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 \( tf(t)/d \) 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 \((A) F(x_1^{n_1}, \ldots, x_k^{n_k}) \) or \((B) F(x_1^{n_1}, \ldots, x_n^{n_k}) \). 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:

\[
F(x_1, \ldots, x_n) \equiv \text{const} \prod_{\sigma=1}^k F_\sigma(x_1, \ldots, x_n)^{e_\sigma},
\]

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 \([n_1, \ldots, n_k] \) consisting of positive integers there exist integer vectors \([\mu_1, \ldots, \mu_k] \) and \([u_1, \ldots, u_k] \) such that

(i) \( 0 < \mu_i \leq c(F) \),

(ii) \( n_i = \mu_i u_i \),

(iii) \( F(x_1^{n_1}, x_2^{n_2}, \ldots, x_k^{n_k}) \equiv \text{const} \prod_{\sigma=1}^k F_\sigma(x_1, \ldots, x_k)^{e_\sigma} \)

implies

\[
F(x_1^{n_1}, \ldots, x_k^{n_k}) \equiv \text{const} \prod_{\sigma=1}^k F_\sigma(x_1^{n_1}, \ldots, x_k^{n_k})^{e_\sigma}.
\]

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

\[
\phi(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \prod_{i=1}^k x_i^{\delta_i},
\]

where \( f \) is a polynomial not divisible by any \( x_i \), then \( J\phi(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \).

Let

\[
J\phi(x_1, \ldots, x_k) \equiv \text{const} \prod_{\sigma=1}^k f_\sigma(x_1, \ldots, x_k)^{e_\sigma}.
\]

We set

\[
K\phi(x_1, \ldots, x_k) = \text{const} \Pi_1 f_\sigma(x_1, \ldots, x_k)^{e_\sigma},
\]

\[
L\phi(x_1, \ldots, x_k) = \text{const} \Pi_2 f_\sigma(x_1, \ldots, x_k)^{e_\sigma},
\]

where \( \Pi_1 \) is extended over all \( f_\sigma \) which do not divide \( J(x_1^{\delta_1} \ldots x_k^{\delta_k} - 1) \) for any \([\delta_1, \ldots, \delta_k] \neq \emptyset\), \( \Pi_2 \) is extended over all \( f_\sigma \) such that

\[
Jf_\sigma(x_1^{-1}, \ldots, x_k^{-1}) \neq \pm f_\sigma(x_1, \ldots, x_k).
\]

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]).
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) \( 0 < \mu_i \leq C_1(F) \)

(ii) \( n_i = \mu_i u_i \)

(iii) \( LF(x_1^{n_1}, \ldots, x_k^{n_k}) = const \prod_{\sigma=1} F_{\sigma}(x_1, \ldots, x_k)^{u_{\sigma}} \)

implies

\( LF(x_1^{n_1}, \ldots, x_k^{n_k}) = const \prod_{\sigma=1} F_{\sigma}(x_1^{n_1}, \ldots, x_k^{n_k})^{u_{\sigma}}. \)

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 \( N = [v_{ij}]_{1 \leq i \leq k} \) of rank \( r \) and an integral vector \( v = [v_1, \ldots, v_r] \) such that

(i) \( \max |v_{ij}| \leq C_2(F) \)

(ii) \( n = vN \)

(iii) \( LF(\prod_{i=1}^{\gamma_1^{n_1}}, \ldots, \prod_{i=1}^{\gamma_k^{n_k}}) = const \prod_{\sigma=1} F_{\sigma}(y_1, \ldots, y_r)^{u_{\sigma}} \)

implies

\( LF(x^{n_1}, \ldots, x^{n_k}) = const \prod_{\sigma=1} LF_{\sigma}(x_1^{n_1}, \ldots, x_k^{n_k})^{u_{\sigma}}. \)

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 \( y_1 n_1 + \ldots + y_k n_k = 0 \), where \( 0 < \max |y_i| < C(a_0, \ldots, a_k) \). 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 \( 1 + \frac{1}{52n \log 6n} \), 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 $f(0) \neq 0$, $f(1) \neq -1$ no choice of $n$ gives an irreducible polynomial. For $a = 1$ the corresponding problem is related to the so-called 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 Pelczyński, [35], [36]) and $f(x_1, \ldots, x_m) + g(y_1, \ldots, y_n)$ is reducible in any field if and only if

$$f = f_1(f_2(x_1, \ldots, x_n), \quad g = g_1(g_2(y_1, \ldots, y_n))$$

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

REDUCIBILITY OF POLYNOMIALS


[21] —. — A factorization theory for functions \( \sum_{i=1}^{n} a_i e^{ix} \), Trans. Amer. Math. Soc., 29 (1927), pp. 584-596.


[35] H. Tverberg. — On the irreducibility of the trinomials \(x^n \pm x^m \pm 1\), *Math. Scand.*, 8 (1960), pp. 121-126.


Mathematical Institute of the Polish Academy of Sciences Warsaw (Pologne)