TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 197, 1974

MODULES OVER QUADRATIC AND QUATERNION RINGS AND TRANSFORMATIONS OF QUADRATIC FORMS

BY

BART RICE

ABSTRACT. A study is made of transformations carrying certain quadratic and quaternary quadratic forms into multiples of themselves, and it is shown how these are related to the study of modules over quadratic and quaternion rings. Special automorphic transformations of n-ary quadratic forms may also exhibit a structure like those in the quadratic and quaternary cases.

1. Introduction. In this paper we will be concerned with Z-orders in composition algebras (cf. [4]) of dimensions 2 and 4 over Q (Z denotes the ring of integers, Q the rationals), the quadratic and quaternion algebras, respectively. Specifically, we will identify modules over quadratic and quaternion rings with automorphic transformations of related quadratic forms. Certain automorphic transformations of n-ary quadratic forms are also discussed. The author wishes to express his appreciation to Professor Gordon Pall for his encouragement and many helpful suggestions concerning this research. Also, Dennis Estes, in several letters to the author and to Dr. Pall, communicated a number of (heretofore unpublished) ideas and results which have been utilized in this paper. Accordingly, the author wishes to acknowledge Professor Estes' contribution.

The reader will recall that a *composition algebra* over a field K, of characteristic not 2, is a pair $(\mathfrak{A}, N)$, where $\mathfrak{A}$ is an algebra over K and N is a function (called the *norm*), $N: \mathfrak{A} \to K$, such that, for $\alpha, \beta \in \mathfrak{A}$, $c \in K$,

(i) $N(\alpha\beta) = (N\alpha)(N\beta)$;

(ii) $N(c\alpha) = c^2 N\alpha$;

(iii) the inner product $(\alpha, \beta) = N(\alpha + \beta) - N\alpha - N\beta$ is bilinear;

(iv) N is nondegenerate; that is, if $(\alpha, \beta) = 0$ for each $\beta \in \mathfrak{A}$, then $\alpha = 0$; and

(v) $\mathfrak{A}$ has an identity element ι: $\iota\alpha = \alpha\iota = \alpha$ for all $\alpha \in \mathfrak{A}$.

Presented to the Society, April 22, 1972 under the title *Modules over orders and transformations of quadratic forms*; received by the editors December 14, 1970.

AMS (MOS) subject classifications (1970). Primary 10C05, 16A42; Secondary 12A25, 16A18, 16A28, 13C99.

Key words and phrases. Quaternions, quadratic forms, composition algebras, automorphic transformations.

An element $\alpha \in \mathfrak{A}$ will be called *pure* if $\alpha \in (K\iota)$; that is, if $(\alpha, \iota) = 0$. Thus if $\gamma \in \mathfrak{A}$, we may write γ uniquely as $\gamma = c\iota + \alpha$, where $c \in K$ and α is pure. The *conjugate* of γ is defined by $\bar{\gamma} = c\iota - \alpha$. It is easily shown that $(\alpha\beta, \gamma) = (\alpha, \gamma\bar{\beta}) = (\beta, \bar{\alpha}\gamma)$ and $\alpha\bar{\beta} = \overline{\beta\alpha}$. It is well known (cf. [4]) that a composition algebra $\mathfrak{A}$ over Q has dimension 1 (Q itself), 2 (the quadratic fields), 4 (the quaternion algebras), or 8 (nonassociative algebras). Henceforth we assume that the dimension of $\mathfrak{A}$ over Q is 2 or 4.

Whenever we speak of a *module* in $\mathfrak{A}$ we shall mean a finitely generated Z-submodule $\mathfrak{M}$ of $\mathfrak{A}$ such that $Q\mathfrak{M} = \mathfrak{A}$; that is, such that $\mathfrak{M}$ is free over Z of rank 2 or 4. We define the *norm* of $\mathfrak{M}$ to be the least positive integer in $\mathfrak{M}$. Let $\beta_1, \cdots, \beta_n$ be a basis for $\mathfrak{M}$. We will sometimes write $\mathfrak{M} = [\beta_1, \cdots, \beta_n]$. $N(\Sigma_k x_k\beta_k)$ is a quadratic form $\psi = \Sigma_{i,j} b_{ij}x_ix_j$, $b_{ij} \in Q$, called the *norm form* of $\mathfrak{M}$ for the basis $\beta_1, \cdots, \beta_n$. We may extract a rational number q and write $\psi = q\psi'$, where ψ' is a primitive n-ary quadratic form with coefficients in Z, called a *primitive norm* of $\mathfrak{M}$ for the basis $\beta_1, \cdots, \beta_n$. We verify easily that $|q|$ is an invariant of the choice of basis, and that equivalent bases give rise to equivalent norm forms.

A composition algebra of order 2 over Q is a field $F_j = Q(j)$, where $j^2 \neq 1$ is a square free integer, or, if j is a symbol such that $j^2 = 1$, F_j is the commutative associative algebra over Q with basis $1, j$. If $\alpha = a_0 + a_1j$, $\bar{\alpha} = a_0 - a_1j$, and $N\alpha = a_0^2 - j^2a_1^2$, and thus if $j^2 < 0$, $N\alpha = 0$ if and only if $\alpha = 0$. Set $d_0 = j^2$ or $4j^2$ according as $j^2 \equiv 1$ or $\not\equiv 1 \pmod 4$. Let $\mathfrak{D} = \{d_0s^2 : s = 1, 2, 3, \cdots\}$. To each $d \in \mathfrak{D}$ corresponds an order R_d in F_j given by

$$R_d = \{x_0 + x_1\omega : x_0, x_1 \in Z\},$$

where

(1.2) $\omega = \omega_d = (\epsilon + \sqrt{d})/2$, $\epsilon = 0$ or 1 according as $d \equiv 0$ or $1 \pmod 4$.

It follows that $N(x + y\omega) = x^2 + \epsilon xy + (\epsilon - d)y^2/4$, the norm form of R_d for the basis $1, \omega$.

The four-dimensional composition algebras over K are the quaternion algebras, 4-dimensional central algebras which are isomorphic to either a division algebra or the algebra of 2×2 matrices over K. O'Meara in [7] gives what is probably the best known definition of a quaternion algebra. However, for our purposes, a more suitable definition is the one which follows, first given by Pall in [9].

Let f be an integral ternary form, (a_{ij}) the matrix of f. Let $(A_{ij}) = \text{adj}(a_{ij})$ [if K is an $n \times n$ matrix, by "adj K" we mean the transpose of the matrix of cofactors of K], and let adj f be the ternary form with matrix (A_{ij}). The quaternion algebra $\mathfrak{A}(f)$ pertaining to the form f has Q-basis $1, i_1, i_2, i_3$, where $i_k^2 = -A_{kk}$,

$k = 1, 2, 3$, and $i_r i_s = -A_{rs} + \Sigma_k a_{tk} i_k$, $i_s i_r = -A_{sr} - \Sigma_k a_{tk} i_k$, where (r, s, t) is a cyclic permutation of $(1, 2, 3)$. If $\alpha = x_1 i_1 + x_2 i_2 + x_3 i_3 \in \mathfrak{A}(f)$ such that x_1, x_2, $x_3 \in Z$, then α is said to be *purely integral*. If, in addition, $(x_1, x_2, x_3) = 1$, then α is termed *purely primitive*.

The norm form of $\mathfrak{A}$ for the basis $1, i_1, i_2, i_3$ is

$$N\left(x_0 + \sum_k x_k i_k\right) = x_0^2 + \text{adj } f(x_1, x_2, x_3) = x_0^2 + \sum_{k,j} A_{ij} x_i x_j,$$

which need not always be an integral form. However, it is found (cf. [9]), for $\{i, j, k\} = \{1, 2, 3\}$, that if $\epsilon_k = 0$ or 1 according as $2a_{ij}$ is even or odd, then the "Brandt norm form",

$$F = \left(x_0 + \frac{1}{2}\sum_k \epsilon_k x_k\right)^2 + \text{adj } f(x_1, x_2, x_3),$$

has integral coefficients. Accordingly, if we let $j_k = i_k + \epsilon_k/2$, $k = 1, 2, 3$, then the norm form of $\mathfrak{A}$ for the basis $1, j_1, j_2, j_3$ is F. Further, it may be verified that $R(f) = \{x_0 + \Sigma_k x_k j_k : x_k \in Z\}$ is a Z-order, which will be called the integral order "associated with ", or "obtained from", f. When it is convenient, we will write simply $\mathfrak{A}$ and R for $\mathfrak{A}(f)$ and $R(f)$. An element $\alpha = x_0 + \Sigma_k x_k j_k \in R$ will be termed *primitive* if $1 = (x_0, x_1, x_2, x_3)$; primitive (mod m) if $(x_0, x_1, x_2, x_3, m) = 1$; *pure* (mod m) if $(\alpha, 1) \equiv 0 \pmod{m}$. If α is pure and primitive, α will sometimes be called "pure-primitive" (as distinguished from "purely primitive"). The most familiar quaternion algebra is the Hamilton algebra obtained from the form $x^2 + y^2 + z^2$. The corresponding order R_0 is the "Lipschitz ring" of integral quaternions.

We remark in passing that no generality is lost by studying the rings $R(f)$; for Estes has shown that every ring R of integral quaternions containing four linearly independent elements such that $1 \in R$ is isomorphic to a quaternion order associated with an integral ternary form.

2. Modules and automorphic transformations.

2.1. *The quadratic case.* Suppose α_1, α_2 are elements of the quadratic order $R_d = [1, \omega]$ such that α_1, α_2 are linearly independent over Q. Let $\mathfrak{M}$ be the two-dimensional Z-module $[\alpha_1, \alpha_2]$. Then we may select a Z-basis $k[a, r + s\omega]$ for $\mathfrak{M}$, where $a, r, s \in Z$, $(a, r, s) = 1$, $k \in Q$. In the Z-module $[a, r + s\omega]$, s is the least positive integer coefficient of ω among the elements of the module, a is the norm of the module, and r is unique (mod a).

Now $[a, r + s\omega]$ with $(a, r, s) = 1$ is an ideal in R_d if and only if $s = 1$ and $a | N(r + \omega)$ (cf. [2, p. 32]). We may then set

$$r + \omega = \tfrac{1}{2}(b + \sqrt{d}), \qquad N(r + \omega) = \tfrac{1}{4}(b^2 - d) = ac,$$

whence $b = (r + \omega, 1)$, the trace of $r + \omega$. Thus with the Z-module $\mathfrak{M} = [a, r + \omega]$ we may associate the form $\psi = [a, b, c]$. Notice that if $(a, 2d) = 1$, or if d is fundamental, then ψ is primitive; for if $p|(a, b, c)$, then $p^2|b^2 - 4ac = d$, and $(b^2 - 4ac)/p^2$ is a discriminant.

Let A denote the matrix of ψ, and suppose $\alpha \in F_j$ such that $\alpha\mathfrak{M} \subset \mathfrak{M}$ or $\alpha\overline{\mathfrak{M}} \subset \mathfrak{M}$. Then we may select integers t_1, t_2, t_3, t_4 such that

$$\alpha a = t_1 a + t_3(r + \omega); \quad \text{and}$$

(2.1.1)

$$\alpha(r + \omega) = t_2 a + t_4(r + \omega), \quad \text{or} \quad \alpha(r + \bar{\omega}) = t_2 a + t_4(r + \omega).$$

One verifies easily that if

$$T = \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix}, \tag{2.1.2}$$

then $T'AT = (N\alpha)A$. Also, $\det T = N\alpha$ or $-N\alpha$ according as $(2.1.1)_2$ or $(2.1.1)_3$ is the case.

Conversely, suppose $\psi = [a, b, c]$ is a binary quadratic form of discriminant d with matrix A, and that T is a 2×2 integral matrix such that $T'AT = eA$. If T is given by (2.1.2), then $\det T = t_1 t_4 - t_2 t_3 = \pm e$. Choose r so that $r + \omega_d = (b + \sqrt{d})/2$, and let $\alpha_1 = t_1 a + t_3(r + \omega)$, $\alpha_2 = t_2 a + t_4(r + \omega)$.

Assume $\det T = e$. Then from the Gauss lemma (cf. [1, p. 160]) we obtain the equations $-at_2 = ct_3$, $bt_3 = at_4 - at_1$, whence $\alpha = (1/a)\alpha_1 = (r + \omega)^{-1}\alpha_2$ satisfies $N\alpha = e$ and $\alpha[a, r + \omega] \subset [a, r + \omega]$. If $\det T = -e$, the Gauss lemma yields $bt_1 = at_2 - ct_3$, $t_4 = -t_1$, whence $\alpha_1(r + \bar{\omega}) = \alpha_2 a$. Hence if $\alpha = (1/a)\alpha_1$, then $N\alpha = e$ and $\alpha[a, r + \bar{\omega}] \subset [a, r + \omega]$.

(2.1.3) **Theorem.** *Let A be the matrix of a binary quadratic form $\psi = [a, b, c]$ of discriminant d, $r + \omega = r + \omega_d = (b + \sqrt{d})/2$, and $\mathfrak{M} = [a, r + \omega]$. Then to each 2×2 matrix T such that $T'AT = eA$ corresponds an $\alpha \in F_j$ such that $\alpha\mathfrak{M} \subset \mathfrak{M}$ or $\alpha\overline{\mathfrak{M}} \subset \mathfrak{M}$. Specifically, $\alpha = (1/a)\alpha_1$ and $N\alpha = \pm e$, where $(\alpha_1, \alpha_2) = (a, r + \omega)T$. If ψ is primitive, those T's such that $T: \alpha\mathfrak{M} \to \mathfrak{M}$ form a ring R, isomorphic with R_d. Conversely, if $\alpha\mathfrak{M}$ or $\alpha\overline{\mathfrak{M}} \subset \mathfrak{M}$, $\alpha \in F_j$, there is an integral 2×2 matrix T_α satisfying $T_\alpha' A T_\alpha = (N\alpha)A$.*

Clearly $\alpha\mathfrak{M} \subset \mathfrak{M}$, $\beta\mathfrak{M} \subset \mathfrak{M}$ imply $(\alpha + \beta)\mathfrak{M} \subset \mathfrak{M}$, $\alpha\beta\mathfrak{M} \subset \mathfrak{M}$, and we easily verify that $T_{\alpha+\beta} = T_\alpha + T_\beta$, $T_{\alpha\beta} = T_\alpha T_\beta = T_\beta T_\alpha = T_{\beta\alpha}$. Also, $R' = \{\alpha \in F_j: \alpha\mathfrak{M} \subset \mathfrak{M}\} \supset R_d$, surely. And if ψ is primitive, R_d is the largest order within which $\mathfrak{M}$ is an ideal (cf. [2]). Thus $R' = R_d$.

2.2. *The four-dimensional case.* Let $\mathfrak{A}$ be a quaternion algebra over the rational field Q containing a four dimensional Z-module $\mathfrak{M} = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ with norm form $N(\Sigma_i x_i \alpha_i) = mF(x_1, x_2, x_3, x_4)$ and having A as the matrix of its primitive norm F.

Suppose that $\sigma, \rho \in \mathfrak{A}$ satisfy $\rho\mathfrak{M}\sigma \subset \mathfrak{M}$. Then we can find integers t_{ij}, $1 \leq i, j \leq 4$, such that $\rho\alpha_i\sigma = \Sigma_j t_{ij}\alpha_j$. Let $T = (t_{ij})$. Now $\frac{1}{2}(\alpha_i, \alpha_j) = ma_{ij}$, so that

$$(\rho\alpha_i\sigma, \rho\alpha_j\sigma) = (N\rho)(N\sigma)(\alpha_i, \alpha_j) = 2m(N\rho)(N\sigma)a_{ij}.$$

But also,

$$(\rho\alpha_i\sigma, \rho\alpha_j\sigma) = \left(\sum_r t_{ri}\alpha_r, \sum_s t_{sj}\alpha_j\right) = \sum_{r,s} t_{ri}(\alpha_r, \alpha_s)t_{sj} = 2m\sum_{r,s} t_{ri}a_{rs}t_{sj},$$

which is $2m$ times the (i, j) entry in $T'AT$. Hence $T'AT = (N\rho)(N\sigma)A$. Virtually identical reasoning yields this same result if we assume instead that $\rho\mathfrak{M}\sigma \subset \mathfrak{M}$.

The following useful lemma was essentially proved above:

(2.2.1) **Lemma.** *Let $\mathfrak{M}$, A be as above, and suppose that S is a nonsingular 4×4 matrix. Let β_j, $1 \leq j \leq 4$, be given by $(\beta_1, \beta_2, \beta_3, \beta_4) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)S$. Then $S'AS = 1/2m((\beta_i, \beta_j))$.*

(2.2.2) **Lemma (Estes).** *Let $1, \rho_1, \rho_2, \rho_3$ be linearly independent elements of $\mathfrak{A}$ such that $(\rho_i, 1) = 0$, $i = 1, 2, 3$. Let $A = \frac{1}{2}((\rho_i, \rho_j)) = (A_{ij})$. Then* det A *is the square of a rational number d, and, for a cyclic permutation (i, j, k) of $(1, 2, 3)$, $\rho_i\rho_j = -A_{ij} + \Sigma_n a_{nk}\rho_n$, where $(a_{ij}) =$* (adj A)$/d$.

Proof. Let $\rho_i\rho_j = r_0 + r_1\rho_1 + r_2\rho_2 + r_3\rho_3$, $i \neq j$. Since $(\rho_i\rho_j, 1) = -(\rho_i, \rho_j) = -2A_{ij} = 2r_0$, we have that $r_0 = -A_{ij}$. Now $(\rho_i\rho_j, \rho_i) = (\rho_i\rho_j, \rho_j) = 0$, hence $(0, 0, (\rho_i\rho_j, \rho_k)) = 2(r_1, r_2, r_3)A$, $k \neq i, j$. Since $1, \rho_1, \rho_2, \rho_3$ are linearly independent, det $A \neq 0$, and $(r_1, r_2, r_3) = (\frac{1}{2}\det A)(0, 0, (\rho_i\rho_j, \rho_k))$ adj A. Expanding the three terms $N(\rho_i\rho_j + A_{ij})$, $(\rho_i\rho_i\rho_j, \rho_k)$, and $(\rho_i\rho_j\rho_j, \rho_k)$, we obtain the three equations

$$a_{kk} = (\rho_i\rho_j, \rho_k)^2 a_{kk}/4 \det A;$$

$$2a_{ik} = (\rho_i\rho_j, \rho_k)^2 a_{ij}/2 \det A;$$

$$2a_{jk} = (\rho_i\rho_j, \rho_k)^2 a_{jk}/2 \det A.$$

Since one of a_{kk}, a_{ik}, a_{jk} is not zero, $(\rho_i\rho_j, \rho_k)^2 = 4 \det A$. Choose $d = \pm\sqrt{\det A}$ so that $(\rho_1\rho_2, \rho_3) = 2d$. Then $\rho_1\rho_2 = -A_{12} + a_{13}\rho_1 + a_{23}\rho_2 + a_{33}\rho_3$. Since $(\rho_1\rho_2, \rho_3) = (\rho_3\rho_1, \rho_2) = (\rho_2\rho_3, \rho_1)$, the lemma follows. Q.E.D.

Now suppose that T is a 4×4 nonsingular matrix such that $T'AT = eA$ (whence $e \neq 0$), and let $(\beta_1, \beta_2, \beta_3, \beta_4) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$. Assume further that α_1 is of nonzero norm. Then from (2.2.1) we conclude that $(\beta_i, \beta_j) = e(\alpha_i, \alpha_j)$, $1 \leq i, j \leq 4$. Thus $N\beta_1 \neq 0$. Also, $(1, \bar{\beta}_1\beta_j) = e(1, \bar{\alpha}_1\alpha_j)$, so that $(N\beta_1)(1, \beta_1^{-1}\beta_j) = (1, \bar{\beta}_1\beta_j) = e(1, \bar{\alpha}_1\alpha_j) = (eN\alpha_1)(1, \alpha_1^{-1}\alpha_j)$. Therefore, $(1, \beta_1^{-1}\beta_j) = (1, \alpha_1^{-1}\alpha_j)$, $1 \leq j \leq 4$.

Thus we may apply a transformation

$$U = \begin{bmatrix} 1 & u_1 & u_2 & u_3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

so that if $(1, \gamma_1, \gamma_2, \gamma_3) = (1, \alpha_1^{-1}\alpha_2, \alpha_1^{-1}\alpha_3, \alpha_1^{-1}\alpha_4)U$ and $(1, \delta_1, \delta_2, \delta_3) = (1, \beta_1^{-1}\beta_2, \beta_1^{-1}\beta_3, \beta_1^{-1}\beta_4)U$, then each γ_i, δ_j is pure. Therefore

$$U'AU = (N\alpha_1/2m)\begin{bmatrix} 1 & 0 \\ 0 & ((\gamma_i, \gamma_j)) \end{bmatrix}.$$

But also, $eU'AU = U'T'ATU$, and $(1, \delta_1, \delta_2, \delta_3) = \beta_1^{-1}(\beta_1, \beta_2, \beta_3, \beta_4)U = \beta_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)TU$. Hence

$$eU'AU = (N\beta_1/2m)\begin{bmatrix} 1 & 0 \\ 0 & ((\delta_i, \delta_j)) \end{bmatrix} = e(N\alpha_1/2m)\begin{bmatrix} 1 & 0 \\ 0 & ((\delta_i, \delta_j)) \end{bmatrix}.$$

Consequently, $((\gamma_i, \gamma_j)) = ((\delta_i, \delta_j))$, and so by (2.2.2) the γ_i's have the same multiplication table as either the δ_j's or the $\bar{\delta}_j$'s. Hence we can find a quaternion ξ and a sign $\tau = \pm 1$ such that $\tau\delta_j = \xi\gamma_j\xi^{-1}$, $1 \leq j \leq 3$ (cf. [9, p. 285]).

If $\tau = +1$, then $(1, \delta_1, \delta_2, \delta_3)$ equals both $\beta_1^{-1}(\beta_1, \beta_2, \beta_3, \beta_4)$ and $\xi(1, \gamma_1, \gamma_2, \gamma_3)\xi^{-1} = \xi\alpha_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\xi^{-1}U$. Thus, taking $\rho = \beta_1\xi\alpha_1^{-1}$, $\sigma = \xi^{-1}$, we have $\rho\alpha_i\sigma = \beta_i$, $1 \leq i \leq 4$.

If $\tau = -1$, we observe that $\xi\alpha_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\xi^{-1}U = (1, \bar{\delta}_1, \bar{\delta}_2, \bar{\delta}_3) = (\bar{\beta}_1, \bar{\beta}_2, \bar{\beta}_3, \bar{\beta}_4)\bar{\beta}_1^{-1}U$. Letting $\rho = \beta_1\bar{\xi}^{-1}$, $\sigma = \bar{\alpha}_1^{-1}\bar{\xi}$, it follows that $\beta_i = \rho\bar{\alpha}_i\sigma$, $1 \leq i \leq 4$.

We have proved:

(2.2.3) **Theorem.** *Let $\mathfrak{M} = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ be a four-dimensional Z-module in a quaternion algebra $\mathfrak{A}$ such that $N\alpha_1 \neq 0$, and let F be the primitive norm form*

of $\mathfrak{M}$, *A the matrix of F. Suppose T is a* 4×4 *integral matrix such that* $T'AT = eA$, $e \neq 0$. *Then we can find quaternions* $\rho, \sigma \in \mathfrak{A}$ *satisfying*:

(i) $(N\rho)(N\sigma) = e$,

(ii) $\rho\mathfrak{M}\sigma \subset \mathfrak{M}$, $\rho(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\sigma = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$, *or*
$\rho\overline{\mathfrak{M}}\sigma \subset \mathfrak{M}$, $\rho(\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3, \overline{\alpha}_4)\sigma = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$.

Conversely, if $\rho\mathfrak{M}\sigma$ *or* $\rho\overline{\mathfrak{M}}\sigma \subset \mathfrak{M}$, *then the matrix T determined by* (ii) *satisfies* $T'AT = (N\rho)(N\sigma)A$.

Thus (2.2.3) establishes an essentially unique association between pairs $(\rho, \sigma) \in \mathfrak{A} \times \mathfrak{A}$ such that $\rho\mathfrak{M}\sigma \subset \mathfrak{M}$, or $\rho\overline{\mathfrak{M}}\sigma \subset \mathfrak{M}$, with $(N\rho)(N\sigma) \neq 0$, and 4×4 integral matrices $T: \rho\mathfrak{M}\sigma \to \mathfrak{M}$, or $T: \rho\overline{\mathfrak{M}}\sigma \to \mathfrak{M}$, such that $T'AT = eA$, $e \neq 0$; "essentially unique" in the sense that (ρ, σ) and $(q\rho, q^{-1}\sigma)$ gives rise to the same T for any nonzero rational number q. Those matrices $T: \rho\mathfrak{M}\sigma \to \mathfrak{M}$ form a (noncommutative) multiplicative semigroup, and those associated with pairs $(\rho, 1)$ form a ring R', as is easily verified; for if $T: \rho\mathfrak{M} \to \mathfrak{M}$, then we may identify T and ρ. A necessary and sufficient condition that R' be isomorphic with $R = [1, j_1, j_2, j_3]$ is evidently that $\mathfrak{M}$ be an ideal in R and not in any larger ring. Clearly the same remarks apply for those T's associated with pairs $(1, \sigma)$.

With any 4×4 rational matrix V we may associate a 4-tuple of quaternions $(\beta_1, \beta_2, \beta_3, \beta_4) = (1, j_1, j_2, j_3)V$. Conversely, with any 4-tuple $(\beta_1, \beta_2, \beta_3, \beta_4)$ we may associate a 4×4 matrix $V = (v_{ij})$, where, for $1 \leq s \leq 4$, $\beta_s = v_{1s} + v_{2s}j_1 + v_{3s}j_2 + v_{4s}j_3$. Thus the quaternions β_s may be regarded as the columns of V, and we may write $V = [\beta_1\ \beta_2\ \beta_3\ \beta_4]$. β_s may be termed the "sth column quaternion" of V.

(2.2.4) **Lemma.**

$$[\alpha\mu\ \alpha\zeta\ \alpha\rho\ \alpha\sigma] = [\alpha\ \alpha j_1\ \alpha j_2\ \alpha j_3][\mu\ \zeta\ \rho\ \sigma],$$

$$[\mu\alpha\ \zeta\alpha\ \rho\alpha\ \sigma\alpha] = [\alpha\ j_1\alpha\ j_2\alpha\ j_3\alpha][\mu\ \zeta\ \rho\ \sigma].$$

The proof is easy. Also, a matrix $[\alpha\ \alpha j_1\ \alpha j_2\ \alpha j_3]$ may be termed a "right quaternion matrix," $[\alpha\ j_1\alpha\ j_2\alpha\ j_3\alpha]$ a "left quaternion matrix". The following has already been observed:

(2.2.5) **Corollary.** $[\alpha\ \alpha j_1\ \alpha j_2\ \alpha j_3][\beta\ j_1\beta\ j_2\beta\ j_3\beta] = [\beta\ j_1\beta\ j_2\beta\ j_3\beta][\alpha\ \alpha j_1\ \alpha j_2\ \alpha j_3]$. *These are matrices* $\alpha R \to R$, $R\beta \to R$. *Also,*

$$[\alpha\mu\beta\ \alpha\zeta\beta\ \alpha\rho\beta\ \alpha\sigma\beta] = [\alpha\ \alpha j_1\ \alpha j_2\ \alpha j_3][\beta\ j_1\beta\ j_2\beta\ j_3\beta][\mu\ \zeta\ \rho\ \sigma].$$

If $T_1: \rho\mathfrak{M} \to \mathfrak{M}$, $T_2: \mathfrak{M}\sigma \to \mathfrak{M}$, then $T_1T_2 = T_2T_1: \rho\mathfrak{M}\sigma \to \mathfrak{M}$ since

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4)T_1T_2 = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T_2T_1 = \rho(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\sigma.$$

Thus suppose $F(x_1, x_2, x_3, x_4) = N(x_1 + x_2 j_1 + x_3 j_2 + x_4 j_3)$, the "Brandt norm form" of R (cf. [9]), whence $\mathfrak{M} = [1, j_1, j_2, j_3]$. If $T = [\beta_1\ \beta_2\ \beta_3\ \beta_4]$ satisfies $T'AT = eA$, then we can factor $T = T_1 T_2 U$, where U is unit modular and T_1, T_2 are left and right quaternion matrices, whenever we can write $(\beta_1\ \beta_2\ \beta_3\ \beta_4) = \alpha(\mu, \zeta, \rho, \sigma)\beta$, with $\det[\mu\ \zeta\ \rho\ \sigma] = \pm 1$. We shall see that this is always possible when $R = R_0$, the Lipschitz ring of integral quaternions.

2.3 *The Lipschitz ring.* Let $R_0 = [1, i_1, i_2, i_3]$ denote the Lipschitz ring of integral quaternions, and suppose that m is a positive integer, I the 4×4 identity matrix, and $T = (t_{ij})$ a 4×4 integral matrix satisfying $T'T = mI$. We assume with no loss of generality that T is primitive. Notice that $T'T = mI$ implies that $TT' = mI$. Let α_s, β_s denote the sth column quaternion, row quaternion of T, respectively. It follows from (2.2.1) that $\frac{1}{2}(\alpha_i, \alpha_j) = \frac{1}{2}(\beta_i, \beta_j) = m\delta_{ij}$, where δ_{ij} is the Kronecker symbol.

Since T is primitive, if p is an odd prime dividing m, then at least two of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are primitive (mod p); for if three are imprimitive (mod p), so must be the fourth. We may assume α_1, α_2 are primitive (mod p). Because $N\alpha_i = m$, $1 \leq i \leq 4$, α_1, α_2 have either the same right divisors, or the same left divisors (or both) of norm p, and such divisors certainly exist (cf. [8]). Thus α_1 and α_2 have a common right (say) divisor γ or norm p. If α_k, $k = 3$ or 4, is also primitive, then α_1 and α_k have γ as a common left or right divisor. If γ is a right divisor of α_1 and α_k, then all three of $\alpha_1, \alpha_2, \alpha_k$ have γ as a right divisor. If α_1 and α_k have γ as a left divisor, we consider γ as a factor of α_2 and α_k. If γ is a right [left] divisor of α_2 and α_k, then γ is a right [left] divisor of all three of $\alpha_1, \alpha_2, \alpha_k$. If the fourth α_i is also primitive (mod p), the above argument may be reapplied to yield the result that γ is a common left divisor or a common right divisor of each of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Further, if a quaternion μ satisfies $\mu \equiv 0 \pmod{p}$, then any quaternion of norm p is both a left and a right divisor of μ. Also, the above reasoning applies if the words "right" and "left" are interchanged. Hence:

(2.3.1) **Lemma.** *Suppose T is a primitive 4×4 nonsingular integral matrix such that $T'T = mI$, and that p is an odd prime dividing m. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the column quaternions of T. Then there exists a quaternion $\gamma \in R_0$ of norm p such that γ is a common left or right divisor of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.*

Suppose $\alpha_i = \alpha_i' \gamma$, $1 \leq i \leq 4$. Then from (2.2.3) we conclude that $T = US = [\gamma\ i_1\gamma\ i_2\gamma\ i_3\gamma][\alpha_1'\ \alpha_2'\ \alpha_3'\ \alpha_4']$. Now $U'U = (N\gamma)I$, so that $T'T = mI$ implies $S'S = (m/N\gamma)I$. A similar result holds if γ is a common left divisor of α_i, $1 \leq i \leq 4$, only then $T = VS = [\gamma\ \gamma i_1\ \gamma i_2\ \gamma i_3][\alpha_1'\ \alpha_2'\ \alpha_3'\ \alpha_4']$. Also, $UV = VU$. Hence, in view of (2.3.1), we may take $N\gamma = p$ for any odd prime factor p of m, repeat the process

with S, and so on until the supply of such factors is exhausted. We thus obtain a factorization $T = LRE = RLE$, where

$$L = [\mu\ \mu i_1\ \mu i_2\ \mu i_3], \qquad R = [\zeta\ i_1\zeta\ i_2\zeta\ i_3\zeta], \tag{2.3.2}$$

$\det R = m_1^2$, $\det L = m_2^2$, where $(2, m_1m_2) = 1$ and $2^\lambda = m/m_1m_2$ is such that $E'E = 2^\lambda I$. Further, $\lambda = 0$, 1, or 2, since T is primitive, and if 8 divides a sum of four squares, each term must be even.

Suppose δ_i is the ith column quaternion of E, $1 \le i \le 4$. Assume $\lambda = 2$. Then $N\delta_i = 4$ implies $\delta_i(1 - i_k) \equiv (1 - i_k)\delta_i \equiv 0 \pmod 2$, $1 \le k \le 3$, since $N(\delta_i(1 - i_k)) = 8$. Hence $1 + i_k$ is both a left and right divisor of each δ_i, and so we may write $E = RE_1 = LE_2$, R, L as in (2.3.2), each of determinant 4, and $E_1'E_1 = E_2'E_2 = 2I$. Thus the case $\lambda = 2$ may be reduced to the case $\lambda = 1$.

If $\lambda = 1$, then we see that $\delta_1, \delta_2, \delta_3, \delta_4$ must in some order be given by $\pm 1 \pm i_k$, $\pm 1 \mp i_k$, $\pm i_j \pm i_n$, $\pm i_j \mp i_n$, with j, k, n distinct. Now $1 + i_k$ and $1 - i_k$ are divisors (left and right) of $1 \pm i_k$, and, if $j, n \ne k$, $i_j \pm i_n$ is equal to $i_j(1 + i_k) = (1 - i_k)i_j$, or to $i_j(1 - i_k) = (1 + i_k)i_j$. Hence we may write $E = RW_1 = LW_2$, where R, L are given by (2.3.2), and each is of determinant 4. W_1, W_2 have determinants ± 1.

(2.3.3) **Theorem.** *Suppose $T'T = mI$, T primitive. Then there exists a factorization $T = RLW = LRW$, W unit-modular (i.e., $\det W = \pm 1$), $\det R = m_1^2$, $\det L = m_2^2$, $m = m_1m_2$, with R, L as in (2.3.2). Further, if m is odd, the factorization $m = m_1m_2$ is unique.*

Everything has been shown but uniqueness. We need several lemmas:

(2.3.4) **Lemma.** *Suppose $\rho_1, \rho_2, \rho_3 \in R_0$ such that $(\rho_k, 1) = 0$, and such that ρ_1, ρ_2, ρ_3 have the same multiplication as i_1, i_2, i_3. Then there exists a sign $\sigma = \pm 1$ and a unit $\xi \in R_0$ such that*

(2.3.5) $\sigma\rho_k = \xi i_k \bar{\xi}$, $k = 1, 2, 3$.

This follows from the proof of Lemma 1 in [9, p. 285].

(2.3.6) **Lemma.** *Suppose R, L are right, left quaternion matrices respectively, and $\det U = \pm 1$. Then if $RL = qU$, q rational and not zero, then R and L are within unimodular factors of a diagonal matrix.*

Proof. Let $U = [\theta_0\ \theta_1\ \theta_2\ \theta_3]$, $N\theta_k = 1$, $0 \le k \le 3$. Let $\rho_k = \bar{\theta}_0\theta_k$, $k = 1, 2, 3$. Since $U'U = I$, it follows that ρ_1, ρ_2, ρ_3 satisfy the hypothesis of (2.3.4). Choose $\sigma = \pm 1$ and $\xi \in R_0$ as in (2.3.5). Then $U = R_1L_1J$, where

$$R_1 = [\theta_0\xi\ \theta_0\xi i_1\ \theta_0\xi i_2\ \theta_0\xi i_3], \quad L_1 = [\bar{\xi}\ i_1\bar{\xi}\ i_2\bar{\xi}\ i_3\bar{\xi}], \quad J = [1\ \sigma i_1\ \sigma i_2\ \sigma i_3].$$

Further, $\sigma = 1$, since $\sigma^3 = \det J = \det U = (1/q^4)(\det R)(\det L) > 0$. Hence $J = I$, and $R_1'R = L_1L'$ is thus both a left and right quaternion matrix. Consequently, $R_1'R$ is a scalar multiple of I. Q.E.D.

Proof of (2.3.3). Suppose $T = R_1L_1W_1 = R_2L_2W_2$, R_1, R_2 right quaternion matrices, L_1, L_2 left quaternion matrices, and W_1, W_2 unit-modular. Since T is primitive, so are L_1 and R_1. Let $U = W_2W_1'$. Then $(R_2'R_1)(L_2'L_1) = mU$, and hence we can find integral unimodular matrices V, W, and integers q, s such that $R_2'R_1 = qV$, $L_2'L_1 = sW$. Let

$$R_1'R_1 = r_1I, \quad R_2'R_2 = r_2I, \quad L_1'L_1 = t_1I, \quad L_2'L_2 = t_2I.$$

It follows that $q^2 = r_1r_2$, $s^2 = t_1t_2$, and that $L_1 = (s/t_2)L_2W$, $R_1 = (q/r_2)R_2V$. Since R_1 and L_1 are primitive, $s|t_2$ and $q|r_2$. Hence $(r_2/q)r_1 = q$, $(t_2/s)t_1 = s$, so $r_1|q$, $t_1|s$. Also, $q^2s^2 = r_1r_2t_1t_2 = m^2 = r_1^2t_1^2 = |\det T|$, so $r_1t_1 = qs$. Thus $r_1 = q$, $t_1 = s$. Similarly, $r_2 = q$, $t_2 = s$. Consequently, the factorization $T = R_1L_1W_1$ is essentially unique. Q.E.D.

(2.3.7) **Corollary.** *Let R and L be as in* (2.3.2). *Then RL is primitive if and only if R and L are.*

Proof. In the proof of (2.3.3) just above, we obtained essential uniqueness using only the fact that R_1 and L_1 were primitive. Clearly essential uniqueness does not follow if T is imprimitive. Q.E.D.

We remark in passing that, if m is even, the factorization $T = RLU$, $|\det T| = (\det R)(\det L)$ is not unique, even if T is primitive; for the quaternion matrices of determinant 4 may be taken as left or right, as has been shown.

(2.4) *Remarks on rings of transformations: The n-dimensional case.* Let A be an $n \times n$ positive-definite symmetric matrix over the reals $\mathfrak{R}$, and let $\mathfrak{S}$ be a set of matrices over $\mathfrak{R}$ such that:

(a) $\mathfrak{S}$ is an $\mathfrak{R}$-module and a ring containing the identity matrix;

(b) if $S \in \mathfrak{S}$, then there is an $r \in \mathfrak{R}$ such that $S'AS = rA$; and

(c) if $S \in \mathfrak{S}$ satisfies $S^2 = 0$, then $S = 0$.

For $S \in \mathfrak{S}$, define the norm of S by $NS = r$, where $S'AS = rA$. It follows that if S, $S_1 \in \mathfrak{S}$, $\lambda \in \mathfrak{R}$, then $N(SS_1) = (NS)(NS_1)$, and $N(\lambda S) = \lambda^2(NS)$. Define the inner product (S, T) by $(S, T) = N(S + T) - NS - NT$. Then $(S, T) = (T, S)$, and

$$N(S + T)A = (S' + T')A(S + T) = (NS)A + (NT)A + S'AT + T'AS.$$

Therefore $S'AT + T'AS = (S, T)A$. From this follows $(\lambda_1S_1 + \lambda_2S_2, S) = \lambda_1(S_1, S) + \lambda_2(S_2, S)$, so the inner product is bilinear.

Suppose that $S_0 \in \mathfrak{S}$ such that $(S_0, S) = 0$ for each $S \in \mathfrak{S}$. Then, in particular,

$(S_0, I) = 0$, so $S_0'A = -AS_0$, whence $-A^{-1}S_0'A = S_0$. Thus $S_0^2 = 0$, so $S_0 = 0$.

Therefore $\mathcal{S}$ is a nondegenerate, associative composition algebra over $\mathcal{R}$. Hence dim $\mathcal{S}$: $\mathcal{R} = 1$, 2, or 4 (cf. [4]).

Suppose that dim $\mathcal{S}$: $\mathcal{R} = 4$. Then $\mathcal{S}$ has a basis I, E_1, E_2, E_3 over R with norm form $x^2 + y^2 + z^2 + w^2$ or $x^2 + y^2 - z^2 - w^2$ (the determinant of the norm form must be a square, thus precluding index 1 or 3). Since A is positive definite, the former must be the case, since for $S \in \mathcal{S}$, NS is represented by the n-ary quadratic form with matrix A. Also, it follows easily that $(E_{ij}, I) = (E_j, E_k) = 0$ if $1 \leq j, k \leq 3$, $j \neq k$, and hence that $E_j'A = -AE_j$. Thus $A = E_j'AE_j = -AE_j^2$, $E_j^2 = -I$. Further, if $i \neq j$, $0 = (E_i, E_j)A = E_i'AE_j + E_j'AE_i = -A(E_iE_j + E_jE_i)$. Therefore, E_1, E_2, E_3 satisfy

$$E_j^2 = -I, \quad E_iE_j + E_jE_i = 0, \quad i \neq j. \tag{2.4.1}$$

Accordingly, we recall two theorems of M. H. A. Newman in [6]:

(2.4.2) **Theorem.** *If $n = 2^q p$ where p is odd, and $\{E_1, E_2, \cdots, E_M\}$ is a set of $n \times n$ matrices satisfying* (2.4.1), *then $M \leq 2q + 1$; and this maximum is attained.*

A set satisfying (2.4.1) Newman calls an "E-set". A "maximal" E-set has the obvious meaning. It is easily shown that a maximal E-set contains an odd number of elements.

(2.4.3) **Theorem.** *If all members of a maximal E-set are real or pure imaginary, say R real and I imaginary, then $R - I = -1$ or 7.*

Therefore we may conclude that $\{E_1, E_2, E_3\}$ is not a maximal E-set, and that if $n = 2^q p$, p odd, then $2q + 1 \geq 5$, $q \geq 2$. Hence $n \equiv 0 \pmod 4$.

Now suppose that dim $\mathcal{S}$: $\mathcal{R} = 2$. Then $\mathcal{S}$ has a basis $1, E$ over $\mathcal{R}$ with norm form $x^2 + y^2$. From (2.4.2) and (2.4.3) we conclude $2q + 1 \geq 3$, n even.

Thus if n is odd, dim $\mathcal{S}$: $\mathcal{R} = 1$. We remark in passing that, if we remove the restriction that A be definite, we can still conclude that n is even when dim $\mathcal{S}$: $\mathcal{R} = 4$.

BIBLIOGRAPHY

1. Hubert S. Butts and Dennis Estes, *Modules and binary quadratic forms over integral domains*, Linear Algebra and Appl. 1 (1968), 153–180. MR 38 #4503.

2. Hubert S. Butts and Gordon Pall, *Modules and binary quadratic forms*, Acta Arith. 15 (1968), 23–44. MR 39 #6822.

3. Dennis Estes, private letters.

4. N. Jacobson, *Composition algebras and their automorphisms*, Rend. Circ. Mat. Palermo (2) 7 (1958), 55–80. MR 21 #66.

5. R. Lipschitz, *Transformation d'une somme de deux ou de trois carrés*, J. Math. (4) II (1886), 373–439.

6. M. H. A. Newman, *Note on an algebraic theorem of Eddington*, J. London Math. Soc. 7 (1932), 93–99.

7. O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der math. Wissenschaften, Academic Press, New York; Springer-Verlag, Berlin, 1963. MR 27 #2485.

8. Gordon Pall, *On the arithmetic of quaternions*, Trans. Amer. Math. Soc. 47 (1940), 487–500. MR 2, 36.

9. ———, *On generalized quaternions*, Trans. Amer. Math. Soc. 59 (1946), 280–332. MR 8, 318.

10. C. Carter Waid, *Modules of quaternions and their related quadratic forms*, Ph.D. Thesis, Louisiana State University, Baton Rouge, La., 1967.

1436 KNIGHTSBRIDGE TURN, CROFTON, MARYLAND 21113