CONJUGACY IN THE REAL THREE-DIMENSIONAL ORTHOGONAL GROUPS

BY
BARTH POLLAK

Introduction

There are two three-dimensional orthogonal groups over the field $\mathbf{R}$ of real numbers determined by whether or not the quadratic form which defines the "metric" on the space is anisotropic (ordinary Euclidean 3-space) or not. In both cases the commutator subgroup $\boldsymbol{\Omega}$ is a simple group. (When the space is anisotropic, the commutator subgroup is the set of all isometries of determinant $+1$; when the space is isotropic, it is a normal subgroup of index 2 in that group.) Thus if $a \neq 1$ is in $\boldsymbol{\Omega}$ and $b \in \boldsymbol{\Omega}$, there exists a positive integer n such that

$$(*) \qquad b = \textstyle\prod_{i=1}^{n} t_i a^{\pm 1} t_i^{-1}.$$

Let $\mathbf{N}_a(b)$ denote the smallest n for which $(*)$ is true. By the use of quaternions, we give an explicit formula for $\mathbf{N}_a(b)$ in both cases.

1. Quaternion algebras

Let K be a field of characteristic $\neq 2$. By a *quaternion algebra* $\mathbf{H}$ over K we mean a central simple associative algebra of dimension 4 over K. It is well known that $\mathbf{H}$ has a basis of the form $1, I, J, IJ$ with 1 the multiplicative identity, $I^2 = \alpha$, $J^2 = \beta$, $IJ = -JI$, where $\alpha, \beta \in K^*$ (the multiplicative group of nonzero elements of K). (See [1, Theorem 27, p. 146].) We shall use the notation (α, β) for a quaternion algebra possessing such a basis. $\mathbf{H}$ possesses an antiautomorphism of period 2 called *conjugation*, the image of $X \in \mathbf{H}$ being denoted X^c. Then we have $X + X^c = S(X)1$, $XX^c = N(X)1$ with $S(X)$, $N(X) \in K$ called respectively the *trace* and *norm* of X, and $X^2 - S(X)X + N(X)1 = 0$ for each $X \in \mathbf{H}$. If $S(X) = 0$, we call X *pure*. If $X = \xi_0 1 + \xi_1 I + \xi_2 J + \xi_3 IJ$, we have

$$(1) \qquad N(X) = \xi_0^2 - \alpha\xi_1^2 - \beta\xi_2^2 + \alpha\beta\xi_3^2 .$$

For future use we set $\mathbf{H}_1 = \{X \in \mathbf{H} \mid N(X) = 1\}$. We conclude this section by stating

THEOREM 1. *Let $A, B \in \mathbf{H}$. There exists $T \in \mathbf{H}$ such that $B = TAT^{-1}$ if and only if $N(A) = N(B)$ and $S(A) = S(B)$. There exists $T \in \mathbf{H}_1$ such that $B = TAT^{-1}$ if and only if in addition to the above conditions,*

(i) *$(N(B - A^c), S^2(A) - 4N(A)) \cong \mathbf{M}_2(K)$, the algebra of all 2×2 matrices over K provided $N(B - A^c)$ and $S^2(A) - 4N(A)$ are both nonzero;*

(ii) *if $S^2(A) - 4N(A) = 0$, then $N(B - A^c) \in K^2$.*

Received July 10, 1962.

Proof. The first assertion is well known, and the second one follows immediately from the Main Theorem of [3].

2. Rotations in a three-dimensional space

Let V be a three-dimensional vector space over K upon which is defined a nonsingular quadratic form f. Let $\mathbf{O}(V)$ denote the orthogonal group of V, $\mathbf{O}^+(V)$ the subgroup of elements of determinant $+1$ (called *rotations*), $\mathbf{O}'(V)$ the spinorial kernel, and $\mathbf{\Omega}(V)$ the commutator subgroup of $\mathbf{O}(V)$.

We denote by s_C the symmetry with respect to the hyperplane perpendicular to the anisotropic vector C and remark that every $t \in \mathbf{O}^+(V)$ is of the form $t = s_C\, s_D$ (see [2] for details). We note that replacing f by γf for some $\gamma \in K^*$ leaves $\mathbf{O}(V)$ unchanged, and hence if we choose a basis for V and write $f = \alpha_1 \eta_1^2 + \alpha_2 \eta_2^2 + \alpha_3 \eta_3^2$, replace f by $(\alpha_1 \alpha_2 \alpha_3)f$, and set $-\alpha = \alpha_2 \alpha_3$, $-\beta = \alpha_3 \alpha_1$, we may assume f has the form $f = -\alpha\xi_1^2 - \beta\xi_2^2 + \alpha\beta\xi_3^2$. Comparing this with (1) we see that there is no loss in generality in assuming that V is the set of pure quaternions in the algebra $\mathbf{H}$. We also note that $s_C(X) = -CXC^{-1}$, and hence for each $t \in \mathbf{O}^+(V)$ we have $t(X) = TXT^{-1}$ where $T = CD$ if $t = s_C s_D$. If $\theta(t)$ denotes the spinor norm of t, we have $\theta(t) = N(T)K^{*2}$. It is easily seen that the epimorphism $\varphi : \mathbf{H}_1 \to \mathbf{O}'(V)$ given by $T \to TXT^{-1}$ has kernel $\{\pm 1\}$. We finally observe that $\mathbf{O}'(V) = \mathbf{\Omega}(V)$ since $\dim V = 3$. We shall use this epimorphism in the sequel.

3. The number $\mathbf{N}_a(b)$

Let $a, b \in \mathbf{\Omega}(V)$, and suppose $a \neq 1$. If there exists a positive integer n such that

$$b = \textstyle\prod_{i=1}^{n} t_i\, a^{\pm 1} t_i^{-1}, \qquad t_i \in \mathbf{\Omega}(V), \tag{2}$$

set $\mathbf{N}_a(b)$ = smallest n for which (2) is true. If (2) is false for all n, set $\mathbf{N}_a(b) = +\infty$. We shall give explicit formulas for $\mathbf{N}_a(b)$ when $K = \mathbf{R}$, the field of real numbers. We can reformulate our problem in terms of $\mathbf{H}_1$. Let $A, B \in \mathbf{H}_1$, $A \neq \pm 1$. If there exists a positive integer n such that

$$B = \textstyle\prod_{i=1}^{n} T_i\, A^{\pm 1}\, T_i^{-1}, \qquad T_i \in \mathbf{H}_1, \tag{3}$$

set $\mathbf{N}_A(B)$ = smallest positive integer such that (3) is true. If (3) is false for all n, set $\mathbf{N}_A(B) = +\infty$. Then if we adopt the convention that $n < +\infty$ for all positive integral n and apply our epimorphism φ, we immediately have

PROPOSITION 1. $\mathbf{N}_a(b) = \min\{\mathbf{N}_A(B), \mathbf{N}_A(-B)\}$ *where A and B are preimages of a and b respectively under φ.*

It will prove sufficient to consider the weaker condition

$$B = \textstyle\prod_{i=1}^{n} T_i\, A^{\pm 1}\, T_i^{-1}, \qquad T_i \in \mathbf{H}. \tag{4}$$

We define a number $\mathbf{V}_A(B)$ in an obvious manner and note that $\mathbf{V}_A(B) \leqq$

$\mathbf{N}_A(B)$. Because of the first part of Theorem 1, we see that (4) is equivalent to

$$B = \textstyle\prod_{i=1}^{n} A_i, \quad A_i \in \mathbf{H}_1, \quad S(A_i) = S(A) \quad \text{for} \quad i = 1, \cdots, n. \tag{5}$$

4. A factorization theorem in quaternion algebras

We first establish the following.

LEMMA 1. *Suppose C and D are pure quaternions such that*

$$N(C)\cdot N(CD - DC) \neq 0.$$

Then $1, C, CD - DC, C(CD - DC)$ *are linearly independent over* K, *and hence* $(C^2, (CD - DC)^2) \cong \mathbf{H}$.

Proof. Suppose

$$\alpha 1 + \beta C + \gamma(CD - DC) + \delta C(CD - DC) = 0. \tag{6}$$

Multiply (6) successively by $1, C, CD - DC, C(CD - DC)$, and take traces. One obtains a system of four homogeneous linear equations in $\alpha, \beta, \gamma, \delta$ whose coefficient matrix has determinant $2(N(C))^2(N(CD - DC))^2 \neq 0$. Thus $\alpha = \beta = \gamma = \delta = 0$, and we have linear independence. The remaining assertion follows from the fact that C and $CD - DC$ are pure and

$$C(CD - DC) = -(CD - DC)C.$$

We now prove a factorization theorem for elements of $\mathbf{H}_1$ from which all our subsequent results will follow.

THEOREM 2. *Let* $\alpha_1, \alpha_2 \in K$ *and* $B \in \mathbf{H}_1$ *satisfying* $S^2(B) \neq 4$. *There exist* $A_1, A_2 \in \mathbf{H}_1$ *such that*

(i) $B = A_1 A_2$,

(ii) $S(A_i) = \alpha_i$ *for* $i = 1, 2$

if and only if

$$(S^2(B) - 4, S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2) \cong \mathbf{H}$$

provided the left-hand side is defined. If

$$S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2 = 0,$$

then there always exist $A_1, A_2 \in \mathbf{H}_1$ *satisfying* (i) *and* (ii).

Proof. First suppose that $S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2 = 0$. Set

$$A_2 = \frac{\alpha_2}{2} + \left(\frac{2\alpha_1 - \alpha_2 S(B)}{4 - S^2(B)}\right)\left(B - \frac{1}{2} S(B)\right).$$

Then $A_2 \in \mathbf{H}_1$ and $S(A_2) = \alpha_2$. Set $A_1 = BA_2^c$. Then $A_1 \in \mathbf{H}_1$ and $S(A_1) = \alpha_1$. Since $B = A_1 A_2$, we are through.

We now assume that $S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2 \neq 0$ and prove necessity. $B = A_1 A_2$ implies $A_1 = BA_2^c$, and thus writing

$$A_1 = \alpha_1/2 + C_1, \qquad A_2 = \alpha_2/2 + C_2, \qquad B = S(B)/2 + C$$

with $S(C_1) = S(C_2) = S(C) = 0$, we obtain

$$\alpha_1/2 + C_1 = (S(B)/2 + C)(\alpha_2/2 - C_2);$$

hence $S(CC_2) = \alpha_2 S(B)/2 - \alpha_1$. Also $CC_2 - C_2 C = 2CC_2 - S(CC_2)$. Thus

$$\begin{aligned} N(CC_2 - C_2 C) &= 4N(C)N(C_2) - S^2(CC_2) \\ &= 4(1 - S^2(B)/4)(1 - \alpha_2^2/4) - (\alpha_2 S(B)/2 - \alpha_1)^2 \\ &= -(S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2). \end{aligned}$$

Since C and $CC_2 - C_2 C$ are pure and have nonzero norms,

$$(C^2, (CC_2 - C_2 C)^2) \cong \mathbf{H}$$

by our lemma. But $C^2 = (S^2(B) - 4)/4$, and

$$(CC_2 - C_2 C)^2 = S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2 .$$

Hence necessity is proved.

Now we prove sufficiency. By hypothesis, there exist pure quaternions $X, Y \in \mathbf{H}$ such that

$$X^2 = S^2(B)/4 - 1, \qquad Y^2 = S^2(B) - 4 + \alpha_1^2 - S(B)\alpha_1\alpha_2 + \alpha_2^2,$$
$$XY + YX = 0.$$

Set $B' = S(B)/2 + X$,

$$A_2' = \frac{\alpha_2}{2} + \left(\frac{\alpha_2 S(B) - 2\alpha_1}{S^2(B) - 4}\right) X + \frac{2XY}{S^2(B) - 4},$$

$A_1' = B'A_2'^{c}$. By direct calculation one shows that $B', A_1', A_2' \in \mathbf{H}_1$, $S(B') = S(B)$, $S(A_i') = \alpha_i$ for $i = 1, 2$, and of course, $B' = A_1' A_2'$. By Theorem 1, there exists $T \in \mathbf{H}$ such that $B = TB'T^{-1}$. Set $A_1 = TA_1' T^{-1}$, $A_2 = TA_2' T^{-1}$, and we have $B = A_1 A_2$ with $A_1, A_2 \in \mathbf{H}_1$ and $S(A_i) = \alpha_i$ for $i = 1, 2$ as desired.

5. Determination of $\mathbf{N}_a(b)$ when $K = \mathbf{R}$ and V is anisotropic

We may assume that f is positive definite. Then the quaternion algebra $\mathbf{H}$ is the classical quaternion algebra of Hamilton, and $(\lambda, \mu) \cong \mathbf{H}$ if and only if both λ and μ are negative. We also observe that $\mathbf{\Omega}(V) = \mathbf{O}^+(V)$ in this case. We now have

LEMMA 2. $\mathbf{N}_a(b) = \min\{\mathbf{V}_A(B), \mathbf{V}_A(-B)\}$ *where A and B are preimages of a and b respectively under φ.*

Proof. Since f is positive definite, we may replace T_i in (4) by $T_i/N(T_i)^{1/2}$ and obtain (3). Thus $\mathbf{N}_A(B) \leqq \mathbf{V}_A(B)$. Since $\mathbf{V}_A(B) \leqq \mathbf{N}_A(B)$ in general, $\mathbf{N}_A(B) = \mathbf{V}_A(B)$, and we are through by Proposition 1.

LEMMA 3. *Let $\alpha, \beta \in (-2, 2)$, and suppose $\alpha \neq 0, |\alpha| > (2 + \beta)^{1/2}$. For $x \in (-2, 2)$ define $2f(x) = |\alpha| x + [(\alpha^2 - 4)(x^2 - 4)]^{1/2}$. Set $f^{(0)}(x) = x$, $f^{(1)}(x) = f(x)$, and $f^{(k+1)}(x) = f(f^{(k)}(x))$ for $k = 1, 2, \cdots$. Then there exists a positive integer n such that $|\alpha| \leqq [2 + f^{(n)}(\beta)]^{1/2}$.*

Proof. Set $\beta_k = f^{(k)}(\beta)$. Thus $\beta_0 = \beta$. Now $|\alpha| > (2 + \beta_k)^{1/2}$ if and only if $\beta_{k+1} < |\alpha|$ as a simple calculation shows. Thus $\beta_1 < |\alpha|$. We shall establish the lemma by showing that the assumption $\beta_k < |\alpha|$ for all k leads to a contradiction. One easily verifies that $x < f(x)$ if $-2 < x < (2 + |\alpha|)^{1/2}$. Since $|\alpha| < (2 + |\alpha|)^{1/2}$, the sequence $\{\beta_k\}$ is strictly monotone increasing; hence $\lim_{k\to\infty} \beta_k$ exists. Set $\gamma = \lim \beta_k$, and note that $\gamma \leqq |\alpha|$. But $f(\gamma) = f(\lim \beta_k) = \lim f(\beta_k) = \lim \beta_{k+1} = \gamma$. If $\gamma < |\alpha|$, we get the contradiction $\gamma < f(\gamma)$. Hence $\lim \beta_k = |\alpha|$. Thus

$$
\begin{aligned}
0 &= \lim_{k\to\infty} (\beta_{k+1} - \beta_k) \\
&= \lim_{k\to\infty} \tfrac{1}{2}(|\alpha| \beta_k + [(\alpha^2 - 4)(\beta_k^2 - 4)]^{1/2}) - \beta_k = 2 - |\alpha|,
\end{aligned}
$$

whence $|\alpha| = 2$. But $\alpha \in (-2, 2)$ by hypothesis. This is our desired contradiction, and the lemma is proved.

THEOREM 3. *Let V be three-dimensional Euclidean space. Let $a, b \in \mathbf{O}^+(V)$ and $a \neq 1$. Let $\varphi(A) = a, \varphi(B) = b$ where $\varphi : \mathbf{H}_1 \to \mathbf{O}^+(V)$ is the epimorphism of §2. Of the two choices for B, assume B is chosen so that $S(B) \geqq 0$. Then $\mathbf{N}_a(b) = 1$ if $|S(A)| = |S(B)|$. $\mathbf{N}_a(1) = 2$. If $|S(A)| \neq |S(B)|$ and $b \neq 1$, $\mathbf{N}_a(b) = n + 2$ where n is the smallest nonnegative integer such that $|S(A)| \leqq [2 + f^{(n)}(S(B))]^{1/2}$. Here $f^{(n)}(x)$ has the same meaning as in Lemma 3, and $2f(x) = |S(A)| x + [(S^2(A) - 4)(x^2 - 4)]^{1/2}$.*

Proof. Setting $\alpha = S(A)$, $\beta = S(B)$, we compute $\mathbf{V}_A(B)$, temporarily ignoring the assumption $\beta \geqq 0$. Obviously $\mathbf{V}_A(B) = 1$ if and only if $|\alpha| = |\beta|$, so let us assume $|\alpha| \neq |\beta|$. We may also assume that $|\beta| \neq 2$, for $|\beta| = 2$ implies $B = \pm 1$, whence $b = 1$, and obviously $\mathbf{N}_a(1) = 2$. Since $|\beta| \neq 2, \beta^2 - 4 < 0$, and Theorem 2 tells us that $B = A_1 A_2$, A_1, $A_2 \in \mathbf{H}_1$, $S(A_i) = \alpha_i$ $(i = 1, 2)$ if and only if the point (α_1, α_2) lies in the interior or on the boundary of the ellipse $\mathbf{E}(\beta)$ defined by the equation

$$
x^2 - \beta xy + y^2 = 4 - \beta^2 \tag{7}
$$

in the (x, y) plane of elementary analytical geometry. As β varies, we obtain a one-parameter family of ellipses, all internally tangent to the square having corners $\pm(2, 2)$, $\pm(2, -2)$, and major axis the line $x = y$ when $\beta > 0$, and major axis the line $x = -y$ when $\beta < 0$. (Of course we have a circle when

$\beta = 0$.) Observe that $\mathbf{E}(\beta)$ touches the line $x = 2$ at the point $(2, \beta)$. Let us denote by $\Delta(\beta)$ the abscissa of the point in the first quadrant lying on both $\mathbf{E}(\beta)$ and the line $x = y$. Then we see that $\mathbf{V}_A(B) = 2$ if and only if $|\alpha| \leqq \Delta(\beta)$. If $|\alpha| > \Delta(\beta)$, we choose a point $(\alpha, (\operatorname{sgn}\alpha)\beta_1)$ on the line $x = \alpha$ and inside or on the boundary of $\mathbf{E}(\beta)$. Then by Theorem 2, we have

$$B = A_1 B_1, \qquad A_1, B_1 \in \mathbf{H}_1, \qquad S(A_1) = \alpha, \qquad S(B_1) = (\operatorname{sgn}\alpha)\beta_1 .$$

Can β_1 be chosen so that $B_1 = A_2 A_3$, $A_2, A_3 \in \mathbf{H}_1$, $S(A_2) = S(A_3) = \alpha$ (and hence $\mathbf{V}_A(B) = 3$)? We must have $|\alpha| \leqq \Delta(\beta_1)$. It is clear that the best choice for β_1 is the one that makes $\Delta(\beta_1)$ as large as possible. From the geometry of the situation, we see that this β_1 is determined as follows: $(\alpha, (\operatorname{sgn}\alpha)\beta_1)$ lies on $\mathbf{E}(\beta)$, and of the two possibilities we take that one having larger ordinate if $\alpha > 0$, and smaller ordinate if $\alpha < 0$ ($\alpha = 0$ is trivial). Analytically, $2\beta_1 = |\alpha|\beta + [(\alpha^2 - 4)(\beta^2 - 4)]^{1/2}$. If $|\alpha| \leqq \Delta(\beta_1)$, we are through, and $\mathbf{V}_A(B) = 3$. If not, we repeat the process on B_1. We continue in this way until we obtain our minimal factorization. Analytically this means the following. Set

$$2f(x) = |\alpha| x + [(\alpha^2 - 4)(x^2 - 4)]^{1/2},$$

and denote by $f^{(n)}(x)$ the n^{th} iterate of $f(x)$. Then $\beta_n = f^{(n)}(\beta)$ and $\Delta(\beta_n) = (2 + \beta_n)^{1/2}$. Hence $\mathbf{V}_A(B) = n + 2$ if n is the first iterate of $f(x)$ such that $|\alpha| \leqq [2 + f^{(n)}(\beta)]^{1/2}$. The existence of n is guaranteed by Lemma 3.

As one easily checks, $f(x)$ is strictly monotone increasing on $-2 < x < |\alpha|$, and $f(x) < |\alpha|$ if $|\alpha| > (2 + x)^{1/2}$. From these facts it is obvious that $\mathbf{V}_A(C_1) \geqq \mathbf{V}_A(C_2)$ if $S(C_1) < S(C_2)$. This is the reason for assuming $\beta = S(B) \geqq 0$, for now $\min\{\mathbf{V}_A(B), \mathbf{V}_A(-B)\} = \mathbf{V}_A(B)$. By Lemma 2 we are through.

Corollary 1. *$\mathbf{O}^+(V)$ is a simple group.*

Corollary 2. *$\mathbf{N}_a(b)$ is unbounded. Indeed if $b \neq 1$, $\mathbf{N}_a(b) \to \infty$ as $|S(A)| \to 2^-$. (See [2, p. 210].)*

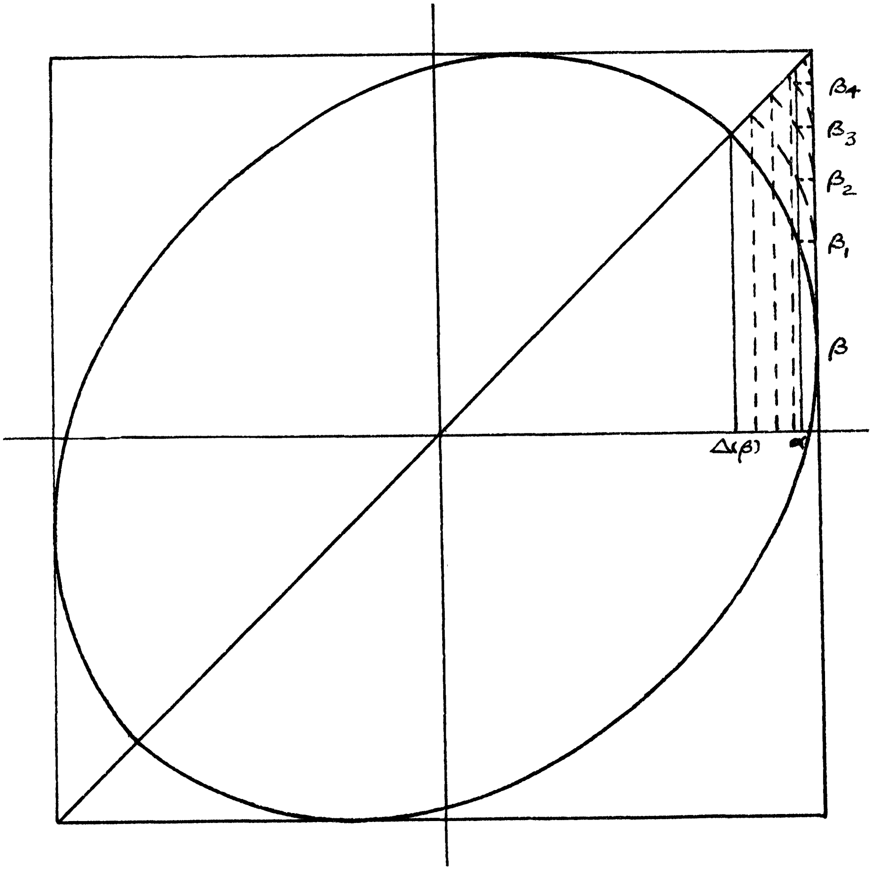
Proof. Adopting the notation of the proof of Theorem 3, we have

$$\beta_{k+1} - \beta_k = \tfrac{1}{2}((|\alpha| - 2)\beta_k + [(\alpha^2 - 4)(\beta_k^2 - 4)]^{1/2}) \to 0$$

as $|\alpha| \to 2^-$ for $k = 0, 1, \cdots$. Let α_0 be a real number such that $|\alpha_0| < 2$ and $\alpha_0^2 - 2 - \beta > 0$. ($\alpha_0$ exists since $|\beta| < 2$ by hypothesis.) Let n be a positive integer. Choose $\varepsilon > 0$ so small that $\alpha_0^2 - 2 - \beta > n\varepsilon$. Find α so close to 2 that $\beta_k - \beta_{k-1} < \varepsilon$ for $k = 1, \cdots, n$ and also $\alpha_0 \leqq \alpha < 2$. Then

$$\alpha^2 - 2 \geqq \alpha_0^2 - 2 > \beta + n\varepsilon = \beta_0 + n\varepsilon > \beta_0 + \textstyle\sum_{k=1}^{n} (\beta_k - \beta_{k-1}) = \beta_n .$$

Thus $\mathbf{N}_a(b) > n$. As n was arbitrary, we are through.



COROLLARY 3. *The smallest positive integer n such that $\mathbf{N}_a(b) \leqq n + 2$ for all b is the smallest positive integral n such that* $|S(A)| \leqq [2 + f^{(n)}(0)]^{1/2}$.

Proof. We observed in the proof of Theorem 3 that $\mathbf{V}_A(C_1) \geqq \mathbf{V}_A(C_2)$ if $S(C_1) < S(C_2)$. Since $S(B) \geqq 0$, the smallest possible value is $S(B) = 0$. Apply Theorem 3.

COROLLARY 4. $\alpha = 0$ *is the unique real number such that every quaternion of norm one can be written as the product of at most two quaternions of norm one and trace* α.

Proof. $\Delta(\beta) = (2 + \beta)^{1/2} \to 0$ as $\beta \to -2$. Let $|\alpha| > 0$. Then there exists β such that $|\beta| < 2$ and $|\alpha| > \Delta(\beta)$.

6. Determination of $\mathbf{N}_a(b)$ when $K = \mathbf{R}$ and V is isotropic

In this case the quaternion algebra $\mathbf{H}$ is $\mathbf{M}_2(\mathbf{R})$, and $(\lambda, \mu) \cong \mathbf{H}$ if and only if at least one of λ and μ is positive. We also observe that $\mathbf{\Omega}(V) = \mathbf{O}'(V)$

has index 2 in $\mathbf{O}^+(V)$ since $\mathbf{O}^+(V)/\mathbf{O}'(V)$ is isomorphic to $\mathbf{R}^*/\mathbf{R}^{*2}$ in this case.

LEMMA 4. $\mathbf{N}_a(b) = \min\{\mathbf{V}_A(B), \mathbf{V}_A(-B)\}$.

Proof. We must show that $\mathbf{N}_A(B) = \mathbf{V}_A(B)$. Since $\mathbf{V}_A(B) \leqq \mathbf{N}_A(B)$, we need only prove the reverse inequality. It will suffice to show that an equation of type (5) for a given n implies an equation of type (3) for the same n. Thus we must demonstrate the existence of $T_i \in \mathbf{H}_1$ such that $A_i = T_i A^{\pm 1} T_i^{-1}$ for $i = 1, \cdots, n$. (Incidentally $A^{-1} = A^c$ since $A \in \mathbf{H}_1$.) This will follow from the following identity:

$$N(A_i - A^c) + N(A_i - A) = 4 - S^2(A). \tag{8}$$

Thus suppose $S^2(A) \neq 4$. If $S^2(A) - 4 > 0$, then by (8) at least one of $N(A_i - A^c)$ and $N(A_i - A)$ is nonzero, and our T_i is guaranteed by Theorem 1(i). If $S^2(A) - 4 < 0$, then at least one of $N(A_i - A^c)$ and $N(A_i - A)$ is positive by (8), and again we have our T_i by Theorem 1(i). If $S^2(A) = 4$, then at least one of $N(A_i - A^c)$ and $N(A_i - A)$ is nonnegative by (8), and our T_i is guaranteed by Theorem 1(ii). This completes the proof.

THEOREM 4. *Let V be a three-dimensional isotropic space over* $\mathbf{R}$. *Let $a, b \in \mathbf{O}'(V)$ and $a \neq 1$. Let $\varphi(A) = a$, $\varphi(B) = b$ where $\varphi : \mathbf{H}_1 \to \mathbf{O}'(V)$ is the epimorphism of* §2. *Then* $\mathbf{N}_a(b) = 1$ *if* $|S(A)| = |S(B)|$. $\mathbf{N}_a(1) = 2$. *If* $|S(A)| \neq |S(B)|$ *and* $b \neq 1$,

$$\begin{aligned} \mathbf{N}_a(b) &= 2 \quad \textit{if} \quad S^2(B) > 4, \\ &\qquad \textit{or} \quad S^2(B) = 4 \quad \textit{and} \quad S(A) \neq 0, \\ &\qquad \textit{or} \quad S^2(B) < 4 \quad \textit{and} \quad |S(A)| \geqq [2 - |S(B)|]^{1/2}, \\ &= 3 \quad \textit{otherwise}. \end{aligned}$$

Proof. Suppose $S^2(B) \neq 4$. If $S^2(B) - 4 > 0$, then $\mathbf{V}_A(B) = 2$ by Theorem 2. If $S^2(B) - 4 < 0$, we are in the elliptical situation of Theorem 3, and we may use the same type of argument. However now we want our point in the exterior or on the boundary of $\mathbf{E}(\beta)$. Thus $\mathbf{V}_A(B) = 2$ if and only if $|\alpha| \geqq \Delta(\beta) = (2 + \beta)^{1/2}$. Of the two choices for B, the one with nonpositive trace gives us our minimum $\mathbf{V}_A(B)$ and hence the formula $|S(A)| \geqq [2 - |S(B)|]^{1/2}$. If this condition does not obtain, select $\gamma \in \mathbf{R}$ so large that $\gamma^2 - 4 > 0$ and $S^2(B) - 4 + S^2(A) - S(A)S(B)\gamma + \gamma^2 > 0$. Then $\mathbf{V}_A(B) = 3$ by Theorem 2.

Suppose $S^2(B) = 4$. Since $\mathbf{H} \cong \mathbf{M}_2(\mathbf{R})$, we shall use matrices. Of the two choices for B, select B so that $S(B) = -2$. Replacing B by a conjugate if necessary, we may assume

$$B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

If $S(A) \neq 0$, we have

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} S(A) & [2S(A)]^{-1} \\ -2S(A) & 0 \end{pmatrix} \begin{pmatrix} 0 & [2S(A)]^{-1} \\ -2S(A) & S(A) \end{pmatrix},$$

and $\mathbf{V}_A(B) = 2$.

If $S^2(B) = 4$ and $S(A) = 0$, we proceed as follows: replacing B by a conjugate if necessary, we may assume B has the form

$$\begin{pmatrix} \varepsilon & 1 \\ 0 & \varepsilon \end{pmatrix}$$

where $\varepsilon = \pm 1$. An obvious brute force calculation shows us that $\mathbf{V}_A(B) > 2$. Write

$$\begin{pmatrix} \varepsilon & 1 \\ 0 & \varepsilon \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ \mu & 0 \end{pmatrix} C$$

where λ, μ are to be chosen so that $\lambda\mu = -1$. Then

$$C = \begin{pmatrix} 0 & -\lambda\varepsilon \\ -\mu\varepsilon & -\mu \end{pmatrix}.$$

If we now choose μ so that $\mu^2 - 4 > 0$, we may apply our preceding results to C and obtain $\mathbf{V}_A(C) = 2$, and hence $\mathbf{V}_A(B) = 3$. By Lemma 4 we are through.

Corollary 5. $\mathbf{O}'(V) = \mathbf{\Omega}(V)$ *is a simple group.*

References

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, 1939.
2. E. Artin, *Geometric algebra*, New York, Interscience Publishers, 1957.
3. B. Pollak, *The equation $\bar{t}at = b$ in a composition algebra*, Duke Math. J., vol. 29 (1962), pp. 225–230.

Institute for Defense Analyses
Princeton, New Jersey
Syracuse University
Syracuse, New York