FURTHER DEVELOPMENT OF THE THEORY OF
ARITHMETICS OF ALGEBRAS

BY PROFESSOR L. E. DICKSON,
University of Chicago, Chicago, Illinois, U.S.A.

1. INTRODUCTION

The writer recently* gave a new conception of integral elements of a rational
associative algebra $A$ having a modulus 1, which avoids the serious objections
against all earlier conceptions.

The integral elements of $A$ are defined to be the elements which belong to
a set $S$ of elements having the following four properties:

$C$ (closure): The sum, difference and product of any two elements of $S$
are also elements of $S$.

$R$ (rank equation†): For every element of $S$, the coefficients of the rank
equation are all ordinary integers.

$U$ (unity): The set contains the modulus 1.

$M$ (maximal): The set is a maximal (i.e., is not contained in a larger set
having properties $C$, $R$, $U$).

It is proved in §2 for the first time that there exists a set of integral elements
in any rational algebra.

The above conception of integral elements may be extended to algebras
over an algebraic field (or any field for which the notion of integer is defined). In
particular, quaternions over any quadratic field are investigated in §§ 4-9.

2. EXISTENCE OF INTEGRAL ELEMENTS IN ANY ALGEBRA

THEOREM. In any rational algebra $A$ having a modulus, there exists a
maximal set of elements having properties $C$, $R$, $U$.

First, let $A$ be semi-simple. We can choose‡ new basal units $u_1$, $u_2$, . . ., $u_n$
of $A$ such that the new constants of multiplication $\gamma_{ijk}$ are all integers.
With this simplification we shall prove the existence of a maximal set. The
latter remains a maximal set when its elements are expressed in terms of the

*Algebras and Their Arithmetics, University of Chicago Press.
†The element $x$ whose coordinates $\xi$ are independent variables of the field of rational numbers
is a root of a uniquely determined rank equation in which the leading coefficient is unity, while
the remaining coefficients are polynomials in $\xi_1$, . . ., $\xi_n$ with rational coefficients. Also, $x$ is not
a root of an equation of lower degree all of whose coefficients are such polynomials.
‡Algebras and Their Arithmetics, p. 160, bottom.
initial basal units, since properties C, R, U are invariant under transformation of the basal units.

Consider the set I of all linear functions of $u_1, \ldots, u_n$ with integral coefficients. Evidently I has properties $U$ and $C$ (since the $\gamma_{ijk}$ are integers). It has property $R$ since the rank function $R(w)$ has the same irreducible factors as the characteristic determinant whose coefficients are integers (and leading coefficient is unity) when the element is in I, and the same is true also of its irreducible factors by Gauss's lemma, and hence for a product $R(w)$ of powers of them.

Let S be any set of elements (of A) having properties $C$ and $R$ and containing $u_1, \ldots, u_n$; one such S is I. Every element $x$ of S can be expressed* in the form

$$x = \sum_{i=1}^{n} d_i u_i,$$

where $d$ and every $d_i$ is an integer, while $d$ is a function $\neq 0$ of the $\gamma$'s only and is independent of $x$. Let $q_i$ be the quotient and $r_i$ the remainder when $d_i$ is divided by $d$, whence

$$d_i = dq_i + r_i, \quad 0 \leq r_i \leq d - 1.$$

Then

$$x = q + r, \quad q = \sum q_i u_i, \quad r = \sum \frac{r_i}{d} u_i,$$

where $q$ is in I. Hence S is derived from I by annexing one or more of the $d^n$ elements $r$. Since there is only a finite number of such annexations, there is only a finite number of sets $S$ having properties $C$ and $R$ and containing $u_1, \ldots, u_n$. Hence there is a maximal $S^*$ of such sets. It is a maximal of all sets $S$ having properties $C, R, U$, since a $S$ which contains $S^*$ contains $u_1, \ldots, u_n$, and is one of the preceding sets $S$.

Second, let $A$ be not semi-simple. By the principal theorem on algebras, $A = S + N$, where $N$ is the maximal nilpotent invariant sub-algebra of $A$, and $S$ is a semi-simple sub-algebra having a modulus. Let $[\sigma]$ be a maximal set of elements $\sigma$ of $S$ having properties $C, R, U$. When $\nu$ ranges over $N$, all sums $\sigma + \nu$ form a maximal set $\Sigma$ (of $A$) having properties $C, R, U$. To show that $\Sigma$ has property $C$, let $\sigma$ and $\sigma'$ be any elements of $[\sigma]$, so that $\sigma \pm \sigma'$ and $\sigma \sigma'$ are elements of $[\sigma]$. Evidently $\sigma + \nu \pm (\sigma' + \nu')$ is in $\Sigma$; also

$$(\sigma + \nu) (\sigma' + \nu') = \sigma \sigma' + \nu_1, \quad \nu_1 = \sigma \nu' + \nu \sigma' + \nu \nu',$$

so that $\nu_1$ is the invariant sub-algebra $N$ of $A$. The modulus of $A$ is of the form $\sigma_0 + \nu_0$; hence, if $s$ is any element of $S$, $(\sigma_0 + \nu_0)s = s$, whence $\nu_0 s$ is zero, being in $N$. From $s_0 s = s$ and the similar result $s_0 s = s$, we see that $\sigma_0$ is the modulus of $S$. Hence $\Sigma$ has property $U$. It has also property $R$ since† the rank function of the general element $s + \nu$ of $A$ is independent of $N$ and has integral coefficients when the rank function for $S$ of element $s$ has integral coefficients.

†Ibid., p. 186.
3. ALGEBRAIC INTEGERS, BASIS.

Let \( n \) be an integer \( \neq 1 \) without a square factor >1. Write \( \mu = \sqrt{n} \) and denote by \( \mathbb{R}(\mu) \) the field composed of all \( a+b\mu \) in which \( a \) and \( b \) are rational numbers. We call \( a+b\mu \) an algebraic integer if the quadratic equation having it and \( a-b\mu \) as roots has integral coefficients and unity as leading coefficient.

Consider a set \( S \) such that the sum and difference of any two of its elements are also elements of \( S \). Then \( S \) is said to have a basis \( b_1, \ldots, b_n \) if each \( b_i \) belongs to \( S \) and if every element of \( S \) is expressible as a linear function of \( b_1, \ldots, b_n \) with integral coefficients.

It is well known* that the algebraic integers of the field \( \mathbb{R}(\mu) \) have the basis 1 and \( \theta \), where \( \theta = \mu \) if \( m \equiv 2 \) or \( m \equiv 3 \) (mod 4), while \( \theta = \frac{1}{2}(1+\mu) \) if \( m \equiv 1 \) (mod 4).

QUATERNIONS OVER A QUADRATIC FIELD

4. DEFINITIONS, RANK EQUATION

Let \( A_\mu \) be the algebra of quaternions

\[
q = \sigma + \xi i + \eta j + \zeta k,
\]

whose coordinates \( \sigma, \xi, \eta, \zeta \) range independently over the field \( \mathbb{R}(\mu) \), \( \mu = \sqrt{n} \), every number of which is assumed to be commutative with every \( q \). We may regard \( A_\mu \) as a rational algebra \( A \) with the eight basal units

\[
1, \mu, i, \mu i = \mu i, j, \mu j = \mu j, k, \mu k = \mu k,
\]

and having rational coordinates.

The product in either order of \( q \) and its conjugate

\[
q' = \sigma - \xi i - \eta j - \zeta k
\]

is the norm \( N(q) = \sigma^2 + \xi^2 + \eta^2 + \zeta^2 \) of \( q \). Thus \( q \) and \( q' \) are roots of

\[
w^2 - 2\sigma w + N(q) = 0.
\]

We may write \( 2\sigma = a + b\mu, N(q) = c + d\mu \), where \( a, b, c, d \) are rational. The product of (2) by

\[
w^2 - (a - b\mu)w + c - d\mu = 0
\]

is the quartic equation

\[
(w^2 - aw + c)^2 - m(bw - d)^2 = 0,
\]

whose coefficients are rational and which has the root \( q \). It is the rank equation of \( A \). For, if the latter be of degree<4, the special quaternion \( q = f\mu + i \), in which \( f \) is rational and not zero, would satisfy an equation of type

\[
C x + yq + zq^2 + wq^3 = 0
\]

with rational coefficients. Here

\[
q^2 = f^2\mu m - 1 + 2f\mu i, q^3 = (f^2\mu m - 3f)\mu + (3f^2m - 1)i.
\]

*Cf. Algebras and Their Arithmetics, pp. 128-130.
The part of $C$ free of $i$ and the part involving $i$ are separately zero. In each such part, the component free of $\mu$ and that involving $\mu$ are both zero. Hence $x=z=0,$

$$y+\omega(3f^p-1)m-1)=0, \quad yf+\omega(f^p(m-3f))=0.$$ 

The determinant of the coefficients of $y$ and $\omega$ is not zero if $f \neq 0, f^2 \neq -1/m$, and then $y=\omega=0, C=0$. Thus (4) is the rank equation of algebra $A$.

5. Property $R$.

Let $q$ be such that the coefficients of (4) are all integers, whence its roots are algebraic integers. Sums and products of these roots in pairs give the coefficients of (2) and (3), which are therefore algebraic integers.

Conversely, let the coefficients of (2) be algebraic integers. Then the same is true of (3), and the four roots of (4) are algebraic integers. Thus the coefficients of (4) are algebraic integers and at the same time are rational numbers; hence they are integers.

In other words, a set $S$ of quaternions $q$ has property $R$ if and only if the coefficients of the quadratic (2) are algebraic integers for every $q$ in $S$.

We seek all maximal sets $S$ of quaternions over the field $R(\mu)=R(\theta)$ which have properties $C$ and $R$ and contain 1, $i$, $j$, $k$, $\theta$. Such a set $S$ will be called a normal set of integral elements. In $iq,jq$, $kq$ (which belong to $S$), the terms free of $i$, $j$, $k$ are $-\xi, -\eta, -\xi$ respectively. Thus by (2),

$$2\sigma = A+B\theta, \quad 2\xi = C+D\theta, \quad 2\eta = E+F\theta, \quad 2\xi = G+H\theta$$

are algebraic integers, whence $A, \ldots, H$ are ordinary integers. We obtain from $q$ another element of $S$ by subtracting the products of 1, $i$, $j$, $k$, $\theta$, $\theta i$, $\theta j$, $\theta k$ by integers. Hence we may replace an odd value of $A, \ldots, H$ by 1 and an even value by 0.

For $m \equiv 2$ or 3 (mod 4), $\theta = \sqrt{m}$ and $N(q)$ is an algebraic integer, as required by property $R$ and (2), if and only if

$$A^2+C^2+E^2+G^2+m(B^2+D^2+F^2+H^2) \equiv 0 \quad \text{(mod 4)},$$

$$AB+CD+EF+GH \equiv 0 \quad \text{(mod 2)}.$$ 

6. Case $m \equiv 2$ (mod 4)

Then $A+C+E+G$ is even by (6).

First, suppose that $A$, $C$, $E$, $G$ are all even in every element $q$ of $S$. If also $B$, $D$, $F$, $H$ are all even in every $q$, $S$ is

$$\text{the set } I \text{ with basis } 1, i, j, k, \theta, \theta i, \theta j, \theta k,$$

which is in the larger set (15). In the contrary case, we use $iq$, $jq$, or $kq$ in place of $q$, if necessary, and have $B$ odd. Treating only one of three similar cases arising from one by cyclic permutations of $i$, $j$, $k$, we may take also $D$ odd. If every such $q$ has also $F$ and $H$ odd, $S$ is derived from $I$ by annexing $\theta \rho$, where
\[(9) \quad \rho = \frac{1}{2}(1 + i + j + k),\]
whence \(S\) is in the larger set (15). Since \(B + D + F + H\) is even by (6), there remains only the case \(B = D = 1, F = H = 0 \pmod{2}\) whence we may take \(q = \frac{1}{2}(1 + i).\) Then \(S\) contains the set \(S_1\) with the basis \(q, qj = \frac{1}{2}(j + k), \theta j, \theta, 1, i, j, k.\) After subtracting products of these by integers from any element of \(S\) we get \(r = \frac{1}{2}(B + Fj),\) where \(B + F\) is even. If \(B\) and \(F\) are odd, the set \(S\) contains
\[qr = \frac{1}{2}m(B + Bi + Fj + Fk) = \frac{1}{2}A' + \ldots,\]
where \(A'\) is odd, contrary to hypothesis. Hence \(B\) and \(F\) are even and \(r\) is in \(S_1.\) But \(S_0S_1\) is in the larger set (15). Hence there exists no maximal set in this first case.

Second, let \(S\) contain an element \(q\) in which \(A, C, E, G\) are not all even. Since \(iq, jq, kq\) are in \(S\) and have \(-C, -E, -G\) in place of the \(A\) in \(q, S\) contains an element having \(A\) odd, and hence one or all of \(C, E, G\) odd. Treating only one of three similar cases, we permute \(i, j, k\) cyclically if necessary and take \(C\) odd. Hence we may take \(A = C = 0.\) Then \(E + G\) is even.

(i) Let also \(E = G = 0.\) Then \(B + D\) is even by (7) and \(F + H\) is odd by (6). Since we may take \(iq\) in place of \(q,\) we may apply the substitution (signs apart)
\[(10) \quad (ax) (yj) : (AC) (BD) (EG) (FH),\]
and hence take \(H = 0, F = 1.\) Since \(D = B + 2p, S\) contains
\[l = q - p\theta i = \frac{1}{2}(1 + B\theta) (1 + i) + \frac{1}{2}\theta j,\]
\[
\theta l - \frac{1}{2}m[B(1 + i) + j] = \frac{1}{2}\theta j(1 + i) = t_1, \phi = t_l j = \frac{1}{2}\theta (j + k),
\]
\[L = l - Bl = \frac{1}{2}(1 + i + \theta j), s = kL + t_1 = \frac{1}{2}(j + k + \theta).
\]
Hence \(S\) contains
\[(11) \quad \text{the set } T \text{ with basis } t_1, \phi, L, s, 1, i, j, k.
\]

It is easily verified that this set \(T\) has the closure property \(C.\) To prove that \(T\) is a maximal, annex any new element \(q.\) By subtracting in turn products of \(\phi, L, t_1, s\) by integers, we may assume that the coefficients \(H, F, D, B\) of \(\frac{1}{2}\theta k, \frac{1}{2}\theta j, \frac{1}{2}\theta, \frac{1}{2}\theta\) are all zero. Then, by (6), \(A^2 + C^2 + E^2 + G^2 = 0 \pmod{4},\) whence \(A, C, E, G\) are either all even and \(q\) would be in \(T,\) contrary to hypothesis, or all odd and then we may take \(q = \rho.\) Then the enlarged set contains
\[(12) \quad \rho t_1 = \frac{1}{2}\theta (i + j) = t_1 + t_2 - \theta, t_1 \rho = \frac{1}{2}\theta (i + k) = t_1 + t_2 - \theta,
\]
and hence contains
\[(13) \quad \rho t_1 = \frac{1}{2}\theta (i + j) = t_1 + t_2 - \theta, t_1 \rho = \frac{1}{2}\theta (i + k) = t_1 + t_2 - \theta,
\]
the double of whose scalar part is \(\frac{1}{2}(\theta - m),\) which is not an algebraic integer. Hence \(T\) is a maximal set.

(ii) Let \(E = G = 1.\) Then either (6) or (7) states merely that \(B + D + F + H\) is even. If \(B, D, F, H\) are all even, we may take \(q = \rho.\) In the contrary case, we may take \(B = 1\) since we may employ \(iq\) [cf. (10)], \(jq\) or \(kq\) in place of \(q.\) Per-
muting \(i, j, k\) cyclically if necessary, we have \(D = 1\). Then if \(F\) and \(H\) are odd, \(S\) contains \(q = (1 + \theta)\rho\) and \(\theta q\) and hence also \(\theta p\) and \(\rho\). If \(F\) and \(H\) are even, \(S\) contains \(\rho + t_1\). Since we employed cyclic permutations of \(i, j, k\), we conclude that the initial set may be derived from the set (8) by annexing one or more of \(\rho, \rho + t_1, \rho + t_2, \rho + t_3\), and hence is contained in

\[(15)\] the set \(\Sigma\) with basis \(\rho, i, j, k, \theta, t, t_2, t_3\), obtained by annexing all of them. This set has the closure property and is a maximal. For, if we annex \(l\) in (i) and therefore \(L\), we annex (14).

The general element of \(\Sigma\) is

\[X = x_0\rho + x_1 i + x_2 j + x_3 k + x_4 \rho + x_5 t_1 + x_6 t_2 + x_7 t_3 = a + a_1 i + a_2 j + a_3 k,\]

where the \(x\)'s are integers. Write

\[\xi_1 = x_0 + 2x_1, \quad \xi_2 = x_0 + 2x_2, \quad \xi_3 = x_0 + 2x_3, \quad \xi_4 = 2x_4 + x_5 + x_6 + x_7, \quad m = 2n.\]

Then

\[\alpha = \frac{1}{2} x_0 + \frac{1}{2} \xi_0, \quad \alpha_2 = \frac{1}{2} \xi_1 + \frac{1}{2} \theta x_4 + s (s = 1, 2, 3), \quad N(X) = U + V\theta, \]

\[4U = x_3^2 + x_4^2 + x_5^2 + x_6^2 + 2n(x_2^2 + x_3^2 + x_4^2 + x_5^2), \quad 2V = x_0 \xi_4 + \xi_1 x_5 + \xi_2 x_6 + \xi_3 x_7.\]

Hence if \(n > 0\), \(U\) is never negative and is zero only when \(X = 0\).

If \(n > 0\), \(X^2 = -1\) implies \(N(X) = +1\), \(X' + X = 0\), \(a = 0\), \(x_0 = 0\), \(\xi_4 = 0\).

Then if \(n > 1\), whence \(n \geq 3\), \(4U = 4\) implies \(x_5 = x_6 = x_7 = 0\), two of \(\xi_1^2, \xi_2^2, \xi_3^2\) are zero and one is 4, whence \(X = \pm i, \pm j, \pm k\). Hence if \(n > 1\), \(\Sigma\) is not equivalent to the set \(T\) defined by (11).

But if \(n = 1, m = 2\), the sets \(\Sigma\) and \(T\) are equivalent. Write

\[I = i, \quad J = j, \quad K = IJ = \frac{1}{2} \theta (k - j).\]

Then

\[I^2 = J^2 = K^2 = -1, \quad \theta k = J + K, \quad \theta j = J - K, \]

\[t_1 = \frac{1}{2} \theta (1 + I), \quad s = \frac{1}{2} \theta (1 + J), \quad \theta s - j = \frac{1}{2} \theta (1 + K), \]

\[L + K = \frac{1}{2} (1 + I + J + K).\]

**Theorem.** If \(m \equiv 2 \pmod{4}\), the only maximal sets are \(T\) and \(\Sigma\) defined by (11) and (15) and two sets derived from \(T\) by permuting \(i, j, k\) cyclically. If \(m = 2\), these four sets are equivalent. But if \(m > 2\), \(T\) and \(\Sigma\) are not equivalent.

7. Case \(m \equiv 1 \pmod{4}\)

The algebraic integers have the basis 1 and \(\theta = \frac{1}{2} (1 + \sqrt{m})\). Thus \(\theta^2 = \theta + n\), where \(n = \frac{1}{2} (m - 1)\). Then

\[N(q) = \frac{1}{4} (U + V\theta),\]

\[U = A^2 + C^2 + E^2 + G^2 + n(B^2 + D^2 + F^2 + H^2) \equiv 0 \pmod{4},\]

\[V = 2(AB + CD + EF + GH) + BF + DI + F^2 + H^2 \equiv 0 \pmod{4}.\]

*Also if \(n\) is negative.
THEOREM. If $n$ is even, the only maximal set $\Sigma$ is composed of all elements
$Q+\theta Q_0$, where $Q$ and $Q_0$ range over the Hurwitz integral quaternions with the basis
$p, i, j, k$. For $n$ odd there are only two maximal sets: $\Sigma_1$, which has the basis
(18)
$g_1 = \frac{1}{2}(1+i)+\frac{1}{2}(1+j)+\frac{1}{2}(1+k), g_2 = \frac{1}{2}(1+k)+\frac{1}{2}(1+i), \theta, p, i, j, k,$
and $\Sigma_2$, which is derived from $\Sigma$ by interchanging $i$ with $j$ and changing the sign of $k$
(and this leaves invariant the multiplication table of quaternions).

By (17), $B^2+D^2+F^2+H^2$ is even, whence, by (16), $A+C+E+G$ is even. If $A, C, E, G$
are all even, they may be taken to be zero; then, by (17), $B, D, F, H$
are all even or all odd, whence $q=\theta Q$, where $Q$ is a Hurwitz integral quaternion.
All such $q's$ belong to $\Sigma$ and to $\Sigma_1$, since
(19) $\theta \rho = q_1 + q_2 - 1 - \theta - \rho$, $\theta i = 2q_2 - 1 - k - \theta$, $\ldots$, $\theta k = 2q_2 - 1 - j - \theta$.

A set $S$ which contains a $q$ in which $A, C, E, G$ are not all even contains a
$q$ in which $A$ is odd (§6, second case). Treating only one of three similar cases
arising from one by a cyclic permutation of $i, j, k$, we may assume that $S$
contains a $q$ having $A$ and $C$ odd. We may therefore take $q = p$
or $(1+\theta)\rho$.

(I) Let also $E=G=1$. Then (17) is equivalent to
$$(B+1)^2+(D+1)^2+(F+1)^2+(H+1)^2=0 \pmod{4}.$$  
Hence $B+1, \ldots, H+1$ are all even or all odd, whence $B, D, F, H$
are all even or all odd. We may therefore take $q = \rho$ or $(1+\theta)\rho$.

(II) Let $A=C=1, E=G=0$. Then (16), (17) become
$$n(B^2+D^2+F^2+H^2)=2, 2(B+D)+B^2+D^2+F^2+H^2=0 \pmod{4}.$$  
The first shows that $n$ is not divisible by 4. If $n=2 \pmod{4}$, the first shows
that $B^2+D^2+F^2+H^2$ is odd, and contradicts the second. Hence case (I)
arises only when $n$ is odd and then
$$B^2+D^2+F^2+H^2=2 \pmod{4}, B+D=\text{odd}, F+H=\text{odd}.$$  
In view of (10), we may take $H=0, F=1$, whence
$q = \frac{1}{2} + \frac{1}{2}B(1+\theta) + (\frac{1}{2}D\theta)i + \frac{1}{2}\theta j, B+D=\text{odd}.$

If $B=1, D=0, q$ becomes $g_1$ in (18). Hence the set $S$ contains
$$(k-i)q_1+(1+\theta)i=q.$$
If $B=0, D=1, q$ becomes $R$:
(20) $$R = (1+i)+\frac{1}{2}(i+j), (i+j)R+1+\theta+k=q.$$  
In either case, $S$ contains $\rho$.

Consider first a set $S$ which contains $\rho$ and hence all $Q+\theta Q_0$, where $Q$
and $Q_0$ are Hurwitz integral quaternions. If possible, let $S$ contain a further element $q$.
Replacing $q$ by $q+\rho$ if necessary, we may take $A=1$. As before (I), we may take also $C=1$. Case (I)
is excluded since $q$ was assumed to be not of the form
\(Q + \theta Q\). Also case (II) is excluded if \(n\) is even. Hence if \(n\) is even, \(S\) coincides with \(\Sigma\) of the theorem and \(\Sigma\) is a maximal set.

Next, let \(n\) be odd. Then by (II), \(q\) is either \(q_1\) or \(R\) in (18) or (20). A set \(S\) which contains \(\rho\) and \(q_1\) contains

\[z = \theta q_1 - q_1 + \frac{1}{2}(1-n)(1+j) = \frac{1}{2}(\theta + \theta i - i + j),\]
and \(q_2 = i q_1 - z - i - \theta k\).

Thus \(S\) contains the set \(\Sigma_i\). The latter has the closure property.

To prove that \(\Sigma\) is a maximal set, annex any element \(q\). By subtracting products of \(q_1, q_2, q_3, \rho\) by integers, we get a \(q\) having \(F = H = D = A = 0\). Then \(B\) is even by (17) and we may take \(B = 0\). Then (16) becomes \(C^2 + E^2 + G^2 \equiv 0 \mod 4\), whence \(C, E, G\) are all even and may be taken to be zero. Then \(q = 0\).

For \(n\) odd, consider a set \(S\) containing \(\rho\) and \(R\), defined by (20). It contains

\[w = \theta R - R - \frac{1}{2}(n-1)(i+j) + 1 = \frac{1}{2}(1+j) + \frac{1}{2}(1+i)\]
Interchange \(i\) with \(j\) and change the sign of \(k\). From \(w\) we get \(q_i\); from \(iR\) we get \(j - q_i\); from \(\rho\) we get \(\rho - k\). The new set has \(q_0 + k - kg_1 = q_3\) and hence coincides with \(\Sigma_i\).

Finally, consider a set \(S\) having \((1+\theta)\rho\). If \(n\) is odd, \(S\) contains \(\theta(1+\theta)\rho\) and hence \(\rho\), a case treated above. If \(n\) is even, and \(S\) contains an element \(q\) not in \(\Sigma\), we may take \(A = 1\) by adding \((1+\theta)\rho\) to \(q\) if necessary. As before (I), we may take also \(C = 1\). Since case (II) is excluded, and the elements in (I) lie in \(\Sigma\), we have a contradiction. Hence \(S\) is in \(\Sigma\).

8. Case \(m \equiv 3 \mod 4\)

The algebraic integers have the basis 1, \(\theta = \sqrt{m}\).

If \(A, C, E, G\) are all even in every element \(q\) of \(S_i\),

\[\theta q = \frac{1}{2}(mB + A\theta) + \frac{1}{2}(mD + C\theta)i + \frac{1}{2}(mF + E\theta)j + \frac{1}{2}(mH + G\theta)k\]
shows that \(mB, \ldots, mH\) are all even. Hence \(B, D, F, H\) are all even and \(S\) is the set \(I\) in (8) and is contained in the larger set (21).

In the contrary case, \(S\) contains a quaternion \(q\) in which \(A = 1\)

First, let \(C, E, G\) be all even. We may take them to be zero. Then \(B\) is even by (7); take \(B = 0\). Then (6) is equivalent to \(D^2 + F^2 + H^2 \equiv 1 \mod 4\), whence two of \(D, F, H\) are even and one is odd. We treat only one of three similar cases arising from one by the cyclic permutation of \(i, j, k\), and hence take \(D = 1, F = H = 0\). Then

\[q = \frac{1}{2} + \frac{1}{2}(q, r = iq = \frac{1}{2}i - \frac{1}{2}\theta, s = qj = \frac{1}{2}j + \theta k, t = kq = \frac{1}{2}k + \frac{1}{2}\theta j\).

Consider

(21) the set \(\Sigma\) with the basis \(q, r, s, t, 1, i, j, k\).

It possesses the closure property.

To prove that \(\Sigma\) is a maximal set, annex a new \(q\). After subtracting the products of \(r, q, i, s\) by integers, we may take \(B, D, F, H\) all zero. By (6), \(A, C, E, G\) are all integers (whereas \(q\) is not in \(\Sigma\)) or all halves of odd integers.
Hence we may take \( q = \rho \). But the double of the scalar part of \( \tau \rho \) is \(-\frac{1}{2}(1+\theta)\) which is not an algebraic integer.

From this maximal set \( \Sigma \), we obtain two more by permuting \( i, j, k \) cyclically.

Second, let \( C, E, G \) be not all even. If necessary we permute \( i, j, k \) cyclically and have \( C \) odd. We may take \( A = C = 1 \).

(i) Let also \( E = G = 1 \). By (6), \( B^2 + D^2 + F^2 + H^2 \) is divisible by 4, so that \( B, D, F, H \) are all even or all odd, and we may take \( q = \rho \) or \((1+\theta)\rho \).

(ii) Let \( E = G = 0 \). By (7), \( B + D \) is even. By (6),
\[ B^2 + D^2 + F^2 + H^2 \equiv 2 \pmod{4}. \]
If \( B \) is even, \( D \) is even and \( F \) and \( H \) are odd; thus \( q \) becomes
\[ q = \frac{1}{2}(1+\theta)(1+j). \]
If \( B \) is odd, \( D \) is odd and \( F \) and \( H \) have even, whence
\[ q = \frac{1}{2}(1+\theta)(1+i). \]

(iii) Let one of \( E \) and \( G \) be odd and the other even. Since we may use \( iq \) instead of \( q \), we may by (10) interchange \( E \) with \( G \) and take \( E = 1, G = 0 \). By (6), \( B^2 + D^2 + F^2 + H^2 \equiv 3 \pmod{4} \). By (7), \( B + D + F \) is even. Hence \( H \) is odd. Then \( B^2 + D^2 + F^2 \equiv 2 \pmod{4} \). Thus two of \( B, D, F \) and \( H \) are odd and one is even. According as the even one is \( F, D, \) or \( B \), we get
\[ q = \frac{1}{2}(1+\theta)(1+j). \]

\[ q = \frac{1}{2}(1+\theta)(1+i). \]

In \( q_j \) and \( q_k \) permute \( i, k, j \) cyclically; we get
\[ \frac{1}{2} - \frac{1}{2} \theta k + (\frac{1}{2} + \frac{1}{2} \theta)(j - 1) = q_j - 1 - \theta - \theta k, (\frac{1}{2} + \frac{1}{2} \theta)(i - 1) + \frac{1}{2} j - \frac{1}{2} \theta k = q_k - 1 - \theta - \theta k. \]
It therefore suffices to consider a set having \( q_k \) and hence also
\[ r = q, q_j - 1 - \theta = \frac{1}{2}(j + k) + \frac{1}{2} \theta (k - j), jr + 1 = q_k. \]
Hence case (iii) has been reduced to \( q_k \) of case (ii).

Consider a set \( S \) containing \( q_k \) and therefore also
\[ q = q_j = b \theta k = \frac{1}{2}(1+\theta)(j+k). \]
Annex to \( S \) a new \( q \). Subtracting products of \( q_k \) and \( q \) by integers, we make the coefficients of \( \frac{1}{2} \theta i \) and \( \frac{1}{2} \theta k \) zero; thus take \( D = H = 0 \) in \( q \). Then, by (6) and (7),
\[ AB + EF \equiv \text{even}, \ A^2 + C^2 + E^2 + G^2 + 3(B^2 + F^2) \equiv 0 \pmod{4}. \]

(i) Let \( F \equiv 0, A \equiv 1 \pmod{2} \). By (22), \( B \equiv 0, C \equiv E \equiv G \equiv 1 \pmod{2} \). Thus we may take \( q = \rho \). Since
\[ q_j \rho = \frac{1}{2}(1+\theta)(i+k), \ q_k \rho = \frac{1}{2}(1+\theta)(j-1), \]
\( S \) lies in a set \( \Sigma \), having the basis
\[ (23) \quad q, q_j, q_k, f = \frac{1}{2}(1+\theta)(1+k), g = \frac{1}{2}(1+\theta)(1+j), \theta, \rho, i, j, k. \]
It is easily verified that \( \Sigma \) has the closure property. To prove it is a maximal
Let set, annex $q$. Subtracting products of $q$, $f$, $g$, $p$ by integers, we may take $D = F = H = A = 0$. Then $C^2 + E^2 + G^2 - B^2 \equiv 0 \pmod{4}$ by (6). If $B \equiv 0$, then $C \equiv E \equiv G \equiv 0 \pmod{4}$, $q \equiv 0$. Hence $B = 1$, and two of $C$, $E$, $G$ are 0 and one is 1. Permuting $i$, $j$, $k$ cyclically (which leaves $\Sigma_1$ unaltered), we may take $C = 1$, $E = G = 0$. Then $$ q = \frac{1}{2}(\theta + i), \ qf = \frac{1}{2}(\theta + m)(1 + k) + \frac{1}{2}(1 + \theta)(i - j), $$ the double of whose scalar part is $\frac{1}{2}(\theta + m)$ and is not an algebraic integer.

(II) Let $F \equiv 0, A \equiv 0 \pmod{2}$. By (22), $C^2 + E^2 + G^2 - B^2 \equiv 0 \pmod{4}$. As just noted, $B = 1$ and two of $C$, $E$, $G$ are 0 and one is 1. We interchange $j$ with $k$ and change the sign of $i$ and note that $q_2$ and $\sigma$ are essentially unaltered, while $E$ and $G$ are interchanged and $F$ and $H$; hence we may drop the case in which $E = 1$. If $G = 1$, $C = E = 0$, then $$ q = \frac{1}{2}\theta + \frac{1}{2}k, \ qg_2 = \frac{1}{2}(\theta + m)(1 + i) + \frac{1}{2}(1 + \theta)(k + j), $$ the double of whose scalar part is $\frac{1}{2}(\theta + m)$ and is not an algebraic integer. Hence $C = 1, E = G = 0, q = \frac{1}{2}\theta + \frac{1}{2}i, q_1 - q = \frac{1}{2} + \frac{1}{2}i$, which has been treated at the beginning of §8.

(III) Let $F \equiv A \equiv 1 \pmod{2}$. By (22), $B \equiv E \pmod{2}$ and $C^2 + G^2 \equiv 0 \pmod{4}$, whence $C$ and $G$ are even, $$ q = \frac{1}{2} + \frac{1}{2}B\theta + \frac{1}{2}Bj + \frac{1}{2}k. $$ If $B = 0$, we permute $i, k, j$ cyclically and get $\frac{1}{2} + \frac{1}{2}i$, treated earlier. If $B = 1$, $q$ is in (23). The set has $$ f = \pi - g + 1 + \theta, \ qf = \frac{1}{2}(1 + m + 2\theta)(\rho - j), \ \theta(\rho - j), \ \theta\rho, \ q_2 + \pi = \rho + \rho\theta, \ \rho. $$ Hence we have the set $\Sigma_1$ in case (1).

(IV) Let $F \equiv 1, A \equiv 0 \pmod{2}$. By (22), $E \equiv 0, C^2 + E^2 + G^2 - B^2 \equiv 1 \pmod{4}$. If $B \equiv C \equiv 0$, then $G \equiv 1, q = \frac{1}{2}j + \frac{1}{2}k, jg + \theta = \frac{1}{2}i + \frac{1}{2}\theta$. Subtracting this from $q_2$, we get $\frac{1}{2}(1 + \theta i)$, treated in (21). If $B \equiv 0, C \equiv 1$, then $G \equiv 0, q = \frac{1}{2}i + \frac{1}{2}j, q + q_2 + j = \frac{1}{2}(1 + \theta)(i + j)$. From this and $q_2$, we get $f$, treated in (III). Finally let $B \equiv 1$, whence $C \equiv G \equiv 1, $$ q = \frac{1}{2}(i + k + \theta + j), \ r = \pi - g + \theta + i = \frac{1}{2}(i + j + \theta + k). $$ Consider the set $\Sigma_2$ with the basis $q, r, q_2, \theta, 1, i, j, k$. It has the closure property.

To prove $\Sigma_2$ is not a maximal set annex a new $Q$. By subtracting products of $q, r, q_2$ by integers, we may take $D = F = H = 0$. By (22), $AB$ is even. If $A = 1, B = 0$ and $1 + C^2 + E^2 + G^2 \equiv 0 \pmod{4}$, whence $C = E = G = 1, Q = \rho$. Now $\rho$ extends $\Sigma_2$ to the larger set $\Sigma_1$ of case (1). Next, let $A = 0$, whence $C^2 + E^2 + G^2 \equiv B^2 \pmod{4}$. If $B \equiv 0$, then $C \equiv E \equiv G \equiv 0, Q \equiv 0$. Hence $B \equiv 1$ and two of $C, E, G$ are $\equiv 0$ and one is $\equiv 1$. We may interchange $j$ with $k$ without altering $\Sigma_2$ and hence take $Q = \frac{1}{2}\theta + \frac{1}{2}i$ or $\frac{1}{2}j + \frac{1}{2}k$. In the former case we obtain the maximal set $\Sigma$ in (21). The second case is excluded by (II).

It remains to consider a set $S$ not containing $q_2$ such that the two sets derived from $S$ by cyclic permutations of $i, j, k$ do not contain $q_2$. If every
element \( q \) of \( S \) having \( A = 1 \) is of type (i), and hence is \( \rho \) or \( (1+\theta)\rho \), \( S \) is not a maximal, but is contained in \( \Sigma_1 \) of (I). Hence \( S \) contains \( q_1 \) of (ii) and therefore \( t_i = j_0 \). The sub-set \( S_i \) with the basis \( q_i, t_i, \theta j, \theta, 1, i, j, k \) has the closure property. It is not maximal, being extended by \( \rho \) to set \( \Sigma_1 \) of (I). To \( S_i \) annex any element \( q \). Since we may add the products of \( q_1 \) and \( t_i \) by integers, we may take \( A = 1 \) in \( q \), and assume that \( E \) and \( G \) are not both even. Interchanging \( j \) and \( k \) if necessary (which leaves \( S_i \) unaltered), we may take \( A = E = 1 \). If also \( C = 1 \), \( q \) is of type (i) or (iii), of which the latter is excluded by the hypothesis on \( q_2 \). But \( (1+\theta)\rho = q_1 + t_i + k + \theta \) is in \( S_i \), while \( \rho \) extends \( S_i \) to a set containing

\[
t_i + \rho - j + \theta = q_2.
\]

Hence \( C = 0 \). The cyclic substitution \( (i, k, j) \) replaces \( q \) by \( q' \) having \( A' = A = 1 \), \( C' = E = 1 \), \( G' = C = 0 \), so that \( q' \) is of type (ii) or (iii) and hence is \( q_1 \). The inverse substitution \( (i, j, k) \) replaces \( q_1 \) by

\[
q = \frac{1}{2}(1+j) + \frac{1}{2}\theta(k+i).
\]

The enlarged set contains \( q - t_i = \frac{1}{2}(1+\theta)(1+k) \). Applying \( (i, j, k) \), we get a set containing \( q_2 \).

**Theorem.** For \( m = 3 \) (mod 4), there are just four maximal sets: \( \Sigma \) and \( \Sigma_1 \) defined by (21) and (23), and the two sets derived from \( \Sigma \) by cyclic permutations of \( i, j, k \).

The general element of \( \Sigma_1 \) is

\[
X = x_0 + x_1 i + x_2 j + x_3 k + x_4 \theta + x_5 i^2 + x_6 i^3 + x_7 = a + \alpha i + \beta j + \gamma k,
\]

where the \( x \)'s are integers. Write

\[
x_0 = x_0 + x_4 + x_7, \quad x_1 = x_0 + 2x_1 + x_4 + (s = 1, 2, 3), \quad x_2 = 2x_1 + x_4 + x_7.
\]

Then

\[
a = \frac{1}{2}(\xi + \xi \theta), \quad a_j = \frac{1}{2}(\xi_i + x_{4+s} \theta), \quad N(X) = U + V \theta
\]

\[
4U = \xi \xi + \xi \xi + \xi \xi + \xi \xi + n(\xi i^2 + x_1 \xi + x_2 \xi + x_7), \quad 2V = \xi \xi + \xi \xi + \xi \xi + \xi \xi.
\]

It follows readily as at the end of §6 that, if \( m \equiv 3 \), \( X^2 = -1 \) only when \( X = \pm i, \pm j, \pm k \). Hence if \( m > 0 \), \( \Sigma \) and \( \Sigma_1 \) are not equivalent.

### 9. Division Algebras

Consider the algebra \( Q \) of quaternions over the quadratic field \( R(\theta) \). It is called a division algebra if a product is zero only when one of the factors is zero. If \( Q \) is a division algebra, then \( N(z) = z \bar{z} \) is zero only when \( z = 0 \), and conversely. For, if the converse is false, \( Q \) is not a division algebra and hence contains elements \( x \) and \( y \), each not zero, whose product is zero. Then the product of their norms (which are algebraic numbers) is zero, so that one of the norms is zero, contrary to hypothesis.

Since a sum of squares of real numbers is zero only when all those numbers are zero, the converse shows that \( Q \) is a division algebra when \( \theta \) is real.
THEOREM. If \( m \) is a negative integer, the algebra \( Q \) of all quaternions over the field \( R(\sqrt{m}) \) is a division algebra if and only if \( m \equiv 1 \pmod{8} \).

First, let \( m = 2 \) or \( m \equiv 3 \pmod{4} \), so that 1 and \( \theta = \sqrt{-m} \) form a basis of the algebraic integers of the field. Write \( m = -M \), \( X = \theta + xi + yj + zk \), where \( x, y, z \) are integers. Then \( N(X) = 0 \) if \( M = x^2 + y^2 + z^2 \). Since \( m \equiv 2 \) or \( 1 \pmod{4} \), this equation has integral solutions by the well known theorem that every positive integer \( M \) not of the form \( 8l + 7 \) or \( 4l \) is a sum of three integral squares.

Second, let \( m = 1 \pmod{8} \). Then 1 and \( \theta = i(1 + \sqrt{-m}) \) form a basis of the algebraic integers of the field. Thus

\[
\theta^2 = \theta + m, \quad n = \frac{1}{3}(m - 1).
\]

For \( n \) odd, consider \( X = \rho - \theta + xi + yj + zk \). Then

\[
4N(X) = 1 + 4n + (1 + 2x)^2 + (1 + 2y)^2 + (1 + 2z)^2.
\]

By hypothesis, \( n = -(2l + 1) \). By the theorem just quoted, \( -1 - 4n = 8l + 3 \) is a sum of three integral squares, necessarily all odd. Hence there exist integers \( x, y, z \) for which \( N(X) = 0 \).

Finally, let \( n \) be even, so that \( m \equiv 1 \pmod{8} \). We shall prove that \( -1 \) is not of the form \( \alpha^2 + \beta^2 \), where \( \alpha \) and \( \beta \) are in \( R(\theta) \), and conclude* that \( Q \) is a division algebra. Suppose that \( -1 = \alpha^2 + \beta^2 \). The product of any number of \( R(\theta) \) by a suitably chosen integer is known to be an algebraic integer. Hence

\[
\begin{align*}
da &= x + y\theta, \\
d\beta &= z + w\theta,
\end{align*}
\]

where \( d, x, y, z, w \) are integers whose g.c.d. is 1. Thus \( -d^2 = d^2(\alpha^2 + \beta^2) \) is equivalent to the pair of equations

\[
-d^2 = x^2 + z^2 + n(y^2 + w^2), \\
2xy + 2zw + y^2 + w^2 = 0.
\]

Since \( y^2 + w^2 \) and \( n \) are both even, \( d^2 + x^2 + z^2 \) must be divisible by 4. Hence \( d, x, z \) are all even. Then the second equation shows that \( y^2 + w^2 \) is divisible by 4, so that \( y \) and \( w \) are even. Thus \( d, x, y, w \) have the common factor 2, contrary to hypothesis.

COROLLARY. Every normal set of integral elements of any algebra of quaternions over an imaginary quadratic field contains an element, not zero, whose norm is zero, with the exception of the set \( \Sigma \) in \( \S 7 \) composed of the elements \( q + \theta q_1 \), where \( q \) and \( q_1 \) range over all Hurwitz integral quaternions, and \( \theta = \frac{1}{3}(1 + \sqrt{-m}) \), \( m \equiv 1 \pmod{8} \).

For, in the first case of the proof of the theorem, any normal set contains \( \theta, i, j, k \) and hence \( X \). In the second case, it may be assumed (\( \S 7 \)) to contain also \( \rho \) and therefore \( X \).

Such elements \( X \neq 0 \) of norm zero can not be chosen as \( b \) in a division process† (if one exists) \( a = qb + c \), such that the algebraic norm of the quaternion norm of \( c \) is less than that of \( b \).

*Algebras and Their Arithmetics, p. 67.
†Ibid., p. 149.