{X}_P$. De considérations topologiques faciles il résulte que cet indice est borné explicitement en fonction du genre du corps K_P, du genre de la courbe X_P et du nombre de ses points où la courbe a mauvaise réduction ; par suite, ce nombre est borné uniformément par rapport à P.

Quant à la conjecture $C1$, elle a été démontrée récemment ([13]) pour les courbes hyperelliptiques (dans le cas d'un corps de fonctions, il faut supposer k fini) et pour les courbes sur un corps de fonctions de caractéristique nulle avec un ensemble S vide ([9]). Dans le cas fonctionnel, on montre aussi dans [9] que l'ensemble des courbes étudiées a une « hauteur bornée ».

Enonçons maintenant l'analogue de $C1$ pour les variétés abéliennes.

Conjecture $S1$. — Soient N et d des entiers et soit S un ensemble fini de places du corps K. Alors, il existe seulement un nombre fini de variétés abéliennes X sur K telles que

1) $\dim X = N$ et il existe sur X une polarisation de degré d ;
2) X a une bonne réduction en dehors de S.

Cette conjecture a été énoncée par J.-P. Serre ([10]) dans le cas $N = 2$, $d = 1$. J'ignore le lien entre $C1$ et $S1$ dans le cas d'un corps de nombres, sauf pour la situation triviale $N = d = 1$. Les tentatives en vue d'utiliser le théorème de Torelli pour déduire $C1$ de $S1$ se heurtent au fait que, pour une variété abélienne sur un corps de nombres, il peut exister une infinité de polarisations de degré donné définies sur K non équivalentes à automorphisme près. Il est possible que, dans cette conjecture, il faille tenir compte des « points de dégénérescence » de la polarisation, définis de façon convenable. Noter aussi qu'une courbe sur K peut avoir en une certaine place v mauvaise réduction alors que sa variété jacobienne a bonne réduction. La conjecture $S1$ a été démontrée dans [13] pour les courbes elliptiques. On peut formuler la conjecture suivante, plus accessible.

Conjecture $S2$. — Il existe seulement un nombre fini de variétés abéliennes X sur K de dimension N donnée ayant une polarisation de degré d donné et de conducteur A donné.

On se reportera à [12] pour la définition du conducteur. Remarquons seulement que X a une mauvaise réduction seulement aux places v divisant A ; donc $S1$ implique $S2$. Réciproquement $S2$ entraine $S1$ pour les ensembles S tels que

$$\forall v \in S, \qquad \text{car} \quad k(v) = 0 \qquad \text{ou} \qquad > 2N + 1.$$

De $S1$, et aussi de $S2$, résulte que :

Conjecture T [15]. — Soit X une variété abélienne sur K et soit d un entier $\geqslant 1$. Il existe seulement un nombre fini, à K-isomorphisme près, de variétés abéliennes Y/K telles que

1) Y est isogène à X ;
2) il existe sur Y une polarisation de degré d donné.

J. Tate a considéré un énoncé un peu plus faible. La conjecture T est liée à la conjecture de Tate sur les homomorphismes des variétés abéliennes (cf. [15], [16]). L'implication $S1 \Rightarrow T$ résulte de ce que les ensembles S coincident pour des variétés abéliennes isogènes (cf. [12]). Introduisons maintenant la nouvelle définition suivante : soit X et Y des variétés abéliennes (ou des schémas) avec des polarisations λ et ω respectivement; une isogénie $f : X \to Y$ s'appelle une isogénie de Tate si deg $f = \mathscr{K}^g$, $g = \dim X$ et $f^*\omega = \mathscr{K}\lambda$ (de telles isogénies ont été considérées par Tate dans [15]).

Théorème 2. — Soient K un corps de nombres, X/K une variété abélienne ayant potentiellement une bonne réduction (cf. [12]) et λ une polarisation de X de degré 1. Alors, il n'existe qu'un nombre fini de variétés abéliennes Y avec une polarisation ω telles qu'il existe une isogénie de Tate $f : X \to Y$ satisfaisant à la condition suivante: si v est une place non archimédienne du corps K et car $k(v) \mid \deg f$, alors X a en v une bonne réduction et f définit une isogénie étale des modèles minimaux de Néron des variétés X et Y sur Spec O_v.

Théorème 3. — Soient K un corps de fonctions sur un corps fini k, d un entier $\geqslant 1$, X une variété abélienne sur K ayant potentiellement bonne réduction. Désignons par $M(K, X, d)$ l'ensemble des couples (Y, λ) — ou Y est une variété abélienne et λ sa polarisation de degré d — tels qu'il existe une isogénie $f : Y \to X$ degré premier à $p = \text{car } k$. Alors, pour tout p n'appartenant pas à un ensemble fini $I(d, N)$, qui ne dépend que de d et $\dim X = N$, les ensembles $M(K, X, d)$ sont finis modulo les K-isomorphismes conservant la polarisation.

Corollaire. — Sous les hypothèses du théorème, $S1$ entraine $C1$ pour presque tout p.

Comme l'a remarqué J.-P. Serre [10], on peut, en utilisant la méthode de Tate [15] et une considération additionnelle, déduire du théorème 3 le résultat suivant.

Théorème 4. — Soient X et Y des courbes elliptiques sur un corps de fonctions K, de corps des constantes k fini avec car $k \notin I(1, 2)$, et soient $T_l(X)$ et $T_l(Y)$ leurs modules de Tate. Alors, la représentation naturelle

$$\mathrm{Hom}_K(X, Y) \otimes \underline{Q}_l \to \mathrm{Hom}(T_l(X), T_l(Y))$$

est bijective.

Corollaire. — Sous les hypothèses du théorème, les assertions suivantes sont équivalentes :

1) il existe l tels que les modules $T_l(X)$ et $T_l(Y)$ soient isomorphes ;
2) les courbes X et Y sont isogènes.

Probablement, les théorèmes 3 et 4 sont vrais quelle que soit la caractéristique du corps k. On peut montrer qu'il en est ainsi si le théorème d'irréductibilité de Mumford et Deligne [1] est vrai pour les schémas de modules des variétés abéliennes, et si le groupe de Picard de l'espace modulaire de Siegel module la torsion est égal à $\underline{Z}$ (1).

Terminons en disant maintenant quelques mots de la conjecture $C2$. Elle a été démontrée pour $g = 1$ (cf, [13]) et pour $g = 2$ (B. V. Martinov, non publié). Si $K = k(x)$, car $k = 0$, alors $C2$ est vraie pour tout $g \geqslant 1$, cf. [14], [3] (dans ce cas, il n'y a pas de variété abélienne non constante). Dans le cas d'un corps de fonctions, $C2$ est aussi vérifiée si K est un corps de genre 1 et car $K = 0$, cf. [9].

Bien que, dans le cas ou $g = 1$ et où K est un corps de nombres, les conjectures $S2$ et $C2$ aient été démontrées, on peut dire qu'elles résultent aussi de la conjecture sur l'équation fonctionnelle des fonctions zêta, de la conjecture de Tate, et du travail de Weil [17]. Pour $C2$, cela a été remarqué par A. Ogg [8]. Il est possible que cela soit encore vrai en dimension supérieure. Ce point doit être lié à la forme la plus précise, due à Serre [11], de la conjecture sur l'équation fonctionnelle.

BIBLIOGRAPHIE

[1] P. Deligne and D. Mumford. — The irreducibility of the space of curves of given genus, *Pub. Math. I. H. E. S.*, No. 36 (1969), pp. 75-109.

[2] H. Grauert. — Mordells Vermütung über Rationale Punkte auf Algebraischen Kurven und Funktionenkörper, *Pub. Math. I. H. E. S.*, No. 25 (1965), pp. 131-149.

[3] A. Grothendieck. — Un théorème sur les homomorphismes de schémas abéliens, *Inv. Math.*, 2 (1966), pp. 59-78.

[4] K. Kodaira. — A certain type of irregular algebraic surfaces, *J. Analyse Math.*, 19 (1967), pp. 207-215.

[5] S. Lang. — *Diophantine geometry*, Interscience (New York, 1962).

[6] Ю. И. Манин. — Рациональные точки алгебраических кривых над функциональными полями, Изв. АН СССР, 27 (1963), pp. 1397-1442.

[7] L. J. Mordell. — On the rational solutions of the indeterminate equation of the third and fourth degrees, *Proc. Cambridge Philos. Soc.*, 21 (1922).

[8] A. P. Ogg. — Abelian curves of small conductor, *Journ, für die reine und ang. Math.*, 226 (1967), pp. 204-215.

[9] А. Н. Паршин. — Алгебраическпе кривые над функциональными полями, Изв. АН СССР, 32 (1968), pp. 1191-1219, English summary, *Soviet Math. Doklady*, 9 (1968), No. 6, pp. 1419-1421.

[10] J. P. Serre. — *Abelian l-adic representations and Elliptic curves*, Benjamin (New York, 1968).

(*) Comme me l'a communiqué D. Mumford, c'est toujours le cas et par suite le théorème 4 est vrai pour tout k.

[11] —. — *Facteurs locaux des fonctions zêta des variétés algébriques* (Définitions et conjectures), Séminaire Delange-Pisot-Poitou (Théorie des nombres), n° 19, (1969-1970).
[12] — and J. Tate. — Good reduction of abelian varieties, *Ann. of Math.*, 88 (1968), pp. 492-517.
[13] И. Р. Шафаревич. — Поля алгебраических чисел, *Proc. Intern. Congress Math.*, Stockholm (1962), pp. 163-176.
[14] —. — Главные однородные пространства, определенные над полем функций, Труды МИАН СССР, 64 (1961), 316-346.
[15] J. Tate. — Endomorphisms of abelian varieties over finite fields, *Inv. Math.*, 2 (1966), pp. 134-144.
[16] —. — *Algebraic cycles and poles of zeta functions*, in *Arithmetical algebraic geometry*, Harper and Row (New York, 1965), pp. 93-110.
[17] A. Weil. — Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.*, 168 (1967), pp. 149-156.

Mathematical Institute
AN SSSR
Ul Vavilova 42,
Moscow V 333
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 473 à 477.

VARIÉTÉS ABÉLIENNES ET GÉOMÉTRIE RIGIDE

par MICHEL RAYNAUD

Soient R un anneau de valuation discrète complet, K son corps des fractions, k son corps résiduel et π une uniformisante. Soit d'autre part A une courbe elliptique sur K dont l'invariant j n'est pas entier. Quitte alors à remplacer éventuellement R par son normalisé dans une extension quadratique de K, on peut prolonger A en un R-schéma en groupes $\boldsymbol{A}$, dont la fibre spéciale $\boldsymbol{A} \otimes_R k$ est isomorphe au groupe multiplicatif $(G_m)_k$. De plus, Tate a montré que A est le quotient analytique rigide du groupe multiplicatif $(G_m)_K$ par un sous-groupe discret M engendré par les puissances d'un élément q de K^*, avec $|q| < 1$. Une démonstration de ce théorème est parue récemment dans [6]. Nous allons indiquer comment ce résultat s'étend aux variétés abéliennes.

1. Structure des schémas semi-abéliens.

Soit A_{alg} une variété abélienne sur K. Grothendieck a montré que A_{alg} avait potentiellement une réduction semi-abélienne sur R [2]. Cela signifie, que quitte à remplacer R par son normalisé dans une extension finie convenable de K, on peut prolonger A_{alg} en un R-schéma en groupes $\boldsymbol{A}_{\mathrm{alg}}$, lisse sur R, dont la fibre spéciale $\overline{\boldsymbol{A}} = \boldsymbol{A}_{\mathrm{alg}} \otimes_R k$ est extension d'une variété abélienne $\overline{\boldsymbol{B}}$ par un torc $\overline{\boldsymbol{T}}'$. Supposons maintenant que A possède sur R une réduction semi-abélienne $\boldsymbol{A}$ et notons A le groupe analytique rigide défini par A. C'est un groupe lisse, connexe, propre au sens de Kiehl [3]. Un groupe rigide qui possède ces propriétés sera appelé une variété abéloïde. Les variétés abéloïdes sont l'analogue en géométrie rigide des tores complexes de la géométrie analytique classique. Soit $\boldsymbol{A}$ le R-schéma formel en groupes complétion de $\boldsymbol{A}_{\mathrm{alg}}$ le long de sa fibre formelle $\overline{\boldsymbol{A}}$. Rappelons que tout R-schéma formel $\boldsymbol{X}$ définit *ipso-facto* un K-espace rigide $\boldsymbol{X}_K$: « la fibre générique » de $\boldsymbol{X}$. Dans le cas présent, la fibre générique $\boldsymbol{A}_K$ de $\boldsymbol{A}$ correspond à un sous-groupe ouvert rigide connexe de A. On a $\boldsymbol{A}_K = A$ si et seulement si A a bonne réduction sur R, c'est-à-dire encore, si le tore $\overline{\boldsymbol{T}}'$ est nul.

Pour tout entier $n \geqslant 0$ et tout R-schéma formel $\boldsymbol{X}$, posons $R_n = R/\pi^{n+1}R$, $\boldsymbol{X}_n = \boldsymbol{X} \otimes_R R_n$. Il résulte des propriétés infinitésimales des relèvements des sous-tores des schémas en groupes lisses [1], que $\overline{\boldsymbol{T}}'$ se relève, de manière unique en un sous-tore $\boldsymbol{T}'_n$ de $\boldsymbol{A}_n$. Posons $\boldsymbol{B}_n = \boldsymbol{A}_n/\boldsymbol{T}'_n$ qui est un R_n-schéma abélien, qui relève $\overline{\boldsymbol{B}}$. Par passage à la limite, on trouve que le schéma formel $\boldsymbol{A}$ est extension du R-schéma abélien formel $\boldsymbol{B} = \varinjlim \boldsymbol{B}_n$, par le tore formel $\boldsymbol{T}' = \varinjlim \boldsymbol{T}'_n$. Par suite, le groupe rigide $\boldsymbol{A}_K$ est extension de la variété abéloïde $\boldsymbol{B}_K = B$ par le groupe rigide $\boldsymbol{T}'_K$. Soit M' le groupe des caractères du tore $\overline{\boldsymbol{T}}'$. Il s'identifie canoniquement au groupe des caractères du tore formel $\boldsymbol{T}'$ et c'est aussi le groupe des caractères d'un tore rigide T' sur K. Le groupe rigide T'_K, fibre générique de $\boldsymbol{T}'$, est un sous-groupe ouvert de T' ; c'est le sous-groupe ouvert de T' où les caractères de T' prennent des valeurs de valuation 0 ; nous dirons aussi que T'_K est le groupe des unités de T'.

Ceci étant, on peut utiliser l'immersion ouverte $T'_K \to T'$, pour déduire du groupe A_K, extension de B par T'_K, un groupe rigide E extension de B par le tore T'. Le théorème de Tate mentionné au début, se généralise alors comme suit :

THÉORÈME 1. — Soient $i: A_K \to A$ et $j: A_K \to E$ les immersions ouvertes canoniques. Alors, il existe un unique morphisme rigide $p: E \to A$ tel que le diagramme suivant soit commutatif:

$$\begin{tikzcd} A_K \arrow[r] \arrow[dr, "j"'] & A \\ & E \arrow[u, "p"'] \end{tikzcd}$$

De plus, p est surjectif et son noyau M est un sous-groupe discret de E, sans torsion, de rang égal à la dimension du tore T'.

Autrement dit, A est le quotient, par un sous-groupe discret M, du groupe E, extension d'une variété abéloïde B ayant bonne réduction par un tore T non ramifié sur R.

2. **Indications sur la démonstration du théorème 1.**

Soit X un K-espace rigide propre [3], tel que $\Gamma(X, 0_X) = K$ et possédant un point rationnel. Procédant comme dans le cas algébrique, on peut définir le foncteur de Picard P de X au-dessus de K. Lorsque X provient d'un schéma propre X_{alg}, il résulte de théorèmes du type « Gaga », que P est représenté par le groupe rigide associé au schéma de Picard de X_{alg}. Soit $H^1(X, \mathbb{Z})$ le groupe des revêtements galoisiens de X, localement triviaux, de groupe $\mathbb{Z}$. En interprétant $\mathbb{Z}$ comme groupe des caractères du groupe multiplicatif G_m et du groupe des unités U, on trouve un diagramme commutatif canonique :

$$\begin{tikzcd} H^1(X, \mathbb{Z}) \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & \mathrm{Hom}\,(G^m, P) \arrow[d, "\text{res.}"] \\ & \mathrm{Hom}\,(U, P) \end{tikzcd}$$

Il résulte alors formellement de la nullité des faisceaux $\mathit{Ext}^1(G_m, G_m)$ (resp. $\mathit{Ext}^1(U, G_m)$) que les flèches α et β sont des isomorphismes. Par suite, tout morphisme $U \to P$ se relève de manière unique en un morphisme $G_m \to P$. Appliquons ce résultat en prenant pour X la variété abélienne duale de A. On prouve ainsi l'existence de la flèche $p: E \to A$. Le fait que p soit surjectif se voit par exemple en étudiant les composantes connexes du modèle de Néron de A.

3. **Description de certaines variétés abéloïdes.**

Partons maintenant d'un groupe rigide E extension d'une variété abéloïde B qui a potentiellement bonne réduction par un tore T'. L'extension E est décrite par un morphisme

$$\Phi': M' \to B'$$

du groupe M' des caractères de T' dans la variété duale B' de B. Soit d'autre part $M \to E$ un morphisme d'un groupe discret M sans torsion dans E. Cherchons à quelles conditions M est un sous-groupe de E tel que le quotient de E par M soit une variété abéloïde A. Soit

$$\Phi: M \to B$$

la flèche canonique composée de $M \to E$ et de la projection $q: E \to B$ et soit P le faisceau inversible universel sur $B \times B'$. On sait que P est muni d'une structure de bi-extension [2]. La donnée du morphisme $M \to E$ qui relève Φ équivaut alors à la donnée d'une trivialisation s de l'image réciproque de P par le morphisme

$$\Phi \times \Phi': M \times M' \to B \times B'$$

qui dépend bi-additivement de $(m, m') \in M \times M'$.

$$\begin{tikzcd} & P \arrow[d] \\ M \times M' \arrow[ur, "s"] \arrow[r, "\Phi\times\Phi'"'] & B \times B' \end{tikzcd}$$

Nous allons maintenant associer à s une donnée discrète.

a) Supposons d'abord que T' et M soient déployés et que B ait bonne réduction sur R, donc provient d'un R-schéma abélien formel $\boldsymbol{B}$. Le dual B' provient alors du schéma formel dual $\boldsymbol{B}'$ et le faisceau inversible P se prolonge en un faisceau inversible $\boldsymbol{P}$ sur $\boldsymbol{B} \times \boldsymbol{B}'$. Sur le groupe multiplicatif G_m on dispose de la fonction définie par la valuation

$$v: G_m \to \Gamma$$

où Γ est le groupe de la valuation de K. En utilisant le prolongement $\boldsymbol{P}$ de P, on montre que l'on a aussi une « valuation » canonique sur P $v_P: P \to \Gamma$. Composant v_P avec la section s, on obtient une application bi-additive canonique

$$u: M \times M' \to \Gamma.$$

Le fait que $M \to E$ soit injectif et que le quotient de E par l'image de M soit une variété abéloïde A est alors équivalent au fait que u soit non dégénéré.

b) Dans le cas général, par descente, on trouve un accouplement canonique

$$\bar{u}: M \times M' \to \bar{\Gamma}$$

où $\bar{\Gamma}$ est le divisé du groupe Γ. Cet accouplement est compatible avec l'action du groupe de Galois fini qui « tord » M et M'.

Nous résumons la construction précédente dans le diagramme suivant

$$\begin{tikzcd} & & 0 \arrow[d] & & \\ & & M \arrow[d] & & \\ 0 \arrow[r] & T' \arrow[r] & E \arrow[r, "q"] \arrow[d, "p"'] & B \arrow[r] & 0 \\ & & A \arrow[d] & & \\ & & 0 & & \end{tikzcd}$$

Notons que l'on passe de A à la variété abéloïde duale A' en échangeant les rôles de B et B', M et M', Φ et Φ'.

4. Algébrisation des variétés abéloïdes.

Partons de la variété abéloïde A construite au n° 3 et cherchons à quelle condition A provient d'une variété abélienne. Il revient au même de chercher s'il existe un faisceau inversible L ample sur A. Supposons pour simplifier que B a bonne réduction et que T' est déployé. Soit L un faisceau inversible sur A, $p^*(L)$ son image réciproque sur E. On peut montrer qu'il existe un faisceau inversible N sur B tel que $p^*(L) \simeq q^*(N)$. Réciproquement, si N est un faisceau inversible sur B, $q^*(N)$ provient d'un faisceau inversible sur A, si et seulement si $q^*(N)$ est muni d'une donnée de descente relativement au sous-groupe M.

Soit A' la variété abéloïde duale de A, de sorte que A' est extension de B' par le tore T dont le groupe des caractères est M. Si L est un faisceau inversible sur A, il lui correspond de la manière habituelle un homomorphisme $\varphi_L : A \to A'$. Celui-ci se relève en un morphisme $\varphi : E \to E'$, d'où un morphisme $\varphi : M \to M'$. Par passage au quotient, on obtient un morphisme de B dans B', qui n'est autre que φ_N. De plus, le diagramme suivant est commutatif :

$$\begin{array}{ccc} M & \xrightarrow{\Phi} & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_N} \\ M' & \xrightarrow{\Phi'} & B' \end{array}$$

En composant u avec φ, on obtient une forme quadratique sur M à valeurs dans Γ

$$m \mapsto u(m, \varphi(m))$$

qui est symétrique.

Ceci étant, supposons que L possède une section non nulle a, donc est de la forme $O_A(\Delta)$, où Δ est un diviseur > 0. Alors $p^*(\Delta)$ est un diviseur > 0 sur E, invariant par M. Lorsque $B = 0$, donc $E = T'$, $p^*(\Delta)$ est un diviseur principal, défini par une équation

$$\sum_{m' \in M'} a_{m'} T^{m'} = 0$$

du type fonction thêta non archimédienne étudié par Morikawa [4]. Dans le cas général, $p^*(\Delta)$ n'est pas principal, mais on a $p^*(L) \simeq q^*(N)$. Pour tout $m' \in M'$, notons $P_{m'}$ le faisceau inversible sur B qui correspond au point $\Phi'(m')$ de B'. La donnée d'une section de L, donc de $p^*(L)$, définit alors une famille $a_{m', m' \in M'}$ de sections de $N \otimes P_{m'}$. Ces coefficients $a_{m'}$ jouent le rôle des coefficients de la série de Laurent du cas de réduction torique. Finalement, on obtient le résultat suivant :

THÉORÈME 2. — Pour que L soit ample sur A, auquel cas A provient d'une variété abélienne, il faut et il suffit que les deux conditions suivantes soient réalisées :

1) La forme quadratique $m \mapsto u(m, \varphi(m'))$ est positive non dégénérée sur M.

2) Le faisceau inversible N est ample sur B.

COROLLAIRE. — Sous les hypothèses du théorème 1, la variété abéloïde B et l'extension E sont algébrisables.

BIBLIOGRAPHIE

[1] M. DEMAZURE et A. GROTHENDIECK. — SGA 3, chap. VI. Schémas en groupes. *Notes de l'I. H. E. S.*
[2] A. GROTHENDIECK. — SGA VII. Exposé IX : modèles de Néron et monodromie. *Notes de l'I. H. E. S.*
[3] R. KIEHL. — Der endlichkeitssatz für eigentliche abbildungen in der nichtarchimedischen funktionentheorie, *Invent. Math.*, 2 (1967), pp. 191-214.
[4] H. MORIKAWA. — On theta functions and abelian varieties over valuation fields of rank one, *Nagoya Math. Journ.*, 20 (1962), pp. 1-27 et 21 (1962), pp. 231-250.
[5] A. NÉRON. — Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, publ. I. H. E. S., n° 21 (1964).
[6] P. ROQUETTE. — Analytic theory of elliptic functions over local fields. Hamburger Mathematische Einzelschriften. Neue folge, Heft 1 (1970).

Faculté des Sciences d'Orsay
Département de Mathématiques
91-Orsay (France)

Actes, Congrès intern. math., 1970. Tome 1, p. 479 à 482.

QUOTIENT SPACES MODULO REDUCTIVE ALGEBRAIC GROUPS AND APPLICATIONS TO MODULI OF VECTOR BUNDLES ON ALGEBRAIC CURVES

by C. S. SESHADRI

It has been known for quite some time that the problem of constructing moduli spaces e. g. of curves, abelian varieties or vector bundles on algebraic curves can be reduced to one of constructing quotient spaces under an algebraic group (in these examples it is the projective group). In his book [2], Mumford developed a theory of quotient spaces and showed how this can be applied to the above moduli problems. However his general theory is valid only in characteristic zero and for the purpose of carrying it over in arbitrary characteristic he made a conjecture. In § 1, we report on some progress (made in collaboration with D. Mumford) towards the proof of this conjecture. In § 2 we give a resume of our results on the moduli of vector bundles on algebraic curves. It is interesting to note that whereas there are now alternative methods for the construction of moduli for abelian varieties (or curves), for the case of vector bundles on algebraic curves, the construction of moduli (at least in the difficult cases) rests on Mumford's theory [2].

NOTATION. — We work with a base field k which is algebraically closed. However a more systematic treatment would involve a more general base scheme.

§ 1. Geometric reductivity.

An affine algebraic group G is said to be *geometrically reductive* if $\forall$ rational representation of G on a finite dimensional vector space V and a G-invariant point $v \in V$, $v \neq 0$, $\exists$ a G-invariant polynomial f on V such that $f(v) \neq 0$, $f(0) = 0$ or equivalently, $\exists$ a G-invariant homogeneous form f on V such that $f(v) \neq 0$. If the characteristic of the ground field k is zero and G is *reductive* (i. e. the radical of G is a torus group), then by the complete reducibility of every linear representation of G one concludes easily that G is geometrically reductive. A torus group is easily seen to be geometrically reductive in arbitrary characteristic. The conjecture of Mumford states that a reductive algebraic group is geometrically reductive. It has been proved in [6] that $GL(2)$ is geometrically reductive.

Let G be a *geometrically reductive* algebraic group acting on an affine algebraic scheme $X = \operatorname{Spec} A$ and X_1, X_2 two G-invariant closed subsets of X such that

$X_1 \cap X_2 = \emptyset$. We see easily that $\exists$ a G-morphism $\varphi : X \to V$, V being the affine variety associated to a rational G-module such that $\varphi(X_1) = 0$ and $\varphi(X_2) = v$, v being a non-zero G-invariant point of V. From this it follows easily that $\exists f \in A^G$ such that $f(X_1) = 0$ and $f(X_2) = 1$. Thus geometric reductivity is equivalent to separation of disjoint closed G-invariant subsets (in affine schemes).

Let G be a *reductive* algebraic group acting on the affine space A^{n+1} through a rational linear representation. Then G operates on the projective space P^n. Let X be a closed G-invariant subscheme of P^n and $X =$ Proj R, R being the homogeneous coordinate ring of X. We say that a (k-valued) point $x \in X$ is *semi-stable* (resp. *stable*) (with respect to the above projective imbedding or the ample line bundle L defining this imbedding) if for some $x \in \hat{X}$ ($\hat{X}$, the cone over X), the closure of the G-orbit through $\hat{x}$ does not pass through the vertex (0) (resp. the orbit morphism $G \to \hat{X}$ defined by $g \mapsto \hat{x} \circ g$ is proper). We denote these subsets by $X^{ss} = X^{ss}(L)$ (resp. $X^s = X^s(L)$).

Let X, G be as above. Suppose moreover that G is *geometrically reductive.* Then we see that X^{ss} coincides precisely with the set of points x such that $\exists f \in R^G$ with $f(x) \neq 0$ (or equivalently $\exists f \in \Gamma(X, L^n)$ for some $n > 0$ such that $f(x) \neq 0$ and f is G-invariant); in particular X^{ss} would be open. Conversely, since a G-invariant point of X is in X^{ss}, we see that this property characterizes geometric reductivity. Let $Y =$ Proj R^G. Then it can be shown that R^G is a k-algebra of finite type (cf. [3], if $k = C$ this is classical) so that Y is a *projective* algebraic scheme. Let $\varphi : X \to Y$ be the rational morphism defined by the inclusion $R^G \subset R$. Then φ is *regular* in X^{ss} and if the same φ denotes the canonical morphism $X^{ss} \to Y$ induced by φ, it can be shown that (*i*) φ is a surjective, G-invariant affine morphism and $(\varphi_*(O_X))^G = O_Y$; (*ii*) φ separates disjoint closed G-invariant subsets of X and (*iii*) X^s is *φ-saturated* (i. e. $\exists$ an open subset Y^s of Y such that $X^s = \varphi^{-1}(Y^s)$) and the morphism $X^s \to Y^s$ is a *geometric quotient* i. e. Y^s is the orbit space X^s mod G. These properties have been proved, for example when $k = C$ in [2] and are the ones used in moduli problems; further we see trivially that these properties again characterize geometric reductivity. *Thus geometric reductivity of G is equivalent to constructing a nice quotient* $\varphi : X^{ss} \to Y$ *as above.*

Suppose now that G is a reductive group G operating on X as above. Then using the techniques introduced in [2], one can prove the following (*i*) X^{ss}, X^s are G-invariant open subsets of X; (*ii*) the action of G on X^s is *proper* i. e. the canonical morphism $X^s \times G \to X^s \times X^s$ defined by $(x, g) \mapsto (x, x \circ g)$ is proper (this would imply that the orbit space X^s mod G is a separated *algebraic space* in the sense of Artin) and (*iii*) there is a *generalized completeness property for* X^{ss} mod G, for example if $X^{ss} = X^s$, this means that the algebraic space X^s mod G is *complete.* Now the main results are as follows:

THEOREM 1. — Suppose that $X^{ss} = X^s$. Then a suitable multiple of the line bundle L on X descends to an ample line bundle on the complete orbit space $Y = X^s$ mod G. In particular Y is projective.

THEOREM 2. — Let $Z = X \times G/B$ where B is a Borel subgroup of G (G semi-simple) and p: $Z \to X$ the canonical projection (p is a G-morphism for the diagonal action of G on Z). Then we can find an ample line bundle M on G/B such that for the ample line bundle

$$N = aL + bM, \qquad a, b \in Z, \qquad a, b > 0$$

on Z ($aL + bM$ means a fold tensor product of $L \otimes b$ fold tensor product of M) if $\frac{b}{a}$ is sufficiently small, we have

(*i*) $p^{-1}(X^s(L)) \subset Z^s(N)$; (*ii*) $p(Z^{ss}(N)) \subset X^{ss}(L)$ and (*iii*) $Z^{ss}(N) = Z^s(N)$.

One proves Theorem 1 by appealing to the criterion of Nakai-Moishezon. It can be supposed without loss of generality that G operates *freely* on X^s, that Y exists in the category of algebraic schemes and that L descends down to a line bundle M on Y. One proves first that if C is a closed integral curve in Y, $\deg(M|_C) > 0$ and that if Y is integral of dimension n that $M^n = M \cdots M$ (n times) > 0 by blowing up a smooth point of Y and using functorial properties of stable points.

Suppose that $X^s \neq \emptyset$, X integral and that we have a *nice* quotient X^{ss} mod G as in the case when G is geometrically reductive. By Theorem 1, Z^s mod G ($Z^s = Z^s(N)$) is a projective variety. Let $q: Z^s$ mod $G \to X^{ss}$ mod G be the canonical morphism induced by p. Then by Theorem 2 we see that q is proper, surjective and that over X^s mod G, q is an equidimensional fibration. Then one concludes easily that X^s mod G is *quasi-projective* without supposing that a *nice* quotient X^{ss} mod G exists. In fact we have the following

Cor. (to Th. 2). — Let X, G be as in Theorem 2. Then given $x \in X^s$, $\exists\ s \in \Gamma(X, L^n)$ for some $n > 0$ such that $s(x) \neq 0$ and s is G-invariant. A suitable multiple of L descends to an ample line bundle on X^s mod G.

§ 2. Moduli of vector bundles.

Let X be a smooth projective curve defined over k. We say (after Mumford [1]) that an algebraic vector bundle on X is *stable* (resp. *semi-stable*) if $\forall$ proper subvector bundle W of V, $\frac{\deg W}{rkW} < \frac{\deg V}{rkV}$ (resp. $\leqslant$). If V is a semi-stable vector bundle such that $\alpha = \frac{\deg V}{rkV}$, one sees easily (cf. [5]), that $\exists$ a *Jordan-Hölder series*

$$V_1 \subset \ldots \subset V_i \subset \ldots \subset V$$

such that $W_i = V_i/V_{i-1}$ is *stable* and $\frac{\deg W_i}{rkW_i} = \alpha$. The vector bundle $\operatorname{gr} V = \oplus\, W_i$ is uniquely determined upto isomorphism. Let $S(n, \alpha)$ denote the set of equivalence classes of semi-stable vector bundles V on X such that $rkV = n$ and $\frac{\deg V}{rkV} = \alpha$ under the equivalence relation $V_1 \sim V_2$ if $\operatorname{gr} V_1 = \operatorname{gr} V_2$. The subset $S(n, \alpha)^s$ of $S(n, \alpha)$ formed by equivalence classes containing stable bundles is just the isomorphism classes of stable vector bundles V such that $rkV = n$ and $\frac{\deg V}{rkV} = \alpha$. We have then

THEOREM 3. — Let $k = C$ and genus of $X \geqslant 2$. Then on $S(n, \alpha)$, there is a natural structure of a normal projective variety and $S(n, \alpha)^s$ is a smooth open subvariety (cf. [1], [5]).

We note that if $(n, n\alpha) = 1$ ($n\alpha$ is the degree of any $V \in S(n, \alpha)$), $S(n, \alpha)^s = S(n, \alpha)$;

in particular $S(n, \alpha)$ is smooth in this case. When $n = 2$, Theorem 3 has been proved in arbitrary characteristic by using the geometric reductivity of $GL(2)$ (cf. [6]). For more general rank by applying Theorem 1 and Theorem 2, we have

THEOREM 4 (characteristic of k is arbitrary). — Let genus of $X \geqslant 2$. On $S(n, \alpha)^s$ there is a natural structure of a smooth quasi-projective variety. In particular if $(n, n\alpha) = 1$, $S(n, \alpha)$ is a smooth projective variety.

In [4] the following result was proved

THEOREM 5. — The underlying topological space of $S(n, 0)$ can be identified with the set of equivalence classes of unitary representations of rank n of the fundamental group of X. A similar property holds also for $S(n, \alpha)$ by means of unitary representations of rank n and of a particular type of a Fuchsian group Γ acting on the upper half plane H such that $X = H \bmod \Gamma$ (genus of $X \geqslant 2$).

One can ask whether on the set $U(\Gamma, n)$ of equivalence classes of unitary representations of rank n of a Fuchsian group Γ acting on the upper half plane H such that $H \bmod \Gamma$ has *finite measure*, there is a natural " algebraic structure ". If H mod Γ is *compact* this is the case as has been checked in [7]. Similar results seem to hold even in the more general case. If X is the canonical compactification of $H \bmod \Gamma$, this problem can be studied *algebraically* on X *via* the functor p_*^Γ (cf. [4] and [7]) and one gets a situation similar to Theorem 2. In fact this served as the motivation for Theorem 2.

REFERENCES

[1] D. MUMFORD. — Projective invariants of projective structures and applications, *Proc. Intern. Cong. Math.*, Stockholm (1962), pp. 526-530.
[2] —. — *Geometric Invariant Theory*, Springer-Verlag (1965).
[3] M. NAGATA. — Invariants of a group in an affine ring, *J. Math. Kyoto Univ.*, 3 (1964), pp. 369-377.
[4] M. S. NARASIMHAN and C. S. SESHADRI. — Stable and unitary vector bundles on a compact Riemann surface, *Ann. of Math.*, 82 (1965), pp. 540-567.
[5] C. S. SESHADRI. — Space of unitary vector bundles on a compact Riemann surface, *Ann. of Math.*, 85 (1967), pp. 303-336.
[6] —. — Mumford's conjecture for $GL(2)$ and applications, Algebraic geometry (Papers presented at the Bombay Colloquium, 1968), Oxford University Press (1969).
[7] —. — Moduli of π-vector bundles over an algebraic curve, *Questions on algebraic varieties*, C. I. M. E. (1969), III CICLO, pp. 141-260).

Tata Institute
of Fundamental Research
Department of Mathematics,
Colaba, Bombay 5 (Inde)

Actes, Congrès intern. math., 1970. Tome 1, p. 483 à 485.

B_6 - THÉORIE DES NOMBRES, ÉLÉMENTAIRE ET ANALYTIQUE

TRANSCENDENCE AND DIFFERENTIAL ALGEBRAIC GEOMETRY

by JAMES AX

There are certain problems whose resolution ultimately depends upon the algebraic intersection properties of analytic varieties defined by algebraic differential equations. The problem of this sort which first attracted our attention (and still holds it most strongly) is Schanuel's conjecture [1 and 2, § 1] on the transcendentality properties of the exponential function:

(S) Let $y_1, \ldots, y_n \in C$ be Q-linearly independent. Then

$$\dim_Q Q(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n.$$

Here $\dim_E F$ for any extension of fields F/E denotes the cardinality of a maximal E-algebraically independent subset of F.

(S) Implies all the known transcendentality properties of the exponential function including the theorems of Lindemann and Baker as well as all reasonable conjectures such as the algebraic independence of π and e.

Let G be the algebraic group defined over Q consisting of the product of n copies of the additive group with n copies of the multiplicative group and identified with its C-valued points $C^n \times C^{*n}$. Let A be the analytic subgroup which is the graph of the map $C^n \xrightarrow{\exp} C^{*n}$. Then we can restate S as

(S') If V is an algebraic subset of G defined over Q of dimension less than n, then for all $p \in V \cap A$ there exists a proper subgroup L of C^n such that $L \times \exp(L)$ is an *algebraic* subgroup of G and contains p.

S' is a statement of the type described at the beginning since A can be described as the integral manifold through the identity of the completely integrable system of one forms $dy_\nu - dz_\nu/z_\nu$, $\nu = 1, \ldots, n$. Of course, S' involves an arithmetic aspect since V is required to be defined over Q.

Schanuel also conjectured a formal version of S:

(SF) Let $y_1, \ldots, y_n \in tC[[t]]$ be Q-linearly independent. Then

$$\dim_C C(y_1, \ldots, y_n e^{y_1}, \ldots, e^{y_n}) \geq n + 1.$$

This conjecture is a consequence of the following result.

THEOREM 1. — Let G be an algebraic group, V an algebraic subvariety, A an analytic subgroup. Let K be a component of $V \cap A$ containing the identity. Then the

Zariski closure of K is the unique component of $V \cap G'$ which contains K, where G' is the smallest algebraic subgroup of G containing K.

This theorem also implies the generalizations of SF to several variables and to the exponential map of any commutative algebraic group. Applied to the case where G is the product of multiplicative groups (over the completion of the algebraic closure of the p-adic numbers) it yields the results of Chabauty's thesis [3, § 2]. The corollary below contains these last results as well as Chabauty's proof [4] of Mordell's conjecture in the special case of a curve of genus > 1 whose Jacobian J is simple and such that the rank of the group of rational points of J does not exceed the genus.

COROLLARY. — Let G be an algebraic group defined and simple over $C \supseteq \underline{Q}$. Let R be a finitely generated subgroup of the C-valued points of G. Let V be an algebraic subvariety of G.

If $R \cap V$ is infinite then rank R + dim $V >$ dim G.

Another problem of the kind mentioned at the beginning also occurs in the literature of transcendental numbers. In [1], Lang asked whether a hyperplane section V of an abelian variety G necessarily meets every Zariski-dense one parameter subgroup A. The affirmative answer to Lang's question is contained in the following result.

THEOREM 2. — Let G be an abelian variety, V the intersection of d hyperplane sections of G and $C^d \xrightarrow{\sigma} G$ an analytic homomorphism. Then there exists $\varepsilon > 0$ such that for all sufficiently large r,

$$\# \{ z \in \underline{C}^d \mid \ \| z \| < r, \sigma(z) \in V \} > \varepsilon r^{2d},$$

provided no coset of $A = \sigma(\underline{C}^d)$ in G intersects V in a positive dimensional set.

The proviso must hold if $d = 1$ and A is Zariski dense so Lang's problem is thereby resolved (actually V need not be a hyperplane section, but only of codimension one). The proviso is also satisfied if G is simple; this follows from Theorem 1. The assumption that V is a complete intersection is probably avoidable when G is simple. In the proof it is used to insure that the harmonic $2d$-form ω which represents the cohomology class corresponding to V by Poincaré duality is positive whenever evaluated on $2d$ tangent vectors spanning a complex subspace of the tangent space. By (topological) intersection theory we conclude $V \cap \bar{A} \neq \emptyset$ where $\bar{A}$, the topological closure of A, is a compact (possibly of odd topological dimension!) subgroup of G and therefore carries an integral fundamental homology class. The completion of the proof depends on noting that we need only prove $(V + A) \cap A \neq \emptyset$ and that by the Proper Mapping Theorem $V + A$ is an open subset of G since our proviso guarantees that the map $V \times A \to G$, given by $(v, u) \to v + a$, has discrete fibres.

The generalization of Theorem 2 to complex tori also holds. Here is another formulation of the answer to Lang's question.

COROLLARY. — Let θ be a reduced theta function on $\underline{C}^g$ and L a complex line in $\underline{C}^g$. Then either $(\theta \mid L)$ is constant or has an infinite set of zeroes (in fact its associated canonical product is a function of order 2).

Finally, let us indicate two well-known results of the same type as we first mentioned which it seems to us, call out for extension. One is Siegel's theorem [5, 6] on the algebraic independence of Bessel functions. It would be nice to have a satisfactory criterion for determining the dimension of the field generated by the solutions of a linear system of differential equations over the field of rational functions.

The last result we mention is taken from physics: Brun's theorem [7, Ch. XIV] on the algebraic integrals of the three body problem. Here we consider a certain real algebraic variety S (state spaces) of dimension 19 together with a certain algebraic vector field W defined on S whose value on any function is its Poisson bracket with the Hamiltonian of this system. An *algebraic integral* is an algebraic function F on S which is constant on the orbits of W. One such is the energy function. Nine more independent algebraic integrals were also known classically. These come from the linearity of the motion of the center of gravity together with the constancy of linear and angular momenta. In 1887 Bruns proved that the frequent efforts to obtain other independent algebraic integrals were doomed to failure: all algebraic integrals are functions of the classical ones. In order to restate this result in a convenient form it is necessary to pass to a finite covering T of the complexification of S so that there is a (single-valued) vector field Y on T corresponding to W.

Brun's theorem then says there exists a universal morphism $T \xrightarrow{\varphi} T_0$ of algebraic varieties with φ constant on the orbits of Y and that $\dim T_0 = 10$.

Thus if $T \xrightarrow{\psi} T'$ is any morphism either there exists $T_0 \xrightarrow{\tau} T'$ such that $\psi = \tau \circ \varphi$ (in which case $\dim \tau(T_0) \leq 10$) or else for some fibre V of ψ and some orbit A of Y we have $\emptyset \neq V \cap A \neq A$. This statement shows that Brun's theorem is again of the type originally mentioned and reveals that one aspect of this same problem is the algebraic analogue of the theory of dynamical systems.

REFERENCES

[1] S. LANG. — *Introduction to transcendental numbers*, Addison-Wesley, Reading, Massachusetts, 1966.

[2] J. AX. — On Schanuel's conjectures, *Annals of Math.* (to appear).

[3] C. CHABAUTY. — Sur les équations diophantiennes liées aux unités d'un corps de nombres algébrique fini, *Ann. Mat. Pure Appl.*, 17, pp. 127-168.

[4] —. — Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, *Comptes Rendus*, 212 (1941), pp. 1022-1024.

[5] C. L. SIEGEL. — Über einige Anwendungen diophantischer Approximationen, *Abh. der preussichen Akad. der Wissenschaften, phys.-math. Klasse*, 1929, Nr. 1 (1930), pp. 1-70.

[6] E. KOLCHIN. — Algebraic groups and algebraic dependence, *Amer. Jour.*, 90 (1968), pp. 1151-1164.

[7] E. T. WHITTAKER. — *A treatise on the analytical dynamics of particles and rigid bodies*, Dover, New York (1944).

Suny at Stony Brook
Department of Mathematics,
Stony Brook,
New York 11790
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 487.

ON THE GENERALIZED CHARACTERS

by N. CHUDAKOV

For a Dirichlet's character $\chi(n, \mathscr{D})$ it has been proved that

$$\sum_{n \leqslant x} \chi(n) = \alpha x + O(1)$$

where $x \to \infty$; $\alpha = \varphi(\mathscr{D})/\mathscr{D}$ for $\chi = \chi_0$ and $\alpha = 0$ for $\chi \neq \chi_0$.

The generalized character is a completely multiplicative function $h(n)$ (morphism of the set of natural numbers) for which an analogous relation is satisfied:

$$S(x) = \sum_{n \leqslant x} h(n) = \alpha x + O(1).$$

The basis of a function $h(n)$ is the set $E\{\,p,\ p\text{-prime},\ h(p) \neq 0\,\}$.

Hypothesis: if $h(n)$ has an almost complete basis, i. e. containing almost all primes p, there is an identity: $h(n) = \chi(n, \mathscr{D})$ where $\chi(n, \mathscr{D})$ is a Dirichlet's character.

For $\alpha \neq 0$ this hypothesis has been proved by Glazkov V. V. (1964). The question is open for $\alpha = 0$. When the basis of $h(n)$ contains a finite set of elements or its density has a logarithmic order, then $S(x)$ is not bounded for $x \to \infty$ (Bredihin, Linnik, Chudakov).

It has been proved that

$$S(x) = \Omega(\sqrt{\log_4 x})$$

(Chudakov, Pavliuchuk).

More precisely:

$$S(x) = \Omega(\sqrt{\log_3 x})$$

(Chudakov, Leibovich).

REFERENCES

[1] V. V. Glazkov. — On a class of finite homomorphisms, *Dokl. Akad. Nauk URSS*, 158 (1) (1964), pp. 33-36.

[2] B. M. Bredihin. — On the sum functions of characters of numerical semigroups, *Dokl. Akad. Nauk URSS*, 94 (4) (1954).

[3] N. Chudakov and A. Pavliuchuk. — On the sum functions of characters of numerical groups with finite base, *Proc. Stekloff Math. Inst.* (Russian), 38 (1951).

[4] N. G. Tchudakoff (Chudakov). — Theory of the characters of number semigroups, Report of an International Colloquium on Zeta-functions, Bombay (1956).

Mathematical Institute
of Academy of Sciences
Fontanka 25,
Leningrad D 11
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 489.

THE EFFECTIVE METHODS IN THE THEORY OF QUADRATIC FIELDS

by N. CHUDAKOV

Let Q be the field of the rational numbers, $k = Q(\sqrt{-\Delta})$ be the imaginary quadratic field with the discriminant $= -\Delta$, $Q_\nu(x, y) = a_\nu x^2 + b_\nu xy + c_\nu y^2$ ($\nu = 1, 2 \ldots h$, h is equal to the class-number of k) be the reduced quadratic forms of discriminant $-\Delta$, corresponding to the ideal-classes of k,

$$a(\Delta) = \max a_\nu \qquad (\nu = 1, 2 \ldots h).$$

H. Heilbronn (1935) has proved that $a(\Delta) \geqslant \left(\frac{1}{4}\Delta\right)^{1/h}$ if $(a, \Delta) = 1$. Using new A. Baker's papers on the linear forms of logarithm of algebraic numbers we have obtained a new amelioration of Heilbronn's result: for every given value of h there is an effective finite set of values of Δ for which

$$a(\Delta) \leqslant \sqrt{\Delta}\,(\log \Delta)^{-\tau(h)}$$

where $\tau(h)$ is an effective function of h.

For $h = 1$ we can prove Stark's theorem [3] using only a Gelfond theorem (1939) for two logarithms (in print) (see also [2]).

REFERENCES

[1] E. A. ANFERT'EVA and N. G. ČUDAKOV. — Minima of the norm function in imaginary quadratic fields, *Sovied Math. Dokl.*, v. 9, No. 6 (1968).

[2] N. CHUDAKOV. — On the upper bound for the « tenth » discriminant with $h = 1$, *Research in the number theory*, v. 3, Saratov (1969).

[3] H. STARK. — Michigan, *Math. J.*, 14 (1967), pp. 1.

Mathematical Institute
of Academy of Sciences
Fontanka 25,
Leningrad D 11
(U. R. S. S.)

Actes, Congrès intern. math., 1970. Tome 1, p. 491 à 496.

REDUCIBILITY OF POLYNOMIALS

by A. SCHINZEL

Reducibility without qualification means in this lecture reducibility over the rational field. Questions on such reducibility occupy an intermediate place between questions on reducibility of polynomials over an algebraically closed field and those on primality. I shall refer to these two cases as to the algebraic and the arithmetic one and I shall try to exhibit some of the analogies considering several irreducibility theorems as opposed to numerous irreducibility criteria (cf. [34], p. 140) usually without analogues.

Historically first is Hilbert's irreducibility theorem (1892 [13]), which asserts that a polynomial $f(x_1, \ldots, x_n, t)$ irreducible as a polynomial in $n + 1$ variables becomes irreducible as a polynomial in n variables for infinitely many integer values of the parameter t. As its analogon in the algebraic case one can consider the theorem of Salomon (1915 [22]) which precises the conditions under which a polynomial $f(x_1, \ldots, x_n, t)$ irreducible over an algebraically closed field as a polynomial in $n + 1$ variables becomes irreducible as a polynomial in n variables ($n > 1$) by suitable choice of the parameter t (In contrast to Hilbert's theorem certain conditions must be fulfilled).

In the arithmetic case an analogon of Hilbert's theorem is formed by the following conjecture of Bouniakowsky (1857 [3]). If a polynomial $f(t)$ with integer coefficients and the leading coefficient positive is irreducible and has the greatest constant factor d then for infinitely many values of t $f(t)/d$ is a prime. The only case where the conjecture was proved is—no need to say—Dirichlet's theorem on arithmetic progression.

Hilbert's theorem in its full generality applies to arbitrarily many polynomials with any number of parameters (see [15]). Similar generalizations are possible in the algebraic and the arithmetic case (for the former see [14], for the latter see [23], [24] and [1]). However in contrast to the latter case, the m, say, parameters occuring in Hilbert's theorem can be chosen independently from m suitable arithmetic progressions ([27]).

Hilbert's theorem for $n = 1$ is closely related to the following statement: if an equation $f(x, t) = 0$ is soluble in rational x for any integer value of t then it is identically satisfied by a certain rational function of t. The question arises whether an analogous statement holds for $n > 1$. It can be easily disproved for $n > 2$; for $n = 2$. Davenport, Lewis and I proved it for polynomials quadratic in x_1, x_2, [7]; there are several open problems here for which I refer to [25] and [27].

The second irreducibility theorem I wish to comment upon is the theorem of Capelli (1901 [4]). It gives a necessary and sufficient condition for the reducibility of a binomial $x^n - a$ over an arbitrary field. Originally it was proved for algebraic number fields but the proof extends easily to the general case ([39]). In virtue of Galois theory this implies a necessary and sufficient condition for the reducibility of $F(x^n)$, where F is any fixed polynomial.

The question arises whether one can give such a condition for the reducibility of polynomials of the form (*A*) $F(x_1^{n_1},\dots,x_k^{n_k})$ or (*B*) $F(x^{n_1},\dots,x^{n_k})$. For the complex field the question (*A*) has been settled by the work of Ritt [21] and Gourin [12] about 1930. In order to state the result it is convenient to introduce the notation:

$$F(x_1,\dots,x_n) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x_1,\dots,x_n)^{e_\sigma},$$

which means that the polynomials on the right hand side are irreducible and relatively prime in pairs. Now Gourin's theorem can be stated as follows.

Let F consist of more than two terms. Then for each vector $[n_1,\dots,n_k]$ consisting of positive integers there exist integer vectors $[\mu_1,\dots,\mu_k]$ and $[u_1,\dots,u_k]$ such that

(i) $$0 < \mu_i \leqslant c(F),$$

(ii) $$n_i = \mu_i u_i,$$

(iii) $$F(x_1^{\mu_1},\dots,x_k^{\mu_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x_1,\dots,x_k)^{e_\sigma}$$

implies

$$F(x_1^{n_1},\dots,x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{u_1},\dots,x_k^{u_k})^{e_\sigma}.$$

The first progress with the rational field and the question (*B*) was made by Selmer [33], Tverberg [34] and Ljunggren [18] about 1960. Selmer proved the irreducibility of $x^n \pm x \pm 1$ deprived of its cyclotomic factors, Tverberg extended this to $x^n \pm x^m \pm 1$ and Ljunggren developed a new method which permitted him to decide about reducibility of $x^n \pm x^m \pm x^p \pm 1$ (see also [19]). Following the idea of Ljunggren I have recently proved a certain though not quite satisfactory analogon of the result of Gourin for both questions (*A*) and (*B*). In order to formulate the theorems it is unfortunately necessary to introduce some more notation.

If

$$\phi(x_1,\dots,x_k) = f(x_1,\dots,x_k)\prod_{i=1}^{k} x_i^{\alpha_i},$$

where f is a polynomial not divisible by any x_i, then $J\phi(x_1,\dots,x_k) = f(x_1,\dots,x_k)$. Let

$$J\phi(x_1,\dots,x_k) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x_1,\dots,x_k)^{e_\sigma}.$$

We set

$$K\phi(x_1,\dots,x_k) = \text{const}\ \Pi_1 f_\sigma(x_1,\dots,x_k)^{e_\sigma},$$
$$L\phi(x_1,\dots,x_k) = \text{const}\ \Pi_2 f_\sigma(x_1,\dots,x_k)^{e_\sigma},$$

where Π_1 is extended over all f_σ which do not divide $J(x_1^{\delta_1}\dots x_k^{\delta_k} - 1)$ for any $[\delta_1,\dots,\delta_k] \neq \overline{0}$, Π_2 is extended over all f_σ such that

$$Jf_\sigma(x_1^{-1},\dots,x_k^{-1}) \neq \pm f_\sigma(x_1,\dots,x_k).$$

For $k = 1$, $K\phi$ *is* $J\phi$ deprived of all its cyclotomic factors, $L\phi$ *is* $J\phi$ deprived of all its reciprocal factors. We have (see [29], [31], [40] and [41].

(A) For any polynomial $F \neq 0$ and any vector $[n_1, \ldots, n_k]$ consisting of positive integers there exist integral vectors $[\mu_1, \ldots, \mu_k]$ and $[u_1, \ldots, u_k]$ such that

(i) $$0 < \mu_i \leqslant C_1(F),$$

(ii) $$n_i = \mu_i u_i,$$

(iii) $$LF(x_1^{\mu_1}, \ldots, x_k^{\mu_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma > 1}^{s} F_\sigma(x_1, \ldots, x_k)^{e_\sigma}$$

implies
$$LF(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma = 1}^{s} F_\sigma(x_1^{u_1}, \ldots, x_k^{u_k})^{e_\sigma}.$$

(B) For any polynomial F and any integral vector $[n_1, \ldots, n_k]$ such that $F(x^{n_1}, \ldots, x^{n_k}) \neq 0$ there exist an integral matrix $N = [\nu_{ij}]_{\substack{i \leqslant r,\\ j < k}}$ of rank r and an integral vector $\overline{v} = [v_1, \ldots, v_r]$ such that

(i) $$\max |\nu_{ij}| \leqslant C_2(F),$$

(ii) $$\overline{n} = \overline{v} N,$$

(iii) $$LF\Big(\prod_{i=1}^{r} y_i^{\nu_{i1}}, \ldots, \prod_{i=1}^{r} y_i^{\nu_{ik}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma = 1}^{s} F_\sigma(y_1, \ldots, y_r)^{e_\sigma}$$

implies
$$LF(x^{n_1}, \ldots, x^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma = 1}^{s} LF_\sigma(x^{v_1}, \ldots, x^{v_r})^{e_\sigma}.$$

The example $F = x - 1$ shows that without the operation L applied to the left hand side of (iii) both (A) and (B) would be false. However, they still may be true with L replaced by K. I have proved it for $k = 1$ and for $k = 2$ under the condition $KF(x_1, x_2) = LF(x_1, x_2)$. ($B$) which lies much deeper than (A) has the following consequence: if $k > 1$, $a_i \neq 0$ $(i = 0, 1, \ldots, k)$ and $L(a_0 + a_1 x^{n_1} + \ldots + a_k x^{n_k})$ is reducible then between $n_1, \ldots, n_k$ holds a linear relation $\gamma_1 n_1 + \ldots + \gamma_k n_k = 0$, where $0 < \max |\gamma_i| < C(a_0, \ldots, a_k)$. Another consequence is this: the number $N(f)$ of irreducible non-reciprocal factors of a polynomial f with integer coefficients does not exceed a bound depending only on $\| f \|$ = the sum of squares of the coefficients of f. The bound which follows from the quantitative form of (B) is extremely large ([29]). Recently, C. J. Smyth has proved that for a monic non-reciprocal polynomial the product of all zeros lying outside the unit circle is in absolute value greater than $\frac{1}{2}\sqrt{5}$ (*). This implies $N(f) = O(\log \| f \|)$.

The modified form of (B) with L replaced by K is related to an analogon of the theorem of Smyth for reciprocal but not cyclotomic polynomials. According to the recent result of Blanksby and Montgomery [2] the product of the zeros of such a polynomial lying outside the unit circle is in absolute value greater than $1 + \dfrac{1}{52n \log 6n}$, where n is the degree. It was asked by D. H. Lehmer (1933 [16]) whether this product can be made arbitrarily close to one but this seems to be difficult.

The aforesaid modified form of (B) form $k = 2$ has the following consequence. For any non-zero integers a, b and any polynomial f with $f(0) \neq 0$, $f(1) \neq -a-b$

(*) Soon after the Congress SMYTH proved that the product in question is greater than or equal to the least Pisot number ([42]).

there exist infinitely many integers m, n such that $ax^m + bx^n + f(x)$ is irreducible ([30]). The arithmetic analogon of this theorem has not been proved and may well be false. If instead of $ax^m + bx^n + f(x)$ we take $ax^n + f(x)$ then for $a = 12$ and suitable $f(x)$ with integer coefficients and $f(0) \neq 0$, $f(1) \neq -a$ no choice of n gives an irreducible polynomial. For $a = 1$ the corresponding problem is related to the socalled covering systems of congruences. In particular if there is no covering system with distinct odd moduli then for any $f(x)$ with $f(0) \neq 0$, $f(1) \neq -1$ there exists n such that $x^n + f(x)$ is irreducible ([28]).

In connection with the result of Gourin I have evoked the name of Ritt. In the theory of polynomials he is perhaps best remembered for his theorem about the quasi uniqueness of representation of a polynomial in the form of a superposition of indecomposable polynomials. This was proved originally for the complex field (1922, [20]), but later Engstrom [8] and Levi [17] proved it for any field of characteristic zero. Recently, M. Fried has found remarkable connection between reducibility and decomposability of polynomials. He has proved that if $f(x)$ is indecomposable then either $(f(x) - f(y))/(x - y)$ is absolutely irreducible or $f(x)$ is up to a linear transformation x^p or the Chebyshev polynomial $T_p(x)$. This has led him [9] to the solution of 50 years old Schur problem on permutation polynomials. Fried has also proved [10], [11] that if f, g have rational coefficients and the degree of f is a power of an odd prime or f is indecomposable then $f(x) - g(y)$ is reducible over complex field if and only if $f(x) = h(f_1(x))$, $g(y) = h(g_1(y))$, where degree $h > 1$. Cassels [5] and Fried [11] have translated the problem into one in combinatorial group theory. However, no necessary and sufficient condition for the reducibility of $f(x) - g(y)$ over rational or complex field in terms of f and g has been found and puzzling examples of reducibility over complex field were given by Guy and Birch (see [5]), Tverberg [37] and Fried [11]. On the other hand $f(x) + g(y) + h(z)$ is absolutely irreducible for all non constant f, g and h (see [25] for the proof due to Ehrenfeucht and Pelcyński, [35], [36]) and $f(x_1, \ldots, x_m) + g(y_1, \ldots, y_n)$ is reducible in any field if and only if

$$f = f_1(f_2(x_1, \ldots, x_n)), \qquad g = g_1(g_2(y_1, \ldots, y_n))$$

and $f_1(x) + g_1(y)$ is reducible in the said field ([6] and [26]). The unsolved problems could be multiplied but I hope I have said enough to witness that the topic abounds in simple and interesting questions.

REFERENCES

[1] P. T. Bateman and R. Horn. — Primes represented by irreducible polynomials in one variable, *Proc. Symposia in Pure Math.*, 8 (1965), pp. 119-132.

[2] P. E. Blanksby and H. L. Montgomery. — Algebraic integers near the unit circle, *Acta Arithm.*, 18 (1971).

[3] V. Bouniakowsky. — Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, *Mém. Acad. Sci. Saint-Pétersbourg* (6), *Sci. math. et phys.*, 6 (1857), pp. 305-329.

[4] A. Capelli. — Sulla riduttibilità della funzione $x^n - A$ in un campo qualunque di rationalità, *Math. Ann.*, 54 (1901), pp. 602-603.

[5] J. W. S. CASSELS. — Factorization of polynomials in several variables, *Proc. XVth Scandinavian Congress Oslo* (1968), pp. 1-17.

[6] H. DAVENPORT and A. SCHINZEL. — Two problems concerning polynomials, *J. Reine Angew. Math.*, 214-215 (1964), pp. 386-391 ; *Corrigendum*, 218 (1965), p. 220.

[7] —, D. J. LEWIS and A. SCHINZEL. — Quadratic Diophantine equations with a parameter, *Acta Arith.*, 11 (1966), pp. 353-358.

[8] H. T. ENGSTROM. — Polynomial substitutions, *American J. Math.*, 63 (1941), pp. 249-255.

[9] M. FRIED. — On a conjecture of Schur, *Michigan Math. J.*, 17 (1970), pp. 41-50.

[10] —. — On the Diophantine equation $f(y) - x = 0$, *Acta Arith.*, 19 (1971).

[11] —. — Families of Riemann Surfaces with application to Diophantine problems, *J. Number Theory.*

[12] E. GOURIN. — On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves, *Trans. Amer. Math. Soc.*, 32 (1931), pp. 485-501.

[13] D. HILBERT. — Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *J. Reine Angew. Math.*, 110 (1892), pp. 104-129.

[14] W. KRULL. — Über einen Irreduzibilitätsatz von Bertini, *J. Reine Angew. Math.*, 177 (1937), pp. 94-104.

[15] S. LANG. — *Diophantine geometry*, Interscience Tracts in Pure and Applied Mathematics, No. 11, New York and London (1962).

[16] D. H. LEHMER. — Factorization of certain cyclotomic functions, *Ann. Math.* (2), 34 (1933), pp. 461-479.

[17] H. LEVI. — Composite polynomials with coefficients in an arbitrary field of characteristic zero, *Amer. J. Math.*, 64 (1942), pp. 389-400.

[18] W. LJUNGGREN. — On the irreducibility of certain trinomials and quadrinomials, *Math. Scand.*, 8 (1960), pp. 65-70.

[19] —. — On the irreducibility of certain lacunary polynomials, *Kong. Norske Vid. Selsk. Forhandlinger*, 36 (1963), pp. 159-164.

[20] J. F. RITT. — Prime and composite polynomials, *Trans. Amer. Math. Soc.*, 23 (1922), pp. 51-66.

[21] —. —. A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$, *Trans. Amer. Math. Soc.*, 29 (1927), pp. 584-596.

[22] G. SALOMON. — Über das Zerfallen von Systemen von Polynomen, *Jber. Deutsch. Math. Verein*, 24 (1915), pp. 225-246.

[23] A. SCHINZEL et W. SIERPINSKI. — Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.*, 4 (1958), pp. 185-208, *Corrigendum*, 5 (1959), p. 259.

[24] —. — Remarks on the paper « Sur certaines hypothèses concernant les nombres premiers », *Acta Arith.*, 7 (1961), pp. 1-8.

[25] —. — Some unsolved problems on polynomials, *Matematička Biblioteka*, 25 (1963), pp. 63-70.

[26] —. — Reducibility of polynomials in several variables, *Bull. Acad. Polon. Sci., Ser. sci. math. astr. phys.*, 11 (1963), pp. 633-638.

[27] —. — On Hilbert's irreducibility theorem, *Ann. Polon. Math.*, 16 (1965), pp. 333-340.

[28] —. — Reducibility of polynomials and covering systems of congruences, *Acta Arith.*, 13 (1967), pp. 91-101.

[29] —. — Reducibility of lacunary polynomials I, *Acta Arith.*, 16 (1969), pp. 123-159.

[30] —. — Reducibility of lacunary polynomials II, *Acta Arith.*, 16 (1970), pp. 372-392.

[31] —. — Reducibility of lacunary polynomials, *Proc. Symposia in Pure Math.*, 20 (1971).

[32] —. — Reducibility of polynomials, *Proc. Symposium « Computers in number theory ».*

[33] E. S. SELMER. — On the irreducibility of certain trinomials, *Math. Scand.*, 4 (1956), pp. 287-302.

[34] N. G. TSCHEBOTARÖW and H. SCHWERDTFEGER. — *Grundzüge der Galoischen Theorie*, Groningen, Djakarta (1950).

[35] H. TVERBERG. — On the irreducibility of the trinomials $x^n \pm x^m \pm 1$, *Math. Scand.*, 8 (1960), pp. 121-126.
[36] —. — A remark on Ehrenfeucht's criterion for irreducibility of polynomials, *Prace mat.*, 8 (1964), pp. 117-118.
[37] —. — On the irreducibility of polynomials $f(x) + g(y) + h(z)$, *Quart. J. Math. Oxford* (2), 17 (1966), pp. 364-366.
[38] —. — Thesis, Bergen (1968).
[39] L. RÉDEI. — Algebra I, Budapest (1967).
[40] A. SCHINZEL. — Reducibility of lacunary polynomials III (in preparation for *Acta Arith.*).
[41] — and J. WÓJCIK. — A note on the paper « Reducibility of lacunary polynomials I », *Acta Arith.*, 19 (1971).
[42] C. J. SMYTH. — On the product $\prod_{|\alpha| \geqslant 1} |\alpha_i|$ for the conjugates of an algebraic integer α, *Bull. London Math. Soc.*, 3 (1971).

Mathematical Institute
of the Polish Academy
of Sciences
Warsaw (Pologne)

Actes, Congrès intern. math., 1970. Tome 1, p. 497 à 503.

SOME RECENT PROGRESS IN DIOPHANTINE APPROXIMATIONS

by WOLFGANG M. SCHMIDT

1. Considerable progress has recently been made in this field. A. Baker's result on linear forms whose coefficients are logarithms of algebraic numbers, which has spectacular applications on transcendental numbers, on diophantine equations and elsewhere, may be considered as being at least on the border line of diophantine approximations. There is no need to go into details since he will give an account of this work in a lecture next week. Mahler's classification of transcendental numbers into S-, T- and U-numbers also may be regarded as belonging to our subject. A few years ago Sprindžuk showed that almost every number is an S-number of type 1, and thereby proved a long standing conjecture of Mahler. Sprindžuk and Turan will also next week speak on recent results and applications of diophantine approximations. The problem of the existence of T-numbers was solved less than two years ago. Erdös recently proved the following difficult metrical result. *Let $n_1 < n_2 < \ldots$ be a sequence of positive integers with $\Sigma_{i=1}^{\infty}\varphi(n_i)/n_i^2 = \infty$, where φ is Euler's φ-function. Then for almost every α and for every $\varepsilon > 0$, the inequality*

$$\left|\alpha - \frac{a}{n_i}\right| < \frac{\varepsilon}{n_i^2}$$

has infinitely many solutions in rationals a/n_i in reduced form.

Last winter I was able to extend Roth's famous theorem on rational approximation to an algebraic irrational to simultaneous approximations. I hope you will forgive me if I devote the rest of this lecture to this subject; I had not anticipated this result when I gave the title of my talk in the fall of 1969.

2. In the year 1842 Dirichlet, using the pigeonhole principle, showed that every irrational α has infinitely many rational approximations p/q with

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

In 1844 Liouville proved a result pointing in the opposite direction. He showed that if α is algebraic of degree $d \geqq 2$, then there is a constant $c(\alpha) > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

for every rational p/q. In 1908 Thue showed that for an algebraic number α of degree $d \geqq 2$ and every

$$\mu > \frac{d}{2} + 1, \tag{1}$$

there is a constant $c(\alpha, \mu)$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha, \mu)}{q^{\mu}}$$

for every rational p/q. This had an important application on diophantine equations. Namely, if $f(x, y)$ is a form of degree $d \geqq 3$, which has rational coefficients and is irreducible over the rationals, then the equation

$$f(x, y) = c, \tag{2}$$

where c is a constant, has at most finitely many integer solutions (x, y). Thue's result was further improved by Siegel, who showed that (1) may be replaced by $\mu > 2\sqrt{d}$. This was improved to $\mu > \sqrt{2d}$ by Dyson and finally to $\mu > 2$ by Roth [3] in 1955. Putting $\mu = 2 + \varepsilon$ we may state Roth's theorem as follows. *Given an algebraic number α and given $\varepsilon > 0$, there are only finitely many rationals p/q with*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}.$$

In view of Dirichlet's theorem, the number $2 + \varepsilon$ may not be replaced by 2, and thus in a sense Roth's theorem is best possible.

We now turn to simultaneous approximation. Dirichlet showed that *if $\alpha_1, \ldots, \alpha_n$ are any reals which are not all rational, then there are infinitely many n-tuples of rationals $p_1/q, \ldots, p_n/q$ with*

$$\left| \alpha_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+(1/n)}} \qquad (i = 1, \ldots, n).$$

Note that the exponent $1 + \dfrac{1}{n}$ is 2 when $n = 1$, and it is less than 2 when $n > 1$. There is a dual theorem. Namely, *for any numbers $\alpha_1, \ldots, \alpha_n$, there exist infinitely many $(n + 1)$-tuples of integers $q_1, \ldots, q_n$, p with*

$$| \alpha_1 q_1 + \ldots + \alpha_n q_n + p | < \frac{1}{q^n},$$

where $q = \max (| q_1 |, \ldots, | q_n |) > 0$.

Recently I proved the following theorems.

THEOREM 1. — *Suppose $\alpha_1, \ldots, \alpha_n$ are algebraic, with $1, \alpha_1, \ldots, \alpha_n$ linearly independent over the rationals. For every $\varepsilon > 0$, the inequalities*

$$\left| \alpha_i - \frac{p_i}{q} \right| < q^{-1-(1/n)-\varepsilon} \qquad (i = 1, \ldots, n) \tag{3}$$

have only finitely many solutions in n-tuples of rationals $p_1/q, \ldots, p_n/q$.

Dual to this is

THEOREM 2. — *Suppose* $\alpha_1, \ldots, \alpha_n$ *and* ε *are as above. There are only finitely many* $(n+1)$*-tuples of integers* $q_1, \ldots, q_n$, p *with* $q = \max(|q_1|, \ldots, |q_n|) > 0$ *and with*

$$|\alpha_1 q_1 + \ldots + \alpha_n q_n + p| < q^{-n-\varepsilon}. \tag{4}$$

By the results of Dirichlet quoted above, the exponents in these theorems are best possible. Both theorems reduce to Roth's theorem when $n = 1$. From Roth's theorem it was clear that Theorem 1 would be true with the exponent $-2-\varepsilon$ instead of $-1-(1/n)-\varepsilon$, and hence the improvement in the exponent may not seem spectacular. On the other hand, in Theorem 2 no exponent depending only on n had been known until now. It had been known, however, that either theorem implies the other.

A very simple application of Theorem 2 yields

THEOREM 3. — *Suppose* α *is algebraic,* k *a positive integer and* $\varepsilon > 0$. *There are only finitely many algebraic numbers* β *of degree* k *with*

$$|\alpha - \beta| < H(\beta)^{-(k+1+\varepsilon)}.$$

Here $H(\beta)$ denotes the *height* of β, defined in the usual way. It can be shown that the number $k+1$ in the exponent is best possible here. Wirsing [7] had proved this result with $2k$ instead of $k+1$. The proofs of our theorems will appear in [4].

3. The proofs of Theorems 1 and 2 have as their basis the method of Roth, which already is rather complicated; but many new complications arise in the present context. It is necessary to refer to a number of results of the Geometry of Numbers.

Let K be a convex symmetric body in Euclidean E^k of volume $V(K)$ with $0 < V(K) < \infty$. The *first minimum* λ_1 of K is defined as the infimum of the numbers $\lambda > 0$ such that λK (i. e. the set of points $\lambda \boldsymbol{x}$ with $\boldsymbol{x} \in K$) contains an integer point $\boldsymbol{g} \neq \boldsymbol{0}$. More generally, the *j-th minimum* λ_j of K, where $1 \leqq j \leqq k$, is the infimum of the numbers $\lambda > 0$ such that λK contains j linearly independent integer points. It is clear that

$$0 < \lambda_1 \leqq \ldots \leqq \lambda_k < \infty.$$

A theorem of Minkowski says that

$$2^k/k! \leqq \lambda_1 \ldots \lambda_k V(K) \leqq 2^k.$$

In our applications, K will be a parallelepiped of volume 2^k, and we may write

$$1 \ll \lambda_1 \ldots \lambda_k \ll 1,$$

with the constants in $\ll$ depending only on k. In particular, we have

$$\lambda_k \gg 1.$$

Suppose now that (3) holds for some $p_1/q, \ldots, p_n/q$. Put

$$k = n+1, \qquad b_1 = \ldots = b_n = q^{-(1/n)-(\varepsilon/2n)}, \qquad b_k = q^{1+(\varepsilon/2)}.$$

Then

$$|\alpha_i q - p_i| < b_i q^{-\varepsilon/2} \quad (1 \leqq i \leqq n), \qquad |q| \leqq b_k q^{-\varepsilon/2}. \tag{5}$$

Put

$$(6)\qquad \begin{aligned} \boldsymbol{a}_1 &= (1, 0, \ldots, 0, -\alpha_1),\\ &\vdots\\ \boldsymbol{a}_n &= (0, 0, \ldots, 1, -\alpha_n),\\ \boldsymbol{a}_k &= (0, 0, \ldots, 0, 1), \end{aligned}$$

and consider the parallelepiped Π in E^k consisting of points $\boldsymbol{x}$ with

$$|\boldsymbol{a}_i\boldsymbol{x}| \leqq b_i \qquad (i = 1, \ldots, k),$$

where $\boldsymbol{a}_i\boldsymbol{x}$ denotes the standard inner product. Since $\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) = 1$ and since $b_1 \ldots b_k = 1$, this parallelepiped has volume 2^k. Now in view of (5), the point $\boldsymbol{x}_0 = (p_1, \ldots, p_n, q)$ satisfies

$$|\boldsymbol{a}_i\boldsymbol{x}_0| \leqq b_i q^{-\varepsilon/2} \qquad (i = 1, \ldots, k).$$

Therefore the first minimum λ_1 of Π satisfies $\lambda_1 \leqq q^{-\varepsilon/2}$. Thus in order to show that the inequalities (3) have only finitely many solutions, it suffices to show that $\lambda_1 = \lambda_1(q) \gg q^{-\delta}$ for every $\delta > 0$. We shall write $f(q) \succ g(q)$ if the functions f, g have $f(q) \gg q^{-\delta}g(q)$ for every $\delta > 0$. We have to show that

$$\lambda_1 \succ 1.$$

In Roth's proof of his theorem, the *index* of a polynomial $P(X_1, \ldots, X_m)$ plays an important role. As it turns out, the most suitable generalization of this index is as follows. Let $P(X_{11}, \ldots, X_{1k}; \ldots; X_{m1}, \ldots, X_{mk})$ be a polynomial in mk variables, and let $r_1, \ldots, r_m$ be positive integers. Let

$$L_1 = \alpha_{11}X_{11} + \ldots + \alpha_{1k}X_{1k}, \ldots, L_m = \alpha_{m1}X_{m1} + \ldots + \alpha_{mk}X_{mk}$$

be linear forms, none of them identically zero. For $c \geqq 0$, we denote by $\mathscr{I}(c)$ the ideal generated by the polynomials

$$L_1^{c_1}L_2^{c_2} \ldots L_m^{c_m} \qquad \text{with} \qquad \frac{c_1}{r_1} + \ldots + \frac{c_m}{r_m} \geqq c.$$

The index of the polynomial P with respect to $(L_1, \ldots, L_m; r_1, \ldots, r_m)$ is the largest value of c such that P lies in $\mathscr{I}(c)$. In the course of some arguments involving this index one has to have available $n = k - 1$ linearly independent integer points of E^k with certain approximation properties. In particular, these points are needed to span the subspace consisting of the zeros of some linear form $L(X_1, \ldots, X_k)$. Thus it turns out that after rather long arguments instead of the desired $\lambda_1 \succ 1$ one only gets

$$\lambda_{k-1} \succ 1.$$

I had reached this stage by the end of 1966. Of course when $n = 1$, then $k - 1 = 1$, and one obtains $\lambda_1 > 1$, i. e. Roth's theorem.

4. Suppose that $1 \leqq p \leqq k - 1$, and put $l = \binom{k}{p}$. Let $i_1, \ldots, i_p$ be integers with

$1 \leqq i_1 < i_2 < \ldots < i_p \leqq k$. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ be the vectors of E^k given by (6). We define $\boldsymbol{a}_{i_1} \wedge \boldsymbol{a}_{i_2} \wedge \ldots \wedge \boldsymbol{a}_{i_p}$ as the vector in E^l whose components are the $(p \times p)$-determinants of the $(p \times k)$-matrix with row vectors $\boldsymbol{a}_{i_1}, \ldots, \boldsymbol{a}_{i_p}$, arranged in lexicographic order (This is a special type of product of the Grassmann algebra of E^k). For brevity we shall write $\boldsymbol{A}_\sigma = \boldsymbol{a}_{i_1} \wedge \ldots \wedge \boldsymbol{a}_{i_p}$ where σ is the set $\{ i_1, \ldots, i_p \}$. There are l such sets σ with $1 \leqq i_1 < \ldots < i_p \leqq k$, hence l such vectors $\boldsymbol{A}_\sigma$ of E^l. Write

$$B_\sigma = \prod_{i \in \sigma} b_i .$$

We recall that Π was the parallelepiped in E^k defined by

$$| \boldsymbol{a}_i \boldsymbol{x} | \leqq b_i \qquad (i = 1, \ldots, k),$$

and that its successive minima were $\lambda_1, \ldots, \lambda_k$. We now define a new parallelepiped $\Pi^{(p)}$ in E^l by

$$| \boldsymbol{A}_\sigma \boldsymbol{X} | \leqq B_\sigma \qquad \text{(all possible sets } \sigma).$$

This parallelepiped $\Pi^{(p)}$ is related to the *p-th* compound body of Π as defined by Mahler [2]; we shall call it the *p-th pseudocompound* of Π. Denote its successive minima by $\nu_1, \ldots, \nu_l$.

Now Mahler [2] could show that except for bounded factors, the numbers $\nu_1, \ldots, \nu_l$ are the same as the l products obtained by multiplying p of the numbers $\lambda_1, \ldots, \lambda_k$. In particular we have

$$\nu_l \ll \lambda_{k-p+1} \lambda_{k-p+2} \ldots \lambda_k \ll \nu_l$$

and

$$\nu_{l-1} \ll \lambda_{k-p} \quad \lambda_{k-p+2} \ldots \lambda_k \ll \nu_{l-1} .$$

For $\Pi^{(p)}$ one can show again that $\nu_{l-1} \succ 1$, and using another argument from the Geometry of Numbers, one obtains $\nu_{l-1} \succ \nu_l$. With the inequalities just stated this implies that $\lambda_{k-p} \succ \lambda_{k-p+1}$. Applying this with $p = k-1,\ k-2, \ldots, 1$, we get $\lambda_1 \succ \lambda_2 \succ \ldots \succ \lambda_k$, and since $\lambda_k \succ 1$, we get $\lambda_1 \succ 1$. This is the desired result.

5. Our main theorems may be generalized in several directions. A sample is the following. Suppose $u \geqq 1$, $v \geqq 1$, $k = u + v$, and let $L_1(\boldsymbol{x}), \ldots, L_v(\boldsymbol{x})$ be linear forms in $\boldsymbol{x} = (x_1, \ldots, x_k)$ with real algebraic coefficients. By Minkowski's lemma on linear forms there is for every $Q > 0$ an integer point $\boldsymbol{x} \neq \boldsymbol{0}$ with

$$| \boldsymbol{x} | \ll Q^v \qquad \text{and with} \qquad | L_i(\boldsymbol{x}) | \ll Q^{-u} \qquad (i = 1, \ldots, v),$$

where $| \boldsymbol{x} | = \max (| x_1 |, \ldots, | x_k |)$. Hence there are infinitely many solutions of

$$| L_i(\boldsymbol{x}) | \ll | \boldsymbol{x} |^{-u/v} \qquad (i = 1, \ldots, v).$$

We shall call $L_1, \ldots, L_v$ a *Roth system* if for every $\delta > 0$, the inequalities

$$| L_i(\boldsymbol{x}) | < | \boldsymbol{x} |^{-(u/v)-\delta} \qquad (i = 1, \ldots, v)$$

have only finitely many solutions.

THEOREM 4. — (To appear in [5]). *Necessary and sufficient for $L_1, \ldots, L_v$ to be a Roth system is that on every rational subspace S^d of dimension d with $1 \leqq d \leqq k$, the restrictions of these forms have a rank r with*

$$r \geqq dv/k.$$

When $v = 1$, this condition simply says that $r \geqq 1$, and hence it means that $L_1(\boldsymbol{x}) \neq 0$ for every integer point $\boldsymbol{x} \neq \boldsymbol{0}$. The form $L_1(\boldsymbol{x}) = \alpha_1 x_1 + \ldots + \alpha_u x_u + x_k$ with $\alpha_1, \ldots, \alpha_u$, 1 linearly independent satisfies this condition, hence is a Roth system, and the inequality $| L_1(\boldsymbol{x}) | < | \boldsymbol{x} |^{-u-\delta}$ has only finitely many solutions. This immediately implies Theorem 2. It is almost as easy to deduce Theorem 1.

6. Finally we return to Thue's equation (2). A binary form $f(x, y)$ as in (2) factors into linear forms with complex coefficients. Now we shall discuss more general forms $f(\boldsymbol{x}) = f(x_1, \ldots, x_k)$ with rational coefficients which are irreducible over the rationals and which are *decomposable*, i. e. which factor into linear forms with complex coefficients. It turns out that there is a number field K, of degree t, say, and a linear form $L(\boldsymbol{x})$ with coefficients in K, such that $f(\boldsymbol{x}) = aL(\boldsymbol{x})L^{(2)}(\boldsymbol{x}) \ldots L^{(t)}(\boldsymbol{x})$ where L, $L^{(2)}, \ldots, L^{(t)}$ are the conjugates of L and where a is a constant. Thus $f(\boldsymbol{x}) = aN(L(\boldsymbol{x}))$, where N denotes the norm. Thus the study of all equations

$$f(\boldsymbol{x}) = c \tag{7}$$

with constants c is equivalent with the study of all equations

$$N(L(\boldsymbol{x})) = c. \tag{8}$$

Now as $\boldsymbol{x}$ runs through the integer points, the numbers $L(\boldsymbol{x})$ run through a module M in K. A slight extension of Dirichlet's unit theorem shows that if M is a *full module*, i. e. if it contains t linearly independent elements over the rationals, and if K is neither rational nor imaginary quadratic, then there are infinitely many μ in M with $| N(\mu)| \ll 1$. The same is true for any *degenerate* module M, namely a module M which contains a submodule M' which is proportional to a full module in a subfield K' of K, where K' is not of the type excluded above. For a degenerate module M there are constants c for which the equation $N(\mu) = c$ has infinitely many solutions μ in M. It had been conjectured (see, e. g. [1, Chap. IV]) that the opposite is also true. This is in fact the case.

THEOREM 5. — (To appear in [6]). *Suppose M is not degenerate. The equation*

$$N(\mu) = c,$$

where c is an arbitrary constant, has only finitely many solutions μ in M.

In other words, the equation (7) above has only finitely many solutions unless $f(\boldsymbol{x})$ is of some obvious exceptional type. When the number of variables $k = 2$, then this is Thue's result, and when $n = 3$, then it contains results of Skolem and of Chabauty, which were obtained by p-adic methods. It now appears that for this type of equation the Geometry of Numbers is more powerful than p-adic methods.

REFERENCES

[1] Z. I. Borevič and I. R. Šafarevič. — Number theory (Transl. from Russian, 1964 ed.). Academic Press, New York, London (1966).
[2] K. Mahler. — *Proc. London Math. Soc.*, (3), 5 (1955), pp. 358-379.
[3] K. F. Roth. — *Mathematika*, 2 (1955), pp. 1-20.
[4] W. M. Schmidt. — *Acta Math.*, 125 (1970), pp. 189-201.
[5] —. — *Journal of Number Theory* (To appear).
[6] —. — *Mathematische Annalen* (To appear).
[7] E. Wirsing. — *Report of the number theory institute*, Stony Brook (1969) (To appear).

University of Colorado
Department of Mathematics,
Boulder, Colorado 80302
(U. S. A.)

Actes, Congrès intern. math., 1970. Tome 1, p. 505 à 509.

NEW APPLICATIONS OF ANALYTIC AND P-ADIC METHODS IN DIOPHANTINE APPROXIMATIONS

by V. G. SPRINDŽUK

1. Metric theory of diophantine approximations to dependent values.

Let $\alpha_1, \ldots, \alpha_n$ be a set of reals and let us consider the inequality

$$\| a_1\alpha_1 + \cdots + a_n\alpha_n \| < a^{-w},$$

where $a_1, \ldots, a_n$ are integers, $a = \max(|a_1|, \ldots, |a_n|) \neq 0$, $\|x\|$ is the distance from x to the nearest integer. Let $w(\alpha_1, \ldots, \alpha_n)$ be the least upper bound of those $w > 0$ for which (1) has infinitely many solutions in $a_1, \ldots, a_n$. It is well known that $w(\alpha_1, \ldots, \alpha_n) \geqslant n$ for every set $\alpha_1, \ldots, \alpha_n$, and there are such $\alpha_1, \ldots, \alpha_n$ that the equality holds

$$w(\alpha_1, \ldots, \alpha_n) = n. \tag{2}$$

It is also well known that (2) holds for almost all sets $(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ (in the sense of Lebesgue measure in $\mathbb{R}^n$). This is the case of " independent " $\alpha_1, \ldots, \alpha_n$, and the theory of the approximation for this case has been developed quite far after the works of many authors; it has reached now the satisfactory stage [3, 10, 14].

Those $\alpha_1, \ldots, \alpha_n$, for which (2) holds, we shall call " badly approximable numbers ". The following problem has arisen recently [2, 15].

PROBLEM. — Let us take a manifold Γ in $\mathbb{R}^n$ of dimension less than n. Under what conditions on Γ can one say that almost all points of Γ (in the sense of the measure on Γ) are the sets of badly approximable numbers ?

The manifold with this property we shall call " extreme ".

Historically the first example of such a problem was Mahler's conjecture [12], having its origin from the theory of transcendental numbers. The conjecture stated that $w(t, t^2, \ldots, t^n) = n$ for almost every real t $(n = 1, 2, \ldots)$. or for almost every t there are only finitely many polynomials $P(x) = a_0 + a_1x + \cdots + a_nx^n$ with integer coefficients, satisfying $|P(t)| < h_P^{-n-\varepsilon}$, where $\varepsilon > 0$ is any number,

$$h_P = \max(|a_0|, \ldots, |a_n|).$$

This conjecture has been proved [2, 3, 6], and also its analogy for the polynomials of the 2nd degree with any number of variables has been proved, but by the different way [3]. At the same time Schmidt [15] proved the general Theorem:

If Γ is a curve in $\mathbb{R}^2$, $\Gamma = (f_1(t), f_2(t))$, where the functions $f_1(t)$, $f_2(t)$ are 3-times differentiable and $(f_1'f_2'' - f_1''f_2')(t)$ does not vanish almost everywhere, then Γ passes almost only through badly approximable numbers.

Schmidt's theorem shows that if the curve Γ is not " very straight ", it is extreme. One easily suppose in general that if the manifold Γ is not " very plane ", it is extreme. In this general approach the following weak result may be obtained easily.

THEOREM 1. — Let us take the curve Γ in $\mathbb{R}^n$, $\Gamma = (f_1(t),\ldots,f_n(t))$, where $f_1(t),\ldots,f_n(t)$ are n-times differentiable functions and $\det\,(f_i^{(j)}(t))$ $(i, j = 1, 2,\ldots, n)$ does not vanish almost everywhere. Then $w(f_1,\ldots,f_n) \leqslant n(n+1)/2$ almost everywhere.

The proof of this theorem is based on the method of trigonometric sums, but the inequality $w(f_1,\ldots,f_n) \leqslant n^2 + n - 1$ can be obtained directly [5].

If we have ehough information on the structure of the manifold Γ, we can prove in many cases that it is extreme using the method of trigonometric sums.

THEOREM 2. — Let m, n be any integers with $1 \leqslant n \leqslant m$,

$$f_i = f_i(t_1,\ldots,t_m) = \alpha_{i1}\varphi_1(t_1) + \cdots + \alpha_{im}\varphi_m(t_m) \qquad (i = 1,\ldots,n),$$

where $\varphi_j(t)$ are differentiable and $\varphi_j''(t) \neq 0$ almost everywhere $(j = 1, 2,\ldots, m)$, α_{ij} are any rationals with rank $(\alpha_{ij}) = n$. Then we have

$$w(t_1,\ldots,t_m, f_1,\ldots,f_m) = m + n \tag{3}$$

for almost all $(t_1,\ldots,t_m) \in \mathbb{R}^m$.

THEOREM 3. — Let s, m, n be positive integers,

$$f_i = f_i(t_1,\ldots,t_m) = \alpha_{i1}t_1^s + \cdots + \alpha_{im}t_m^s + \varphi_i(t_1,\ldots,t_m) \qquad (i = 1, 2,\ldots, n),$$

where $\varphi_i(t_1,\ldots,t_m)$ are polynomials with real coefficients and with degrees not greater than $s - 1$. If $m \geqslant 2^{s-1}$, then we have (3) for almost all $(t_1,\ldots,t_m) \in \mathbb{R}^m$ in the following two cases at any rate:

(*i*) α_{ij} are rationals, $n \leqslant m$, rank $(\alpha_{ij}) = n$,
(*ii*) $\alpha_{ij} = \alpha_j\beta_i$, where $\alpha_j \neq 0$ $(j = 1, 2,\ldots, m)$ are some reals, and $\beta_i \neq 0$ $(i = 1, 2,\ldots, n)$ satisfy $w(\beta_2\beta_1^{-1},\ldots,\beta_n\beta_1^{-1}) \leqslant m + n$.

The inequality $m \geqslant 2^{s-1}$ arises here due to the application of H. Weyl's estimates for the exponential sums. It can be improved to $m \gg s^2 \log s$ for the large s, if we appeal to I. M. Vinogradov's method.

The application of the method of trigonometric sums leads also to the statements of another kind.

THEOREM 4. — Let $T > 0$ and $\xi(t)$ be the stochastic process of the brownian motion, $0 \leqslant t \leqslant T$, $\alpha_1,\ldots,\alpha_n$ are distinct reals. Then almost every random curve

$$\Gamma = (t, \xi(t + \alpha_1),\ldots, \xi(t + \alpha_n))$$

passes almost only through badly approximable numbers in $\mathbb{R}^{n+1}$ for every $n \geqslant 1$.

These were only a few examples of the problems which one can solve using the method of trigonometric sums. In spite of that there are a lot of problems where the application of this method leads to unovercomed difficulties. It is most of all so when the dimension of the manifold Γ in $\mathbb{R}^n$ is " small " compared with n. This is so, for example, if Γ is a curve in $\mathbb{R}^n$ and n is " large " (very often " n is large " means " $n \geqslant 3$ "). We know only one (up to a nonsingular affinity over the field of rationals) curve $\Gamma = (t, t^2, \ldots, t^n)$ in $\mathbb{R}^n$, which is extreme. This curve just corresponds to the Mahler's conjecture mentioned above. I suppose the main ideas of the solution of Mahler's conjecture are quite useful for the investigation of some more general problems of the same kind. But it is clear, of course, that some more technique should be involved. Recently I learned that following this way R. Sliesoraitiene from Vilnius proved the analogy of Mahler's conjecture for the polynomials of the 3rd degree with 2 variables. The work of Baker [6] with its refinements of the proof of Mahler's conjecture was useful there.

2. **Effective rational approximation to algebraic numbers.**

Let $f = f(x, y)$ be an irreducible binary form with integer coefficients and degree $n \geqslant 4$, $p_1, \ldots, p_s$ are any fixed prime numbers, $p_i \neq p_j (i \neq j)$, A is an integer. It was well known due to Mahler [13] that the equation

$$f(x, y) = A p_1^{z_1} \ldots p_s^{z_s}, \qquad (x, y) = 1 \tag{1}$$

has only finitely many solutions in integers $x, y, z_1 \geqslant 0, \ldots, z_s \geqslant 0$. But Mahler's method does not allow to find out all its solutions because it is not effective. Recently A. I. Vinogradov and the author [1] indicated the method of effective determination of all the solutions of (1), using the work of Baker [7]. The same time Baker [8] investigated the equation $f(x, y) = A$ and obtained for its solutions the effective estimate

$$\max (|x|, |y|) < c_1 \exp (\log |A|)^{\mathscr{H}}, \tag{2}$$

where $\mathscr{H} = n + 1 + \varepsilon$, $\varepsilon > 0$ is any number and c_1 is a computable number independing on A. Coates [9] extended the arguments of Baker to the equation (1) and obtained the estimate of the form (2) with $\mathscr{H} = n(s + 1) + 1 + \varepsilon$. Independently the author tried to obtain the best possible estimate of the form (2) and partially succeeded on his way when he proved (2) with $\mathscr{H} = 2 + \varepsilon$ for the forms of special kind and provided that $Ap_1, \ldots, p_s$ has no common factor with the discriminant of $f(x, y)$ [4]. Recently the author realised that further development of his method leads to (2) with $\mathscr{H} = 2 + \varepsilon$ for " almost all " binary forms and without any restrictions on the $A, p_1, \ldots, p_s$.

THEOREM 1. — Suppose $f = f(x, y) = aNm(x - \alpha y)$, where a is an integer. Let us call the form f (and algebraic number α) " exceptional ", if there is such a numeration of the conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ that

$$\frac{\alpha^{(1)} - \alpha^{(i)}}{\alpha^{(2)} - \alpha^{(i)}} \cdot \frac{\alpha^{(2)} - \alpha^{(j)}}{\alpha^{(1)} - \alpha^{(j)}} = \frac{1 - \zeta_i}{1 - \zeta_j} \tag{3}$$

for every i, j ($i \neq j$, $3 \leqslant i, j \leqslant n$), where $\zeta_i \neq 1$ ($i = 3, 4, \ldots, n$) are some roots of 1. All the solutions of (1) satisfy (2) with $\mathscr{H} = 2 + \varepsilon$ provided that f is not an exceptional form.

It follows immediately that we have

THEOREM 2. — If α is not exceptional algebraic number at least of the 4th degree and S is any fixed set of prime ideals of the field $\mathbb{Q}(\alpha)$, then we have for every non-zero pair of integers x, y

$$|x - \alpha y| \prod_{\mathfrak{p} \in S} |x - \alpha y|_{\mathfrak{p}} > c_2 X^{-n+1} \exp (\log X)^{1/2-\varepsilon}, \tag{4}$$

where n is the degree of α, $| \dots |_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic norm in $\mathbb{Q}(\alpha)$, $\varepsilon > 0$ is any number, $c_2 > 0$ is a computable number independing on $X = \max (|x|, |y|)$.

Obviously, if α is totally real or $\alpha = \sqrt[n]{D}$ (D is an integer), it is not exceptional one. More than that, it follows from (3) that if the polynomial $f(x, 1)$ has symmetric Galois group and $n \geqslant 5$, then f is not exceptional. It is well known that " almost all " polynomials with integer coefficients have the symmetric Galois group, so " almost all " binary forms are not exceptional (*).

To introduce a lemma we suppose that p is a rational prime, $\mathbb{Q}_p$ is the p-adic completion of the field of rationals $\mathbb{Q}$, $\mathbb{T}_p$ is the p-adic completion of the algebraic closure of $\mathbb{Q}_p$, $| \dots |_p$ is the p-adic valuation on $\mathbb{T}_p$, $|p|_p = p^{-1}$, $\log z$ is the logarithmic function, defined in the disc $|z - 1|_p < 1$, $z \in \mathbb{T}_p$. For a finite extension $\mathbb{K}$ of $\mathbb{Q}$ the embedding $\mathbb{K} \to \mathbb{T}_p$ defines a valuation $| \dots |_p$ on $\mathbb{K}$.

The height of algebraic α we denote by $h(\alpha)$.

LEMMA. — Let $\alpha_1, \dots, \alpha_n$ be $n \geqslant 2$ algebraic numbers, $\beta_1, \dots, \beta_{n-1}$ are algebraic integers, $h(\alpha_n) = A$, $\max h(\beta_i) \leqslant H$ $(i = 1, 2, \dots, n-1)$,

$$\log A < H^{\frac{1}{2}(1-\varepsilon_1)},$$

where ε_1 is a fixed number with $0 < \varepsilon_1 < 1$, $\mathbb{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1})$, $| \dots |_p$ is a valuation on $\mathbb{K}$, $|\alpha_i^r - 1|_p \leqslant p^{-e_p}$ $(i = 1, 2, \dots, n)$ with some integer $r > 0$ and $e_2 = 2$, $e_p = 1$ for $p \geqslant 3$. Further suppose that $\varepsilon = \varepsilon_1 (n+1)^{-1}$ and the following inequality holds

$$|\beta_1 \log (\alpha_1^r) + \cdots + \beta_{n-1} \log (\alpha_{n-1}^r) - \log (\alpha_n^r)|_p > p^{-H^{\varepsilon/4}}.$$

Then for any $\delta > 0$ we have

$$|\beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1} - \log \alpha_n| > e^{-\delta H} \tag{5}$$

provided that H exceeds a computable value depending on $\mathbb{K}, \alpha_1, \dots, \alpha_{n-1}, \varepsilon_1, p, r, \delta$.

The same suppositions lead to the analogy of (5) in every q-adic metric ($q \neq p$ is any prime).

For the application of this lemma to the study of the equation (1) we need to choose in some appropriate way the prime numbers p and, consequently, to involve some information on the distribution of prime numbers. It can be done due to the theorem of Frobenius [11].

(*) If $n \geqslant 5$ no exceptional form exists, but if $n = 4$ such forms do exist.

As I can see, the method in the consideration may be developed so far to give the best possible estimate of the form (2), i. e. (2) with $\mathscr{H} = 1 + \varepsilon$ (and then (4) with $1 - \varepsilon$ instead of $\frac{1}{2} - \varepsilon$) (*).

REFERENCES

[1] А. И. Виноградов и В. Г. Спринджук. — О представлении чисел бинарными формами, Матем. заметки, 3, N° 4 (1968), pp. 369-376.
[2] В. Г. Спринджук. — Доказательство гипотезы Малера о мере множества S-чисел, Изв. АН СССР, сер. матем., 29, N° 2 (1965), pp. 379-436.
[3] —. — Проблема Малера в метрической теории чисел, Изд. « Наука и техника », Минск (1967) (**).
[4] —. — Эффективные оценки в « тернарных » показательных диофантовых уравнениях, Докл. АН БССР, 13, N° 9 (1969), pp. 777-780.
[5] А. С. Пяртли. — Диофантовы приближения на подмногообразиях евклидова пространства, Функц. анализ и его прилож., 3 N° 4 (1969), pp. 59-62.
[6] A. Baker. — On a theorem of Sprindžuk, *Proc. Roy. Soc.*, 292, No. 1428 (1966), pp. 92-104.
[7] —. — Linear forms in the logarithms of algebraic numbers, *Mathematika*, 14 (1967), pp. 204-216.
[8] —. — Contributions to the theory of diophantine equations. I. On the representation of integers by binary forms, *Philos. Trans. Roy. Soc.* (London), A 263 (1968), pp. 173-191.
[9] J. Coates. — An effective p-adic analogue of a theorem of Thue, *Acta Arithmetica*, 15 (1969), pp. 279-305.
[10] V. Ennola. — On metric diophantine approximation, *Turun yliopiston julk.*, A 1, No. 113 (1967), pp. 3-8.
[11] G. Frobenius. — Über Bezeihungen zwischen den Primidealen eines algebraische Körpers und die Substitutionen seiner Gruppe, *Sitzber. Berl. Akad.* (1896), pp. 689-705.
[12] K. Mahler. — Über das Mass der Menge aller S-Zahlen, *Math. Ann.*, 106 (1932), pp. 131-139.
[13] —. — Über die rationalen Punkte auf Kurven vom geschlecht Eins, *Journ. Reine und Angew. Math.*, 170 (1934), pp. 168-178.
[14] W. Schmidt. — Metrical theorems on fractional parts of sequences, *Trans. Amer. Math. Soc.*, 110 (1964), pp. 493-518.
[15] W. Schmidt. — Metrische Sätze über simultane Approximation abhängiger Grossen, *Monatsch. für Math.*, 63, No. 2 (1964), pp. 154-166.

Institute of Mathematics
of the Academy of Sciences
Minsk (U. R. S. S.)

(*) More sharp result is indicated in *Doklady Acad. Nauk B. S. S. R.*, vol. 15, No. 2 (1971), pp. 101-104.

(**) There is an English translation: « Mahler's problem in metric number theory », *Amer. Math. Soc., Transl. Math. Monographs*, vol. 25 (1969).

Actes, *Congrès intern. math.*, 1970. Tome 1, p. 511 à 518.

CLASS-NUMBER PROBLEMS IN QUADRATIC FIELDS

by H. M. STARK

1. Introduction.

Four years ago, Baker and I gave the first accepted solutions to the problem of finding all complex quadratic fields of class-number one. This paper will be a report on some of the more interesting developments in class-number problems and the functions connected with these problems. It is now possible to completely settle the class-number two problem; this was discovered this summer independently by Baker and myself. The functions connected with this problem lead naturally to a study of the values of Abelian L-functions and more generally Artin L-functions at $s = 1$. An interesting consequence of these studies is a theorem on the factorization of regulators of extension fields. I wish to acknowledge that I have had the benefit of many conversations with Prof. Siegel. He has given me many valuable insights and references.

2. The Heegner method.

We begin with Heegner's discounted solution [5] to the class-number one problem of 18 years ago. For Im $z > 0$, $q = e^{2\pi i z}$, put

$$j(z) = \frac{\{1 + 240 \sum_{n=1}^{\infty} (\sum_{d|n} d^3) q^n\}^3}{q \prod_{n=1}^{\infty} (1 - q^n)^{24}}.$$

Suppose d is the discriminant of a complex quadratic field of class-number $h(d)$. If d is odd, then $J = j\left(\frac{1 + \sqrt{d}}{2}\right)$ is an algebraic integer of degree $h(d)$ and in fact $Q(\sqrt{d}, J)$ is the absolute class field (i. e. the maximal unramified Abelian extension) of $Q(\sqrt{d})$. If $d = -3$ or $3 \nmid d$, the real cube root of J is also of degree $h(d)$; we denote this real cube root by γ.

Let

$$f(z) = q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-1/2})$$

and set $f = f(\sqrt{d})$. Then

$$f^{24} + \gamma f^{16} - 256 = 0. \tag{1}$$

Thus f^8 is an algebraic integer of degree $\leq 3h(d)$. Assume further that $|d| \equiv 3 \pmod 8$. It is an old result of Weber [13] that in this case f^8 is of degree exactly $3h(d)$. Weber proved that f^2 is in fact of degree $3h(d)$ and conjectured that f is of degree $3h(d)$. This conjecture was proved two years ago by Birch [2]. Contrary to popular opinion, this conjecture plays no role in the part of Heegner's paper dealing with class-number one.

Thus $Q(f^2) = Q(f^8)$ is a cubic extension of $Q(\gamma) = Q(J)$. Hence f^2 satisfies a unique cubic equation over $Q(\gamma)$ which we write as

$$f^6 - 2\beta f^4 - 4\alpha f^2 - 4 = 0, \tag{2}$$

since it ultimately turns out that the constant term is -4 and α and β are algebraic integers in $Q(\gamma)$. Transposing $2\beta f^4 + 4$ to the other side and squaring gives

$$f^{12} - (8\alpha + 4\beta^2)f^8 + (16\alpha^2 - 16\beta)f^4 - 16 = 0. \tag{3}$$

Transposing $(8\alpha + 4\beta^2)f^8 + 16$ to the other side and squaring gives

$$f^{24} - 16(2\alpha^2 + 4\alpha\beta^2 + \beta^4 + 2\beta)f^{16} + 128(2\alpha^4 - 4\alpha^2\beta + \beta^2 - 2\alpha)f^8 - 256 = 0\,. \tag{4}$$

This is the unique cubic equation for f^8 over $Q(\gamma)$ as is (1). Equating the coefficients of f^8 in both equations gives

$$2\alpha(\alpha^3 + 1) = (2\alpha^2 - \beta)^2. \tag{5}$$

In the case of $h(d) = 1$, α and β are rational integers and (5) is easily solved. The solutions are

$$(\alpha, \beta) = (0, 0),\ (1, 0),\ (-1, 2),\ (2, 2),\ (1, 4),\ (2, 14).$$

From the coefficients of f^{16} in (1) and (4) we find the corresponding values of γ to be

$$\gamma = 0,\ -32,\ -96,\ -960,\ -5\,280,\ -640\,320$$

which are known to correspond to

$$d = -3,\ -11,\ -19,\ -43,\ -67,\ -163$$

respectively. This gives the six fields of class-number one and $|d| \equiv 3 \pmod 8$; the only other discriminants with $h(d) = 1$ are $d = -4,\ -7,\ -8$. This is my version [10, 12] of Heegner's solution to the class-number one problem; his solution has also been resurrected by Birch [2, 3] and Deuring [4].

Set

$$\zeta = 2\beta - 2\alpha^2\,;$$

the coefficient of f^4 in (3) is simply -8ζ and, thanks to (5) the coefficient of f^8 is just $-2\zeta^2$. The connection of ζ with γ is then seen to be

$$-\gamma + 12 = 4(\zeta + 1)^2(\zeta^2 - 2\zeta + 3). \tag{6}$$

We write it in this form because of a footnote on p. 232 of Heegner's paper (and proved by Birch [3]) which states that $-\gamma + 12$ is 3 times the square of an algebraic integer of degree $h(d)$ when $|d| \equiv 7 \pmod{12}$. This is related to the fact that $-J + 1\,728$ is $|d|$ times a square which was already known by Weber. Hence when we consider

$|d| \equiv 19 \pmod{24}$, so that we also have $|d| \equiv 3 \pmod 8$, we see from (6) that there is an integer δ in $Q(\gamma) = Q(J)$ such that

$$\zeta^2 - 2\zeta + 3 = 3\delta^2. \tag{7}$$

This integer δ is very useful. Let F be defined by the quadratic equation,

$$F - F^{-1} = \begin{cases} \sqrt{2}(\zeta - 1) & \text{if} \quad \dfrac{|d| + 1}{4} \equiv 1 \pmod 4 \\ -\sqrt{2}(\zeta - 1) & \text{if} \quad \dfrac{|d| + 1}{4} \equiv 3 \pmod 4. \end{cases} \tag{8}$$

[The $\pm$ is introduced so that the right side of (8) will always be positive. This comes about because there are four equations of the form

$$f^{12} - 2\zeta^2 f^8 - 8\zeta - 16 = 0$$

that are factors of (1) and only one of them has ζ in $Q(\gamma)$. Two of the values of ζ are complex and certainly not the correct value since $Q(\gamma)$ is a real field. The other two values are real, one positive and one negative. It is a non-trivial fact [11] that the positive value is the correct one if $\dfrac{|d| + 1}{4} \equiv 1 \pmod 4$ and the negative value is the correct one if $\dfrac{|d| + 1}{4} \equiv 3 \pmod 4$]. By its very definition, F is a unit. We will now show that $\varepsilon_{12}^{-1/2}F$ is a unit in $Q(J, \sqrt{3})$ where ε_{12} is the fundamental unit in the field $Q(\sqrt{3})$ of discriminant 12. We find that the positive root of (8) is

$$F = \frac{\pm\sqrt{2}(\zeta - 1) + \sqrt{2(\zeta - 1)^2 + 4}}{2} = \frac{\sqrt{2}}{2}[\pm(\zeta - 1) + \delta\sqrt{3}], \tag{9}$$

and since $\varepsilon_{12}^{-1/2} = (2 - \sqrt{3})^{1/2} = \dfrac{1}{\sqrt{2}}(\sqrt{3} - 1)$, it follows that $\varepsilon_{12}^{-1/2}F$ is a unit in $Q(J, \sqrt{3})$ as claimed.

3. Class-number two.

We wish to examine this unit more closely in the case of class-number two. So suppose $h(d) = 2$ and $|d| \equiv 19 \pmod{24}$; this is the only case that the old methods couldn't settle. Then we may write

$$d = -pq, \qquad p \equiv 1 \pmod 4, \qquad q \equiv 3 \pmod 4,$$

where p and q are odd primes. In this case J is in $Q(\sqrt{p})$ and there are three fundamental units in $Q(J, \sqrt{3}) = Q(\sqrt{p}, \sqrt{3})$. The units ε_{12}, ε_p, ε_{12p} are independent in this field but not fundamental; however, any unit squared is representable in terms of these units. In particular $F^2 = \varepsilon_{12}(\varepsilon_{12}^{-1/2}F)^2$ is so representable and we write

$$F^2 = \varepsilon_{12}^A \varepsilon_{12p}^B \varepsilon_p^C. \tag{10}$$

In fact $C = 0$ since from (8), the quadratic equation for F^2 over $Q(\sqrt{p})$ is

$$F^4 - [2(\zeta - 1)^2 + 2]F^2 + 1 = 0$$

and hence

$$1 = N_{Q(\sqrt{p},\sqrt{3})/Q(\sqrt{p})}(F^2) = \varepsilon_p^{2C}.$$

It can further be shown that A and B are both positive by considering $\varepsilon_{12}^{A}\varepsilon_{12p}^{-B}$ and how it is related to the conjugate of J in $Q(\sqrt{p})$.

Next, using (9) and tracing things back to J, we see that

$$F = e^{-\frac{\pi i\sqrt{d}}{12}} + O(1) = e^{\frac{\pi\sqrt{|d|}}{12}} + O(1) \qquad \text{as} \qquad |d| \to \infty$$

and hence

$$\left[A \log \varepsilon_{12} + B \log \varepsilon_{12p} + \frac{\sqrt{d}}{6}\log(-1)\right] = \log\left(e^{\frac{i\pi\sqrt{d}}{6}}F^2\right) = O\left(e^{-\frac{\pi\sqrt{|d|}}{12}}\right).$$

This gives a very nice linear form in three logarithms with A and $B = O(\sqrt{|d|})$ since they are both positive. However $\log \varepsilon_{12p}$ may be as large as (roughly) $\sqrt{p}\log p$. For a given $\varepsilon > 0$, Baker's earlier transcendence results could handle the class-number two problem when the smaller of p and q were less than $|d|^{\frac{1}{4}-\varepsilon}$. Thus we will further restrict ourselves to $p < |d|^{\frac{1}{4}+\varepsilon}$ and hence

$$\log \varepsilon_{12p} = O(|d|^{\frac{1}{4}+\varepsilon}).$$

Therefore we may write our linear form as

$$|\sqrt{d}\log(-1) + 6A\log\varepsilon_{12} + 6B\log\varepsilon_{12p}| < e^{-H} \tag{11}$$

with

$$A,\ B,\ \sqrt{d} = O(H)$$

and

$$\log \varepsilon_{12p} = O(H^{\frac{1}{2}+2\varepsilon})$$

But $H^{\frac{1}{2}+2\varepsilon}$ is still too large to be able to apply the previous general results of Baker. Here, however, we have only one large logarithm and hence should expect to be able to improve the general transcendence results in this case. This is indeed possible and was done simultaneously this summer by Baker and myself. An exact formulation of my version is

THEOREM 1. — Let $\alpha_1 = -1$ and $\alpha_2, \ldots, \alpha_n$ be the fundamental units of different real quadratic fields ($n \geq 2$). Set

$$A = \max_{1 \leq j \leq n-1} |\log \alpha_j|$$

where $\log \alpha_j$ is the principal value. Let $b_1 = \sqrt{-D}$ where D is a non-negative rational integer and let $b_j\,(j \geq 2)$ be rational integers. Suppose $0 < \varepsilon \leq 1$, $v \geq 1$ and H are real numbers with

$$\varepsilon = (8n^4 + 4n^3 + 4n^2)\Delta$$

such that

$$\max(A, \log \alpha_n) < H^{1-\varepsilon},$$

$$|b_j| < H^v, \qquad j = 1, \ldots, n;$$

$$H > \left(\frac{2^{4n^3}.3^{2n+3}(v+3)^{2n-2}A}{(n\Delta)^{2n-2}}\right)^{1/(8n^2-8n-2)\Delta}$$

If not all the b_j are zero then

$$|b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n| \geq e^{-H}.$$

This theorem clearly applies to the linear form (11). A numerically better version of this theorem, which is too complicated to state here, then leads to the result,

THEOREM 2. — If $h(d) = 2$ then $|d| < 10^{1100}$.

4. The unit F.

It may well be asked how one would dream up the equations leading to F. The answer is that my original solution to the class-number one problem and Heegner's solution are closely related. The unit F comes from my original method as the value of a certain L-function at $s = 1$. Let $Q(x, y)$ be a positive definite binary quadratic form of discriminant d and let k be the discriminant of a quadratic field (real or complex) with $(k, d) = 1$ and the associated real character χ_k defined by the Kronecker symbol $\chi_k(n) = \left(\frac{k}{n}\right)$. Set

$$L(s, \chi_k, Q) = \frac{1}{\omega} \sum_{m,n \neq 0,0} \frac{\chi_k(Q(m, n))}{Q(m, n)^s} \tag{12}$$

where $\omega = 6, 4, 2$ for $d = -3$, $d = -4$, and $d < -4$ respectively. For the particular form

$$Q_0(x, y) = x^2 + xy + \frac{|d| + 1}{4} y^2$$

and $|d| \equiv 19 \pmod{24}$, it turns out that

$$L(1, \chi_{12}, Q_0) = \frac{4\pi}{3\sqrt{|d|}} \log F. \tag{13}$$

Let ε_k denote the fundamental unit of $Q(\sqrt{k})$ when $k > 0$ and set $g = 1$, $t = d$ for $k > 0$, $g = d$, $t = 1$ for $k < 0$. It has been known since Heilbronn's work [6] that for $(k, d) = 1$, $k \neq -3, -4$,

$$\sum_Q L(1, \chi_k, Q) = L(1, \chi_{kg}) L(1, \chi_{kt}) = \frac{2\pi h(kg) h(kt) \log \varepsilon_{kg}}{|k| \sqrt{|d|}} \tag{14}$$

where the sum is over a complete set ($h(d)$ in all) of inequivalent quadratic forms. For example, if $h(d) = 1$ and $|d| \equiv 19 \pmod{24}$ then

$$F = \varepsilon_{12}^{1/2} \varepsilon_{12}^{[h(12d) - 4]/8}$$

which agrees with the general result on the field containing F since in this case $h(12d) \equiv 4 \pmod 8$. It has recently been realized by Baker, myself (after being given the result in terms of ring class characters by Prof. Siegel) and, I believe, L. J. Goldstein that there is a similar formula to (14) for each genus.

Let us decompose d in all possible ways as $d = gt$ where g and t are also discriminants of quadratic fields (or are 1 and d) with g and k having the same sign. There are 2^{r-1} such decompositions where r is the number of distinct prime factors of d.

To each decomposition, there corresponds a genus character $\chi_{g,t}$ (i. e. a character on the group of genera) and for $(k, d) = 1$, $k \neq -3, -4$, we have

$$\sum_{Q \in G} L(1, \chi_k, Q) = 2^{1-r} \sum_{g,t} \chi_{g,t}(G) L(1, \chi_{kg}) L(1, \chi_{kt}) \tag{15}$$
$$= \frac{2^{2-r}\pi}{|k| \sqrt{|d|}} \sum_{g,t} \chi_{g,t}(G) h(kg) h(kt) \log \varepsilon_{kg}$$

where the sum on the left is over a complete set ($h(d)/2^{r-1}$ in all) of inequivalent forms in the genus G.

For example in the case of $h(d) = 2$, $|d| \equiv 19 \pmod{24}$, Q_0 is the principal genus and we have

$$F = \varepsilon_{12}^{h(12d)/16} \varepsilon_{12p}^{h(12p)h(-12q)/16}$$

which incidentally shows that in (10),

$$A = h(12d)/8, \qquad B = h(12p)h(-12q)/8, \qquad C = 0.$$

In fact we may use (15) in the case of one class per genus and $|d| \equiv 19 \pmod{24}$ to calculate $J = j\left(\frac{1 + \sqrt{d}}{2}\right)$ from Dirichlet's class-number formula. This would have saved Weber a lot of trouble.

The result (15) also gives us a good start on $h(d) = 4$ and one class per genus. We can get an effective solution to the problem for odd discriminants except in the case that $d = -p_1 p_2 p_3$; p_1, p_2, p_3 are primes, $p_1 \equiv 3 \pmod 4$ and p_2 and p_3 are between $|d|^{\frac{1}{4}-\varepsilon}$ and $|d|^{\frac{1}{4}+\varepsilon}$. In this case the best that we can do is to find a linear form in four logarithms, two of which are large. The corresponding problem for even discriminants is also still open. Conjectured improvements in Theorem 1 would appear to be capable of effectively settling the problem of class-number 2^n and one class per genus (n fixed) although since the number of logarithms is increasing with n, we still might not get an effective solution to the problem of one class per genus.

5. Values of L-functions at $s = 1$.

The result of (13) is more specific than (14) or (15) when there is more than one class per genus. On the basis of it and similar results for $k = 5$ and 8, we make the following conjecture (Conjectures 1, 2 and 4 are given as conjectures rather than theorems because I have not had sufficient time to examine my proofs which I have found only in the last month);

CONJECTURE 1. — When $(k, d) = 1$,

$$L(1, \chi_k, Q) = r \frac{\pi}{\sqrt{|d|}} \log \varepsilon$$

Where r is a rational number depending on k and ε is a unit in (the real part of) the absolute class field of $Q(\sqrt{d})$ with $\sqrt{k}$ adjoined.

The key to the proof is that $\chi_k(Q(m, n))$ is also a ring class character (mod k). It is in fact a primitive ring (and even ray) class character as may be seen by comparing the functional equations of $L(s, \chi_k, Q)$ with those of Abelian L-functions for complex quadratic fields. If $\chi^{(1)}, \ldots, \chi^{(h)}$ are the characters of the absolute ideal class group, then $\chi_k\chi^{(J)}$ is also a primitive ring class character (mod k) and

$$L(1, \chi_k, Q) = \frac{1}{h(d)} \sum_{J=1}^{h(d)} \bar{\chi}^{(J)}(Q) L(1, \chi_k\chi^{(J)}, \sqrt{d})$$

where $\bar{\chi}^{(J)}(Q)$ is $\bar{\chi}^{(J)}$ evaluated on the ideal class corresponding to the form Q and for ring or ray class characters χ,

$$L(s, \chi, \sqrt{d}) = \sum_{\mathfrak{A}} \frac{\chi(\mathfrak{A})}{(N\mathfrak{A})^s}$$

where the sum is over all integral ideals of $Q(\sqrt{d})$. Conjecture 1 is then a special case of the following conjecture.

CONJECTURE 2. — Let f be an integral ideal in $Q(\sqrt{d})$, $f \neq (1)$, and χ a primitive ray class character (mod f) corresponding to the ray class field $K/Q(\sqrt{d})$ with relative Galois group G. Then

$$L(1, \chi, \sqrt{d}) = \alpha \frac{\pi}{\sqrt{|d|}} \sum_{g \in G} \bar{\chi}(g) \log |\varepsilon_g|$$

where the ε_g are units in K and α is a rational number times a Gaussian sum.

Unless I have missed something, the proof is a simple matter of deciphering the notation of Ramachandra [8] and applying his results to $L(1, \chi, \sqrt{d})$ as expanded by Siegel [9] from Kronecker's second limit formula. Conjecture 2 is a striking analogy to the well known similar results for ordinary Dirichlet L-functions. Because of this, we come to

CONJECTURE 3. — Any Abelian L-function or Artin L-function at $s = 1$ is an algebraic number times π^a times a homogeneous form in logarithms of units from the corresponding over-field with algebraic coefficients and degree b (and which is in fact a b by b determinant of linear forms of logarithms). If the L-function is an Abelian L-function defined over a field k of degree n then $a + b = n$ and a and b can be determined from the gamma factors in the functional equation.

Both extremes of $a = 0$, $b = n$ (a totally real extension of a (totally real) field) and $a = n$, $b = 0$ (a totally imaginary quadratic extension of a totally real field) can occur. Besides the result of Conjecture 2 and Dirichlet L-functions, there are only isolated verifications of this conjecture. When one multiplies all the L-functions at $s = 1$ corresponding to a particular over-field K, one gets the residue of the Dedekind zeta function of K at $s = 1$. Thus a particularly interesting consequence of Conjecture 3 is

CONJECTURE 4. — A regulator of a relatively normal extension field factorizes in accordance with Conjecture 3.

A simple consequence is that if $k \subset K$ then the regulator of k divides (in the obvious sense) the regulator of K. This is simple to prove, we take a set of fundamental units $\varepsilon_1, \ldots, \varepsilon_r$ of k and complete them to a system of independent units $\varepsilon_1, \ldots, \varepsilon_R$ in K. The regulator for $\varepsilon_1, \ldots, \varepsilon_R$ is a rational number times the regulator of K and by subtracting rows is easily seen to have a factor of the regulator of k. The result of this corollary allows us to verify many instances of Conjecture 3 since a zeta function of one field is sometimes an L-function times the zeta function of a subfield.

The simplest case of Conjecture 4 is the case of a totally real relatively normal extension K of a field k. When $k = Q$, the proof is based upon Minkowski's theorem on units [7] which shows that the regulator of K is essentially a group determinant. For $k \neq Q$, Minkowski's theorem is replaced by Artin's generalization [1].

The proofs sketched above of Conjectures 1, 2 and 4 will appear in due course, assuming that they continue to hold up. A proof of Conjecture 3 would appear at this time to be very difficult.

REFERENCES

[1] E. Artin. — Über Einheiten relativ galoisscher Zahlkörper, *Crelle*, 167 (1932), pp. 153-156.

[2] B. J. Birch. — Diophantine analysis and modular functions, in *Algebraic Geometry*, Oxford (1969), pp. 35-42.

[3] —. — Weber's class invariants, *Mathematika*, 16 (1969), pp. 283-294.

[4] Max Deuring. — Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, *Invent. Math.*, 5 (1968), pp. 169-179.

[5] Kurt Heegner. — Diophantische Analysis und Modulfunktionen, *Math. Z.*, 56 (1952), pp. 227-253.

[6] H. Heilbronn. — On the class-number in imaginary quadratic fields, *Quart. J. Math. Oxford Ser.*, 5 (1934), pp. 150-160.

[7] Hermann Minkowski. — Zur Theorie der Einheiten in dem algebraischen Zahlkörpern, *Werke*, vol. 1, pp. 316-319.

[8] K. Ramachandra. — Some applications of Kronecker's limit formulas, *Ann. of Math.*, 2nd series 80 (1964), pp. 104-148.

[9] C. L. Siegel. — *Lectures on advanced analytic number theory*, Tata Institute, Bombay (1961).

[10] H. M. Stark. — On the « gap » in a theorem of Heegner, *J. Number Theory*, 1 (1969), pp. 16-27.

[11] —. — The role of modular functions in a class number problem, *J. Number Theory*, 1 (1969), pp. 252-260.

[12] —. — Recent advances in determining all complex quadratic fields of class number one, *Amer. Math. Soc., Proceedings of the symposium held in Stonybrook in 1969.*

[13] H. Weber. — *Lehrbuch der Algebra*, vol. 3, 3rd ed., Chelsea, New York (1961) (reprint of the 1908 edition).

M. I. T. 2-279
Cambridge
Massachusetts 02139
U. S. A.

Actes, Congrès intern. math., 1970. Tome 1, p. 519 à 528.

DIOPHANTINE APPROXIMATION AND ANALYSIS

by PAUL TURÁN

A fundamental difficulty of complex analysis, inherent in it from the very beginning on, lies in the fact that—apart from trivial cases—the expression

$$\left|\sum_{j=1}^{n} \eta_j\right| \qquad (\eta_j \text{ complex})$$

in general cannot be estimated *from below* neither by $\sum_{j=1}^{n} |\eta_j|$ nor by $\max_j |\eta_j|$ or by $\min_j |\eta_j|$. Calling these Problems I, II or III respectively H. Bohr was the first who—in the case of Problem I—discovered in 1909 two inequalities which could serve in certain situations as substitutes for the required lower bounds. These assert —in slightly more general form than he ever stated or used them—that for arbitrary complex b_j numbers, arbitrarily small $\varepsilon > 0$ and complex z_j-numbers with linearly independent arguments for a suitable integer ν_1 the inequality

$$\frac{\left|\sum_{j=1}^{n} b_j z_j^{\nu_1}\right|}{\sum_{j=1}^{n} |b_j|\, |z_j|^{\nu_1}} \geqq 1 - \varepsilon, \tag{1}$$

further for *positive* b_j's and arbitrarily complex z_j's with a suitable integer ν_2 the inequality

$$\frac{\left|\sum_{j=1}^{n} b_j z_j^{\nu_2}\right|}{\sum_{j=1}^{n} |b_j|\, |z_j|^{\nu_2}} \geqq \cos \frac{2\pi}{5} \tag{2}$$

holds. The great difference between (1) and (2) is that whereas suitable ν_2 in (2) can be found in every interval of form $(\eta, \eta . 5^n)$, no localisation for ν_1 in (1) can be given. Bohr's ingenious proofs were based on two results taken from the seemingly farlying theory of diophantine approximation, due to Kronecker and Dirichlet respectively and he applied (1) and (2) to various questions concerning almost periodical functions, Dirichlet series in particular to Riemann zeta function. No doubt this was the first interaction between the two theories in the title of the talk.

Some years later analysis shot back. H. Weyl's theory of uniform distribution mod 1, the Siegel-Mordell analytical proof for Minkowski's fundamental theorem, Bohr-Jessen's analytical proofs for the above used Kronecker-theorem seemed to give a decisive advantage to " continuous " methods compared to " discontinuous " ones. Much later I observed that the number of fields of applications of diophantine approximations to analysis, envisaged by Bohr, could be essentially enlarged if the absolute value of the " generalised power-sum "

$$f(\nu) = \sum_{j=1}^{n} b_j z_j^{\nu} \qquad (\nu \text{ positive integer})$$

could be estimated for appropriate ν-values from below *without* the above mentioned strong restrictions on the b_j coefficients and z_j-vectors, not necessarily by the " H. Bohr-norm "

$$M_0(\nu) = \sum_{j=1}^{n} |b_j| \, |z_j|^{\nu} \tag{3}$$

but—depending on the intended application—by other " norms " as

$$\begin{aligned} M_1(\nu) &= (\min_j |z_j|)^{\nu} && (\text{" minimum norm "}) \\ M_2(\nu) &= (\max_j |z_j|)^{\nu} && (\text{" maximum norm "}) \\ M_3(\nu) &= \Big(\sum_{j=1}^{n} |b_j|^2 |z_j|^{2\nu}\Big)^{1/2} && (\text{" Wiener norm "}) \\ M_4(\nu) &= \max_j |b_j| && (\text{" Cauchy norm "}) \end{aligned} \tag{4}$$

or even by other appropriate norms. The essential further requirement was however that the ν-values, for which the lower estimation holds, could be localised and even much stronger than in (2). It turned out that such lower bounds can actually be given, furnishing substitutes for problem II and III among others and pursuing systematically this point of view it was possible to extend the scope of applicability quite essentially. We shall discuss the main results of this theory, parallel with some of its applications with a cursory classification of its (to a great extent open) problems.

Generally speaking the problems are extremal problems, more exactly minimax problems. Restricting ourselves to the norms in (3) and (4) a typical among our problems of first type is to determine at given $0 \leqq l \leqq 3$, nonnegative integer m and fixed complex b_j-coefficients

$$\min_{z_1,\ldots,z_n} \max_{\nu=m+1,m+2,\ldots,m+n} \frac{\left|\sum_{j=1}^{n} b_j z_j^{\nu}\right|}{M_l(\nu)} = U_l(m, n) \tag{5}$$

and to determine all extremal-systems $(z_1^*, z_2^*, \ldots, z_n^*)$. A *complete* solution of such problems succeeded seldomly; for the intended applications however generally good estimations are sufficient. Particularly important for applications are the norms $M_1(\nu)$ and $M_2(\nu)$; no wonder since they are the substitutes for Problems II and III. As to the first norm I proved using exclusively classical algebraic tools the inequality

$$U_1(m, n) > \left(\frac{n}{2e(m+n)}\right)^n |b_1 + \ldots + b_n|; \tag{6}$$

by a more cautious treatment of my basic identity de Bruijn and Makai found the best possible inequality

$$U_1(m, n) > \left\{\sum_{j=0}^{n-1} 2^j \binom{m+j}{j}\right\}^{-1} |b_1 + \ldots + b_n|, \tag{7}$$

which is however less fit for the applications. As to the second norm fixing the order of terms by

$$|z_1| \geqq |z_2| \geqq \ldots \geqq |z_n| \tag{8}$$

we found in collaboration with Vera T. Sós the sharpest known inequality

$$U_2(m, n) > \left(\frac{n}{8e(m+n)}\right)^n \min_j |b_1 + \ldots + b_j|. \tag{9}$$

As was shown by Makai in an ingenious example the constant $8e$ cannot be replaced by $4e$. In the very important special case of $b_1 = b_2 = \ldots = b_n = 1$ this is equivalent to

$$\max_{\nu=m+1,m+2,\ldots,m+n} |z_1^\nu + z_2^\nu + \ldots + z_n^\nu| > \left(\frac{n}{8e(m+n)}\right)^n \tag{10}$$

if only $\max_j |z_j| = 1$; it would be of importance to replace in (10) the constant $8e$ by $1 + \varepsilon$ if $\frac{n}{m}$ is " small ". The dependence on the b_j's on the right of (9) is rather clumsy; simple examples show however, that this difficulty is inherent in the matter since they show that the minfactor cannot be replaced either by $|b_1 + \ldots + b_n|$ or by $\min_j |b_j|$ generally.

We open the long sequence of applications with the remark that (6) leads after simple substitutions for arbitrary complex b_j-coefficients to the inequality

$$\max_{\alpha \leqq t \leqq \delta} \left|\sum_{j=1}^n b_j e^{\alpha_j t}\right| \leqq \left(2e\frac{\delta - \alpha}{\gamma - \beta}\right)^n \max_{\beta \leqq t \leqq \gamma} \left|\sum_{j=1}^n b_j e^{\alpha_j t}\right| \tag{11}$$

if only

$$\alpha < \beta < \gamma < \delta \quad \text{and} \quad \min_j \operatorname{Re} \alpha_j = 0. \tag{12}$$

Trivial passage to limit leads from (11) to the inequality

$$\max_{\alpha \leqq t \leqq \delta} |g(t)| \leqq \left(2e\frac{\delta - \alpha}{\gamma - \beta}\right)^n \max_{\beta \leqq t \leqq \gamma} |g(t)| \tag{13}$$

for all solutions of all linear ordinary differential equations with constant coefficients

$$y^{(n)} + a_1 y^{(n-1)} + \ldots + a_n y = 0 \tag{14}$$

if only $\alpha < \beta < \gamma < \delta$ and all zeros of the characteristic equation

$$z^n + a_1 z^{n-1} + \ldots + a_n = 0 \tag{15}$$

are in the half plane $\operatorname{Re} z \geqq 0$ (which is of course only a normalisation). (6) leads also to an L_2-form of (13); this is—in an improved form by R. Tydeman—the inequality

$$\int_\beta^{\beta+\delta} |g(t)|^2 dt \leqq \left(2e\frac{\alpha - \beta + \delta}{\delta}\right)^{2n} \int_\alpha^{\alpha+\delta} |g(t)|^2 dt \tag{16}$$

if only (15) holds and also

$$\alpha > \beta \quad \text{and} \quad \delta > 0. \tag{17}$$

Since (13) and (16) does not depend on (14), only through (15), various transitions from these to the *general* theory of differential equations are possible. One result of these refers to the system in the canonical form

$$\frac{d\underline{X}}{dt} = \underline{\underline{A}}\,\underline{X} + \underline{W}(\underline{X}, t), \qquad \underline{W}(\underline{0}, t) \equiv \underline{0} \tag{18}$$

where $\underline{X} = \underline{X}(t)$ and $\underline{W}(\underline{X}, t)$ stand for $n \times 1$ column-vectors and $\underline{\underline{A}}$ is an $n \times n$ matrix with complex entries; (18) makes sure that $\underline{X} \equiv \underline{0}$ is a solution of the system. Let Λ be such that all eigenvalues of $\underline{\underline{A}}$ are in the half-plane Re $z \geqq \Lambda$ and all a_{ik} elements of $\underline{\underline{A}}$ be such that $|a_{ik}| \leqq d$. Then one can give an *explicit* $\Delta_0 = \Delta_0(n, \Lambda)$ with following property. Let $\Delta > \Delta_0$ and suppose that $\underline{W}(\underline{Z}, t)$ satisfies in some fixed cylindrical neighbourhood of $\underline{Z} = \underline{0}$ in the $(n + 1)$-dimensional $(\underline{Z}, t)$ space the inequality

$$\frac{\| \underline{W}(\underline{Z}, t) \|}{\| Z \|} \leqq c(\Delta, d, n) \tag{19}$$

with a certain *explicit* $c(\Delta, d, n)$. Then for all sufficiently large α's the inequality

$$\max_{\alpha \leqq t \leqq \alpha + \Delta} \| \underline{X}(t) \| \, e^{\left(1 + \frac{2}{\sqrt{\Delta}}\right) |\Lambda| t} > c_1 \tag{20}$$

(c_1 positive numerical constant)

is valid for all $\underline{X}(t) \not\equiv \underline{0}$ -solutions of (18), if only

$$\lim_{t \to +\infty} \| X(t) \| = 0. \tag{21}$$

Qualitatively speaking (and a great deal weaker) an asymptotically stable solution cannot be " too stable " in a very strong " finite " sense.

The same reasoning can be used for difference and retarded differential equations. Also the inequality (20) can be used (negatively) to prove that certain functions cannot satisfy certain types of differential equations, reminding one to Liouville's necessary condition for a number being algebraic of n the degree over the rationals.

Another application of (6) refers to value distribution of solutions of linear differential equations. The germ of these results is the trivial observation that in the simplest type of such equations

$$y^{(n+1)} = 0$$

also the value-distribution is of simplest type namely *all* solution take *all* values in *all* disks of the plane at most n times (with multiplicity). It was a plausible next step to investigate the analogous value distribution problem in the case of linear differential equations in (14) (some problems of this circle of ideas were treated often in the literature (*)). Using a power sum theorem devised especially for this application we

(*) An account of these works is given in S. R. E. Langer's paper, On the zeros of exponential sums and integrals, *Bull. Amer. Math. Soc.*, vol. 37 (1931), pp. 213-239 and more recently the book of R. Bellman and K. L. Cooke, *Differential-difference equations*, London, 1963.

exhibited with I. Dancs an *explicit* upper bound $\psi(n, R, M, m)$ for the number of A-places for *every* solution of (14) in *every* disks $|z - z_0| \leqq R$; here M resp. m stand for the maximal resp. minimal distance of the different roots of the characteristic equation (15) (multiple roots permitted). The point of this theorem was of course the independence of the upper bound from A, z_0 and from the choice of the solution and the very loose dependence on the coefficients of (14). Recently however R. Tydeman discovered that again a proper use of (6) leads to the much more elegant upper bound

$$6n + 4RM \tag{22}$$

which has also the advantage over our upper bound that it does not depend on m too. A consequence of (22) (i. e. a propagation of the effect of (6)) to the theory of transcendental numbers was noted by J. Coates. This refers to the fundamental theorem I of Gelfond dealing with algebraic independence over the rationals of certain types of numbers (see p. 132 of his book " Transcendental and algebraic numbers ") where the most inconvenient restriction (112) from the hypotheses of this theorem can simply be dropped (*).

The inequality (6) has also several consequences in the complex function theory, notably to gap-theorems. From (13) (i. e. from (6)) one can deduce for $0 < \delta < 1$ and real α at once the inequality (λ_j real)

$$\max_{x\,\mathrm{real}} \left| \sum_{j=1}^{k} b_j e^{i\lambda_j x} \right| \leqq \left(\frac{40}{\delta}\right)^k \max_{\alpha \leqq x \leqq \alpha+\delta} \left| \sum_{j=1}^{k} b_j e^{i\lambda_j x} \right| \tag{23}$$

This gives—combined with a simple approximation-lemma—at once Fabry's gap theorem. It offers also a short direct proof to one of the main theorems in Pólya's classical paper from 1929 according which if the entire function of finite order is represented by the power series $\sum_{n=1}^{\infty} a_n z^{\lambda_n}$ with Fabry gaps (**) then with the usual notations the inequality

$$\log M(r_n, \alpha, \alpha + \delta) \geqq (1 - \varepsilon) \log M(r_n) \tag{24}$$

holds for arbitrary small positive ε and δ and real α for an appropriate unbounded r_n-sequence. An appropriate combination of (23) with Wiman-Valiron theory led Kővári to a refined form (24) which in turn enabled W. H. J. Fuchs to the first proof of Pólya's longstanding conjecture according which under the previous conditions the stronger inequality

$$\log m(r) \geqq (1 - \varepsilon) \log M(r) \tag{25}$$

holds for arbitrarily small $\varepsilon > 0$ except an r-set with finite logarithmic measure. Among the further results of Kővári in this direction I mention his proof for (25) for

(*) My conjecture, that conversely from the above type value distribution of all solutions of the linear equation $y^{(n)} + a_1(z)y^{(n-1)} + \ldots + a_n(z)y(z) = 0$ ($a_\nu(z)$ entire functions) one can conclude that all $a_\nu(z)$'s are constants, was subsequently proved by H. Wittich.

(**) I. e. with $\dfrac{n}{\lambda_n} \to 0$ for $n \to \infty$.

all entire functions (i. e. not necessarily of finite order) if only the Fabry-gap-condition is replaced by

$$\lambda_n > n\,(\log n)^{2+\varepsilon}, \qquad \varepsilon > 0$$

which is very close to the gap condition $\sum \frac{1}{\lambda_n} < \infty$ which is probably necessary and sufficient condition for the validity of (25) without any order-condition on the function.

An unexpected further application of (6) via (23) was found by D. Gaier in his first proof of the longstanding conjecture of Hardy-Littlewood according which if the series Σa_n is Borel-summable and lacunary in the sense that $a_n \neq 0$ implies

$$n = n_k, \qquad n_{k+1} - n_k > \partial\sqrt{n_k}$$

with some positive ∂, then the series converges.

From applications to quasi-analytic function classes with one or several variables we mention only the simplest theorem that the class M of functions

$$f(x) = \sum_j a_j e^{i\lambda_j x}$$

with real λ_j's satisfying the condition

$$\overline{\lim_{\omega \to \infty}}\; e^{4\omega \log \omega} \sum_{j > \omega} |\, a_j \,| < \infty \tag{26}$$

form a quasi-analytic class in Mandelbrojt's sense (*). The interest of this class is that it depends exclusively on the coefficients, in contrast to an analogous theorem of Mandelbrojt-Wiener which defines the class exclusively with the (integer) exponents. For the sake of orientation we remark that the functions satisfying (26) can e. g. be nowhere differentiable.

Next we turn to some applications of the inequality (9) and (10). They refer to such farlying subjects as analytic number theory and numerical analysis. As to the second one I mention only the theorem that applying (10) with $m = 0$—or rather the improvements of *this* case by Atkinson, Buchholtz, Cassels—one can construct to each natural n and arbitrarily small $\varepsilon > 0$ an algorithm, with elementary steps the four fundamental operations and taking (the positive value of) roots of positive numbers, the length of which depends exclusively on n and ε and which—applied to arbitrary algebraic equations (15) with complex coefficients and $a_n \neq 0$—gives a complex number ψ such that for a suitable zero z^* of equation (15) the inequality

$$\left| \frac{z^*}{\psi} - 1 \right| \leqq \varepsilon \tag{27}$$

(*) This means that

$$\underline{\lim_{h \to +0}}\; e^{\frac{1}{h}} \int_{x_0 - h}^{x_0} |\, f_1(t) - f_2(t) \,|^2 dt < \infty, \qquad f_1, f_2 \in M$$

with a real x_0 implies $f_1(x) \equiv f_2(x)$.

holds. Since the solubility of (15) by radicals would mean a solving algorithm of length depending only on n, the theorem could be formulated a bit loosely that the analogon of Ruffini-Abel theorem does not hold for the *approximative* solubility of algebraic equations in the sense of (27). Among the applications of (10) to analytical number theory I mention first the theorem which says—again a bit loosely expressed —that the position of roots of the Riemann zeta function $\zeta(s)$ $(s = \sigma + it)$ in the horizontal strip $T \leqq t \leqq 2T$ depends only on primes of the interval $T^2 \leqq p \leqq T^8$. Among the applications to the distribution of zeros of $\zeta(s)$ or more generally to all Dedekind zeta function $\zeta_K(s)$ belonging to the number field K I mention only two theorems, found in collaboration with G. Halász. The first one asserts that denoting for $\alpha \geqq \frac{1}{2}$ the number of roots of $\zeta_K(s)$ in the parallelogram $\alpha \leqq \sigma \leqq 1$, $0 \leqq t \leqq T$ by $N_K(\alpha, T)$, the relation

$$\mu_1(\alpha) \stackrel{\text{def}}{=} \overline{\lim_{T\to\infty}} \frac{\log^+ N_K(\alpha_1 T)}{\log T} < c(1-\alpha)^{3/2} \log^3 \frac{1}{1-\alpha} \tag{28}$$

with $c = c(K)$ holds uniformly in $\alpha \geqq \frac{1}{2}$. This means that the $\mu_1(\alpha)$-function, which would be $\equiv 0$ for $\alpha > \frac{1}{2}$ in the case of truth of the generalised Riemann conjecture, touches at least the α-axis at $\alpha = 1$ in a rather strong sense. The second asserts that the analoga of the Lindelöf conjecture referring to the rate of increase

$$\left|\zeta_K\left(\frac{1}{2} + it\right)\right|$$

for $t \to \infty$, implies $\mu_1(\alpha) = 0$ for $\alpha > \frac{3}{4}$. Another application of (10) refers to Dirichlet L-functions belonging to the modulus D; it asserts—due in its last form to Fogels—that the total number of roots of all L-functions belonging to the modulus D for $\sigma \geqq \alpha$, $0 \leqq t \leqq D$ cannot exceed

$$D^{c_2(1-\alpha)} \tag{29}$$

with a numerical c_2 (the point being the absence of any log-factor). This enabled us with S. Knapowski to give a relatively short proof for the theorem of Linnik, sharpening Dirichlet's classical result, by giving the upper bound D^{c_3} with a positive numerical c_3 for the smallest prime in every coprime residue classes mod D.

The investigation of sign changes of $\pi(x) - \mathrm{Li}\, x$ initiated by Riemann and Littlewood, furthermore analogous general problems in prime number theory led to the necessity to find onesided theorems for generalised power sums under the $M_2(\nu)$-norm. Easy examples show that such theorems cannot exist in general; however it turned out that restricting the z_j-variables (beyond the $M_2(\nu)$-norm which means only normalisation) by the side-condition

$$\delta \leqq |\operatorname{arc} z_j| \leqq \pi \qquad j = 1, 2, \ldots, n \tag{30}$$

the situation is saved. More exactly I found that under (30) for arbitrary nonnegative integer m there exist integer ν_1 and ν_2 with

$$m + 1 \leqq \nu_1, \qquad \nu_2 \leqq m + \frac{2n}{\delta} \tag{31}$$

such that with $f(\nu) = \sum_{j=1}^{n} b_j z_j^\nu$ the inequalities (*)

$$\begin{aligned} \frac{\operatorname{Re} f(\nu_1)}{M_2(\nu_1)} &\geqq \left(\frac{n}{8e\left(m + \frac{2n}{\delta}\right)}\right)^{2n} \min_{1 \leqq l \leqq n} \left|\operatorname{Re} \sum_{j=1}^{l} b_j\right| \\ \frac{\operatorname{Re} f(\nu_2)}{M_2(\nu_2)} &\leqq -\left(\frac{n}{8e\left(m + \frac{2n}{\delta}\right)}\right)^{2n} \min_{1 \leqq l \leqq n} \left|\operatorname{Re} \sum_{j=1}^{l} b_j\right| \end{aligned} \tag{32}$$

hold. Among the many applications we found with S. Knapowski I mention here only one. According to this for $T > c_4$ we have ξ_1 and ξ_2 with

$$\log \log \log T \leqq \xi_2 e^{-\sqrt{\log \xi_2}} < \xi_1 < \xi_2 \leqq T \tag{33}$$

so that (p primes) the inequality

$$\sum_{\substack{p \equiv 1(4) \\ \xi_1 \leqq p \leqq \xi_2}} \log p - \sum_{\substack{p \equiv 3(4) \\ \xi_1 \leqq p \leqq \xi_2}} \log p > \sqrt{\xi_2} \tag{34}$$

holds. I. e. " relatively concentrated " we have " much more " primes $\equiv 1\,(4)$ than $\equiv 3\,(4)$. It is interesting to compare this with the fact that for suitable numerical c_5, c_6, c_7 positive constants for $x > c_5$ the inequality

$$\sum_{p \equiv 1(4)} \log p \, . \, e^{-c_6 \log^2 \frac{p}{x}} - \sum_{p \equiv 3(4)} \log p \, . \, e^{-c_6 \log^2 \frac{p}{x}} < -c_7 \sqrt{x} \tag{35}$$

is equivalent to the truth of the Riemann-Piltz conjecture concerning the L-functions belonging to modulus 4.

I found also the onesided analogon of (6) under the restriction (30). This was applied by Dancs to investigation of onesided stability-properties of differential equations; the usefulness of this theorem seems to me not exhausted by this.

The onesided theorem (32) is also an example of " conditional " power sum theorems where the variables are subjected to some geometrical restrictions. Some further applications (general coefficient estimations, asymptotical periods of entire functions, etc.) made necessary to use the $M_0(\nu)$-norm but replacing the linear independence of the arc z_j's by a more manageable geometrical restriction on the z_j's. As serviceable restriction proved to be the restriction

$$\frac{\min_{\mu \neq \nu} | z_\mu - z_\nu |}{\max_j | z_j |} \geqq \lambda > 0; \tag{36}$$

(*) Under the convention (8).

this implies at any positive integer m the inequality

$$\max_{\nu=m+1,\ldots,m+n} \frac{|f(\nu)|}{M_0(\nu)} \geqq \frac{1}{2n}\left(\frac{\lambda}{2}\right)^{n-1}. \tag{37}$$

Some other applications lead to " dual " problems, a typical being what is

$$\max_{z_j} \min_{\substack{m+1 \leqq \nu \leqq m+n \\ \nu \text{ integer}}} \frac{|f(\nu)|}{M_3(\nu)} \tag{38}$$

if the z_j's satisfy some geometrical restriction Lack of space permits me only to mention one application; this is the inequality

$$\min_{|t-t_0| \leqq n} \left| \sum_{l=1}^{n} a_l l^{-(\sigma_0+it)} \right| \leqq \sqrt{\log n}\,.\, \left\{ \sum_{l=1}^{n} |a_l|^2 l^{-2\sigma_0} \right\}^{1/2} \tag{39}$$

valid for all real t_0's and σ_0's and Dirichlet-polynomials $\sum_{l=1}^{n} a_l l^{-s}$.

Beside the " simultaneous " problems aiming e. g. the proof of existence of

$$x_1 < x_2 < \ldots \to \infty$$

such that with the usual notation the inequalities

$$\pi(x_\nu, 4, 1) > \frac{1}{2}\mathrm{Li}\, x_\nu, \qquad \pi(x_\nu, 4, 3) > \frac{1}{2}\mathrm{Li}\, x_\nu \tag{40}$$

should hold simultaneously I mention the " operatortype " problems, suggested also by some possible applications to the theory of $\zeta(s)$. They refer to minimax problems of type

$$V(g_k) \stackrel{\text{def}}{=} \min_{z_1,\ldots,z_n} \max_{\nu=m+1,\ldots,m+n} \frac{\left| \sum_{j=1}^{n} z_j^\nu g_k(z_j) \right|}{M_2(\nu)} \tag{41}$$

where $g_k(z) = z^k + \ldots$ is a fixed polynomial of k th degree. Then e. g. in the case when all zeros of $g_k(z)$ are in the disk

$$|z| < \frac{m}{m+n+k},$$

the inequality

$$V(g_k) \geqq \left(\frac{n+k}{16e(m+n+k)}\right)^{n+k} \tag{42}$$

holds.

The methods of proofs for the power sum theorems consist generally speaking of construction of suitable rational identities through classical algebra; these are appropriate also to fit to the discrete and diophantine character of the problems. So " discrete " methods seem to be in a successful counterattack. Remembering to a letter written by Weierstrass to H. A. Schwarz in 1875 which says " . . . Je mehr ich über die Prinzipien der Funktionentheorie nachdenke—und ich thue dies unablässig— um so fester wird meine Überzeugung, dass diese auf dem Fundament einfacher algebraischer Wahrheiten aufgebaut werden müssen... " it is perhaps not an unfounded belief that at least Weierstrass would be pleased with the content of this talk.

Mathematical Institute
of the Hungarian
Academy of Sciences
Realtanoda u. 13-15
Budapest V (Hongrie)

TABLE DES MATIÈRES DU TOME 1

DOCUMENTS

MÉDAILLES FIELDS

G - CONFÉRENCES GÉNÉRALES

A - LOGIQUE MATHÉMATIQUE

B - ALGÈBRE

B_1 - ALGÈBRE GÉNÉRALE

B_2 - CATÉGORIES - ALGÈBRE HOMOLOGIQUE

B_3 - GROUPES FINIS

B_4 - CORPS LOCAUX ET GLOBAUX ANALYSE P-ADIQUE

B_5 - GÉOMÉTRIE ALGÉBRIQUE

B_6 - THÉORIE DES NOMBRES, ÉLÉMENTAIRE ET ANALYTIQUE

Imprimerie LOUIS JEAN
Dépôt légal éditeur 1845

Dépôt légal n° 314-1971
N° Dossier : 70. 28

Imprimé en France

Œuvres de JORDAN

Œuvres publiées sous la direction de G. Julia par J. Dieudonné et R. Garnier. 4 volumes 16 x 25 se vendant séparément.

Les tomes I et II sont consacrés à la théorie des groupes.
Dans les « Notes sur les travaux de C. JORDAN relatifs à la théorie des groupes », qui sert d'introduction au premier volume, J. DIEUDONNE classe les travaux de JORDAN sous plusieurs rubriques : I. Généralités sur les groupes ; applications aux équations algébriques (Théorie de Galois). - II. Groupes linéaires sur un corps premier fini. - III. Sous-groupes de GLn (C.). - IV. Groupes transitifs et groupes primitifs.

Le tome III traite de l'algèbre linéaire et multilinéaire et de la théorie des nombres ; il est aussi présenté par J. DIEUDONNE qui répartit ainsi les articles : I. Géométrie à *n* dimensions. - II. Formes bilinéaires et formes quadratiques. - III. Théorie des invariants. - IV. Equivalence arithmétique des formes. - V. Autres travaux de théorie des nombres.

Le quatrième et dernier volume réunit des articles dispersés dans diverses revues sur des questions d'analyse relatives aux équations différentielles et à la topologie des polyèdres, ainsi que quelques travaux intéressant la mécanique, sur l'équilibre et sa stabilité et les petites oscillations autour d'une position d'équilibre. La mise au point des textes a été confiée à R. GARNIER et à J. DIEUDONNE. On y trouvera aussi, en tête du volume, deux portraits de JORDAN et sa biographie, composée par H. LEBESGUE lorsqu'il succéda à JORDAN à l'Académie des Sciences ; la fin du volume est consacrée à des extraits de lettres écrites à JORDAN par A. CLEBSCH, S. LIE, L. CREMONA, L. SYLOW, ainsi qu'aux principaux discours prononcés par JORDAN.

Tome I : 548 pages, 1961,	Broché :	95 F
	Cartonné :	110 F
Tome II : 562 pages, 1961,	Broché :	95 F
	Cartonné :	110 F
Tome III : 574 pages, 1962,	Broché :	95 F
	Cartonné :	110 F
Tome IV : 644 pages, 1964,	Broché :	125 F
	Cartonné :	140 F

GAUTHIER-VILLARS, Editeur, PARIS

Œuvres de H. POINCARÉ

Œuvres publiées sous les auspices de l'Académie des Sciences (Section de Géométrie), par G. Darboux, 11 volumes 23 x 28 se vendant séparément.

Tome I: *Analyse.* Publié sous les auspices de l'Académie des Sciences, par *P. Appell,* avec la collaboration de *J. Drach,* 382 pages, nouveau tirage, 1952.
Broché : 70 F — Cartonné : 85 F

Tome II: *Analyse.* Publié avec la collaboration de *N.-E. Norlund* et *E. Lebon,* 705 pages, 19 figures, un portrait de H. Poincaré, nouveau tirage, 1952.
Broché : 105 F — Cartonné :120 F

Tome III: *Analyse.* Publié avec la collaboration de *J. Drach,* 596 pages, nouveau tirage,1965.
Broché : 105 F — Cartonné : 120 F

Tome IV: *Analyse.* Publié avec la collaboration de *G. Valiron,* 632 pages, 1950.
Broché : 105 F — Cartonné : 120 F

Tome V: *Arithmétique et algèbre.* Publié avec la collaboration de *M. Chatelet,* 560 pages, 1950.
Broché : 105 F — Cartonné : 120 F

Tome VI: *Géométrie.* Publié avec la collaboration de *R. Garnier* et *J. Leray,* 548 pages, 1953.
Broché : 105 F — Cartonné : 120 F

Tome VII: *Mécanique céleste et astronomie.* Publié avec la collaboration de *J. Lévy,* 634 pages, 1952.
Broché : 105 F — Cartonné : 120 F

Tome VIII: *Mécanique céleste et astronomie.* Publié avec la collaboration de *P. Sémirot,* 695 pages, 1952.
Broché : 105 F — Cartonné : 120 F

Tome IX: *Physique mathématique.* Publié avec la collaboration de *G. Petiau,* 720 pages, 1954.
Broché : 105 F — Cartonné :120 F

Tome X: *Physique mathématique.* Publié avec la collaboration de *G. Petiau.* Préface de *G. Julia,* 642 pages, 1954.
Broché : 105 F — Cartonné : 120 F

Tome XI: Publié avec la collaboration de *G. Petiau.* Mémoires divers : *Hommage à H. Poincaré. Livre du Centenaire de H. Poincaré, 1854-1954,* 661 pages, 1956.
Broché : 105 F — Cartonné : 120 F

Œuvres de
LAGRANGE

Œuvres complètes, publiées par les soins de J.-A. Serret et G. Darboux. 14 volumes 23 x 28.

La première série comprend tous les mémoires imprimés dans les *Recueils des Académies de Turin, de Berlin et de Paris,* ainsi que les *Pièces diverses* publiées séparément. Cette série forme 7 volumes (Tomes I à VII, 1867-1877), qui se vendent séparément.

Chaque volume : 120 F.

La deuxième série se compose de 7 volumes qui renferment les ouvrages didactiques, la correspondance et les mémoires inédits :

Tomes VIII et IX : épuisés.

Tome X : *Leçons sur le calcul des fonctions,* 1884.

Tomes XI et XII : épuisés.

Tome XIII : *Correspondance inédite de Lagrange et de d'Alembert,* publiée d'après les manuscrits autographes et annotée par *Ludovic Lalanne,* 1822.

Tome XIV : *Correspondance de Lagrange avec Condorcet, Laplace, Euler et divers savants,* publiée et annotée par *Ludovic Lalanne,* avec deux fac-similés, 1892.

Chaque volume : 120 F.

Œuvres de CAUCHY

Œuvres complètes, publiées sous la direction scientifique de l'Académie des Sciences avec le concours de Valson, Collet et Borel. 26 volumes 23 x 28.

Première série : Mémoires, notes et articles extraits des recueils de l'Académie des Sciences, 12 volumes.

Tomes I, II et III : épuisés.

Tomes IV à XII : *Extraits des comptes-rendus de l'Académie des Sciences,* 1884-1900.

Chaque volume : 90 F

Deuxième série : Mémoires publiés dans divers recueils autres que ceux de l'Académie, ouvrages classiques, mémoires publiés en corps d'ouvrage, mémoires publiés séparément. 14 volumes.

Tome I : Mémoires extraits du *Journal de l'Ecole Polytechnique.*

Tome II : Mémoires extraits de divers recueils : *Journal de Liouville, Bulletin de Férussac, Bulletin de la Société Philomathique, Annales de Gergonne, Correspondance de l'Ecole Polytechnique,* 1958.

Tome III : *Cours d'analyse de l'Ecole Royale Polytechnique,* 1897.

Tome IV : *Résumé des leçons données à l'Ecole Polytechnique sur le calcul infinitésimal, leçons sur le calcul différentiel,* 1899.

Tome V : *Leçons sur les applications du calcul infinitésimal à la géométrie,* 1903.

Tomes VI à IX : *Anciens exercices de mathématiques,* 1887 à 1891.

Tome X : *Résumés analytiques de Turin. Nouveaux exercices de Prague.* (Mémoire sur la dispersion de la lumière), 1895.

Tome XI : épuisé.

Tomes XII, XIII et XIV : *Nouveaux exercices d'analyse et de physique,* 1916-1938.

Chaque volume : 90 F

GAUTHIER-VILLARS, Editeur, PARIS