ON IDEALS IN GENERALIZED QUATERNION ALGEBRAS AND HERMITIAN FORMS*

BY

CLAIBORNE G. LATIMER

1. Introduction. Let $\mathfrak{A}$ be a generalized quaternion algebra. The elements of $\mathfrak{A}$ may be written $X=x+Ey$, where x, y are numbers in a quadratic algebraic field F, $E^2=\alpha$, a rational integer, and $Ey=y'E$, y' being the conjugate of y with respect to F. The conjugate of X is $X'=x'-Ey$ and the norm of X is $N(X)=X'X=xx'-\alpha yy'$. It is well known that if X, Y are in $\mathfrak{A}$, $N(XY)=N(X)N(Y)$ and $(XY)'=Y'X'$. We shall assume that $\alpha\neq 0$.

Let $\mathfrak{G}$ be the ring consisting of all elements of $\mathfrak{A}$ in the form $x+Ey$, where x, y are in the set, G, of all integral algebraic numbers in F. We shall show that there is a one-to-one correspondence between certain classes of left ideals in $\mathfrak{G}$, which we call regular classes, and those classes of binary Hermitian forms in G, of determinant α, which represent positive integers. It will be shown that every ideal in a regular class contains two elements which form a basis with respect to G. The correspondence is then proved by a method which is similar to a method, due to Dickson,† of proving the well known correspondence between the classes of ideals in a quadratic algebraic field and certain classes of binary quadratic forms.

We also prove a theorem on the existence of a g.c.d. and the factorization of elements in $\mathfrak{G}$ under the assumption that all the ideals in a regular class are principal. Applications are made to a number of special quaternion algebras. Some of the results thus obtained have been previously proved by other methods, some are new. In particular, we obtain for an infinitude of algebras the same results on the existence of a g.c.d. and on factorization as were obtained by Dickson for the Lipschitz integral quaternions.

2. Ideals in $\mathfrak{G}$ and component ideals in G. An element in $\mathfrak{G}$ is said to be singular or non-singular according as its norm is or is not zero. An ideal $\mathfrak{L}$ in $\mathfrak{G}$ is defined as a set of elements in $\mathfrak{G}$, not all singular, such that if ξ_1, ξ_2 are in $\mathfrak{G}$ and η_1, η_2 are in $\mathfrak{L}$, then $\xi_1\eta_1+\xi_2\eta_2$ is in $\mathfrak{L}$.‡ If η is a non-singular element in $\mathfrak{L}$, $\eta'\eta=N(\eta)$ is in $\mathfrak{L}$. Hence $\mathfrak{L}$ contains elements in G, not zero. Those elements of $\mathfrak{L}$ which are in G form an ideal in G which we shall call the first

* Presented to the Society, April 19, 1935; received by the editors February 12, 1935.

† This was given in lectures at the University of Chicago in the spring of 1921.

‡ According to MacDuffee's definition, $\mathfrak{L}$ is a non-singular left ideal. See his *An introduction to the theory of ideals* etc., these Transactions, vol. 31 (1929), pp. 71–90. Since we shall not consider any other kind of ideal, we employ the briefer terminology.

component of $\mathfrak{L}$. If $X=x+Ey$ ranges over all the elements of $\mathfrak{L}$, y ranges over all the elements of an ideal in G which we shall call the second component of $\mathfrak{L}$. If an ideal $\mathfrak{p}$ in G has a basis ζ_1, ζ_2, we shall write $\mathfrak{p}=[\zeta_1, \zeta_2]$. A principal ideal in G defined by ρ will be written $\{\rho\}$. We shall now prove

LEMMA 1. *Let* $\mathfrak{a}=[\omega_1, \omega_2]$, $\mathfrak{b}=[\lambda_1, \lambda_2]$ *be the first and second components respectively of an ideal* $\mathfrak{L}$ *in* $\mathfrak{G}$. *Then* $\omega_1, \omega_2, \omega_3=b_1+E\lambda_1, \omega_4=b_2+E\lambda_2$ *form a basis of* $\mathfrak{L}$, *where* b_1, b_2 *are properly chosen numbers in* $\mathfrak{b}$.

By the definition of $\mathfrak{b}$, $\mathfrak{L}$ contains elements $\omega_3\equiv b_1+E\lambda_1$, $\omega_4\equiv b_2+E\lambda_2$, where the b's are in G. Then every element of $\mathfrak{L}$ may be written in the form $X=t+x_3\omega_3+x_4\omega_4$, where the x's are rational integers and t is in G. But $t=X-x_3\omega_3-x_4\omega_4$ is in $\mathfrak{L}$. Hence t is in $\mathfrak{a}$ and $t=x_1\omega_1+x_2\omega_2$, where the x's are rational integers. Since $E\omega_3=\alpha\lambda_1+Eb_1$, $E\omega_4=\alpha\lambda_2+Eb_2$, the b's belong to $\mathfrak{b}$. This proves the lemma.

We shall write $\mathfrak{L}=[\zeta_1, \zeta_2, \zeta_3, \zeta_4]$ if the ζ's form a basis of $\mathfrak{L}$. If ξ is a non-singular element of $\mathfrak{G}$, the product $\mathfrak{L}\xi$ is defined as the set of all elements $\eta\xi$, where η ranges over all the elements of $\mathfrak{L}$. Then $\mathfrak{L}\xi=[\zeta_1\xi, \zeta_2\xi, \zeta_3\xi, \zeta_4\xi]$. We shall now prove

LEMMA 2. *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be the first and second components respectively of an ideal* $\mathfrak{L}$ *in* $\mathfrak{G}$ *and let* Δ *be the discriminant of* G. *Then* $\mathfrak{a}=a\mathfrak{b}\mathfrak{d}$, *where* a *is a positive rational integer and* $\mathfrak{d}$ *is an ideal, without a rational prime factor, which is either the unit ideal or a product of prime ideal divisors of* $\alpha\Delta$.

If u is in $\mathfrak{a}$, Eu is in $\mathfrak{L}$ and hence u is in $\mathfrak{b}$. Therefore $\mathfrak{b}$ contains $\mathfrak{a}$ and $\mathfrak{a}=a\mathfrak{b}\mathfrak{d}$ where a is a positive rational integer and $\mathfrak{d}$ contains no rational prime factor. It remains to show that every prime ideal divisor of $\mathfrak{d}$ divides $\alpha\Delta$.

$\mathfrak{b}$ is narrowly equivalent to an ideal $\mathfrak{b}_1$ which is prime to $\mathfrak{d}\mathfrak{d}'$, where $\mathfrak{d}'$ is the conjugate of $\mathfrak{d}$.* Then $\mathfrak{b}t=\mathfrak{b}_1t_1$ where t, t_1 are in G and $N(t)N(t_1)>0$. By Lemma 1, $\mathfrak{L}=[a\omega_1, a\omega_2, b_1+E\lambda_1, b_2+E\lambda_2]$, where $\mathfrak{b}\mathfrak{d}=[\omega_1, \omega_2]$, $\mathfrak{b}=[\lambda_1, \lambda_2]$, and the b's are in $\mathfrak{b}$. It may then be shown that $\mathfrak{L}t=\mathfrak{L}_1t_1$, where the first and second components of $\mathfrak{L}_1$ are $a\mathfrak{b}_1\mathfrak{d}$ and $\mathfrak{b}_1$ respectively. Therefore we may assume, without loss of generality, that $\mathfrak{b}$ is prime to $\mathfrak{d}\mathfrak{d}'$.

The rational integers $(b_i'-E\lambda_i)(b_i+E\lambda_i)=b_ib_i'-\alpha\lambda_i\lambda_i'$ $(i=1, 2)$ are in $\mathfrak{L}$ and therefore

$$b_ib_i'-\alpha\lambda_i\lambda_i'\equiv 0 \pmod{\mathfrak{a}=a\mathfrak{b}\mathfrak{d}\mathfrak{d}} \qquad (i=1, 2). \tag{1}$$

Let $\mathfrak{d}=[\mu_1, \mu_2]$. Then each $a\lambda_i\mu_j (i, j=1, 2)$ belongs to $\mathfrak{a}$ and hence each of

$$a\mu_j'(b_i+E\lambda_i)-Ea\lambda_i\mu_j=a\mu_j'b_i \qquad (i, j=1, 2)$$

is in $\mathfrak{L}$. Therefore

* Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, p. 373.

$$b_i\mathfrak{b}' \equiv 0 \pmod{\mathfrak{b}} \qquad (i = 1, 2). \tag{2}$$

Let $\mathfrak{b}_1$ be a prime ideal divisor of $\mathfrak{b}$ which is prime to Δ. Since $\mathfrak{b}$ is prime to $\mathfrak{b}\mathfrak{b}'$, we may assume that the λ_i are prime to $\mathfrak{b}_1\mathfrak{b}_1'$. Since $\mathfrak{b}'$ contains no rational prime factor, and $\mathfrak{b}_1$ is prime to Δ, $\mathfrak{b}_1$ is prime to $\mathfrak{b}'$. Then by (2) each $b_i \equiv 0 \pmod{\mathfrak{b}_1}$ and by (1), each $\alpha\lambda_i\lambda_i' \equiv 0 \pmod{\mathfrak{b}_1}$. But the λ_i are prime to $\mathfrak{b}_1\mathfrak{b}_1'$ and hence the same is true of the λ_i'. Therefore $\alpha \equiv 0 \pmod{\mathfrak{b}_1}$ and the lemma is proved.

3. **Classes of ideals in $\mathfrak{G}$; reduced ideals.** Two ideals $\mathfrak{L}$ and $\mathfrak{L}_1$ will be said to be equivalent if there are elements ξ, ξ_1 in $\mathfrak{G}$ such that $\mathfrak{L}\xi = \mathfrak{L}_1\xi_1$ and $N(\xi)N(\xi_1) > 0$. After multiplying both sides of the last equation on the right by ξ', we may assume that ξ is a rational integer and $N(\xi_1) > 0$. It may then be shown that equivalence is transitive. All the ideals equivalent to a given ideal are said to form a class. An ideal in $\mathfrak{G}$ will be called a reduced ideal if its second component is the unit ideal.

LEMMA 3. *Let $\mathfrak{L}$ be an ideal in $\mathfrak{G}$ whose first component is $a\mathfrak{b}\mathfrak{b}$ as in Lemma 2. Then $\mathfrak{L}$ is equivalent to a reduced ideal whose first component is $a_1\mathfrak{b}$, where a_1 is a rational integer.*

Since equivalence is a transitive property, by our proof of Lemma 2, we may assume that the second component $\mathfrak{b}$ of $\mathfrak{L}$ contains no rational prime factor and is prime to $a\alpha\Delta$. By Lemma 1, $\mathfrak{L} = [a\omega_1, a\omega_2, b_1 + E\lambda_1, b_2 + E\lambda_2]$, where $\mathfrak{b}\mathfrak{b} = [\omega_1, \omega_2]$, $\mathfrak{b} = [\lambda_1, \lambda_2]$ and the b's are in $\mathfrak{b}$. Since $\mathfrak{b}$ contains no rational prime factor, we may assume that $\lambda_1 = N(\mathfrak{b}) \equiv B$, where $N(\mathfrak{b})$ is the norm of $\mathfrak{b}$. Then B is prime to $a\alpha\Delta$ and there is a number k in G such that

$$Bk + b_1' \equiv 1 \pmod{a\alpha\Delta}. \tag{3}$$

We shall assume without loss of generality that k is prime to B and that $N(\rho \equiv k + E) = kk' - \alpha > 0$. Then $\mathfrak{L}$ is equivalent to $\mathfrak{L}_1 \equiv \mathfrak{L}\rho$. $\mathfrak{L}_1$ contains

$$\begin{aligned} a\omega_1\rho &= a\omega_1 k + E(a\omega_1'), \\ a\omega_2\rho &= a\omega_2 k + E(a\omega_2'), \\ (b_1 + EB)\rho &= b_1 k + \alpha B + E(Bk + b_1'), \\ (b_2 + E\lambda_2)\rho &= b_2 k + \alpha\lambda_2' + E(\lambda_2 k + b_2'). \end{aligned} \tag{4}$$

Suppose the second component of $\mathfrak{L}_1$ has a prime ideal divisor $\mathfrak{p}$. Since $\mathfrak{b}'\mathfrak{b}' = [\omega_1', \omega_2']$, by (4_1) and (4_2), $\mathfrak{p}$ divides $a\mathfrak{b}'\mathfrak{b}'$. By (4_3) $\mathfrak{p}$ divides $Bk + b_1'$. If $\mathfrak{p}$ divided $a\mathfrak{b}'$, it would divide $a\alpha\Delta$ and then by (3) it would divide 1. Hence $\mathfrak{p}$ is prime to $a\mathfrak{b}'$ and divides $\mathfrak{b}'$. By Lemma 1, $\mathfrak{b}'$ divides b_1', b_2'. Then by (4_3) and (4_4), $\mathfrak{p}$ divides $\mathfrak{b}k = [Bk, \lambda_2 k]$. But k is prime to $\{B\} = \mathfrak{b}\mathfrak{b}'$ and hence k is prime to $\mathfrak{p}$. Therefore $\mathfrak{p}$ divides $\mathfrak{b}$. But we have seen that $\mathfrak{p}$ divides $\mathfrak{b}'$, which is prime to Δ. Hence $\mathfrak{b}$ is divisible by $\mathfrak{p}\mathfrak{p}'$, contrary to our

hypothesis that $\mathfrak{b}$ has no rational prime factor. Therefore the second component of $\mathfrak{L}_1$ has no prime ideal divisor and $\mathfrak{L}_1$ is a reduced ideal.

Consider the first component $\mathfrak{a}_1$, of $\mathfrak{L}_1$. Every element of $\mathfrak{L}_1$ may be written in the form $(u+Ev)\rho = ku+\alpha v'+E(u'+kv)$, where $u+Ev$ is in $\mathfrak{L}$. Hence if $X=u+Ev$ is in $\mathfrak{L}$, $X\rho$ is in $\mathfrak{a}_1$ if and only if $u' = -kv$. Then $X = -v'(k'-E)$ $= -v'\rho'$ and the corresponding element in $\mathfrak{a}_1$ is $-v'\rho'\rho = -v'N(\rho)$. Let $\mathfrak{q}$ be the set of all elements v of G such that $-k'v'+Ev = -v'\rho'$ is in $\mathfrak{L}$. $\mathfrak{q}$ is an ideal in G and $\mathfrak{a}_1 = \mathfrak{q}'N(\rho)$. Let $\mathfrak{d} = [\zeta_1, \zeta_2]$. Then $a\zeta_i(Bk'+b_1)$ is in $ab\mathfrak{d}$ and therefore $-aB\zeta_i\rho' = a\zeta_i(b_1+EB) - a\zeta_i(Bk'+b_1)$ is in $\mathfrak{L}$ $(i=1, 2)$. It follows from the definition of $\mathfrak{q}$ that each $aB\zeta_i'$ is in $\mathfrak{q}$. Hence $\mathfrak{q}$ divides $aB\mathfrak{d}'$ and $\mathfrak{a}_1$ $= \mathfrak{q}'N(\rho)$ divides $aBN(\rho)\mathfrak{d}$.

By Lemma 1, the norm, $n(\mathfrak{R})$, of an ideal $\mathfrak{R}$, according to MacDuffee's definition, is the product of the norms of its components.* Then

$$n(\mathfrak{L}) = N(ab\mathfrak{d})N(\mathfrak{b}) = a^2B^2N(\mathfrak{d}).$$

It will be found that the determinant of the second matrix of an element ξ in $\mathfrak{G}$ is $N^2(\xi)$. Then $n(\mathfrak{L}_1) = n(\mathfrak{L}\rho) = n(\mathfrak{L})N^2(\rho) = a^2B^2N^2(\rho)N(\mathfrak{d})$.† The second component of $\mathfrak{L}_1$ is the unit ideal and therefore $n(\mathfrak{L}_1) = N(\mathfrak{a}_1)$. But we have seen that $\mathfrak{a}_1$ divides $aBN(\rho)\mathfrak{d}$. It follows that $\mathfrak{a}_1 = aBN(\rho)\mathfrak{d}$ and the lemma is proved.

4. A basis of an ideal in $\mathfrak{G}$ with respect to G. An ideal in $\mathfrak{G}$ may contain two elements $\omega_i = g_{i1}+g_{i2}E (i=1, 2)$, where the g's are in G, such that an element of $\mathfrak{G}$ is in $\mathfrak{L}$ if and only if it may be written $x\omega_1+y\omega_2$, where x, y are in G. Such a pair of elements will be called a basis of $\mathfrak{L}$ with respect to G and we shall write $\mathfrak{L} = [\omega_1, \omega_2]$. Let 1, θ be a basis of G. Then $\mathfrak{L} = [\omega_1, \theta\omega_1, \omega_2, \theta\omega_2]$. Since $\mathfrak{L}$ contains a non-singular element, these four basal elements are linearly independent with respect to the rational field.‡ Hence ω_1, ω_2 are left linearly independent with respect to F. It will be understood hereafter when two elements are referred to as a basis of an ideal in $\mathfrak{G}$ that they form a basis with respect to G.

If the determinant $|g_{ij}|$ is a positive rational integer, the ω's will be said to form a proper basis of $\mathfrak{L}$. We then define the norm of $\mathfrak{L}$ as $N(\mathfrak{L}) = |g_{ij}|$. If the ω's form a proper basis of $\mathfrak{L}$ and $\zeta_i = t_{i1}\omega_1+t_{i2}\omega_2$ are elements of $\mathfrak{L}$, it may be shown that they form a proper basis if and only if the determinant $|t_{ij}| = 1$. It may also be shown that $N(\mathfrak{L})$ is independent of the particular proper basis employed. If $\xi = u+vE$ is in $\mathfrak{G}$ and $\omega_i\xi = h_{i1}+h_{i2}E$ $(i=1, 2)$, we find

* Loc. cit., p. 74.

† MacDuffee, loc. cit., p. 78, line 23.

‡ MacDuffee, loc. cit., Theorem 3, p. 74.

$$\begin{pmatrix} h_{11} & h_{12} \\ h_{12} & h_{22} \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} u & v \\ \alpha v' & u' \end{pmatrix}.$$

Taking determinants, we have $|h_{ij}| = N(\mathfrak{L})N(\xi)$. Since $\mathfrak{L}\xi = [\omega_1\xi, \omega_2\xi]$, it follows that if $N(\xi) > 0$, the $\omega_i\xi$ form a proper basis of $\mathfrak{L}\xi$ and $N(\mathfrak{L}\xi) = N(\mathfrak{L})N(\xi)$.

LEMMA 4. *If an ideal has a proper basis, every ideal in the same class has a proper basis.*

Let $\mathfrak{L} = [\omega_1, \omega_2]$, the indicated basis being proper, and let $\mathfrak{L}_1$ be an ideal in the same class. Then $\mathfrak{L}\xi = \mathfrak{L}_1\xi_1$ where $N(\xi)N(\xi_1) > 0$. $\mathfrak{L}_1$ contains elements ζ_1, ζ_2, such that $\omega_i\xi = \zeta_i\xi_1 (i = 1, 2)$ and $\mathfrak{L}_1 = [\zeta_1, \zeta_2]$. To show that the ζ's form a proper basis, let $\xi = u + vE$, $\xi_1 = u_1 + v_1E$, $\zeta_i = h_{i1} + h_{i2}E$ $(i = 1, 2)$. Then from $\omega_i\xi = \zeta_i\xi_1$ we have

$$\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} u_1 & v_1 \\ \alpha v_1' & u_1' \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} u & v \\ \alpha v' & u' \end{pmatrix}.$$

Hence $|h_{ij}| N(\xi_1) = N(\mathfrak{L})N(\xi)$. But $N(\mathfrak{L})$ and $N(\xi)N(\xi_1)$ are positive integers and $|h_{ij}|$ is an integral algebraic number. Hence $|h_{ij}|$ is a positive rational integer and the ζ's form a proper basis of $\mathfrak{L}_1$. This proves the lemma.

An ideal $\mathfrak{L}$ in $\mathfrak{G}$ will be called a regular ideal if the corresponding ideal $\mathfrak{d}$ of Lemma 2 is the unit ideal. We shall now prove

THEOREM 1. *An ideal in $\mathfrak{G}$ has a proper basis if and only if it is a regular ideal.*

Suppose $\mathfrak{L}$ is a regular ideal. By Lemma 3, $\mathfrak{L}$ is equivalent to a reduced ideal $\mathfrak{L}_1$ whose first component is the principal ideal defined by a positive rational integer a. Then by Lemma 1, $\mathfrak{L}_1 = [a, a\theta, b_1 + E, b_2 + E\theta]$ where the b's are in G. Since $\theta'(b_1 + E) - (b_2 + E\theta) = \theta'b_1 - b_2$ is in $\mathfrak{L}_1$, $b_2 \equiv \theta'b_1 \pmod{a}$. Hence we may assume that $b_2 = \theta'b_1$. Since $1, \theta'$ also form a basis of G, it follows that $\mathfrak{L}_1 = [a, b_1 + E]$. The indicated basis of $\mathfrak{L}_1$ is proper and therefore by Lemma 4, $\mathfrak{L}$ has a proper basis.

Suppose $\mathfrak{L}$ has a proper basis and let $a\mathfrak{b}\mathfrak{d}$ and $\mathfrak{b}$ be the first and second components respectively of $\mathfrak{L}$, as in Lemma 2. By Lemmas 3 and 1, $\mathfrak{L}$ is equivalent to an ideal $\mathfrak{L}_1 = [a_1\omega_1, a_1\omega_2, b_1 + E, b_2 + E\theta]$ where a_1 is a positive rational integer, $\mathfrak{b} = [\omega_1, \omega_2]$, and the b's are in G. Since $\mathfrak{L}$ has a proper basis, by Lemma 4, $\mathfrak{L}_1$ has a proper basis $\mu_i = g_{i1} + g_{i2}E (i = 1, 2)$ and $N(\mathfrak{L}_1) = |g_{ij}|$. $\mathfrak{L}_1$ contains $b_1 + E$ and therefore for properly chosen numbers t_1, t_2 in G, $t_1\mu_1 + t_2\mu_2 = b_1 + E$. Then $t_1g_{12} + t_2g_{22} = 1$ and

$$\zeta_1 = g_{22}\mu_1 - g_{12}\mu_2 = N(\mathfrak{L}_1),$$

$$\zeta_2 = t_1\mu_1 + t_2\mu_2$$

form a proper basis of $\mathfrak{L}_1$. Since ζ_1 is a rational integer, ζ_2 is not in G. Therefore the first component of $\mathfrak{L}_1$ is the principal ideal defined by ζ_1. But the first component of $\mathfrak{L}_1$ is $a_1\mathfrak{d}$ and $\mathfrak{d}$ contains no rational prime factor. Hence $\mathfrak{d}=\{1\}$ and $\mathfrak{L}$ is a regular ideal. This proves the theorem.

A class of ideals which contains a regular ideal will be called a regular class. By Lemma 4 and Theorem 1, every ideal in a regular class is regular.*

5. **The class of forms corresponding to a regular ideal.** If a, c are rational integers, b is in G, x and y range over all the numbers of G, and b', x', y' are the conjugates of b, x, y respectively, then

$$f(x, y) = axx' + bx'y + b'xy' + cyy' \tag{5}$$

will be said to be an Hermitian form in G of determinant $bb'-ac$. If $f_1(x_1, y_1)$ is obtained from f by a linear homogeneous transformation on x, y of determinant unity, with coefficients in G, f and f_1 will be said to be equivalent. f_1 is an Hermitian form of determinant $bb'-ac$. All the forms equivalent to a given form will be said to form a class.

Let $\mathfrak{L}$ be a regular ideal. By Theorem 1, it has a proper basis $\omega_i=g_{i1}+g_{i2}E (i=1, 2)$ and $N(\mathfrak{L})=|g_{ij}|$. Since each $E\omega_i$ belongs to $\mathfrak{L}$, we have

$$E\omega_i = b_{i1}\omega_1 + b_{i2}\omega_2 \qquad (i = 1, 2), \tag{6}$$

where the b's are in G. The general element of $\mathfrak{L}$ is X as written below, where x, y range over all the numbers of G:

$$X = x\omega_1 + y\omega_2 = (g_{11}x + g_{21}y) + (g_{12}x + g_{22}y)E,$$

$$EX = l_1\omega_1 + l_2\omega_2 = (g_{11}l_1 + g_{21}l_2) + (g_{12}l_1 + g_{22}l_2)E,$$

where $l_i=b_{1i}x'+b_{2i}y'$ $(i=1, 2)$. Then

$$N(X) = \begin{vmatrix} g_{11}x + g_{21}y & g_{12}x + g_{22}y \\ g_{11}l_1 + g_{21}l_2 & g_{12}l_1 + g_{22}l_2 \end{vmatrix} = \begin{vmatrix} x & y \\ l_1 & l_2 \end{vmatrix} \cdot \begin{vmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{vmatrix} = N(\mathfrak{L})f(x, y)$$

where

$$f(x, y) = \begin{vmatrix} x & y \\ l_1 & l_2 \end{vmatrix} = b_{12}xx' - b_{11}x'y + b_{22}xy' - b_{21}yy'. \tag{7}$$

Since $f(x, y)$ is rational and is in G for every x, y in G, it is a rational integer for every such x, y. It may then be shown that b_{12}, b_{21} are rational integers and $b_{11}=-b_{22}'$. Hence f is an Hermitian form in G. We shall see later that the determinant of f is α. f will be said to correspond to the proper basis, ω_1, ω_2, of $\mathfrak{L}$.

* It may be shown that for a regular ideal $\mathfrak{L}$, $n(\mathfrak{L})=N^2(\mathfrak{L})$.

We have seen that $\zeta_i = t_{i1}\omega_1 + t_{i2}\omega_2 (i = 1, 2)$ form a proper basis if and only if the t's are in G and $|t_{ij}| = 1$. The form corresponding to such a basis is $f_1(x_1, y_1) = N(x_1\zeta_1 + y_1\zeta_2)/N(\mathfrak{L})$. Hence f is transformed into f_1 by the transformation

$$x = t_{11}x_1 + t_{21}y_1, \qquad y = t_{12}x_1 + t_{22}y_1, \tag{8}$$

and f is equivalent to f_1. Conversely if f is transformed into f_1 by (8), the t's being in G and $|t_{ij}| = 1$, then f_1 is the form corresponding to the proper basis $\zeta_i = t_{i1}\omega_1 + t_{i2}\omega_2$ $(i = 1, 2)$. Hence there is a one-to-one correspondence between the proper bases of $\mathfrak{L}$ and the forms in the class C, containing f. We shall say that C corresponds to $\mathfrak{L}$.

THEOREM 2. *If C and C_1 are the classes of Hermitian forms in G which correspond to the regular ideals $\mathfrak{L}$ and $\mathfrak{L}_1$ respectively, then $C = C_1$ if and only if $\mathfrak{L}$ and $\mathfrak{L}_1$ are equivalent.*

Let $f(x, y)$ of (5) be a form in C. We may assume, without loss of generality, that $a \neq 0$. Suppose $C = C_1$. Then f corresponds to a proper basis ω_1, ω_2 of $\mathfrak{L}$ and to a proper basis ζ_1, ζ_2 of $\mathfrak{L}_1$. From (5), (6), and (7) we have

$$E\omega_1 = -b\omega_1 + a\omega_2, \qquad E\zeta_1 = -b\zeta_1 + a\zeta_2,$$
$$E\omega_2 = -c\omega_1 + b'\omega_2, \qquad E\zeta_2 = -c\zeta_1 + b'\zeta_2,$$

and $(b+E)\omega_1 = a\omega_2$, $(b+E)\zeta_1 = a\zeta_2$. From $N(x\omega_1 + y\omega_2) = N(\mathfrak{L})f(x, y)$, it follows that $N(\omega_1) = aN(\mathfrak{L}) \neq 0$. Similarly, $N(\zeta_1) = aN(\mathfrak{L}_1)$. Then $N(\omega_1)N(\zeta_1) > 0$. We have

$$\mathfrak{L}a\omega_1' = [a\omega_1, a\omega_2]\omega_1' = [a\omega_1, (b + E)\omega_1]\omega_1' = \lfloor a, b + E\rfloor N(\omega_1).$$

Similarly, $\mathfrak{L}_1 a\zeta_1' = [a, b+E]N(\zeta_1)$. Since $a \neq 0$, $\mathfrak{L}\omega_1' N(\zeta_1) = \mathfrak{L}_1\zeta_1' N(\omega_1)$ and $\mathfrak{L}_1$ and $\mathfrak{L}$ are equivalent.

Conversely, suppose $\mathfrak{L}$ and $\mathfrak{L}_1$ are equivalent. Let ω_1, ω_2 form a proper basis of $\mathfrak{L}$. As in the proof of Lemma 4, $\omega_i\xi = \zeta_i\xi_1$ $(i = 1, 2)$, where $N(\xi)N(\xi_1) > 0$ and the ζ's form a proper basis of $\mathfrak{L}_1$. Let f of (7) be the form in C corresponding to the above basis of $\mathfrak{L}$. The coefficients of f are defined by (6). But from the last equations and $N(\xi_1) \neq 0$, it follows that each ω_i in (6) may be replaced by the corresponding ζ_i. Hence f is also the form in C_1 corresponding to the above basis of $\mathfrak{L}_1$. The theorem follows.

6. The correspondence between regular classes of ideals and classes of forms. We shall prove

THEOREM 3. *There is a one-to-one correspondence between the regular classes of ideals in $\mathfrak{G}$ and the classes of Hermitian forms in G, of determinant α, which represent positive integers.*

By Theorem 2, for every regular class of ideals there is a uniquely determined class of Hermitian forms in G. Also no class corresponds to two classes of ideals. To prove the above theorem, it is therefore sufficient to show that (a) if C is a class of forms corresponding to a class of ideals, then C contains a form which represents a positive integer and is of determinant α, and (b) every class of Hermitian forms in G of determinant α, which represent a positive integer, corresponds to a regular class of ideals in $\mathfrak{G}$.

By Lemmas 3 and 4 and Theorem 1, every regular class of ideals contains an ideal $\mathfrak{L}=[a, b+E]$, where a is a positive integer and b is in G. The indicated basis of $\mathfrak{L}$ is proper, $N(\mathfrak{L})=a$, and the form corresponding to this basis is $N[ax+y(b+E)]/a=f(x, y)$ where f is given by (5) and $c=(bb'-\alpha)/a$. Then f represents the positive integer a, the determinant of f is $bb'-ac=\alpha$ and the class containing f corresponds to the regular class containing $\mathfrak{L}$. This proves (a).

Let C be a class of Hermitian forms in G of determinant α, which represent a positive integer, and let f of (5) be a form in C. We may assume, without loss of generality, that $a\neq 0$. Since $bb'-ac=\alpha$, it is readily shown that there is an ideal $\mathfrak{L}=[a, b+E]$. If $X=ax+y(b+E)$ is the general element in $\mathfrak{L}$, $N(X)=af(x, y)$. If $a>0$, the above basis of $\mathfrak{L}$ is proper, $N(\mathfrak{L})=a$, and C corresponds to the class of ideals containing $\mathfrak{L}$. Suppose $a<0$. From $af(x, y)=N(X)$ and our hypothesis that f represents a positive integer, it follows that $\mathfrak{G}$ contains an element ξ, of negative norm. Then $\mathfrak{L}\xi=[a\xi, (b+E)\xi]$, the indicated basis of $\mathfrak{L}\xi$ is proper, $N(\mathfrak{L}\xi)=aN(\xi)$, $N[xa\xi+y(b+E)\xi]=aN(\xi)f(x, y)$, and C corresponds to the class of ideals containing $\mathfrak{L}\xi$. This completes the proof of the theorem.

7. **Principal ideals.** If $\eta_1, \eta_2, \cdots, \eta_r$ are elements in $\mathfrak{G}$ not all singular, the set of all elements $\sum\xi_i\eta_i$, where the ξ's are in $\mathfrak{G}$, form an ideal which will be written $\mathfrak{L}=\{\eta_1, \eta_2, \cdots, \eta_r\}$. If $r=1$, $\mathfrak{L}$ will be called a principal ideal. It will be observed that a principal ideal $\{\eta\}$ has a proper basis $\pm\eta$, $E\eta$ and hence by Theorem 1 it is a regular ideal. It may be shown that if $\mathfrak{L}$ is a principal ideal and $\mathfrak{L}\xi=\mathfrak{L}_1\xi_1$ where $N(\xi)N(\xi_1)\neq 0$, then $\mathfrak{L}_1$ is a principal ideal.

If $\lambda=\lambda_1\delta\neq 0$, where λ, λ_1, δ are in $\mathfrak{G}$, δ is said to be a right divisor of λ. If δ is also a right divisor of an element μ in $\mathfrak{G}$ and if every common right divisor of λ, μ is a right divisor of δ, then δ is said to be a greatest common right divisor, or g.c.r.d., of λ, μ. An element of $\mathfrak{G}$ of norm ± 1 is said to be a unit. Let α_1 be the product of the rational prime divisors of α which are divisible by prime ideals of the first degree in G or let $\alpha_1=1$ if α has no such divisors. Then every prime ideal divisor of $\mathfrak{d}$ of Lemma 2 is a divisor of $\alpha_1\Delta$. We shall now prove

THEOREM 4. *Let every regular ideal in $\mathfrak{G}$ be principal. Let λ, μ be elements in $\mathfrak{G}$ and assume that $N(\lambda) \neq 0$. If $\mathfrak{G}$ contains a non-regular ideal, assume that $N(\lambda)$ is prime to $\alpha_1\Delta$. Then λ, μ have a* g.c.r.d., *δ, which is uniquely determined apart from a unit left factor, and $\delta = \xi\lambda + \eta\mu$, where ξ, η are in $\mathfrak{G}$. If λ has no rational prime factor and $N(\lambda) = \pm p_1 \cdot p_2 \cdot \cdots \cdot p_r$, where the p's are rational primes arranged in an arbitrary but fixed order, then $\lambda = \pi_1 \cdot \pi_2 \cdot \cdots \cdot \pi_r$ where $N(\pi_i) = \pm p_i$ $(i = 1, 2, \cdots, r)$ and each π_i is uniquely determined apart from a unit left factor.*

Every rational integer in an ideal is divisible by the first component of the ideal. Therefore by Lemma 2 and the definition of α_1, an ideal is regular if it contains a rational integer prime to $\alpha_1\Delta$. Consider the ideal in $\mathfrak{G}$, $\mathfrak{L} = \{\lambda, \mu\}$. If $\mathfrak{G}$ contains a non-regular ideal, by hypothesis $\mathfrak{L}$ contains a rational integer, $\lambda'\lambda = N(\lambda)$, which is prime to $\alpha_1\Delta$. Hence in every case $\mathfrak{L}$ is a principal ideal $\{\lambda, \mu\} = \{\delta\}$, where δ is in $\mathfrak{G}$. Then $\lambda = \lambda_1\delta$, $\mu = \mu_1\delta$, $\delta = \xi\lambda + \eta\mu$, where λ_1, μ_1, ξ, η are in $\mathfrak{G}$. If ζ is a common right divisor of λ and μ, by the last equation it is a right divisor of δ, and $\delta = \epsilon_1\zeta$ where ϵ_1 is in $\mathfrak{G}$. Then δ is a g.c.r.d. of λ and μ. Suppose ζ is also a g.c.r.d. of λ and μ. Then $\zeta = \epsilon_2\delta$ where ϵ_2 is in $\mathfrak{G}$. λ is non-singular and therefore δ is non-singular. It follows that $\epsilon_1\epsilon_2 = 1$ and the ϵ's are units in $\mathfrak{G}$. This proves the first part of the theorem.

To prove the second part, consider the ideal $\mathfrak{L} = \{p_r, \lambda\}$. As before $\mathfrak{L} = \{\pi_r\}$, $\lambda = \lambda_1\pi_r$, $p_r = \nu_r\pi_r$ where λ_1, π_r, ν_r are in $\mathfrak{G}$. Dropping the subscripts r, we have $p^2 = N(\nu)N(\pi)$. Suppose $N(\pi) = \pm 1$. Then $\mathfrak{L}$ is the unit ideal, and for properly chosen ξ, η in $\mathfrak{G}$, $\xi\lambda = 1 + \eta p$. Taking norms, we have $N(\xi)N(\lambda) \equiv 1 \pmod{p}$, whereas $N(\lambda) \equiv 0 \pmod{p}$. Suppose $N(\pi) = p^2$. Then $N(\nu) = \pm 1$, $\lambda = \lambda_1\pi = p\lambda_1\nu^{-1}$ and ν^{-1} is in $\mathfrak{G}$. Then p is a divisor of λ, contrary to hypothesis. Hence $N(\pi) = \pm p$. Employing the ideal $\{p_{r-1}, \lambda_1\}$, we find similarly $\lambda_1 = \lambda_2\pi_{r-1}$ where λ_2 is in $\mathfrak{G}$ and $N(\pi_{r-1}) = \pm p_{r-1}$. Continuing this process, we find $\lambda = \pi_1 \cdot \pi_2 \cdot \cdots \cdot \pi_r$ where $N(\pi_i) = \pm p_i$ $(i = 1, 2, \cdots, r)$. By the first part of the theorem, these π's are uniquely determined, apart from unit left factors. This completes the proof of the theorem.

8. **Applications.** In this paragraph, we shall employ the foregoing results to determine a number of special quaternion algebras for which the conclusions of Theorem 4 are valid.

LEMMA 5. *If for every rational integer $a > 1$ and for every number b in G such that $N(b) - \alpha \equiv 0 \pmod{a}$, there is a number b_0 in G such that $b_0 \equiv b \pmod{a}$ and $0 < |N(b_0) - \alpha| < a^2$, then every regular ideal in $\mathfrak{G}$ is principal.*

By Lemma 3, every regular ideal $\mathfrak{L}$ is equivalent to an ideal $\mathfrak{L}_1 = [a, b+E]$, where a is a positive rational integer and b is in G. If $a = 1$, $\mathfrak{L}_1 = \{1\}$ and $\mathfrak{L}$ is principal. Suppose $a > 1$. $\mathfrak{L}_1$ contains $(b'-E)(b+E) = bb' - \alpha \equiv 0 \pmod{a}$.

Then by hypothesis, $\mathfrak{L}_1=[a,\ b_0+E]$, $b_0b_0'-\alpha=ac$, $0<|c|<a$ and $\mathfrak{L}_1(b_0'-E)=[c,\ -b_0'+E]a$. If $|c|=1$, it follows as before that $\mathfrak{L}$ is principal. If $|c|>1$, repetition of the process leads to the case $a=1$. Hence $\mathfrak{L}$ is principal and the lemma is proved.

Let F be the field defined by $\tau^{1/2}$. It may be shown for each of the following cases that the hypothesis of Lemma 5 is valid. Hence the conclusions of Theorem 4 are valid for these cases.*

$$(\tau,\ \alpha) = (-1,\ -1),\ (-1,\ 3),\ (-3,\ \mp 2),\ (-3,\ 5),\ (5,\ \pm 2),\ (5,\ \pm 3),\ (5,\ \pm 7),\ (5,\ \pm 13),\ (-7,\ -1),\ (13,\ \pm 2),\ (13,\ \pm 5),\ (-3,\ -1). \tag{9}$$

Consider the question of the existence of non-regular ideals in $\mathfrak{G}$. By Lemma 3, every non-regular ideal is equivalent to a reduced ideal $\mathfrak{L}$ whose first component is $a\mathfrak{d}$, where a is a positive rational integer, $\mathfrak{d}\neq\{1\}$, and every rational prime divisor of $N(\mathfrak{d})$ is a divisor of $\alpha_1\Delta$. Let $\mathfrak{d}=[\omega_1,\ \omega_2]$. Then $\mathfrak{L}=[a\omega_1,\ a\omega_2,\ b_1+E,\ b_2+E\theta]$ where the b's are in G. By (1),

$$N(b_1)-\alpha\equiv 0 \pmod{\mathfrak{d}}. \tag{10}$$

Suppose now $\alpha_1=1$ and $\Delta\equiv 1 \pmod 4$. Then every rational prime divisor, p, of $N(\mathfrak{d})$ is a divisor of Δ, and by (10), $N(2b_1)\equiv u^2\equiv 4\alpha \pmod p$, where u is a rational integer. We have then

LEMMA 6. *If $\Delta\equiv 1 \pmod 4$, $\alpha_1=1$ and if α is a quadratic non-residue of every prime factor of Δ, then every ideal in $\mathfrak{G}$ is regular.*

It will be observed that, by this lemma, the conclusions of Theorem 4 are valid for each of the cases (9), except the first three, with no restrictions on $N(\lambda)$ except that $N(\lambda)\neq 0$.

Consider the case where $\alpha\equiv\tau\equiv 3 \pmod 4$, $\alpha>0$, $\tau<0$ and $\alpha\tau$ contains no square factor. It may be shown that if f of (5) is an Hermitian form in G of determinant α, then a and c are not both even and a, b, c have no rational prime factor in common. Hence f is a properly primitive form. By a result due to Humbert,† there is only one class of such forms. Hence by Theorem 3, every regular ideal in $\mathfrak{G}$ is principal and Theorem 4 is applicable. It will be noted that $\Delta=4\tau$.

* For the case $(-1,\ -1)$, see Dickson, *Arithmetic of quaternions*, Proceedings of the London Mathematical Society, (2), vol. 20 (1922), pp. 225–232, Theorems 3, 8. For the cases $(-3,\ -1)$ and $(-7,\ -1)$, see Dickson, *Algebren und ihre Zahlentheorie*, pp. 163, 167, 193, 195. Several of the remaining cases above were treated by Griffiths, *Generalized quaternion algebras and the theory of numbers*, American Journal of Mathematics, vol. 50 (1928), pp. 303–314; in particular, see pp. 309–310.

† Humbert, *Sur le nombre des classes de formes à indéterminées conjuguées, indéfinies, de determinant donné*, Comptes Rendus, Paris, vol. 166 (1918), pp. 865–870; Dickson, *History of the Theory of Numbers*, vol. 3, p. 275.

Suppose, in addition to the above conditions on α and τ, that for every prime factor p of α and every prime factor q of τ, the Legendre symbols

$$\left(\frac{\tau}{p}\right) = \left(\frac{\alpha}{q}\right) = -1.$$

It may then be shown that in (10), $N(\mathfrak{d})$ has no odd prime divisor. Hence in this case every ideal containing an odd rational integer is a principal ideal and Theorem 4 is valid with $\alpha_1\Delta$ replaced by 2.

Griffiths showed that a certain condition was satisfied by each of the algebras she considered.* This condition is similar to our Lemma 5 in that it insures a certain descent. By employing our Lemma 3, it may be shown that if her Lemma 2 is valid for a given $\mathfrak{G}$, then every regular ideal in $\mathfrak{G}$ is principal and hence Theorem 4 is applicable.

Throughout this paper, we have considered only left ideals. It will be observed that if X, Y are in $\mathfrak{G}$, then $(X+Y)'=X'+Y'$ and $(XY)'=Y'X'$ are in $\mathfrak{G}$. Hence $\mathfrak{G}$ is reciprocal to itself and from each of our results we may obtain at once a parallel result for right ideals.

* Loc. cit., Lemma 2, p. 305.

UNIVERSITY OF KENTUCKY,
LEXINGTON, KY.