INTEGRAL SETS OF QUATERNION ALGEBRAS
OVER A FUNCTION FIELD

BY
LEONARD TORNHEIM

1. Introduction. The theory of rational quaternion algebras suggests a
corresponding theory for quaternion algebras over a rational function field
$F(z)$. We can anticipate points of close analogy because of many similarities
between the set of all rational integers and the set of polynomials $F[z]$. We
may also expect results peculiar to each of these theories traceable to certain
fundamental differences between these two integral domains.

We find a basis for every integral set $S$ of $Q$ after suitably normalizing a
basis of $Q$. When $F$ is the field of all real numbers, canonical bases for both $Q$
and $S$ are obtained. We discuss properties of $Q$ which make $S$ be a principal
ideal ring or not. Conditions are provided for a quantity in $F[z]$ to generate a
prime ideal in $S$. Throughout applications are made in the cases for which $F$
is either a real number field or a finite field.

2. Integral sets of $Q$ with characteristic not two. When $F$ has characteris-
tic not two, a quaternion algebra\(^1\) $Q$ has a basis $1, i, j, ij$ with $i^2 = \tau, j^2 = \sigma,$
$ij = -ji$. The basis can be chosen as normalised\(^2\); that is, $\sigma, \tau$ lie in $F[z]$, are
relatively prime, and contain no square factors. If $F$ is a Hilbert irreducibility
field\(^3\), it is possible in addition to take $\tau$ a prime (i.e., irreducible) in $F[z]$.

Integral sets\(^4\) $S$ of $Q$ are defined by the usual four properties $R, C, U,$
and $M$. We obtain a basis for an integral set $S$ of $Q$ in

**Theorem\(^5\)** 1. Let $Q$ have a normalized basis. Let $\tau'$ be the product of all
prime factors of $\tau$ for which $\sigma$ is a quadratic residue, and $\tau'' = \tau/\tau'$ be monic\(^6\).
Let $\sigma'$ and $\sigma''$ be defined similarly. Then every integral set $S$ of $Q$ has a basis
over $F[z]$ of the form $1, i, j, \omega$, where

\[
\omega = a i/\tau' + b j/\sigma' + i j/\sigma' \tau'
\]

Presented to the Society, April 8, 1938; received by the editors November 16, 1939.

\(^1\) A. A. Albert, *Structure of Algebras*, American Mathematical Society Colloquium Publica-

\(^2\) A. A. Albert, *Integral domains of rational generalized quaternion algebras*, Bulletin of the

\(^3\) For a summary of results on Hilbert irreducibility fields see A. A. Albert, *Involutorial


\(^5\) For analogous results for rational algebras see, in addition to the references already cited, C. G. Latimer,*Arithmetics of generalised quaternion algebras*, American Journal of Mathematics, vol. 48 (1926), pp. 57–66; M. D. Darkow,*Determination of a basis for the integral ele-
tments of certain generalised quaternion algebras*, Annals of Mathematics, (2), vol. 28 (1926),
pp. 263–270.

\(^6\) A polynomial is monic if its leading coefficient is unity.
with \( a, b \) any quantities in \( F[z] \) satisfying

\[
\tau b^2 \equiv \tau''^2 \quad (\sigma'), \quad \sigma a^2 \equiv \sigma''^2 \quad (\tau').
\]

For, by conditions \( U, C, \) and \( R, \) if \( \xi \) is in an integral set \( S, \) then the traces of \( \xi, i\xi, j\xi, \) and \( ij\xi \) are in \( F[z]. \) Thus \( \xi = x_0 + x_1i/\tau + x_2j/\sigma + x_3ij/\sigma\tau \) with the \( x \)'s all in \( F[z]. \) Now \( N(\xi) \) is in \( F[z] \) if and only if

\[
\begin{align*}
2x_1^2 &\equiv x_2^2 \quad (\tau), \\
2x_2 &\equiv x_3^2 \quad (\sigma).
\end{align*}
\]

Since \( \sigma \) is not a quadratic residue of any factor of \( \tau'' \) and \( \tau \) is not a quadratic residue of any factor of \( \sigma'' \), we see from the congruences (3) that \( x_1 \) is divisible by \( \tau''', \) \( x_2 \) by \( \sigma''', \) and \( x_3 \) by \( \sigma''\tau'''. \) It follows that every quaternion in an integral set \( S \) lies in a domain \( (1, i, j, \omega) \) over \( F[z], \) where \( \omega \) is defined in (1).

Let \( r_3/\sigma'\tau' \) be the g.c.d. of all the coefficients of \( ij \) for quantities in \( S. \) Then \( r_3/\sigma'\tau' \) is a linear combination (with multipliers in \( F[z] \)) of the coefficients of \( ij \) of a finite set of quaternions of \( S. \) Let \( \rho \) be the corresponding linear combination of the same quaternions. Hence \( \rho \) is in \( S. \) Also \( \rho = r_0 + r_1i + r_2j + r_3\omega', \) where the \( r \)'s are in \( F[z], \) \( \omega' = a'i/\tau' + b'j/\sigma' + ij/\sigma'\tau', \) and \( a', b' \) satisfy (2).

If \( \eta \) is also in the integral set \( S, \) \( \eta = y_0 + y_1i + y_2j + y_3\omega \) and \( y_0 \) is divisible by \( r_3. \) Using the fact that \( N(\rho + \eta) \) must be in \( F[z], \) we find that \( \eta \) is in \( S' = (1, i, j, \omega'). \) It is easily verified that \( S' \) satisfies conditions \( R, C, U. \) Inasmuch as it contains the maximal set \( S, \) we have \( S = S'. \) This completes the proof.

If \( \sigma' \) has \( m \) factors and \( \tau' \) has \( n \) factors, then there are \( 2^{m+n} \) pairs of incongruent solutions \( a, b \) of (2). The corresponding \( 2^{m+n} \) integral sets may be proved distinct by calculating \( N(\omega + \omega') \) for \( \omega \neq \omega'. \)

The monic quantity \( d = \sigma''\tau''', \) although defined by a particular basis, is an invariant of the algebra called the *fundamental number* (7) of \( Q. \) It is in fact, except for a factor in \( F, \) the square root of the discriminant of an integral set of \( Q. \) Every integral set is a maximal order of \( Q \) and all maximal orders of \( Q \) have the same discriminant (8). This implies the invariance of the fundamental number \( d. \) We proceed to give a direct proof based upon our definition of \( d. \)

**Theorem 2.** The fundamental number \( d = \sigma''\tau''' \) of a quaternion algebra \( Q \) is an invariant of the algebra.

For, let \( Q \) have a normalized basis, 1, \( i, j, ij, \) with \( i^2 = \tau, j^2 = \sigma. \) If 1, \( i_0, j_0, \) \( i_0j_0 \) is another normalized basis, \( \tilde{\tau} = \tau, \tilde{\sigma} = \sigma, \) then

\[
\begin{align*}
i_0 &= (x_1i + x_2j + x_3ij)/x_4, & (x_1, x_2, x_3) &= 1, \\
j_0 &= (y_1i + y_2j + y_3ij)/y_4, & (y_1, y_2, y_3) &= 1,
\end{align*}
\]

where the \( x \)'s and \( y \)'s are in \( F[z]. \)


Let $d_i$ be a prime divisor of $d = \sigma'' \tau''$, the fundamental number corresponding to the basis $1, i, j, ij$. We first assume that $d_i$ divides $\tau''$. Then $d_i$ divides $x_2y_2$ because $i_0j_0 + j_0i_0 = 0$. Now $d_i$ cannot divide both $x_2$ and $x_4$; if so, we would have on computing
\[
x_1^2 - x_3^2 \sigma \equiv 0 \quad (d_i),
\]
and thus
\[
x_1^2 - x_3^2 \sigma \equiv 0 \quad (d_i),
\]
an impossibility for $d_i$ a divisor of $\tau''$. Similarly $d_i$ does not divide both $y_2$ and $y_4$.

Suppose that $d_i$ divides $x_2$. Then $d_i$ does not divide $x_4$ and consequently $d_i$ divides $\tau_0$. If $d_i$ did not divide $\tau_0''$, we would have
\[
\sigma_0 \equiv c^2 \quad (d_i)
\]
and thus
\[
y_1^2 + y_3^2 \sigma - y_2^2 \sigma \equiv c^2 y_4 \quad (d_i),
\]
(4)
\[
y_2^2 \equiv c^2 y_4 \quad (d_i).
\]
Since $(\sigma_0, \tau_0) = 1$, we have $(\sigma_0, d_i) = 1$ and also $(c, d_i) = 1$. Noticing also that $(\sigma, d_i) = 1$, we see that congruence (4) implies that $\sigma$ is a quadratic residue of $d_i$, a contradiction to the assumption that $d_i$ divides $\tau''$. We have proved that $d_i$ divides $\tau_0''$ and hence that it also divides $d_0 = \sigma_0'' \tau_0''$.

If $d_i$ divides $y_2$, similar reasoning would show that $d_i$ divides $\sigma_0''$.

A parallel proof is used in case we had assumed $d_i$ to be a divisor of $\sigma''$ to demonstrate that $d_i$ divides either $\sigma_0''$ or $\tau_0''$.

Hence every prime divisor of $d$ divides $d_0$ and, of course, conversely. Since $d$ and $d_0$ are square-free and monic, $d = d_0$.

We shall use this lemma of Albert(9).

**Lemma 1.** If in the generalized quaternion algebra $Q$ we replace $\sigma$ by $(g^2 - \tau h^2)\sigma$ with $g, h$ in $F(\sigma)$, we obtain an equivalent algebra.

In the remainder of this section $F$ is specialized to be the field of all real numbers. We apply Lemma 1 to prove

**Theorem 3.** Let $F$ be the field of all real numbers. Then $Q$ over $F(\sigma)$ has a basis $1, i, j, ij$, with $i^2 = -1$ and $j^2 = \sigma$, where $\sigma$ has leading coefficient $\pm 1$, is a product of distinct linear factors, and is, except for sign, the fundamental number of $Q$. There is a single integral set $S$ and it has a basis $1, i, j, ij$. Furthermore there is a one-to-one correspondence between the classes of equivalent quaternion

(9) See footnote 2.
algebras (including non-division algebras) over \( F(z) \) and the square-free polynomials \( \sigma \) in \( F[z] \) of leading coefficient \( \pm 1 \) containing only linear factors.

By a theorem of Tsen(10), there are no normal division algebras of order greater than 1 over the field of complex numbers with one indeterminate adjoined. Hence \( F((-1)^{1/2}) \) splits \( Q \) and we may take \( i^2 = -1 \) since \( Q \) contains(11) a field equivalent to \( F((-1)^{1/2}) \). Now \( j^2 = \sigma \) and we may take \( \sigma \) square-free and in \( F[z] \). The leading coefficient may be taken as \( \pm 1 \), since if \( \sigma \) has leading coefficient \( a \) then \( \sigma/(|a|^{1/2}) \) has the desired property.

If \( r = z^2 + 2bz + c \), with \( b \) and \( c \) in \( F \), and is positive definite, the discriminant \( d_0 \) of \( r \) is \( 4(b^2 - c) \) and is negative. Then \( r \) is a sum of two squares in \( F[z] \);

\[
r = (z + b)^2 + (\frac{1}{2}(-d_0)^{1/2})^2.
\]

If \( r \) divides \( \sigma \), an application of Lemma 1 in reverse when \( \tau = -1 \) serves to remove the factor \( r \) from \( \sigma \). In this way all positive definite prime factors of \( \sigma \) are removed, and we can assume now that \( \sigma \) contains no such factors. The only other irreducible polynomials in \( F[z] \) are linear. Hence \( \sigma \) is a product of linear factors and they are distinct because \( \sigma \) is square-free.

The fact that 1, \( i \), \( j \), \( ij \) form a basis of the integral set \( S \) follows immediately from Theorem 1, since \( i + j = 0 \) and \( -1 \) is never a quadratic residue of a linear function of \( F[z] \). Hence the fundamental number of \( Q \) is \( \pm \sigma \).

Let \( \sigma \) have leading coefficient \( \pm 1 \) and contain only distinct linear factors. If the norm

\[
(5) x_0^2 + x_1^2 - \sigma(x_2^2 + x_3^2)
\]

of a quaternion in \( S \) is zero, it must be zero for every value taken in \( F \) by the indeterminate \( z \). Setting \( z \) in turn equal to each of the roots of \( \sigma \) and using the fact that \( x_0^2 + x_1^2 \) is positive definite, we deduce that both \( x_0 \) and \( x_1 \) are divisible by \( \sigma \). Dividing (5) by \( \sigma \) and using the same reasoning, we find that \( x_2 \) and \( x_3 \) are both divisible by \( \sigma \). Continuing in this way, we find that \( x_0, x_1, x_2, x_3 \) are all divisible by every power of \( \sigma \). This is possible only when \( \sigma \) is in \( F \), i.e., \( \sigma = \pm 1 \). But \( \sigma \neq -1 \), for then (5) is positive definite. Consequently when \( Q \) is not a division algebra, \( \sigma = 1 \).

If \( Q \) contains quantities having norms with negative leading coefficient, then using (5) we conclude that \( \sigma \) is monic; otherwise \( -\sigma \) is monic. Hence the sign of \( \sigma \) is determined by the algebra.

We know then that \( \sigma \) is uniquely determined by the algebra since except for sign it is the fundamental number of the algebra.

3. **Integral sets of \( Q \) with characteristic two.** Let the field \( F \) have characteristic two. Then \( Q \) has a basis(12) 1, \( i \), \( j \), \( ij \) where \( i^2 + i + \alpha = 0 \), \( j^2 = \gamma \), \( ij \)

---

LEONARD TORNHEIM

\[ j(i+1), \text{ and } \alpha \text{ and } \gamma \text{ are in } F(z). \] Choose \( m_0 \neq 0, m_0 \in F(z) \) so that \( \gamma_0 = m_0^2 + \gamma m_0^2 \) is in \( F[z] \) and has minimal degree in the set of all quantities of that form. Now \( \gamma_0 \neq 0 \) because otherwise the nonzero quaternion \( m_0 + m_2j \) would be a divisor of zero. Evidently \( \gamma_0 \) is square-free. Whenever \( \gamma_0' = m_0'^2 + \gamma_0 m_0'^2 \), then \( \gamma_0' = (m_0^2 + m_2m_2')^2 + \gamma(m_2m_2')^2 \); hence \( \gamma_0 \) has minimal degree in the set of all quantities of \( F[z] \) of the form \( m_0'^2 + \gamma_0 m_0'^2 \), where \( m_0' \neq 0 \). The transformation

\[ i_1 = i + m_0ij/\gamma m_2, \quad j_1 = m_0 + m_2j \]

replaces \( \gamma \) by \( \gamma_0 \).

Let \( \beta_0 \) be a nonzero quantity of lowest degree for which the equation \( xj_1 = j_1(x+\beta_0) \) has a solution with \( x \) an integral quaternion. Denote such a solution \( x \) by \( r_0 + r_1i_1 + r_2j_1 + r_3i_1j_1 \). Necessarily \( r_3 = 0 \). Let \( b' \) be the leading coefficient of \( \beta_0 \). The transformation

\[ i_0 = (r_0 + r_1i_1 + r_2j_1)/b', \quad j_0 = j_1 \]

produces a new basis of \( Q \) of the type described in

**Theorem 4.** An algebra \( Q \) of characteristic two has a basis \( 1, i, j, ij \) where

\[ i^2 = \beta i + \alpha, j^2 = \gamma, ij = j(i + \beta); \alpha, \beta, \gamma \text{ are in } F[z]; \beta \text{ is monic and has least degree among all nonzero } \beta_0 \text{ in } F[z] \text{ for which the equation } xj = j(x+\beta_0) \text{ has an integral quaternion } x \text{ as solution}; \text{ and } \gamma \text{ is a square-free polynomial and has the least degree for all polynomials of the form } m_0^2 + m_2^2 \gamma \text{ having } m_0, m_2 \text{ in } F(z) \text{ and } m_0 \neq 0. \]

A basis of the type given in Theorem 4 will be called a normalised basis.

When \( F \) is perfect we can take \( \gamma = z \). This is implied by a result of Albert\(^{(13)}\). We give here a direct proof. First, \( \gamma \) cannot be in \( F \) for then \( \gamma^{1/2} + j \) would be a divisor of zero. Hence \( \gamma \) has degree \( \geq 1 \). Since \( \gamma \) is in \( F[z] \) and \( F \) is perfect, \( \gamma = c_1^2 + c_2^2z \) with \( c_1 \) and \( c_2 \) in \( F[z] \). Thus \( z = (c_1/c_2)^2 \gamma + (1/c_2)^2 \) and has minimal degree. We have proved part of

**Theorem 5.** When \( F \) is perfect, then in Theorem 4 we may take \( \gamma = z \) and \( \beta \) monic, square-free, and prime to \( z \).

A value of \( \beta \), because of the minimal degree property, is necessarily square-free. For, if \( \beta = \beta_0 p^2 \), then \( i' = (m_0 + i + m_2j)/p \) is integral if \( m_0 \) and \( m_2 \) are chosen in \( F[z] \) to satisfy \( m_0^2 + m_2^2 \gamma = \alpha \). Furthermore \( i'j = j(i' + \beta/p) \), and \( \beta/p \) has degree less than that of \( \beta \). These properties of \( i' \) contradict the assumptions made about \( \beta \).

In addition, \( \beta \) is not divisible by \( z \). Otherwise, if we take \( r_0 \in F \) to be the square root of the constant term of \( \alpha \) and \( r_2 \) to be the square root of the coefficient of the linear term of \( \beta r_0 + \alpha \), we have that \( i' = (r_0 + i + r_2j)/z \) is integral, \( i'j = j(i' + \beta/z) \), and \( \beta/z \) has degree less than that of \( \beta \). We have here a contradiction to the defining property of \( \beta \).

Theorem 6. Let $Q$ have a normalized basis. Then every integral set $S$ in $Q$ has a basis $1, i, j, \omega = (x_1x_2 + x_1i + x_2j + ij)/m$, where $m$ is the largest factor of $\beta \gamma$ for which there are solutions $x_1, x_2$ of

$$x_1^2 \equiv \gamma, \quad x_2^2 \equiv \beta x_2 + \alpha \ (m).$$

Furthermore $m$ is square-free.

Let $\xi$ be in $S$. By properties $R, C$, and $U$, the traces of the quaternions $\xi, i\xi, j\xi, ij\xi$ are in $F[z]$. Hence $\xi = [x_0 + x_1i + (x_2 + x_3)j]/\beta\gamma$ with the $x$'s in $F[z]$. Since the denominators of integral quantities divide $\beta \gamma$, an integral set $S$ must have a basis. This basis can be taken in the form

$$\omega_1 = e_0/\beta \gamma, \quad \omega_2 = (f_0 + f_1i)/\beta \gamma, \quad \omega_3 = (g_0 + g_1i + g_2j)/\beta \gamma, \quad \omega_4 = (h_0 + h_1i + h_2j + h_3ij)/\beta \gamma,$$

with the $e_0, f_1, g_2, h_3$ either equal $\beta \gamma$ or else have degree less than that of $\beta \gamma$ and the remaining $f_0, g_0, h_0$'s, and $h_1$'s have degrees less than $D(\beta \gamma)$ (the degree of a polynomial $a$ is designated by $D(a)$).

Obviously, $\omega_1$ is not integral unless $e_0 = \beta \gamma; \omega_1 = 1$.

If $D(f_1) < D(\beta \gamma)$, then $D(T(\omega_1)) < D(\beta)$ while $\omega_2 = j(\omega_2 + T(\omega_3))$. This contradicts the choice of $\beta$; hence $D(f_1) = D(\beta \gamma)$ and in fact $f_1 = \beta \gamma$. Since $\omega_2 = i$ is in $S$, $f_0/\beta \gamma$ is in $F[z]$; hence $f_0 = 0$, and $\omega_2 = i$.

From $D(g_1) < D(\beta \gamma)$, it follows that $D(T(\omega_3)) < D(\beta)$ and $\omega_4 = j(\omega_2 + T(\omega_3))$, a contradiction to the choice of $\beta$ unless $g_1 = 0$. If $D(g_2) < D(\beta \gamma)$, then $\omega_3$ has its norm $(g_0/\beta \gamma)^2 + (g_2/\beta \gamma)^2 \gamma$ in $F[z]$ and of degree less than that of $\gamma$, a contradiction to the choice of $\beta$. Thus $g_2 = \beta \gamma$, and since $\omega_2 = j$ is in $S$, $g_2 = 0$, so that $\omega_3 = j$.

Since $ij$ is in $S$, necessarily $h_3$ divides $\beta \gamma; \beta \gamma = h_3m'$ with $m'$ in $F[z]$. Now $\omega_4m' - ij = h_0/h_3 + h_1i/h_3 + h_2j/h_3$ is in $S$. Thus $h_0, h_1, h_2$ are all divisible by $h_3$ and $\omega_3 = (d_0 + d_1i + d_2j + ij)/m'$ with the $d$'s in $F[z]$. In $S$ must be $i\omega_4$ and $\omega_4j$. This is possible if and only if

$$d_1^2 \equiv \gamma, \quad d_2^2 \equiv d_2 \beta + \alpha, \quad d_0 \equiv d_1d_2 \ (m').$$

Now $m'$ has no square factors. Otherwise, if $p^2$ were a divisor of $m$, $p^2$ would divide $\beta \gamma$. If $p$ were a divisor of $\gamma$, then because $d_1^2 = \gamma (p^2)$, $p$ would divide $d_1$ and $p^2$ divide the square-free $\gamma$. Hence $p$ would not divide $\gamma$, so that $p^2$ would be a divisor of $\beta$. But then $i_1 = (d_2 + i)/\beta$ would be integral, $i_1j = j(i_1 + \beta/p)$, and $\beta/p$ have smaller degree than $\beta$. This is impossible from our choice of $\beta$.

Our next step is to give a construction of $\omega_4$. Let $m = \beta \gamma$ for which there exist solutions of
By means of a discussion similar to that for $m'$ we can show that $m$ is also square-free, i.e., $\epsilon_n = 1$. Using the Chinese remainder theorem we can find a unique solution $x_1$, $x_2$ modulo $m$ of the congruences (7) common to all $p_n$. Therefore

$$x_1 \equiv \gamma, \quad x_2 \equiv x_2 \beta + \alpha \pmod{m}.$$  

The quantity $\omega = (x_1 x_3 + x_3 + x_3 j + ij)/m$ is integral. Its trace is $\beta x_1 / m$. This is in $F[z]$ since any factor of $m$ dividing $\gamma$ divides $x_1$ because of (7) and the remaining factors of $m$ divide $\beta$. Furthermore

$$m^2 N(\omega) = x_1 x_2 + x_1 x_2 \beta + x_1 \alpha + \gamma(x_2^2 + x_2 \beta + \alpha) = (x_1 + \gamma)(x_2 + x_2 \beta + \alpha) = 0 \pmod{m};$$  

thus $N(\omega)$ is in $F[z]$.

The quantity $\omega$ with $1$, $i$, $j$ forms a basis for an integral set $S'$. The conditions $C$, $R$, and $U$ are easily verified to be satisfied. To show that maximality is true only for such a set $S'$, we need only show that every integral set $S$ is necessarily contained in such a set; in fact, only that $\omega_4$ is in some $S'$.

Since (6) holds for $m'$, it is true of every prime factor of $m'$. Also $m'$ divides $\beta \gamma$. From the definition of $m$, every prime factor of $m'$ divides $m$. Thus $m'$ divides $m$; $m = m'm''$. We can find a solution $x_1$, $x_2$ of (7) for which $x_1 \equiv d_1$, $x_2 \equiv d_2 (p_n)$ whenever $p_n$ is a divisor of $m'$. Consequently $\omega_4$ is in $S$. We have proved our theorem.

Another form for the basis of $Q$ of characteristic two is $1$, $u_1$, $u_2$, $u_1 u_2$, where

$$u_1 = \tau, \quad u_2 = \sigma, \quad u_1 u_2 + u_2 u_1 = \rho \quad (\rho, \sigma, \tau \in F(z)).$$

Such a basis can be obtained by taking $u_1 = j$, $u_2 = ij$. A basis of $Q$ of this form can be found which is normalized to have $\rho$, $\sigma$, $\tau$ in $F[z]$, $u_1$ a quantity with norm of lowest degree in the set of all inseparable integral quantities over $F(z)$, and $u_2$ an integral quantity linearly independent of $1$ and $u_1$, inseparable over $F(z)$, and having for $\rho$ a value in $F[z]$ of lowest degree. Using much the same reasoning as before we can prove

**Theorem 7.** An integral set $S$ with respect to a basis $1$, $u_1$, $u_2$, $u_1 u_2$ normalized as above has a basis $1$, $u_1$, $u_2$, $\omega$, where

$$\omega = (y_1 + y_1 u_1 + y_2 u_2 + y_3 u_1 u_2) / \rho.$$

---

Here $y_3$ is determined as one of the quantities of lowest degree for which there exists a solution of

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 + \rho(y_0y_2 + y_1y_3) = 0 \quad (\rho)$$

with the $y$'s in $F[z]$.

4. Factorization when $S$ is a principal ideal ring. Theorems 8 and 9 give sufficient conditions for an integral set $S$ to possess a weakened form of a Euclidean algorithm. This form of the algorithm, however, is equivalent to the algorithm itself for quaternion algebras.

**Theorem 8.** Let $Q$ of characteristic not two have a normalized basis with $\sigma, \tau$ having degrees not greater than 1, and if both have degree 1, then one of them being a quadratic residue of the other. Then if $\theta$ is in an integral set $S$ of $Q$, and $m$ is a nonzero polynomial in $F[z]$, there exists a quaternion $\kappa$ in $S$ such that $D(N(\theta - \kappa m)) < D(N(m))$.

A proof of this theorem is easily effected when an explicit basis of $S$ is known.

If $\sigma$ and $\tau$ are both in $F$, $S = (1, i, j, ij)$.

Suppose $\sigma$ is linear and $\tau$ is in $F$. Were $\tau$ a quadratic residue of $\sigma$, we would have $\tau = a^2$ and $Q$ would not be a division algebra. Hence $\tau$ is not a quadratic residue of $\sigma$ and $S = (1, i, j, ij)$. The case $\sigma$ in $F$ and $\tau$ linear is treated similarly.

Suppose that both $\sigma$ and $\tau$ are linear. If $(\sigma | \tau) = (\tau | \sigma) = -1$ (this case is excluded in the theorem), $S = (1, i, j, ij)$. If however $(\sigma | \tau) = -(\tau | \sigma) = 1$, then $\sigma = a^2(\tau)$, with $a$ in $F$. Hence $S = (1, i, j, \omega)$, where $\omega$ is one of $(a \pm j)/\tau$. The case $(\sigma | \tau) = -(\sigma | \tau) = 1$ is handled similarly. Finally if $(\sigma | \tau) = (\tau | \sigma) = 1$, then $\sigma = a^2(\tau)$, $\tau = b^2(\sigma)$, with $a$ and $b$ in $F$. Thus $\sigma = a^2 + k\tau$, $b^2 = -a^2/k$, and $i/\sigma r + j/br + ij/\sigma \tau$ has norm 0; $Q$ is total matric.

If in Theorem 8 we write $\theta = g_0 + g_1i + g_2j + g_3\omega$, the quaternion $\kappa = q_0 + q_1i + q_2j + q_3\omega$ is found by choosing the polynomials $q_k$ to satisfy $D(g_k - q_km) < D(m)$; i.e., the $q_k$ are the quotients on dividing the $g_k$ by $m$.

**Theorem 9.** Let $Q$ have characteristic two, with $\gamma$ linear and $\alpha$ and $\beta$ in $F$.

If $\theta$ is in the integral set $S = (1, i, j, ij)$ of $Q$, and $m$ is in $F[z]$, then there exists a quaternion $\kappa$ in $S$ such that $D(N(\theta - \kappa m)) < D(m^2)$.

That $S$ has a basis 1, $i, j, ij$ follows from the discussion in §3 and the fact that $x^2 + \beta x + \alpha = N(x + i)$ is irreducible in $F$ when $Q$ is a division algebra. The quaternion $\kappa$ is determined as in the proof of Theorem 8.

When $Q$ has characteristic two and $F$ is perfect, we can take $\gamma = z$ by Theorem 5. If in addition $\beta$ is in $F$, then we can assume $\beta = 1$. We can also have $\alpha$ in $F$. For, since $F$ is perfect, $\alpha$ has the form $a^2 + a^2z$. The degree of $\alpha$ is reduced to zero by repeated application of the transformation

$$i' = a_1 + i + a_2z, \quad j' = j.$$
We then have a basis for this $Q$ satisfying the hypothesis of Theorem 9. Theorems 8 and 9 imply the existence of a Euclidean algorithm for the integral sets involved\(^{(16)}\). The presence of such a process assures us that $S$ is a principal ideal ring.

Whenever $S$ is a principal ideal ring, the following decomposition theorem is true. A proof can be made using a procedure developed for rational algebras\(^{(16)}\).

**Theorem 10.** Let $S$ be a principal ideal ring. Let $\theta$ be a quaternion in $S$ not divisible by a polynomial in $F[z]$. If $N(\theta) = p_1 p_2 \cdots p_n$, where the $p_k$ are irreducible polynomials, then $\theta = \pi_1 \pi_2 \cdots \pi_n$ where $N(\pi_k) = p_k$ and $\pi_1$ is unique except for multiplication by units of $S$ on the right, $\pi_2, \ldots, \pi_{n-1}$ are unique but for multiplication by units on the right or left, and $\pi_n$ is unique except for left unit factors.

5. **Prime quaternions in $S$.** In this section we seek to determine when a quaternion is prime in $S$. In particular we want to know when a prime in $F[z]$ is prime in $S$. All ideals considered are left ideals.

**Theorem 11.** Let $F$ have characteristic not two. Then a necessary and sufficient condition that the principal ideal $(p)$ defined by a prime $p$ of $F[z]$ not dividing the fundamental number $d$ of $Q$ be divisorless in $S$ is that there exist no solution in $F[z]$ of the congruence

\[ 1 - x_1^2 - x_2^2 + x_3^2 \equiv 0 \pmod{p}. \]

If (8) holds, let

\[ \xi = 1 + x_1 i + x_2 j + x_3 k, \]

and let $P$ be the left ideal $(\xi, p)$; $P$ is a proper divisor of $(p)$. Also $P \neq (1)$. For otherwise $1 = \alpha \xi + \beta p$ with $\alpha, \beta$ in $S$, $\xi = \alpha (\xi \xi) + \beta \xi p \equiv 0 \pmod{(p)}$, an impossibility. Hence $(p)$ is not a divisorless ideal.

Conversely, suppose there is a left ideal $P \neq (1)$ which properly divides $(p)$; i.e., $P$ contains a quaternion $\xi$ not divisible by $p$. Necessarily $N(\xi)$ is divisible by $p$. If $p$ does not divide $\sigma \tau'$, by multiplying $\xi$ by $i, j, \text{ or } ij$ if necessary, we can obtain an element $\xi_0$ whose coefficient $x_0$ of 1 is not congruent to 0 \(\pmod{p}\). We can find a solution $m$ in $F[z]$ of $m \sigma \tau' x_0 = 1 + r p$. Then $\xi_0 m \sigma \tau' - rp = 1 + y_1 i + y_2 j + y_3 ij$ has norm congruent to 0 \(\pmod{p}\), and the $y_k$ are in $F[z]$. Hence congruence (8) has a solution.

If $p$ divides $\sigma \tau'$, then from the property of such a prime factor we know that (8) has a solution.

If the ideals of $S$ are all principal, then $kp = \pi_1 \pi_2$, where $k$ is in $F$ and

\[ \text{(16) } H. \text{ Rauter, Quaternionenalgebren mit Komponenten aus einem Körper von Primzahlcharakteristik, Mathematische Zeitschrift, vol. 29 (1929), pp. 234–263.} \]

\[ \text{(16) } C. \text{ G. Latimer, On ideals in generalised quaternion algebras and Hermitian forms, these Transactions, vol. 38 (1935), pp. 443–444.} \]
(π₁) = (ξ, p) with ξ defined in (9). Also π₁ is a divisorless quaternion of S because its norm is a prime in F[z].

It is known (17) that only the prime divisors of the fundamental number d are ramified in S.

**Theorem 12.** Every prime divisor p of the fundamental number of Q of characteristic not two generates an ideal in S which is the square of a two-sided prime ideal R.

A proof of this theorem can be made by following the steps in the demonstration of the analogous theorem for rational quaternion algebras by A. Spaltenstein (18). Let S_p denote the difference algebra S - (p) where p is in F[z]. If p is a prime dividing the fundamental number d of Q, then S_p contains a unique nonzero idempotent element. Using this fact we can prove that the radical R_p of S_p has exponent two and is the only maximal proper two-sided ideal in S_p. The ideal R in Theorem 12 is the set of quantities of S in the residue classes comprising R_p.

**Theorem (19)** 13. Let Q be over F(z), where F is a finite field. Then no prime of F[z] generates a prime ideal in S.

First, let F have characteristic not two. If a quantity p of F[z] generates a prime ideal in Q, it does not divide the discriminant of S, as a result of Theorem 12. Then S_p is semisimple. Also since (p) is prime in S, S_p contains no divisors of zero; hence S_p is a division algebra and because it is also finite, it is a field. Thus −ij = ji = i j (p); whence 2 ≡ 0 (p), an impossibility. If F has characteristic 2, we may take γ = z. Every quantity in F[z] has the form f(z²) + g(z²) · z = f(z)² + g(z)² · z and is therefore the norm of f(z) + g(z) · j. This completes the proof of our theorem.

By a result of Eichler (20), every ideal in S is principal when F is a finite field. This fact, together with Theorem 13, gives

**Theorem 14.** When F is finite, every polynomial in F[z], except for a factor in F, is the norm of a quaternion in S.

As a particular instance we have that every polynomial in F[z] is expressible in the form x₃² - fx₄ + (s - g)(x₄² - fx₃) where f is a non-square fixed quantity in F, g is fixed in F, and the x's take values in F[z].

Combining the results of Theorems 11 and 14 for F finite and of characteristic not two, we see that congruence (8) always has a solution if p does

---

not divide the fundamental number. It can be shown, however, that if \((p, \sigma) = 1\), there is a solution of

\[
x^2 - \sigma y^2 - r \equiv 0 \quad (p),
\]

a more inclusive fact.

For the remainder of this section we restrict \(F\) to be the field of all real numbers; hence we can take \(r = -1\). The primes in \(F[z]\) are either linear or definite quadratic.

If \(p\) is positive definite, \(p = z^2 + 2rz + s\), and the ideal generated by \((r^2 - s)^{1/2} + (z + r)i\) properly contains \((p)\); hence \((p)\) is not a divisorless ideal of \(S\).

If \(p\) is linear, \(p = z - a\), and if there is a solution of the congruence (8), then evaluating the left member at \(z = a\), we get the necessary condition that the polynomial \(\sigma = \sigma(z)\) must have a positive value for \(z = a\). Conversely, if \(\sigma(a) > 0\) and \(p = z - a\), a solution of (8) exists; e.g., \(x_1 = 0 = x_3, x_2 = (1/\sigma(a))^{1/2}\).

We have proved

**Theorem 15.** Let \(Q\) be a generalized quaternion algebra over the field \(F(z)\), where \(F\) is the field of all real numbers. A quantity \(p(z)\) of \(F[z]\) generates a divisorless ideal in the integral set \(S\) of \(Q\) with respect to a normalized basis if and only if \(p(z)\) is linear and the root of \(p(z) = 0\) gives \(\sigma\) a negative value.

As a result of Theorem 8 we know that \(S\) is a principal ideal ring if \(\sigma\) is linear. This and the fact that the product of two norms is a norm give

**Corollary.** If and only if all the monic linear factors of a square-free polynomial \(f\) in \(F[z]\) have their constant terms not less than \(c\), then

\[
f = \pm \left[ x_0^2 + x_1^2 - (x_2^2 + x_3^2)(z - c) \right] \quad (x_k \text{ in } F[z])
\]

If and only if all the constant terms are not greater than \(c\),

\[
f = \pm \left[ x_0^2 + x_1^2 + (x_2^2 + x_3^2)(z - c) \right] \quad (x_k \text{ in } F[z]).
\]

If \(\sigma = -1 = r\), then the left member of (8) is always positive for any value of \(z\). It is never divisible by a linear polynomial. Using this fact and the result that \(S\) is a principal ideal ring, we obtain

**Theorem 16.** Let \(F\) be the field of all real numbers, and \(\sigma = -1 = r\). Then every linear polynomial in \(F[z]\) is prime in \(S\), and every irreducible quadratic polynomial is, except for sign, the norm of a quaternion in \(S\).

When \(F\) is the rational number field, there are some positive definite polynomials\(^{(21)}\), e.g., \(z^2 + 7\), which are prime in \(S\) with \(i^2 = -1 = j^2\).

6. Equivalence of Hermitian forms and left ideals. Denote by $G$ the integral domain $F[z, i]$; if the basis of $Q$ is normalized, $G$ is the set of all integral elements in the quadratic extension $F(z, i)$ of the field $F(z)$. Let $W$ designate the set of all quaternions $\kappa = q_0 + q_1 i + q_2 j + q_3 k i j$ with components $q_k$ in $F[z]$; $W$ has a basis $1, j$ over $G$. Thus $\kappa = p_1 + p_2 j$ with $p_1, p_2$ in $G$ and

$$N(\kappa) = \begin{vmatrix} p_1 & p_2 \\ \eta p_2 & \eta p_1 \end{vmatrix},$$

where $\eta = \gamma$ or $\sigma$ according as $F$ has or has not characteristic two. The conjugate of a quantity $w$ of $G$ is written $\bar{w}$.

A left ideal $L$ of $W$ is called regular if it has a basis (called a regular basis) $\omega_1, \omega_2$ over $G$ where $\omega_m = g_{m1} + g_{m2} j$ ($m = 1, 2$) with the $g_{mn}$ in $G$ and the determinant $|g_{mn}|$ in $F[z]$ and monic. The value of the determinant $|g_{mn}|$ is independent of the basis $\omega_1, \omega_2$ and is the norm $N(L)$ of $L$. A left ideal $L$ is said to be equivalent to a left ideal $L'$ if there exist quantities $\rho, \rho'$ in $W$ for which $L \rho = L' \rho'$ and $N(\rho \rho')$ is monic.

A form

$$(10) \quad f(x_1, x_2) = ax_1 \bar{x}_1 + bx_1 \bar{x}_2 + bx_2 \bar{x}_1 + cx_2 \bar{x}_2$$

with $a, c$ in $F[z]$ and $b$ in $G$ is called a Hermitian form of $G$ and its determinant is defined to be $bb - ac$. We suppose that the $x$'s run over elements of $G$. If another Hermitian form $f' (y_1, y_2)$ can be obtained from $f(x_1, x_2)$ by a linear homogeneous transformation of determinant unity with coefficients in $G$, then $f$ and $f'$ are called equivalent.

Let $L$ be a regular ideal with the regular basis $\omega_m = g_{m1} + g_{m2} j$ ($m = 1, 2$). Since $j \omega_1, j \omega_2$ are in $L$,

$$(11) \quad j \omega_m = b_m \omega_1 + b_m j \omega_2 \quad (m = 1, 2),$$

where the $b$'s are in $G$. If we designate the general element of $L$ by $x$, then

$$\xi = x_1 \omega_1 + x_2 \omega_2 = (g_{11} x_1 + g_{21} x_2) + (g_{12} x_1 + g_{22} x_2) j,$$

$$j \xi = c_1 \omega_1 + c_2 \omega_2 = (g_{11} c_1 + g_{21} c_2) + (g_{12} c_1 + g_{22} c_2) j,$$

where $c_n = b_{1n} x_1 + b_{2n} x_2$ ($n = 1, 2$), and $x_1, x_2$ are in $G$. Then

$$N(\xi) = \begin{vmatrix} x_1 & x_2 \\ c_1 & c_2 \end{vmatrix} \cdot \begin{vmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{vmatrix} = N(L) \cdot f(x_1, x_2),$$

where

\[
f(x_1, x_2) = \begin{vmatrix} x_1 & x_2 \\ c_1 & c_2 \end{vmatrix} = b_{12}x_1\bar{x}_1 - b_{11}x_1x_2 + b_{22}x_1\bar{x}_2 - b_{21}x_2\bar{x}_2.
\]

Since \(N(\xi)\) and \(N(L)\) are in \(F[z]\), \(f(x_1, x_2)\) is in \(F(z)\) for \(x_1, x_2\) in \(G\). Since \(f\) is a polynomial in \(G\), it takes values in \(G\). Hence \(f(x_1, x_2)\) takes values in \(F[z]\) for \(x_1, x_2\) in \(G\), and \(f\) is consequently Hermitian. We say that \(f\) corresponds to the regular basis \(\omega_1, \omega_2\).

The relation between classes of ideals and of forms is described in

Theorem(23) 17. There is a one-to-one correspondence between the classes of regular ideals of \(W\) over \(G\) and the classes of Hermitian forms with determinant \(\eta\) representing a monic quantity in \(F[z]\).

We next prove

Lemma 2. An ideal \(L\) of \(W\) is principal if and only if it is regular and any Hermitian form \(f(x_1, x_2)\) corresponding to it represents a nonzero quantity in \(F\).

Let \(f(x_1, x_2)\) correspond to a regular ideal \(L = (\omega_1, \omega_2)\) and \(f(\tau_1, \tau_2) = a_0\) in \(F\). Then \(a_0 = b_{12}\tau_1\bar{\tau}_1 - b_{11}\tau_1\tau_2 + b_{22}\tau_1\bar{\tau}_2 - b_{21}\tau_2\bar{\tau}_1\), where the \(b_{mn}\) are defined by (11). If \(\rho = r_1\omega_1 + r_2\omega_2\), then \(N(\rho) = a_0N(L)\). The transformation

\[
\rho = r_1\omega_1 + r_2\omega_2,
\]

\[
\rho' = (r_1b_{11} + r_2b_{21})\omega_1/a_0 + (r_1b_{12} + r_2b_{22})\omega_2/a_0
\]

has determinant 1, so that \(\rho, \rho'\) is a regular basis of \(L\). But \(\rho' = j\rho/a_0\). Hence \(L = (\rho)\).

Conversely, if \(L = (\rho)\), \(L\) has the regular basis \((\rho, j\rho/r_0)\), where \(r_0\) is the leading coefficient of \(N(\rho)\). To this basis corresponds \(f(x_1, x_2) = r_0x_1\bar{x}_1 - (\rho/r_0)x_2\bar{x}_2\), which represents \(r_0 = f(1, 0)\) in \(F\).

Noticing that in the last paragraph \(r_0\) determines \(f\), we have the

Corollary. The number of classes of principal ideals is equal to the index of the group of all quantities of \(F\) which are leading coefficients of norms of unit quaternions in \(W\), in the group of all quantities of \(F\) which are leading coefficients of norms of quaternions in \(W\).

We also have the

Corollary. If \(W\) is a principal ideal ring, every ideal is regular.

We next state

Theorem 18. A necessary condition that every ideal in \(W\) be principal is that \(W\) be an integral set \(S\).

Let \( \zeta \) equal \( \beta \gamma \) or \( \sigma \tau \) according as \( F \) has or has not characteristic two, respectively. Suppose that every ideal in \( W \) is principal. Now \( S_\zeta \) is in \( W \), and, since \( W(S_\zeta) \leq S(S_\zeta) = S_\zeta \), we conclude that \( S_\zeta \) is an ideal in \( W \). Therefore \( S_\zeta = W\omega \), with \( \omega \) in \( W \). Since 1 is in both \( S \) and \( W \), we have \( \zeta = \mu \omega \) and \( \nu \zeta = \omega \) with \( \mu \) in \( W \) and \( \nu \) in \( S \). Then \( \nu \mu \omega = \omega \), so that \( \nu \mu = 1 \), and \( \nu, \mu \) are units in \( W \). Next, \( S_\zeta = W\omega = (W\mu)\omega = W\zeta \). Finally \( W = S \).

The conditions of Theorem 18 and the second corollary of Theorem 17 are by no means sufficient as results at the end of this section show.

Every Hermitian form \( f' \) of determinant \( \eta \) is equivalent to a form

\[
f = a_1x_1x_1 + b_1x_1x_2 + b_2x_1x_2 + cx_2x_2 \text{ with } D(b_0) < D(a), \quad D(b_1) < D(a) \leq D(c),
\]

where \( b = b_0 + b_1i \). This result is obtained by successive applications of the two transformations \( x_1 = x_1 + hx_2, \quad x_1' = x_2; \) and \( x_1' = x_2, \quad x_2' = -x_1 \).

We assume in the next two paragraphs that \( D(\alpha) \) and \( D(\beta) \) are not greater than 1, or \( D(\tau) \leq 1 \), according as \( F \) has or has not characteristic two. Then \( D(\alpha) + D(\zeta) = D(\eta) \).

If also \( D(\eta) \leq 1 \), then \( D(\alpha) = 0 \). We see that \( f \) represents a quantity in \( F \), and if \( f \) corresponds to \( L \), \( L \) is principal. Every regular ideal in \( W \) over \( G \) is principal.

But if \( D(\eta) = 2 \), then \( D(\alpha) \leq 1 \), and \( b_0 \) and \( b_1 \) are in \( F \). If \( D(\alpha) = 1 \), \( \eta \) is monic, and \( a_0, c_0 \) are the leading coefficients of \( a, c \), respectively, then \( a_0c_0 = -1 \). Hence \( f(1, a) \) is in \( F \) and consequently \( f \) corresponds to a class of principal ideals. This is also true of \( f \) if \( D(\alpha) = 0 \). We conclude that all regular ideals of \( W \) over \( G \) are principal when \( \eta \) is monic and quadratic.

Now let \( F \) be a field in which not every quantity is a square. Examples of such fields are subfields of real numbers. Also if \( F \) is finite of characteristic not two, then \( F \) contains non-square quantities. For, corresponding to each square \( a^2 \), there are two distinct elements \( a, -a \) in the field—the set of squares does not exhaust the field.

**Theorem 19.** Let \( F \) be a field of characteristic not two in which not every quantity is a square. Let \( \sigma \) in \( F[z] \) be of odd degree and reducible, and \( \tau \) in \( F[z] \) of even degree with leading coefficient not a square. Then the regular ideals of \( W \) are not all principal.

Let \( \sigma = \sigma_1\sigma_2 \), where \( \sigma_1, \sigma_2 \) are in \( F[z] \) and not in \( F \). Then the Hermitian form

\[
f = \sigma_1x_1x_1 - \sigma_2x_2x_2 = \sigma_1(y_0^2 - \tau y_1^2) - \sigma_2(y_2^2 - \tau y_3^2),
\]

where \( x_1 = y_0 + y_1i, \quad x_2 = y_2 + y_3i \), with the \( y \)'s in \( F[z] \), and has determinant \( \sigma \) and \( f \) does not represent a quantity in \( F \). For, \( y_0^2 - \tau y_1^2 \) and \( y_2^2 - \tau y_3^2 \) both have even degrees and one of \( \sigma_1, \sigma_2 \) has even degree and the other odd degree. Thus \( f(x_1, x_2) \) for \( (x_1, x_2) \neq (0, 0) \) has degree at least that of one of \( \sigma_1, \sigma_2 \).

**Theorem 20.** Let \( F \) be the field of all real numbers. The integral set \( S \) with
respect to the normalized basis of Theorem 3 is equal to $W$ and is a principal ideal ring if and only if $\sigma$ has degree not greater than 1, or degree 2 with positive leading coefficient.

The fact that $S$ is a principal ideal ring when $D(\sigma) \leq 1$ is a consequence of Theorem 8.

When $\sigma$ has odd degree greater than 1, Theorem 19 states that $W$ is not a principal ideal ring.

If $D(\sigma) = n \geq 4$ is even and $\sigma$ has leading coefficient $+1$, then

$$f = \sigma_1 \sigma_3 \cdots \sigma_{n-1} x_1 \tilde{x}_1 - \sigma_3 \sigma_4 \cdots \sigma_n x_2 \tilde{x}_2,$$

where the $\sigma_i = \sigma - a_i$ ($a_i < a_{i-1}$) are the linear factors of $\sigma$, cannot represent a nonzero quantity in $F$. For, if we set $z = a_1$, $f$ is always negative or zero; and for $z = a_3$, $f$ is always positive or zero.

If $n \geq 2$ is even and $\sigma$ has leading coefficient $-1$, and if $\sigma_1, \sigma_3$ are two non-constant factors of $\sigma = \sigma_1 \sigma_3$, then (13) cannot represent a quantity in $F$ because the two terms $\sigma_1 x_1 \tilde{x}_1$ and $-\sigma_3 x_2 \tilde{x}_2$ have leading coefficients of the same sign—there can be no reduction in degree by adding values of these two terms.

We have already shown that when the degree of $\sigma$ is 2 and $\sigma$ is monic that the regular ideals of $W$ are principal. It remains to prove that every ideal in $W$ is regular. We can find a basis $a, b+jc$ of an ideal $L$ with $a, b, c$ in $G$, since $G$ is a principal ideal ring. Since $ja$ and $j(b+jc)$ are in $L$, $a = a_1 c, b = b_1 c$. The ideal $L_1 = (a_1, b_1+j)$ is equivalent to $L$ because $L_1/c_0 = L$, where $c_0$ is the square root of the leading coefficient (which is necessarily positive) of $N(c)$.

We shall show that $a_1$ is in $F[z]$. Now $a_1(b_1+j) - ja_1 = a_3 b_1$ is in $L_1$; therefore $a_3 b_1 \equiv 0 (a_1)$. Let $a_1 = a'a''$ where $a'$ is the largest factor of $a_1$ in $F[z]$; i.e., the factors of $a''$ divide no linear polynomials in $F[z]$. Then $b_1 \equiv 0 (a'')$. Also in $L_1$ is $N(b_1+j) = b_1 b_1 - \sigma$; hence $b_1 b_1 - \sigma \equiv 0 (a_1), \sigma \equiv 0 (a'')$. But $\sigma$ is a product of linear factors in $F[z]$; hence $a''$ is in $F$ and $a_1$ is in $F[z]$. We can take the leading coefficient of $a_1$ to be unity. Then $L_1$ has the regular basis $a_1, b_1+j$ and $L_1$ is regular. Also $L$, being equivalent to $L_1$, is likewise regular.

Thus, using Theorem 20, we can always determine whether an integral set of a quaternion algebra $Q$ having as $F$ the field of all real numbers has ideals which are not principal.

University of Chicago,
Chicago, Ill.