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 characteristic 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 *normalized*(2); that is, σ, τ 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 τ 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 τ' be the product of all prime factors of τ for which σ is a quadratic residue, and $\tau''=\tau/\tau'$ be monic*(6). *Let σ' and σ'' be defined similarly. Then every integral set S of Q has a basis over $F[z]$ of the form $1, i, j, \omega$, where*

$$\omega = ai/\tau' + bj/\sigma' + ij/\sigma'\tau' \tag{1}$$

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 Publications, vol. 24, 1939, p. 145.

(2) A. A. Albert, *Integral domains of rational generalized quaternion algebras*, Bulletin of the American Mathematical Society, vol. 40 (1934), p. 166.

(3) For a summary of results on Hilbert irreducibility fields see A. A. Albert, *Involutorial simple algebras and real Riemann matrices*, Annals of Mathematics, (2), vol. 36 (1935), p. 890.

(4) L. E. Dickson, *Algebren und ihre Zahlentheorie*, 1927, p. 155.

(5) For analogous results for rational algebras see, in addition to the references already cited, C. G. Latimer, *Arithmetics of generalized quaternion algebras*, American Journal of Mathematics, vol. 48 (1926), pp. 57–66; M. D. Darkow, *Determination of a basis for the integral elements of certain generalized 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

$$\tau b^2 \equiv \tau''^2 \quad (\sigma'), \qquad \sigma a^2 \equiv \sigma''^2 \quad (\tau'). \tag{2}$$

For, by conditions U, C, and R, if ξ is in an integral set S, then the traces of ξ, $i\xi$, $j\xi$, and $ij\xi$ are in $F[z]$. Thus $\xi = x_0 + x_1 i/\tau + x_2 j/\sigma + x_3 ij/\sigma\tau$ with the x's all in $F[z]$. Now $N(\xi)$ is in $F[z]$ if and only if

$$x_1^2\sigma \equiv x_3^2 \quad (\tau), \qquad x_2^2\tau \equiv x_3^2 \quad (\sigma). \tag{3}$$

Since σ is not a quadratic residue of any factor of τ'' and τ is not a quadratic residue of any factor of σ'', we see from the congruences (3) that x_1 is divisible by τ'', x_2 by σ'', 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 ω 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 ρ be the corresponding linear combination of the same quaternions. Hence ρ is in S. Also $\rho = r_0 + r_1 i + r_2 j + r_3\omega'$, where the r's are in $F[z]$, $\omega' = a'i/\tau' + b'j/\sigma' + ij/\sigma'\tau'$, and a', b' satisfy (2). If η is also in the integral set S, $\eta = y_0 + y_1 i + y_2 j + y_3\omega$ and y_3 is divisible by r_3. Using the fact that $N(\rho+\eta)$ must be in $F[z]$, we find that η 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 σ' has m factors and τ' 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 $1, i_0, j_0, i_0 j_0$ is another normalized basis, $i_0^2 = \tau_0$, $j_0^2 = \sigma_0$, then

$$i_0 = (x_1 i + x_2 j + x_3 ij)/x_4, \qquad (x_1, x_2, x_3) = 1,$$
$$j_0 = (y_1 i + y_2 j + y_3 ij)/y_4, \qquad (y_1, y_2, y_3) = 1,$$

where the x's and y's are in $F[z]$.

([7]) H. Brandt, *Idealtheorie in Quaternionenalgebren*, Mathematische Annalen, vol. 99 (1928), pp. 1–29; C. G. Latimer, *On the fundamental number of a rational generalized quaternion algebra*, Duke Mathematical Journal, vol. 1 (1935), pp. 433–435.

([8]) M. Deuring, *Algebren*, 1935, p. 88.

Let d_1 be a prime divisor of $d=\sigma''\tau''$, the fundamental number corresponding to the basis 1, i, j, ij. We first assume that d_1 divides τ''. Then d_1 divides x_2y_2 because $i_0j_0+j_0i_0=0$. Now d_1 cannot divide both x_2 and x_4; if so, we would have on computing τ_0

$$x_1^2\tau - x_3^2\sigma\tau \equiv 0 \quad (d_1^2),$$

and thus

$$x_1^2 - x_3^2\sigma \equiv 0 \quad (d_1),$$

an impossibility for d_1 a divisor of τ''. Similarly d_1 does not divide both y_2 and y_4.

Suppose that d_1 divides x_2. Then d_1 does not divide x_4 and consequently d_1 divides τ_0. If d_1 did not divide τ_0'', we would have

$$\sigma_0 \equiv c^2 \quad (d_1)$$

and thus

$$y_1^2\tau + y_2^2\sigma - y_3^2\sigma\tau \equiv c^2y_4^2 \quad (d_1),$$

$$y_2^2\sigma \equiv c^2y_4^2 \quad (d_1). \tag{4}$$

Since $(\sigma_0, \tau_0)=1$, we have $(\sigma_0, d_1)=1$ and also $(c, d_1)=1$. Noticing also that $(\sigma, d_1)=1$, we see that congruence (4) implies that σ is a quadratic residue of d_1, a contradiction to the assumption that d_1 divides τ''. We have proved that d_1 divides τ_0'' and hence that it also divides $d_0=\sigma_0''\tau_0''$.

If d_1 divides y_2, similar reasoning would show that d_1 divides σ_0''.

A parallel proof is used in case we had assumed d_1 to be a divisor of σ'' to demonstrate that d_1 divides either σ_0'' or τ_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 σ by $(g^2-\tau h^2)\sigma$ with g, h in $F(z)$, 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 $F(z)$ has a basis 1, i, j, ij, with $i^2=-1$ and $j^2=\sigma$, where σ has leading coefficient ± 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 σ in $F[z]$ of leading coefficient ± 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 σ square-free and in $F[z]$. The leading coefficient may be taken as ± 1, since if σ has leading coefficient a then $\sigma/(|a|^{1/2})^2$ 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 $F[z]$;

$$r = (z+b)^2 + (\tfrac{1}{2}(-d_0)^{1/2})^2.$$

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

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

Let σ have leading coefficient ± 1 and contain only distinct linear factors. If the norm

$$x_0^2 + x_1^2 - \sigma(x_2^2 + x_3^2) \tag{5}$$

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 σ 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 σ. Dividing (5) by σ and using the same reasoning, we find that x_2 and x_3 are both divisible by σ. Continuing in this way, we find that x_0, x_1, x_2, x_3 are all divisible by every power of σ. This is possible only when σ 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 σ is monic; otherwise $-\sigma$ is monic. Hence the sign of σ is determined by the algebra.

We know then that σ 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

(10) C. C. Tsen, *Algebren über Funktionenkörpern*, Göttingen Dissertation, 1934.

(11) M. Deuring, *Algebren*, 1935, p. 46.

(12) A. A. Albert, *Structure of Algebras*, 1939, p. 145.

$=j(i+1)$, and α and γ are in $F(z)$. Choose $m_2 \neq 0$, m_0 in $F(z)$ so that $\gamma_0 = m_0^2 + \gamma m_2^2$ 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 $m_0 + m_2 j$ would be a divisor of zero. Evidently γ_0 is square-free. Whenever $\gamma_0' = m_0'^2 + \gamma_0 m_2'^2$, then $\gamma_0' = (m_0' + m_0 m_2')^2 + \gamma(m_2 m_2')^2$; hence γ_0 has minimal degree in the set of all quantities of $F[z]$ of the form $m_0'^2 + \gamma_0 m_2'^2$, where $m_2' \neq 0$. The transformation

$$i_1 = i + m_0 ij/\gamma m_2, \qquad j_1 = m_0 + m_2 j$$

replaces γ by γ_0.

Let β_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 $r_0 + r_1 i_1 + r_2 j_1 + r_3 i_1 j_1$. Necessarily $r_3 = 0$. Let b' be the leading coefficient of β_0. The transformation

$$i_0 = (r_0 + r_1 i_1 + r_2 j_1)/b', \qquad j_0 = j_1$$

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 $i^2 = \beta i + \alpha$, $j^2 = \gamma$, $ij = j(i+\beta)$; α, β, γ are in $F[z]$; β is monic and has least degree among all nonzero β_0 in $F[z]$ for which the equation $xj = j(x+\beta_0)$ has an integral quaternion x as solution; and γ is a square-free polynomial and has the least degree for all polynomials of the form $m_0^2 + m_2^2\gamma$ having m_0, m_2 in $F(z)$ and $m_0 \neq 0$.*

A basis of the type given in Theorem 4 will be called a *normalized* 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, γ cannot be in F for then $\gamma^{1/2} + j$ would be a divisor of zero. Hence γ has degree $\geqq 1$. Since γ is in $F[z]$ and F is perfect, $\gamma = c_1^2 + c_2^2 z$ 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 β monic, square-free, and prime to z.*

A value of β, because of the minimal degree property, is necessarily square-free. For, if $\beta = \beta_1 p^2$, then $i' = (m_0 + i + m_2 j)/p$ is integral if m_0 and m_2 are chosen in $F[z]$ to satisfy $m_0^2 + m_2^2 z = \alpha$. Furthermore $i'j = j(i' + \beta/p)$, and β/p has degree less than that of β. These properties of i' contradict the assumptions made about β.

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

([13]) A. A. Albert, *p-algebras over a field generated by one indeterminate*, Bulletin of the American Mathematical Society, vol. 43 (1937), p. 735.

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*

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

Furthermore m is square-free.

Let ξ 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 $\xi=[x_0+x_1i+(x_2+x_3i)j/\gamma]/\beta$ 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

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

with the e_0, f's, g's, and h's in $F[z]$. We may assume, since $1, i, j, ij$ are all in S, that 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's, and h's have degrees less than $D(\beta\gamma)$ (the degree of a polynomial a is designated by $D(a)$).

Obviously, ω_1 is not integral unless $e_0=\beta\gamma$; $\omega_1=1$.

If $D(f_1)<D(\beta\gamma)$, then $D(T(\omega_2))<D(\beta)$ while $\omega_2j=j(\omega_2+T(\omega_2))$. This contradicts the choice of β; hence $D(f_1)=D(\beta\gamma)$ and in fact $f_1=\beta\gamma$. Since ω_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 $\omega_3j=j(\omega_3+T(\omega_3))$, a contradiction to the choice of β unless $g_1=0$. If $D(g_2)<D(\beta\gamma)$, then ω_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 γ, a contradiction to the choice of γ. Thus $g_2=\beta\gamma$, and since ω_3-j is in S, $g_0=0$, 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 $\omega_4=(d_0+d_1i+d_2j+ij)/m'$ with the d's in $F[z]$. In S must be $i\omega_4$ and ω_4j. This is possible if and only if

$$d_1^2 \equiv \gamma, \qquad d_2^2 \equiv d_2\beta + \alpha, \qquad d_0 \equiv d_1d_2 \quad (m'). \tag{6}$$

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 γ, then because $d_1^2\equiv\gamma$ (p^2), p would divide d_1 and p^2 divide the square-free γ. Hence p would not divide γ, so that p^2 would be a divisor of β. But then $i_1=(d_2+i)/p$ would be integral, $i_1j=j(i_1+\beta/p)$, and β/p have smaller degree than β. This is impossible from our choice of β.

Our next step is to give a construction of ω_4. Let m be the product of all prime powers $p_n^{e_n}$ dividing $\beta\gamma$ for which there exist solutions of

$$x_{1n}^2 \equiv \gamma, \qquad x_{2n}^2 \equiv x_{2n}\beta + \alpha \quad (p_n^{e_n}). \tag{7}$$

By means of a discussion similar to that for m' we can show that m is also square-free, i.e., $e_n = 1$. 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

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

The quantity $\omega = (x_1x_2 + x_1i + x_2j + ij)/m$ is integral. Its trace is $\beta x_1/m$. This is in $F[z]$ since any factor of m dividing γ divides x_1 because of (7) and the remaining factors of m divide β. Furthermore

$$\begin{aligned} m^2 N(\omega) &= x_1^2x_2^2 + x_1^2x_2\beta + x_1^2\alpha + \gamma(x_2^2 + x_2\beta + \alpha) \\ &= (x_1^2 + \gamma)(x_2^2 + x_2\beta + \alpha) \equiv 0 \quad (m^2); \end{aligned}$$

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

The quantity ω 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 ω_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 ω_4 is in $(1, i, j, \omega m'')$ which is in S. We have proved our theorem.

Another form for the basis of Q of characteristic two[14] is $1, u_1, u_2, u_1u_2$, where

$$u_1^2 = \tau, \qquad u_2^2 = \sigma, \qquad u_1u_2 + u_2u_1 = \rho \qquad (\rho, \sigma, \tau \text{ in } F(z)).$$

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 ρ, σ, τ 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 ρ 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 $1, u_1, u_2, u_1u_2$ normalized as above has a basis $1, u_1, u_2, \omega$, where*

$$\omega = (y_1 + y_1u_1 + y_2u_2 + y_3u_1u_2)/\rho.$$

---

[14] N. Jacobson, *p-algebras of exponent p*, Bulletin of the American Mathematical Society, vol. 43 (1937), pp. 667–670.

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

$$y_0^2 + y_1^2\tau + y_2^2\sigma + y_3^2\sigma\tau + \rho(y_0y_3 + y_1y_2) \equiv 0 \quad (\rho^2)$$

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 σ, τ 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 θ is in an integral set S of Q, and m is a nonzero polynomial in $F[z]$, there exists a quaternion κ 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 σ and τ are both in F, $S=(1, i, j, ij)$.

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

Suppose that both σ and τ 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 $\sigma \equiv a^2\ (\tau)$, with a in F. Hence $S=(1, i, j, \omega)$, where ω is one of $i(a \pm j)/\tau$. The case $(\tau|\sigma) = -(\sigma|\tau) = 1$ is handled similarly. Finally if $(\sigma|\tau) = (\tau|\sigma) = 1$, then $\sigma \equiv a^2\ (\tau)$, $\tau \equiv b^2\ (\sigma)$, with a and b in F. Thus $\sigma = a^2 + k\tau$, $b^2 = -a^2/k$, and $i/a\tau + j/b\sigma + ij/\sigma\tau$ 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 γ linear and α and β in F. If θ is in the integral set $S=(1, i, j, ij)$ of Q, and m is in $F[z]$, then there exists a quaternion κ 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 κ 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 β is in F, then we can assume $\beta = 1$. We can also have α in F. For, since F is perfect, α has the form $a_1^2 + a_2^2z$. The degree of α is reduced to zero by repeated application of the transformation

$$i' = a_1 + i + a_2j, \qquad j' = j.$$

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([15]). 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 θ be a quaternion in S not divisible by a polynomial in $F[z]$. If $N(\theta)=p_1p_2\cdots p_n$, where the p_k are irreducible polynomials, then $\theta=\pi_1\pi_2\cdots\pi_n$ where $N(\pi_k)=p_k$ and π_1 is unique except for multiplication by units of S on the right, $\pi_2, \cdots, \pi_{n-1}$ are unique but for multiplication by units on the right or left, and π_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*

$$1 - x_1^2\tau - x_2^2\sigma + x_3^2\sigma\tau \equiv 0 \quad (p). \tag{8}$$

If (8) holds, let

$$\xi = 1 + x_1 i + x_2 j + x_3 ij, \tag{9}$$

and let P be the left ideal (ξ, p); P is a proper divisor of (p). Also $P\neq(1)$. For otherwise $1=\alpha\xi+\beta p$ with α, β in S, $\bar{\xi}=\alpha(\xi\bar{\xi})+\beta\bar{\xi}p\equiv 0\ (p)$, 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 ξ not divisible by p. Necessarily $N(\xi)$ is divisible by p. If p does not divide $\sigma'\tau'$, by multiplying ξ by i, j, or ij if necessary, we can obtain an element ξ_0 whose coefficient x_0 of 1 is not congruent to 0 (p). We can find a solution m in $F[z]$ of $m\sigma'\tau'x_0\equiv 1\ (p)$, $m\sigma'\tau'x_0=1+rp$. Then $\xi_0 m\sigma'\tau'-rp=1+y_1i+y_2j+y_3ij$ has norm congruent to 0 (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 $kp=\pi_1\bar{\pi}_1$, where k is in F and

([15]) H. Rauter, *Quaternionenalgebren mit Komponenten aus einem Körper von Primzahlcharakteristik*, Mathematische Zeitschrift, vol. 29 (1929), pp. 234–263.

([16]) C. G. Latimer, *On ideals in generalized quaternion algebras and Hermitian forms*, these Transactions, vol. 38 (1935), pp. 443–444.

$(\pi_1)=(\xi, p)$ with ξ defined in (9). Also π_1 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 $-ij=ji\equiv ij\ (p)$; whence $2\equiv 0\ (p)$, an impossibility. If F has characteristic 2, we may take $\gamma=z$. Every quantity in $F[z]$ has the form $f(z^2)+g(z^2)\cdot z=f(z)^2+g(z)^2\cdot z$ and is therefore the norm of $f(z)+g(z)\cdot j$. 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 $x_0^2-fx_1^2\pm(z-g)(x_2^2-fx_3^2)$ 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

([17]) M. Deuring, *Algebren*, 1935, p. 84.

([18]) A. Spaltenstein, *Struktur und Zahlentheorie einer Klasse von Algebren*, Zurich Dissertation, 1934, p. 24.

([19]) For the rational analogue see A. Speiser, "Idealtheorie in rationalen Algebren," in L. E. Dickson, *Algebren und ihre Zahlentheorie*, 1927, p. 302.

([20]) M. Eichler, *Über die Idealklassenzahl hyperkomplexer Systeme*, Mathematische Zeitschrift, vol. 43 (1938), pp. 481–494.

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

$$x^2 - \sigma y^2 - \tau \equiv 0 \quad (p),$$

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 $\tau=-1$. 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 σ a negative value.*

As a result of Theorem 8 we know that S is a principal ideal ring if σ 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*

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

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

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

If $\sigma=-1=\tau$, 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 $\sigma=-1=\tau$. 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 $i^2=-1=j^2$.

([21]) E. Landau, *Über die Zerlegung definiter Funktionen in Quadrate*, Archiv der Mathematik und Physik, (3), vol. 7 (1904), pp. 271–277.

6. **Equivalence of Hermitian forms and left ideals**([22]). 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 $\kappa = q_0 + q_1 i + q_2 j + q_3 ij$ 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

$$N(\kappa) = \begin{vmatrix} p_1 & p_2 \\ \eta \bar{p}_2 & \bar{p}_1 \end{vmatrix},$$

where $\eta = \gamma$ or σ 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) ω_1, ω_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 ω_1, ω_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 ρ, ρ' in W for which $L\rho = L\rho'$ and $N(\rho\rho')$ is monic.

A form

$$f(x_1, x_2) = a x_1 \bar{x}_1 + b \bar{x}_1 x_2 + \bar{b} x_1 \bar{x}_2 + c x_2 \bar{x}_2 \tag{10}$$

with a, c in $F[z]$ and b in G is called a Hermitian form of G and its determinant is defined to be $b\bar{b} - ac$. 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,

$$j\omega_m = b_{m1}\omega_1 + b_{m2}\omega_2 \qquad (m = 1, 2), \tag{11}$$

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

$$\xi = x_1\omega_1 + x_2\omega_2 = (g_{11}x_1 + g_{21}x_2) + (g_{12}x_1 + g_{22}x_2)j,$$
$$j\xi = c_1\omega_1 + c_2\omega_2 = (g_{11}c_1 + g_{21}c_2) + (g_{12}c_1 + g_{22}c_2)j,$$

where $c_n = b_{1n}\bar{x}_1 + b_{2n}\bar{x}_2$ $(n = 1, 2)$, and x_1, x_2 are in G. Then

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

([22]) For the rational analogue see C. G. Latimer, *On ideals in generalized quaternion algebras and Hermitian forms*, these Transactions, vol. 38 (1935), pp. 436–446; C. G. Latimer, *On ideals in a quaternion algebra and the representation of integers by Hermitian forms*, these Transactions, vol. 40 (1936), pp. 439–449; C. G. Latimer, *On the class number of a quaternion algebra with a negative fundamental number*, these Transactions, vol. 40 (1936), pp. 318–323; J. D. H. Teller, *A class of quaternion algebras*, Duke Mathematical Journal, vol. 2 (1936), pp. 280–286.

where

$$(12) \qquad f(x_1, x_2) = \begin{vmatrix} x_1 & x_2 \\ c_1 & c_2 \end{vmatrix} = b_{12}x_1\bar{x}_1 - b_{11}\bar{x}_1x_2 + b_{22}x_1\bar{x}_2 - b_{21}x_2\bar{x}_2.$$

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 ω_1, ω_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 η 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 $f(r_1, r_2) = a_0$ in F. Then $a_0 = b_{12}r_1\bar{r}_1 - b_{11}\bar{r}_1r_2 + b_{22}r_1\bar{r}_2 - b_{21}r_2\bar{r}_2$, 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

$$\rho = r_1\omega_1 + r_2\omega_2,$$
$$\rho' = (\bar{r}_1b_{11} + \bar{r}_2b_{21})\omega_1/a_0 + (\bar{r}_1b_{12} + \bar{r}_2b_{22})\omega_2/a_0$$

has determinant 1, so that ρ, ρ' 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.*

([23]) C. G. Latimer, *On ideals in generalized quaternion algebras and Hermitian forms*, these Transactions, vol. 38 (1935), p. 442.

Let ζ 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 $W(S\zeta) \leqq S(S\zeta) = S\zeta$, we conclude that $S\zeta$ is an ideal in W. Therefore $S\zeta = W\omega$, with ω in W. Since 1 is in both S and W, we have $\zeta = \mu\omega$ and $\nu\zeta = \omega$ with μ in W and ν in S. Then $\nu\mu\omega = \omega$, so that $\nu\mu = 1$, and ν, μ 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 η is equivalent to a form $f = ax_1\bar{x}_1 + b\bar{x}_1x_2 + \bar{b}x_1\bar{x}_2 + cx_2\bar{x}_2$ with $D(b_0) < D(a)$, $D(b_1) < D(a) \leqq D(c)$, where $b = b_0 + b_1 i$. This result is obtained by successive applications of the two transformations $x_1' = x_1 + hx_2$, $x_2' = x_2$; and $x_1' = x_2$, $x_2' = -x_1$.

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

If also $D(\eta) \leqq 1$, then $D(a) = 0$. 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 $D(a) \leqq 1$, and b_0 and b_1 are in F. If $D(a) = 1$, η is monic, and a_0, c_0 are the leading coefficients of a, c, respectively, then $a_0c_0 = -1$. Hence $f(1, a_0)$ is in F and consequently f corresponds to a class of principal ideals. This is also true of f if $D(a) = 0$. We conclude that all regular ideals of W over G are principal when η 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 σ in $F[z]$ be of odd degree and reducible, and τ 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 σ_1, σ_2 are in $F[z]$ and not in F. Then the Hermitian form

$$f = \sigma_1 x_1\bar{x}_1 - \sigma_2 x_2\bar{x}_2 = \sigma_1(y_0^2 - \tau y_1^2) - \sigma_2(y_2^2 - \tau y_3^2), \tag{13}$$

where $x_1 = y_0 + y_1 i$, $x_2 = y_2 + y_3 i$, with the y's in $F[z]$, and has determinant σ 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 σ_1, σ_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 σ_1, σ_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 σ has degree not greater than 1, or degree 2 with positive leading coefficient.

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

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

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

$$f = \sigma_1\sigma_3 \cdots \sigma_{n-1}x_1\bar{x}_1 - \sigma_2\sigma_4 \cdots \sigma_n x_2\bar{x}_2,$$

where the $\sigma_i = z - a_i$ $(a_i < a_{i-1})$ are the linear factors of σ, 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 $n \geqq 2$ is even and σ has leading coefficient -1, and if σ_1, σ_2 are two non-constant factors of $\sigma = \sigma_1\sigma_2$, then (13) cannot represent a quantity in F because the two terms $\sigma_1 x_1\bar{x}_1$ and $-\sigma_2 x_2\bar{x}_2$ 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 σ is 2 and σ 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, $a = a_1c$, $b = b_1c$. The ideal $L_1 = (a_1,\ b_1+j)$ is equivalent to L because $L_1c/c_0 = L$, 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 $\bar{a}_1(b_1+j) - ja_1 = \bar{a}_1b_1$ is in L_1; therefore $\bar{a}_1b_1 \equiv 0\ (a_1)$. 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 $N(b_1+j) = b_1\bar{b}_1 - \sigma$; hence $b_1\bar{b}_1 - \sigma \equiv 0\ (a_1)$, $\sigma \equiv 0\ (a'')$. But σ 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.