PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 27, Number 1, January 1971

QUATERNIONS AND BINARY QUADRATIC FORMS

BART RICE

ABSTRACT. Methods are discussed for studying binary quadratic forms by use of quaternions derived from the ternary quadratic form $f=x^2-yz$. In particular, Gauss composition of binary quadratic forms may be achieved by factoring and multiplying quaternions in a natural way.

1. **Introduction.** In this paper we show how quaternions obtained from a certain ternary quadratic form f may be employed in the study of binary quadratic forms. We use the form $f=x^2-yz$ because $d=4(\det f)=-1$, whence all binary quadratic forms are open to scrutiny. The same methods may be applied using other ternary forms f, only the condition $|d|>1$ precludes application of the methods to binary quadratic forms of certain discriminants. The techniques of this article borrow from a procedure introduced by Gordon Pall in [**5**] which uses quaternions in the familiar Lipschitz ring of integral quaternions to study the representations of a positive integer as a sum of three squares. I wish to thank Professor Pall, my teacher, for his suggestions concerning this material.

2. **Preliminaries.** An integral ternary quadratic form $f=\sum_{i,j} a_{ij}x_ix_j$ (the sum is taken from 1 to 3, as will be the case with all sums henceforth) gives rise to a quaternion algebra $\mathfrak{R}=\mathfrak{R}(f)=Q[1,\ i_1,\ i_2,\ i_3]$ (Q = rational numbers) and an integral order $R=R(f)=Z[1,j_1,j_2,j_3]$ contained in $\mathfrak{R}$. The basal elements $i_1,\ i_2,\ i_3$ have the multiplication table given by Pall in [**6**]; to wit,

$$i_r^2 = -A_{rr}, \qquad r = 1, 2, 3;$$

$$i_ri_s = -A_{rs} + \sum_k a_{kt}i_k; \qquad i_si_r = -A_{sr} - \sum_k a_{kt}i_k;$$

where $(A_{ij})=\operatorname{adj}(a_{ij})$, and (r, s, t) is a cyclic permutation of $(1, 2, 3)$. Also, $j_k=i_k+\frac{1}{2}\epsilon_k$, $k=1, 2, 3$, where $\epsilon_1, \epsilon_2, \epsilon_3$ are chosen 0 or 1 according as $2a_{23}$, $2a_{13}$, $2a_{12}$ are even or odd, respectively. An element $\alpha=\sum x_ki_k\in\mathfrak{R}$ such that $x_1, x_2, x_3\in Z$, is said to be "purely integral"; "purely primitive" if, in addition, $(x_1, x_2, x_3)=1$. In the case $f=x^2-yz$,

Received by the editors November 17, 1969.
AMS 1970 *subject classifications*. Primary 10C05; Secondary 16A18.
Key words and phrases. Quaternions, binary quadratic forms, composition.

$j_1 = i_1 + \frac{1}{2}$, $j_2 = i_2$, $j_3 = i_3$, and adj $f = -\frac{1}{4}(x^2 - 4yz)$. Thus the "Brandt norm-form" of R (cf. [6]) is given by

$$F = \left(x_0 + \tfrac{1}{2} \sum x_k \epsilon_k\right)^2 + \operatorname{adj} f = x_0^2 + x_0 x_1 + x_2 x_3,$$

which is the "norm" $N\alpha$ of $\alpha = x_0 + \sum x_k j_k$. F is indefinite and fundamental, and thus, since $d = -1$ (cf. [6], Theorem 3 and the remark on p. 293), given an integer m and a quaternion $\alpha \in R$ such that $m \mid N\alpha$, there is a unique (up to left unit factors) element $\beta \in R$ of norm m such that β is a right divisor of α. The multiplication in R is as follows: If $\alpha = u_0 + \sum u_k j_k$, $\beta = v_0 + \sum v_k j_k$, then

$$\begin{aligned}\alpha\beta &= u_0 v_0 - u_2 v_3 + (u_0 v_1 + u_1 v_1 + u_1 v_0 + u_2 v_3 - u_3 v_2) j_1 \\ &\quad + (u_0 v_2 + u_2 v_0 + u_2 v_1) j_2 + (u_0 v_3 + u_3 v_0 + u_1 v_3) j_3.\end{aligned}$$

3. **Purely primitive sets.** Let $\eta = \sum x_k i_k$ be a purely integral quaternion. Define $[\eta] = \{\theta\eta\bar{\theta} : N\theta = 1, \theta \in R\}$. Notice that $\mu \in [\eta]$ implies $N\mu = N\eta$, and if η is purely primitive, so is μ. Thus we will call $[\eta]$ "purely primitive of norm q" if η is purely primitive and $N\eta = q$. Let $\psi = [a, b, c]$ be a primitive binary quadratic form of discriminant $d = b^2 - 4ac = -n$. We now define a process by which ψ carries each purely primitive $[\eta]$ of norm $n/4$ $(\neq 0)$ into a unique purely primitive $[\zeta]$ of the same norm.

$N(b/2 + \eta) = \frac{1}{4}(b^2 + n) = ac$, so $b/2 + \eta \in R$. Hence we may write $b/2 + \eta = \sigma\tau$, where $N\sigma = c$, $N\tau = a$, and $\sigma, \tau \in R$. Let $\zeta = \tau\eta\bar{\tau}/a = \tau\sigma - b/2$. It follows easily that ζ is purely integral. Also, ζ is purely primitive; for if $\zeta = \sum y_k i_k$ and $p \mid y_k$, $k = 1, 2, 3$, then $p \mid a$ since $a\eta = \bar{\tau}\zeta\tau$ and $(x_1, x_2, x_3) = 1$. Also, $p \mid n$, since $y_1^2 - 4y_2 y_3 = -n$. Because $b^2 + n = 4ac$, $p \mid b$. Since $\sigma\zeta\bar{\sigma} = c\eta$ and η is primitive, $p \mid c$. This contradicts the primitivity of ψ. Also, if τ is replaced by $\theta\tau$, $N\theta = 1$, ζ is replaced by $\theta\zeta\bar{\theta}$. If η is replaced by $\theta\eta\bar{\theta}$, $N\theta = 1$, then ζ is unchanged, since $b/2 + \theta\eta\bar{\theta} = \theta\sigma\tau\bar{\theta}$, $(1/N(\tau\bar{\theta}))\tau\bar{\theta}(\theta\eta\bar{\theta})\theta\bar{\tau} = (1/N\tau)\tau\eta\bar{\tau} = \zeta$.

(3.1) Lemma. *The process associated with the primitive form* $\psi = [a, b, c]$ *is the same as that for the following forms equivalent to* ψ: $[a, b + 2ah, c + bh + ah^2]$, $[c, -b, a]$.

Proof. See Lemma 14 of [5]. Q.E.D.

(3.2) Corollary. *Any two equivalent forms* ψ *determine the same process.*

Proof. $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and matrices of the type $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ generate $SL_2(Z)$. Q.E.D.

Thus we may speak of a *class* C of primitive forms taking $[\eta]$ to $[\zeta]$, "$[\eta] \xrightarrow{C} [\zeta]$."

(3.3) LEMMA. *If* $[\eta]\xrightarrow{C}[\zeta]$, $[\zeta]\xrightarrow{D}[\xi]$, *then* $[\eta]\xrightarrow{CD}[\xi]$.

The proof involves united forms (i.e., concordant forms in the Dedekind sense, see [**3**, p. 69]). The reader is referred to [**5**, p. 496].

(3.4) LEMMA. *There is at most one primitive class of discriminant* $-n$ *carrying any given purely primitive* $[\eta]$ *of norm* $n/4$ *into a given purely primitive* $[\zeta]$ *of the same norm.*

PROOF. Suppose C, D take $[\eta]$ into $[\zeta]$. Then both CD^{-1} and the principal class E carry $[\eta]$ into $[\eta]$. Suppose m is primitively represented by CD^{-1}. Then m can be made the first coefficient of a form $\psi=[m, b, c]\in CD^{-1}$. ψ takes $[\eta]$ into $[\eta]$, so there is an integral quaternion $\tau\in R$ satisfying $N\tau=m$ and $\tau\eta\bar{\tau}=m\eta$. From this follows $\tau\eta=\eta\tau$, an expansion of which yields $x_it_j=x_jt_i$, $i, j=1, 2, 3$, where $\eta=\sum_k x_ki_k$, $\tau=t_0+\sum_k t_kj_k$. Since $(x_1, x_2, x_3)=1$, we can find an integer g such that $t_k=gx_k$, $k=1, 2, 3$. Thus $m=N\tau=t_0^2+x_1t_0g+x_2x_3g^2$. Clearly $[1, x_1, x_2x_3]\in E$, and thus E represents every integer represented primitively by $F=CD^{-1}$. Since E is ambiguous (cf. [**3**, p. 64]), $E=F$, $C=D$. Q.E.D.

4. The process and composition. We now turn to the equation $\tau\alpha\bar{\tau}=\beta$, where $\tau\in R$ and $\alpha=\sum_k a_ki_k$ and $\beta=\sum_k b_ki_k$ are purely integral. By direct computation,

$$\begin{aligned} b_1 &= 2t_1t_2a_3 - 2t_0t_3a_2 + t_0^2a_1 + t_0t_1a_1 + 2t_0t_2a_3 - t_2t_3a_1;\\ b_2 &= a_2t_0^2 + a_1t_0t_2 + a_3t_2^2;\\ b_3 &= a_2(-t_3)^2 + a_1(-t_3)(t_0+t_1) + a_3(t_0+t_1)^2. \end{aligned} \tag{4.1}$$

Thus, for $\tau=t_0+\sum_k t_kj_k$, the equations (4.1) imply that if

$$T = T(\tau) = \begin{bmatrix} t_0 & -t_3 \\ t_2 & t_0+t_1 \end{bmatrix},$$

then $\det T=N\tau$ and $T'AT=B$, where A, B are respectively the matrices of the forms $\phi(\alpha)=[a_2, a_1, a_3]$, $\phi(\beta)=[b_2, b_1, b_3]$. Conversely, if

$$S = \begin{bmatrix} s_1 & s_2 \\ s_3 & s_4 \end{bmatrix}$$

satisfies $S'AS=B$, then $\sigma=\sigma(S)=s_1+(s_4-s_1)j_1+s_3j_2-s_2j_3$ satisfies $\sigma\alpha\bar{\sigma}=\beta$. Thus, in particular, a set $[\eta]$ "corresponds" to a class $C(\eta)$ in the sense that $\zeta\in[\eta]$ if and only if $\phi(\zeta)\sim\phi(\eta)\in C(\eta)$. Moreover, if $\psi=[a, b, c]$ is primitive of discriminant $-n$, then $\alpha(\psi)=bi_1+ai_2$

$+ci_3$ is purely primitive of norm $n/4$. Also, $\alpha(\phi(\eta))=\eta$, $\phi(\alpha(\psi))=\psi$, $\sigma(T(\tau))=\tau$.

Let $\alpha(C)$ denote a representative of $[\alpha(\psi)]$, where $\psi\in C$. As before, let E denote the principal class of discriminant $-n=-4N\eta$, where $\eta=\sum_k x_k i_k$ is purely primitive. Then $\eta'=x_1i_1+i_2+x_2x_3i_3\in[\alpha(E)]$, since surely $[1, x_1, x_2x_3]\in E$. By direct computation, $x_1/2+\eta'=\sigma\tau$, where $\sigma=x_1j_1+j_2+x_3j_3$ $(N\sigma=x_3)$, and $\tau=x_2+(1-x_2)j_1$ $(N\tau=x_2)$, and $\tau\eta'\bar{\tau}=x_2\eta$. Hence $C(\eta)$ takes $[\alpha(E)]$ into $[\eta]$.

(4.2) THEOREM. *There is a one-to-one correspondence between purely primitive sets $[\eta]$ of norm $n/4$ and classes of primitive binary quadratic forms of discriminant $-n$. Also, given any two such purely primitive sets, $[\eta]$ and $[\zeta]$, there is a unique class C taking $[\eta]$ into $[\zeta]$. If B, C, D are primitive classes of discriminant $-n$, then $BC=D$ if and only if $[\alpha(B)]\xrightarrow{C}[\alpha(D)]$.*

PROOF. The first statement has already been established as fact. From the preceding, $[\alpha(E)]\xrightarrow{C(\eta)}[\eta]$, $[\alpha(E)]\xrightarrow{C(\zeta)}[\zeta]$. Thus,

$$[\eta]\xrightarrow{C(\eta)^{-1}C(\zeta)}[\zeta].$$

Uniqueness has already been established. Suppose that $[\eta]\xrightarrow{C}[\zeta]$. The commutativity of the diagram

$$\begin{array}{ccc} [\eta] & \xrightarrow{C} & [\zeta] \\ C(\eta)\nwarrow & & \nearrow C(\zeta) \\ & [\alpha(E)] & \end{array}$$

yields the validity of the last sentence in the theorem. Q.E.D.

Thus composition of primitive binary quadratic forms may be achieved simply by multiplying quaternions! The correspondence between this method and composition by united forms may be gleaned from the formulae

$$b/2+bi_1+a_1i_2+a_2ci_3=(bj_1+a_1j_2+cj_3)(a_2+(1-a_2)j_1);$$
$$(a_2+(1-a_2)j_1)(bj_1+a_1j_2+cj_3)=b/2+bi_1+a_1a_2i_2+ci_3.$$

For the connection between this "quaternionic composition" and composition by bilinear substitution, we turn to Gauss. Specifically, we answer the question, "Given a quaternionic composition $BC=D$ determined by $[\alpha(B)]\xrightarrow{f'}[\alpha(D)]$, $f'\in C$, is there in evidence a Gaussian bilinear substitution which yields $F=ff'$, $f\in B$, $F\in D$?" . . . And the converse question as well.

Thus suppose that $f=[a,\ b,\ c]\in B$, $f'=[a',\ b',\ c']\in C$. Suppose further that $b'/2+\alpha(f)=\sigma\tau$, $N\tau=a'$, $N\sigma=c'$, $\tau=t_0+\sum_k t_kj_k$, $\sigma=u_0+\sum_k u_kj_k$, $\zeta=(1/a')\tau\alpha(f)\bar\tau=\tau\sigma-b'/2$, and $\phi(\zeta)=F$. Then $F=ff'$. That is, F is a composite of f, f' in the Gauss sense. The reader is invited to verify that the appropriate bilinear substitution is given by $T(\sigma,\ \tau)$, where

$$T(\sigma,\tau) = \begin{bmatrix} t_0+t_1 & u_0 & t_3 & -u_3 \\ -t_2 & u_2 & t_0 & u_0+u_1 \end{bmatrix}.$$

Use of this matrix is prompted by the equations $\bar\tau\zeta\tau=a'\alpha(f)$, $\sigma\zeta\bar\sigma=c'\alpha(f)$, and the famous equations [1]–[9] of article 235 of Gauss' *Disquisitiones arithmeticae* [**4**].

Conversely, suppose $F=ff'$ via the bilinear substitution

$$T=\begin{bmatrix} p & p' & p'' & p''' \\ q & q' & q'' & q''' \end{bmatrix},$$

and that all three forms are primitive of discriminant d. Butts and Estes in [**1**] pointed out that $pq''-qp''=a'$, $p'q'''-q'p'''=c'$. And, in fact, if we choose σ, τ by $T=T(\sigma,\tau)$ (i.e., $t_0=q''$, $u_0=p'$, $t_1=p-q''$, $u_1=q'''-p'$, etc.), then $N\sigma=c'$, $N\tau=a'$, $b'/2+\alpha(f)=\sigma\tau$, and $\tau\alpha(f)\bar\tau=a'\alpha(F)$.

We remark in passing that, evidently, quaternionic and Gaussian composition coincide over every domain which admits composition in the Gauss sense. The following lemma allows us to identify quaternion and Gaussian composition even in the case when discriminants are not equal.

(4.3) LEMMA. *Let p be a prime, $n\equiv 0$ or -1 (mod 4). Every purely primitive ζ of norm $p^2n/4$ is of the form $\zeta=\tau\eta\bar\tau$, where $N\tau=p$ and $N\eta=n/4$. Further, τ and η are unique apart from insertion of unit factors. Thus every purely primitive $[\zeta]$ of norm $p^2n/4$ is derivable from a unique purely primitive $[\eta]$ of norm $n/4$.*

PROOF. Suppose p is odd. Choose $j=0$ or 1 such that $pj/2+\zeta$ is in R. Then $N(pj/2+\zeta)=p^2(j+n)/4$. Hence $pj/2+\zeta=\sigma\tau$, where $N\tau=p$, σ primitive (mod p). If $\sigma\tau=\mu\nu$, with $\mu,\nu\in R$ and $N\mu=p$, then $\bar\mu\sigma\tau\equiv 0$ (mod p). Since τ is necessarily primitive, $\bar\mu\sigma\equiv 0$ (mod p). Therefore, σ and $\sigma\tau$ have the same left divisors of norm p. But $\sigma\tau=pj/2+\zeta=\bar\tau(\tau j-\bar\sigma)$. Thus $\sigma=\bar\tau\eta'$, $pj/2+\zeta=\bar\tau\eta'\tau$, $\zeta=\bar\tau(\eta'-j/2)\tau=\bar\tau\eta\tau$. The factorization is necessarily unique (cf. [**6**]). If $p=2$ the above applies with j chosen 0 or 1 according as $n\equiv 0$ or -1 (mod 4). Q.E.D.

5. Other applications. The techniques developed in this paper may be applied to the study of the quadratic orders

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

where

$$\text{(5.1)} \quad \omega_d = (\epsilon + \sqrt{d})/2, \qquad \epsilon = 0 \text{ or } 1 \text{ according as } d \equiv 0 \text{ or } 1 \pmod 4).$$

We illustrate by using these methods to derive some results obtained by Butts and Pall in [2].

We can, in view of (4.3), map a given primitive class C of binary quadratic forms of discriminant dv^2 onto a unique primitive class D of discriminant d; simply take $D = C(\eta)$, where $\alpha(C) = \tau\eta\bar{\tau}$, $N\tau = v > 0$. An easy argument shows that this factorization is essentially unique. According to Theorem 2.5 in [2], this corresponds to the function $C \to CI_d$.

Now suppose that $d' = dv^2$ $(v > 0)$, and that A', A are invertible fractional ideals in $R_{d'}$, R_d respectively. To study the equation $A = A'R_d$, we may assume $A = [m, r+\omega]$, $A' = k[m', r'+\omega']$, k rational, $m, m', r, r' \in Z$, $m \mid N(r+\omega)$, $m' \mid N(r'+\omega')$, where $\omega = \omega_d$, $\omega' = \omega_{d'}$ as in (5.1). Associated with the invertible fractional ideals A, A' are the primitive forms

$$\Psi(A) = [m, 2r + \epsilon, N(r + \omega)/m], \qquad \Psi(A') = [m', 2r' + \epsilon', N(r' + \omega')/m']$$

of discriminants d and dv^2 respectively. Hence we may associate with A, A' purely primitive sets $[\eta]$, $[\eta']$, where $\eta = \alpha(\Psi(A))$, $\eta' = \alpha(\Psi(A'))$, of norms $-d/4$, $-dv^2/4$ respectively. According to Theorem (5.1) of [2], $A = A'R_d$ implies the existence of a matrix

$$H = \begin{bmatrix} e & h \\ 0 & n_1 \end{bmatrix}, \qquad en_1 = v,$$

such that $k(m', r'+\omega') = (m, r+\omega)H$. It follows that $\Psi(A)^H = \Psi(A')$, and thus $\tau\eta\bar{\tau} = \eta'$, where $\tau = e + (n_1 - e)j_1 - hj_3$ has norm $en_1 = v$. Conversely, if A is an invertible ideal in R_d, and A' is an invertible ideal in $R_{d'}$ obtained from $\tau\eta\bar{\tau} = \eta'$, $N\tau = v$, then $A'R_d = A$.

Now let p be a prime. Then there are $p+1$ ideals $(\tau]$ of norm $N\tau = p$ in R (refer to [6]). Those for which $\tau\eta\bar{\tau} \equiv 0 \pmod p$, $N\alpha = n/4$, are precisely the right divisors of $x_0/2 + \eta$, where $(x_0^2 + n)/4 \equiv 0 \pmod p$, and thus are $1 + (-n/p)$ in number. Also, if τ and τ' are not left associates, then $\tau\eta\bar{\tau}$ and $\tau'\eta\bar{\tau}'$ are not in the same purely primitive set $[\zeta]$, from the uniqueness feature of (4.3). Thus a given purely primitive $[\eta]$ of norm $n/4$ gives rise to $(p+1)-(1+(-n/p))=p-(-n/p)$ purely primitive sets $[\zeta]$ of norm $p^2n/4$. We obtain easily, then, that the number N of purely primitive sets $[\zeta]$ of norm $nv^2/4$, $v>0$, obtainable from a given purely primitive set $[\eta]$ of norm $n/4$ is given by

$$N = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - (-n/p_i)), \tag{5.2}$$

where $v=p_1^{e_1}\cdots p_r^{e_r}$ is a factorization of v into distinct primes. Hence we deduce Theorem 5.2 and Corollary 5.3.1 of [2], namely:

(5.3) THEOREM. *Suppose A is an invertible fractional ideal in R_d, where $d=-n$, and $d'=dv^2$, $v>0$. Let $v=p_1^{e_1}\cdots p_r^{e_r}$ be a factorization of v into distinct primes. Then the number of invertible fractional ideals A' in $R_{d'}$ such that $A'R_d=A$ is given by* (5.2).

REFERENCES

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. Leonard Eugene Dickson, *History of the theory of numbers*. Vol. III, Chelsea, New York, 1952.

4. C. F. Gauss, *Disquisitiones arithmeticae*, Fleischer, Leipzig, 1870; English transl., Yale University Press, New Haven, Conn., 1966. MR **33** #5545.

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

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

7. Bart Rice, *Rings of integral quaternions*, (to appear).

LOUISIANA STATE UNIVERSITY, BATON ROUGE, LOUISIANA 70803