THE AUTOMORPHISM GROUP OF A COMPOSITION OF QUADRATIC FORMS

BY

C. RIEHM

ABSTRACT. Let $U \times X \to X$ be a (bilinear) composition $(u, x) \mapsto ux$ of two quadratic spaces $U$ and $X$ over a field $F$ of characteristic $\neq 2$ and assume there is a vector in $U$ which induces the identity map on $X$ via this composition. Define $G$ to be the subgroup of $O(U) \times O(X)$ consisting of those pairs $(\phi, \psi)$ satisfying $\phi(u)\psi(x) = \psi(ux)$ identically and define $G_x$ to be the projection of $G$ on $O(X)$. The group $G$ is investigated and in particular it is shown that its connected component, as an algebraic group, is isogenous to a product of two or three classical groups and so is reductive. Necessary and sufficient conditions are given for $G_x$ to be transitive on the unit sphere of $X$ when $U$ and $X$ are Euclidean spaces.

Let $U$ and $X$ be nondegenerate quadratic spaces over a field $F$ of characteristic $\neq 2$. We denote both of the quadratic forms by $q$, $q$: $U \to F$, $q$: $X \to F$. A composition of the two forms is a bilinear map $U \times X \to X$, $(u, x) \mapsto ux$ satisfying the identity $q(ux) = q(u)q(x)$.

We shall assume that there is a vector $u_0$ in $U$ satisfying $u_0x = x$ for all $x$.

Define an automorphism group

$$G = \{ (\phi, \psi) \in O(U) \times O(X) : \psi(ux) = \phi(u)\psi(x) \text{ for all } u \text{ and } x \}.$$ 

$O$ is the orthogonal group. Let $G_x$ be the projection of $G$ in $O(X)$. A. Kaplan has asked the following questions in the case when $U$ and $X$ are Euclidean spaces (i.e. $F = \mathbb{R}$, the real numbers, and both quadratic forms are positive definite).

(1) What kind of (algebraic) group is $G$?

(2) Is $G_x$ transitive on the unit sphere $X^* = \{ x \in X : q(x) = 1 \}$?

We shall answer (1) for any $F$ by showing, inter alia, that the connected component of $G$ is a group isogenous to the product of the spin group of $(V, -q)$ and of one or two classical groups (see Corollary to Theorem 4, and Theorems 1, 5–7). We also show (Theorems 8–11) that $G_x$ is transitive on $X^*$ (in the Euclidean case)

<table>
<thead>
<tr>
<th>Condition</th>
<th>$U$</th>
<th>$X$</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>$1, 2, 3$</td>
<td>when dim $U = 1, 2, 3$</td>
</tr>
<tr>
<td>iff $\lambda_1\lambda_2\lambda_3$ is a scalar transformation</td>
<td>$4$</td>
<td>when dim $U = 4$</td>
</tr>
<tr>
<td>iff dim $X = 8$</td>
<td>$6, 7, 8$</td>
<td>when dim $U = 6, 7, 8$</td>
</tr>
<tr>
<td>never</td>
<td>$5$ or $&gt; 9$</td>
<td>when dim $U = 5$ or $&gt; 9$</td>
</tr>
</tbody>
</table>

Received by the editors August 23, 1979 and, in revised form, September 12, 1980.

1980 Mathematics Subject Classification. Primary 10C05; Secondary 10C04.

Key words and phrases. Quadratic forms, composition of quadratic forms, algebraic groups, nilmanifolds.

1 Research supported by N.S.E.R.C. (Canada) grant A8778.
2 The group $G$ and question (2) are of interest for a certain class of nilmanifolds (see [6] and [7]).

© 1982 American Mathematical Society

TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 269, Number 2, February 1982

403
Here \( \lambda_u \) denotes the linear transformations \( x \mapsto ux \) of \( X \) for \( u \in U \), \( V \) is the orthogonal complement \( (F_{u_0})^\perp \) of \( u_0 \) in \( U \), and \( v_1, v_2, v_3 \) is any orthogonal basis of \( V \) (when \( \dim U = 4 \)).

A. Kaplan has also derived these theorems (unpublished) on transitivity when \( \dim U = 2 \) or \( \dim U = \dim X \). Also, D. B. Shapiro has independently given proofs (of a somewhat different nature) of some of these results, especially in the Euclidean case.

I am grateful to W. Rossmann for his generous help on some critical points and to D. B. Shapiro for several helpful conversations.

1. The basic result. If \( (\phi, \psi) \in G \), then \( \phi u_0 = u_0 \) so we may assume that \( G \subseteq O(V) \times O(X) \). We define

\[
G^+ = G \cap (O^+(V) \times O(X)).
\]

It is clearly \( G \) or a subgroup of index 2.

Consider the Clifford algebra \( C(V, -q) \) belonging to the quadratic form \(-q\) on \( V \). We also denote it by \( C \) or \( C(m) \). By the universal property of Clifford algebras, the map \( v \mapsto -v \) of \( V \) can be extended, first of all, to an involution of \( J \) of \( C \) and, secondly, to an involutory automorphism \( K \) of \( C \). Now define a "trace" \( \tau: C \to F \) by letting \( \tau(\alpha) \) be the trace of the linear map \( \beta \mapsto 2^{-m} \alpha \beta \) of \( C \) into itself so \( \tau(1) = 1 \) and \( \tau(\alpha \beta) = \tau(\beta \alpha) \). If \( v_1, \ldots, v_m \) is an orthogonal basis of \( V \), the \( 2^m \) products \( v_i \cdots v_k, 1 < i_1 < \cdots < i_k < m \), form a basis ("standard") of \( C \), each member of which, other than 1, has trace 0. Thus \( \tau(\alpha^J) = \tau(\alpha) \). Define

(1) \[
\gamma = v_1 v_2 \ldots v_m.
\]

We now show that

(1) The action \( x \mapsto vx \) of \( V \) on \( X \) can be extended to an action of \( C \) on \( X \) under which \( X \) is a \( C \)-module and such that (if \( f \) is the bilinearization of \( q \) on \( X \))

(2) \[
f(ax, y) = f(x, a^J y)
\]

for all \( x, y \) in \( X \) and \( a \) in \( C \).

(2) There is a unique nondegenerate hermitian form \( h: X \times X \to C \) making

\[
\begin{array}{ccc}
X \times X & \xrightarrow{f} & F \\
\downarrow h & & \\
C & \xrightarrow{\tau} & C
\end{array}
\]

commutative.

To prove (1), we note that \( X \) is a \( C \)-module satisfying \( f(vx, y) = f(x, -vy) \) for all \( x, y \) in \( X \) and \( v \) in \( V \) by Theorem 5.5 and Remark 5.7, Chapter 5 [8]. Then (1) follows by the definition of \( J \). Statement (2) follows from Theorem 22 [12] or 7.1, [5].

Note that the unitary group \( U(h) \) satisfies

\[
U(h) = O(X) \cap \text{End}_C X.
\]

The inclusion \( \subseteq \) is clear; if \( \phi \in O(X) \), then \( \tau h(\phi x, \phi y) = f(\phi x, \phi y) = f(x, y) \) so \( h(\phi x, \phi y) = h(x, y) \) by the uniqueness of \( h \), whence \( \supseteq \).
COMPOSITION OF QUADRATIC FORMS

405

The algebra $C$ has dimension $2^m$ and the subalgebra $C^+$ generated by the products $v_1w$ has dimension $2^{m-1}$. Furthermore as a vector space $C = C^+ \oplus C^-$ where $C^-$ is the subspace spanned by all odd products $v_1 \cdots v_{2k+1}$ of vectors. Define

$$
\Gamma = \{ \alpha \in C^+ \cup C^- : \alpha^2 = 1 \text{ and } \alpha V \alpha^{-1} = V \}, \quad \Gamma^+ = \Gamma \cap C^+.
$$

$\Gamma^+$ is the spin group of $(V, -q)$. We occasionally denote $\Gamma$ by $\Gamma(m)$, $\Gamma^+$ by $\Gamma^+(m)$. The canonical homomorphism $\rho: \Gamma \to O(V, q)$, $\rho(\alpha)v = \alpha v \alpha^{-1}$, satisfies

$$
\rho\Gamma^+ = O_0^+(V, q) = O_0^+(V, -q)
$$

where $O_0^+(V, q)$ is the "reduced orthogonal group" or "spinorial kernel" and is a subgroup of $O^+(V)$ (cf. n°5, 9 [2]). Note that

$$[\Gamma : \Gamma^+] = 1 \text{ or } 2.$$

The groups $\Gamma$ and $\Gamma^+$ are (the $F$-rational points of) algebraic groups. Over the algebraic closure of $F$, $\rho\Gamma^+ = O^+$ and $\rho\Gamma$ is $O$ or $O^+$ depending on the parity of $m$; the same is true when $U$ and $X$ are Euclidean. The kernel of $\rho$ (on $\Gamma^+$ or $\Gamma$) has order 2 or 4.

**Theorem 1.** The groups $\Gamma$, $\Gamma^+$, $U(h)$ and $G$ are the $F$-rational points of $F$-closed algebraic groups (hence defined over $F$ if $F$ is perfect). There is a homomorphism, rational over $F$,

$$
\theta: \Gamma \times U(h) \to G
$$

given by

$$
\theta(\alpha, \psi) = (\rho(\alpha), \alpha \psi)
$$

with central kernel of order 2 or 4 and satisfying

$$
[\theta(\Gamma^+ \times U(h))] < [O^+(V) : p\Gamma^+],
$$

(4)

where $O^+_0(V, q)$ is the reduced orthogonal group or spinorial kernel of $(V, q)$. Note that $O^+_0(V, q)$ is a subgroup of $O^+(V)$.

**Remark.** By the theorem, the projection $G_\nu$ of $G$ on the first factor in $O(V) \times O(X)$ contains the spinorial kernel $O^+_0(V)$. When $U$ (and $X$) are Euclidean $O^+_0(V) = O^+(V)$ which is transitive on the unit sphere in $V$ if $m > 2$; by a later result (Theorem 7), $G_\nu = \{ \pm 1 \} = O(V)$ when $m = 1$ so $G_\nu$ is transitive on the unit sphere here as well. These facts were also proved by A. Kaplan (unpublished). The transitivity, more generally, of $G_\nu$ can be investigated, in particular cases, by using knowledge of the orbits in $V$ of $O^+_0(V)$—in this regard see [11].

**Proof.** If $\alpha \in \Gamma$ then $(x \mapsto \alpha x) \in O(X)$ by (2) since $\alpha^2 = 1$. Thus $\text{im } \theta \subseteq O(V) \times O(X)$.

Suppose $(\phi, \psi) \in \Gamma \cap (\rho \Gamma \times O(X))$, say $\phi = \rho \alpha$. Then

$$
\alpha \psi \psi^{-1}(x) = \psi(\psi x)
$$

whence $\alpha^{-1} \psi \in (\text{End}_F X) \cap O(X) = U(h)$, $(\phi, \psi) = \theta(\alpha, \alpha^{-1} \psi)$, and (3) follows easily (note that $U(h)$ consists of $C$-endomorphisms of $X$ so $\Gamma$ and $U(h)$ commute in $\text{End}_F X$ and $\theta$ is a homomorphism). (4) follows similarly and the other statements are easily checked.
2. Determination of \( U(h) \). Assume \( F \) algebraically closed, let \( R \) be the matrix algebra \( F^n \) and let \( J \) be an involution on \( R \) of the first kind, i.e. \( J \) is the identity on \( F \). Then it is known that there is a symmetric or skew-symmetric matrix \( S \) such that \( AJ = S^{-1}(A)S \) for all \( A \) in \( R \) where \( \trans A \) is the transpose of \( A \). Since \( S \) is uniquely determined up to a scalar, we can say that \( J \) is of symmetric, resp. skew-symmetric, type.

**Theorem 2.** Let \( g: W \times W \to R \) be a nondegenerate hermitian form on the \( R \)-module \( W \) of finite length \( t \). Then the unitary group \( U(g) \) is isomorphic, as an algebraic group, to the orthogonal group \( O(t, F) \), resp. symplectic group \( \text{Sp}(t, F) \), if \( J \) is of symmetric, resp. skew-symmetric, type.

**Proof.** This is a special case of Morita theory—see Theorems 8.2 and 8.1 in [5]—although some additional checking is needed to see that the isomorphism is rational. The form \( h \) (in the notation of [5]) is a symmetric, resp. skew-symmetric, form on \( F^t \) whose adjoint is \( J \). A direct and elementary proof can be given as follows: Write \( W \) as a direct sum of \( R\omega_1, \ldots, R\omega_t \) where \( \omega_1, \ldots, \omega_t \) have annihilator equal to the ideal of matrices with zero first column. This enables one to identify \( \text{End}_R W \) with \( F^t \). It follows that \( e_i g(w_k, w_j) = 0 = g(w_k, w_j)e_i j \) when \( j > 2 \) where \( e_i j \) is the usual matrix unit, and then that \( g(w_k, w_j) = c_{kj}e_{11}, \text{ resp. } c_{kj}e_{12} \), where \( C = (c_{kj}) \) is symmetric, resp. skew-symmetric. It is easy to check that \( B \in U(g) \subset F^t \) iff \( \trans BCB = C \), whence the theorem.

The next theorem is known and has an elementary proof which we do not include. The context is again a finite-dimensional algebra \( R \) over an algebraically closed field \( F \) but this time \( R \) is a direct sum of two matrix algebras which the involution \( J \) interchanges.

**Theorem 3.** Let \( g: W \times W \to R \) be a nondegenerate hermitian form on the \( R \)-module \( W \) of finite length \( t \). Then \( t \) is even and the unitary group \( U(g) \) is isomorphic, as an algebraic group, to \( \text{GL}(\frac{1}{2}t, F) \).

Now we return to the main problem.

**Theorem 4.** Let \( F \) be algebraically closed, \( h: X \times X \to C \) the hermitian form in Theorem 1. Let \( \dim_F X = n \). As an algebraic group, \( U(h) \) is isomorphic to

\[
O(n^{-m/2}, F), \quad m \equiv 0, 6 \pmod{8},
\]
\[
\text{GL}(n^{-2(m-1)/2}, F), \quad m \equiv 1, 5 \pmod{8},
\]
\[
\text{Sp}(n^{-m/2}, F), \quad m \equiv 2, 4 \pmod{8},
\]
\[
\text{Sp}(n_2^{-2(m-1)/2}, F) \times \text{Sp}(n_1^{-2-(m-1)/2}, F), \quad m \equiv 3 \pmod{8},
\]
\[
O(n_2^{-2(m-1)/2}, F) \times O(n_1^{-2-(m-1)/2}, F), \quad m \equiv 7 \pmod{8}.
\]

When \( m \equiv 3 \) or \( 7 \pmod{8} \), \( n_1 \) and \( n_{-1} = n - n_1 \) are the dimensions of the eigensubspaces of \( X \) with respect to the linear transformation \( \gamma \) defined in (1).

It is understood that the fractions, such as \( n2^{-m/2} \), are all integers—this will follow from the fact that \( X \) is a \( C \)-module.
Proof. If \( u_1, \ldots, u_k \) are mutually orthogonal vectors in \( V \), \( (u_1 \cdots u_k)' = (-1)^{(k+1)/2} u_1 \cdots u_k \) where \([\ ]\) is the greatest integer function, whence (with \((\binom{m}{r}) = 0 = (\binom{m}{r})\) if \( r > m \) and \( C^{(J)} = \{ \alpha \in \mathbb{C} : \alpha' = \alpha \})

\[
\dim C^{(J)} = \sum_{k=0}^{\infty} \left( \binom{m}{4k+1} + \binom{m}{4k} \right) = \sum_{k=0}^{\infty} \binom{m+1}{4k}.
\]

By expanding the 4 binomial powers \((1 \pm 1)^{m+1}\) and \((1 \pm i)^{m+1}\) and adding, the last sum can be evaluated, giving

\[
\dim C^{(J)} = \frac{1}{4} \left( 2^{m+1} + 2(\sqrt{2})^{m+1}\cos((m+1)/4)\pi \right).
\]

But if \( J \) is any involution of the first kind on \( F\), \( \dim F^{(J)} \) is \( \frac{1}{2} l(l+1) \), resp. \( \frac{1}{2} l(l-1) \), if \( J \) is symmetric, resp. skew-symmetric. Thus if \( m = 2p \) the theorem follows from Theorem 2 since \( C \cong F_{2^p} \) and \( \dim X = 2^p \text{ len}_C X \).

Suppose \( m = 2p + 1 \) so \( C \cong F_{2^p} \times F_{2^p} \) with idempotents of the form \( e_1 = \frac{1}{2}(1 + ay) \), \( e_{-1} = \frac{1}{2}(1 - ay) \) for some scalar \( a \). The components of \( C \) are interchanged by \( J \) iff \( m \equiv 1 \) (mod 4) and then the theorem follows from Theorem 3. If \( m \equiv 3 \) (mod 4), \( X = e_1 X \perp e_{-1} X \) and the restrictions \( h_1 \) and \( h_{-1} \) of \( h \) to these two components are hermitian forms over \( F_{2^p} \). The rest of Theorem 4 now follows from Theorem 2 as in the case \( m = 2p \), taking into account that \( e_1 X \) and \( e_{-1} X \) are eigenspaces of \( y \).

Corollary. The connected component of the group \( G \) is a reductive algebraic group, isogenous via \( \theta \) to the connected component of \( \Gamma \times U(h) \), which is a product of two or three classical groups.

Proof. Over the algebraic closure of \( F \), \( \rho : \Gamma^+ \to O^+(V) \) is surjective and hence \( \theta : \Gamma^+ \times U(h) \to G^+ \) is surjective by (4), so \( \theta \) is an isogeny. The connected component of \( \Gamma \) is the spin group \( \Gamma^+ \) so the Corollary follows from Theorem 4.

We now generalize this to an arbitrary \( F \). Let \( D \) be the division algebra in the Brauer class of \( C \) if \( C \) is simple, otherwise in the Brauer class of \( C^+ \). This Brauer class is easily determined from the form \( f \) on \( V \), especially when \( F \) is a local or global field (see [8, Proposition 3.20 in Chapter 5, Theorem 3.6 in Chapter 4]). The \( l \)'s in Theorem 5 are easily determined from those given in Theorem 4 (by extending the scalars to an algebraic closure of \( F \)). The nature of \( J' \) and of \( h' \) (insofar as being hermitian, symmetric of skew-symmetric) follows from Theorem 4 and a knowledge of \( D \). The precise nature of \( h' \) is difficult to determine, but in the Euclidean case it is very easy (see Theorem 6).

Theorem 5. \( U(h) \) is isomorphic as an algebraic group to

\[
\begin{align*}
GL(l, D) & \quad \text{if } m \equiv 1 \text{ (mod 4) and } \gamma^2 \in F^2, \\
U(l_1, h') \times U(l_{-1}, h') & \quad \text{if } m \equiv 3 \text{ (mod 4) and } \gamma^2 \in F^2, \\
U(l, h') & \quad \text{otherwise,}
\end{align*}
\]

where the \( h' \)'s are hermitian, symmetric, or skew-symmetric forms.
This is proved in substantially the same way as Theorem 4, using Morita theory (cf. 2.4 in [9] and 8.2, 8.1 in [5]). Although this process may yield a skew-hermitian form \( h' \), it can be replaced by an hermitian form by scaling.

Let \( \mathbb{C} \) denote the complex numbers, \( \mathbb{H} \) the classical real quaternions.

**Theorem 6.** Suppose \( U \) and \( X \) are Euclidean and let \( h: X \times X \to \mathbb{C} \) be the hermitian form in Theorem 1. Let \( \dim_{\mathbb{R}} X = n \). As an algebraic group \( U(h) \) is isomorphic to

\[
\begin{align*}
O(n^2 - m/2, \mathbb{R}), & \quad m \equiv 0, 6 \pmod{8}, \\
U(n^2 - (m+1)/2, \mathbb{C}), & \quad m \equiv 1, 5 \pmod{8}, \\
U(n^2 - (m/2) - 2, \mathbb{H}), & \quad m \equiv 2, 4 \pmod{8}, \\
U(n_1^2 - (m+3)/2, \mathbb{H}) \times U(n_{-1}^2 - (m+3)/2, \mathbb{H}), & \quad m \equiv 3 \pmod{8}, \\
O(n_1^2 - (m-1)/2, \mathbb{R}) \times O(n_{-1}^2 - (m-1)/2, \mathbb{R}), & \quad m \equiv 7 \pmod{8},
\end{align*}
\]

where each symmetric and each hermitian form involved is positive definite, the involutions on \( \mathbb{C} \) and \( \mathbb{H} \) are the standard ones, and \( n_1 \) and \( n_{-1} \) are as defined in Theorem 4.

**Proof.** The group \( U(h) \) is a real form of the group \( U(h_c) \) where \( h_c \) is the hermitian form arising from the complexification \( U_c \times X_c \to X_c \) of the given real composition. Thus we can apply Theorem 4. Since \( U(h) \) is compact (as a closed subgroup of \( O(X) \)) and the groups listed in Theorem 4 have unique compact real forms, \( U(h) \) is as stated in Theorem 6 (cf. [13], e.g.). The dimensions can be derived from those in Theorem 4 by dividing by 1, 2 or 4 according as the division ring of coefficients is \( \mathbb{R} \), \( \mathbb{C} \) or \( \mathbb{H} \).

3. *F* algebraically closed, or \( U \) and \( X \) Euclidean. In this section we determine the index \([G : G^+]\) in these two cases. Table 1 is derived from [8, p. 131]. Put \( m = 2p \) when \( m \) is even, \( m = 2p + 1 \) when \( m \) is odd.

<table>
<thead>
<tr>
<th>( m \pmod{8} )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{C} )</td>
<td>( \mathbb{R}_2^p )</td>
<td>( \mathbb{C}_2^p )</td>
<td>( \mathbb{H}_{2^p-1} )</td>
<td>( \mathbb{H}<em>{2^p-1} \oplus \mathbb{H}</em>{2^p-1} )</td>
<td>( \mathbb{H}_{2^p-1} )</td>
<td>( \mathbb{C}_2^p )</td>
<td>( \mathbb{R}_2^p )</td>
<td>( \mathbb{R}_2^p \oplus \mathbb{R}_2^p )</td>
</tr>
<tr>
<td>( \dim_{\mathbb{R}} ) (simple module)</td>
<td>( 2^p )</td>
<td>( 2^{p+1} )</td>
<td>( 2^{p+1} )</td>
<td>( 2^{p+1} )</td>
<td>( 2^{p+1} )</td>
<td>( 2^p )</td>
<td>( 2^p )</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1.** Euclidean case

**Lemma 1.** Suppose that \( X \) is a simple \( \mathbb{C} \)-module and that either \( F \) is algebraically closed or \( U \) and \( X \) are Euclidean. Then every symmetric bilinear form \( f' \) on \( X \) satisfying

\[
f'(\alpha x, y) = f'(x, \alpha^* y)
\]

for all \( \alpha \) in \( \mathbb{C} \), \( x \) and \( y \) in \( X \), is of the form \( f' = \alpha f \) for some \( \alpha \in F \).

**Proof.** We prove only the Euclidean case; the proof when \( F \) is algebraically closed is similar and easier.
The map \( y \mapsto h(\cdot, y) \), \( X \to \text{Hom}_C(X, C) \), is bijective since \( h \) is nondegenerate. Let \( h' \) be the hermitian form satisfying \( \tau h' = f' \), and let \( \sigma \in \text{End}_C X \) be the composite of \( y \mapsto h'(\cdot, y) \) followed by the inverse of \( y \mapsto h(\cdot, y) \). Then

\[
h'(x, y) = h(x, \sigma y) \quad \text{for all } x \text{ and } y \quad \text{so also} \quad f'(x, y) = f(x, \sigma y).
\]

If \( C \cong \mathbb{C} \), then \( \sigma \in \text{cen} C = C \) since \( X \) is simple. Now \( \text{cen} C = \mathbb{R} + \mathbb{R}y \) and it is easy to see that \( J \) is complex conjugation on it; since we may assume \( f' \) is not identically 0, \( h'(x, x) \neq 0 \) for some \( x \) and since it and \( h(x, x) \) are \( J \)-symmetric, \( h'(x, x) = h(x, x)\sigma \) implies \( \sigma \in \mathbb{R} \). Thus \( f' = \sigma f \) as desired.

If \( C \cong \mathbb{R} \) or \( \mathbb{R} \oplus \mathbb{R} \), again \( \sigma \in \text{cen} C = \mathbb{R} \) or \( \mathbb{R} \oplus \mathbb{R} \) and it is easy to see that we may assume \( \sigma \in \mathbb{R} \) since \( X \) is simple.

Now suppose \( C \cong H \) or \( H \oplus H \). In the latter case, one of the components, say the first, acts nontrivially on \( X \) and the other acts as 0. Choose an orthonormal basis \( v_1, \ldots, v_m \) of \( V \) and consider the subalgebra \( C(2) \cong H \) of \( C \) generated by \( v_1 \) and \( v_2 \). The restriction of \( J \) to \( C(2) \) is the usual involution \( \alpha \to \bar{\alpha} \) of \( H \). If \( C \) is simple let \( C_1 = C \), otherwise let \( C_1 \) be the first simple component. Let \( D \) be the projection of \( C(2) \) on \( C_1 \). Since the centralizer \( D' \) of \( D \) in \( C_1 \) is \( \cong \mathbb{R} \) and \( D \otimes_\mathbb{R} D' \cong C_1 \) \([3, \text{Corollary of Theorem 2, 10}]\), there is a system of matrix units in \( C_1 \) so that \( C_1 = D_1 \). Thus we may suppose that \( X = D^l \) (column vectors), that \( C_1 = D_1 \) acts on \( X \) by left multiplication, and that \( \text{End}_C X = \text{End}_{D_1} X \) consists of right multiplication by \( D \); suppose in particular that \( \sigma(x) = xa \) for all \( x \) in \( D^l \), where \( a \in D \). We now define \( \tau \beta = \frac{1}{2}(\beta + \bar{\beta}) \) and get hermitian forms \( h_1 \) and \( h'_1 \) satisfying \( \tau h_1 = f \), \( \tau h'_1 = f' \). Since \( f'(x, y) = f(x, y\alpha) \), \( h'_1(x, y) = h_1(x, y\alpha) \) by the uniqueness of \( h'_1 \). Now we may assume \( f' \neq 0 \); since \( D^l \) has a basis lying in \( \mathbb{R}^l \), there exists \( x \) in \( \mathbb{R}^l \) with \( h'(x, x) \neq 0 \); since then \( xa = ax \), \( h'_2(x, x) = h_2(x, x)\bar{a} \) implies \( \alpha \in \mathbb{R} \).

Suppose \( F \) is algebraically closed or \( U \) and \( X \) are Euclidean. We know that \( [G : G^+] = 2 \) when \( m \) is even.

Now suppose \( m \) is odd, so \( \rho \Gamma = \rho \Gamma^+ = O^+(V) \). If \( G^+ \neq G \), there exists \( (\phi, \psi) \in G \) with \( \phi \notin O^+(V) \) and by Theorem 1 we may assume \( \phi = -1 \). Thus

\[
\psi(vx) = -\nu\psi(x)
\]

for all \( v \) in \( V \) and \( x \) in \( X \). Thus \( \psi \) is a \( K \)-linear map in \( O(X) \). Conversely if \( O(X) \) contains a \( K \)-linear map \( \psi \), then \( (-1, \psi) \in G \) and so \( G^+ \neq G \).

If \( C \) is not simple, it is the direct sum of two simple algebras \( C_1 \oplus C_2 \) and so any \( C \)-module \( X \) is \( = X_1 \oplus X_2 \) where \( X_1 = C_1X \) and \( X_2 = C_2X \) are the isotypic components of \( X \).

**Theorem 7.** Suppose \( F \) is algebraically closed or that \( U \) and \( X \) are Euclidean.

(a) If \( m \) is even,

\[
\theta(\Gamma^+ \times U(h)) = G^+, \quad \theta(\Gamma \times U(h)) = G, \quad [G : G^+] = 2.
\]

(b) If \( m \) is odd,

\[
\theta(\Gamma^+ \times U(h)) = \theta(\Gamma \times U(h)) = G^+.
\]

Moreover \( [G : G^+] = 2 \) except that \( G = G^+ \) in the following case: \( C \) is not simple and the isotypic components of \( X \) have different lengths.
PROOF. The canonical homomorphism \( \rho : \Gamma^+ \to O^+(V) \) is surjective (under the hypotheses), as are \( \rho : \Gamma \to O(V) \) when \( m \) is even and \( \rho : \Gamma \to O^+(V) \) when \( m \) is odd; the statements concerning the images of \( \theta \) now follow from Theorem 1, as does \([G : G^+] = 2\) when \( m \) is even. So assume \( m \) is odd.

Take \( \gamma = v_1 \cdots v_m \) where \( v_1, \ldots, v_m \) is an orthonormal basis of \( (V, q) \) so \( \gamma^2 = \pm 1 \). If \( C \) is not simple, \( K \) interchanges the simple components of \( C \) and so a \( K \)-linear automorphism of \( X \) maps each isotypic component of \( X \) bijectively on the other one; thus \( G^+ \neq G \) implies that the isotypic components have the same length.

To prove the necessity of the last condition of the theorem, we first assume that \( C \) is simple so we are in the Euclidean case and \( C \cong C_{2m} \). If \( Y \) is any \( C \)-submodule, its orthogonal complement with respect to \( f \) is also a \( C \)-module by (2) and so it suffices to show the existence of a \( K \)-linear map in \( O(X) \) in the case that \( X \) is simple. We may therefore suppose \( X = C^{2m} \) and we let \( x \mapsto \bar{x} \) be complex conjugation on the coordinates. Since \( K \) is complex conjugation on \( C = C \), the map \( A \mapsto A^K \) is a \( C \)-automorphism of \( C_{2m} \), hence an inner automorphism by the Skolem-Noether theorem, so \( A^K = BAB^{-1} \) for some \( B \in C_{2m} \). Thus \( \phi(x) = Bx \) is \( K \)-linear:

\[
\phi(Ax) = BAX = BAB^{-1} Bx = A^K \phi(x).
\]

Define \( f'(x, y) = f(\phi x, \phi y) \). It is easy to see that \( J \) and \( K \) commute (since they do so on \( V \)) and it follows easily that \( f'(ax, y) = f'(x, a'y) \) for all \( x, y, a \in C \). By Lemma 1, \( f' = af \) for some \( a \in R \), and since \( f' \) is also positive definite, \( a > 0 \). Therefore \( a^{-1/2} \phi \in O(X) \) and is \( K \)-linear.

Now suppose \( C = C_1 \oplus C_2 \). Since \( K \) interchanges the simple algebras \( C_1 \) and \( C_2 \), we may assume that \( C \) is the external direct sum \( C = D \oplus D \) of a simple algebra \( D \) with itself and that \( (d_1, d_2)^K = (d_2, d_1) \) for all \( (d_1, d_2) \in D \oplus D \). Now \( \gamma' = (-1)^{(m+1)/2} \gamma \) so each of \( C_1 \) and \( C_2 \) is stable under \( J \) if \( m \equiv 3 \) (mod 4), while if \( m \equiv 1 \) (mod 4), \( J \) interchanges \( C_1 \) and \( C_2 \).

Assume first that \( C_1 \) and \( C_2 \) are stable under \( J \) (this is always so when \( U \) is Euclidean since then \( C \) is simple when \( m \equiv 1 \) (mod 4)). Since \( J \) and \( K \) commute, the involutions induced by \( J \) on \( D \) through the two isomorphisms \( D \cong C_i \) are identical and are again denoted by \( J \). The \( X_i \) are orthogonal with respect to both \( f \) and \( h \): \( X = X_1 \perp X_2 \). Moreover \( h(X_i, X_i) \subseteq C_i \) for \( i = 1, 2 \). Write each of \( X_1 \) and \( X_2 \) as an orthogonal direct sum of orthogonally indecomposable submodules. By [9, 2.4, 2.5(b)], each of these indecomposable submodules is a simple \( D \)-module, or each is a hyperbolic plane, i.e. is \( \cong Y \oplus Y^* \) where \( Y \) is simple, \( Y^* \) is its dual made into a left \( D \)-module via \( a \eta = \eta a' \) (\( \eta \in Y^* \), \( a \in D \)) and the hermitian form on it is \( h(y + \eta, y' + \eta') = \langle y, \eta' \rangle + \langle y', \eta \rangle \cdots \). We note that in the Euclidean case, only the first case can occur since the restriction of \( f \) to any simple submodule is nondegenerate, hence so also for \( h \). Using Lemma 1 and \( \text{len } X_1 = \text{len } X_2 \), we can now easily construct a \( K \)-linear isometry in \( O(X) \) by pairing off the indecomposables of \( X_1 \) with those of \( X_2 \) and choosing a \( D \)-isometry between the modules in each pair (in the case when indecomposables are simple, such isometries can be shown to exist using Lemma 1 in the same way as in the previous case of \( C \) simple).
Finally suppose $C_1$ and $C_2$ are not stable under $J$, so $C_1^J = C_2$, $C_2^J = C_1$, and $F$ is algebraically closed. Since $h(C_1x, C_1y) = C_1h(x, y)C_1^J = 0$, it follows that $h(X_1, X_1) = 0 = f(x_1, x_1)$. One can make $X_1$ into a $C_2$-module rather than a $C_1$-module by defining $\alpha_2 \cdot x_1 = \alpha_2 x_1$. It has the same length as a $C_2$-module as a $C_1$-module, hence has the same length as $X_2$. We can therefore find a $K$-linear isomorphism $\phi_1: X_1 \rightarrow X_2$. Now the map $X_1 \rightarrow X_2^*$ given by $y_1 \mapsto h(\phi_1 \cdot y_1)$ is $JK$-linear; since $h$ is nondegenerate it is injective and hence bijective. Similarly $x_2 \mapsto h(\cdot, x_2)$ is a $J$-linear isomorphism $X_2 \rightarrow X_2^*$. Thus there is a unique $y_1 =: \phi_2(x_2)$ in $X_1$ so that

$$h(\phi_1 x_1, \phi_2 x_2)^K = h(x_1, x_2)$$

for all $x_1 \in X_1$, $x_2 \in X_2$. Uniqueness implies that $\phi_2: X_2 \rightarrow X_1$ is $K$-linear, hence a $K$-isomorphism.

Define $\phi = \phi_1 \oplus \phi_2: X \rightarrow X$. Application of $\tau$ to (6) yields $f(\phi_1 x_1, \phi_2 x_2) = f(x_1, x_2)$ for all $x_1 \in X_1$ and $x_2 \in X_2$, and so $\phi$ is a $K$-linear isometry in $O(X)$.

4. $U$ and $X$ Euclidean. In this section, the transitivity of $G_X$ on the unit sphere $X^*$ is investigated; we assume throughout that $U$ and $X$ are Euclidean. Let $G_X^+$ be the projection of $G^+$ on $O(X)$. By Theorem 7

$$G_X^+ = \Gamma^+ U(h) = \Gamma U(h) \quad \text{when } m \text{ is odd},$$

$$G_X^+ = \Gamma^+ U(h), \quad G_X = \Gamma U(h) \quad \text{when } m \text{ is even}.$$  

The projection $G \rightarrow G_X$ is actually an isomorphism. For if $(\phi, 1) \in G$, then $\nu x = \phi(\nu)x$ so $(\phi(\nu) - \nu)x = 0$ for all $\nu$ and $x$; since $(V, f)$ is nondegenerate and $f(\nu x, u' x) = f(\nu, u')q(x)$ (see [8, (5.4), Chapter 5]), $\phi$ is the identity.

**Lemma 2.** $G_X$ is transitive on $X^*$ if and only if $G_X^+$ is transitive on $X^*$. Let $G_X^+ x$ be any orbit of $G_X^+$ on $X^*$. Then $G_X$ is transitive on $X^*$ if and only if the dimension of $G_X^+ x$ (as a real manifold) is equal to $\dim X^* = \dim X - 1$.

**Proof.** That $G_X^+ x$ and $G_X x$ are regular submanifolds of $X^*$ follows from the compactness of $G_X^+$ and $G_X$ (continuous images of $G^+$ and $G$ which are closed subsets of the compact group $O(V) \times O(X)$). Clearly $G_X$ is transitive on $X^*$ if $G_X^+$ is. Conversely suppose $G_X x = X^*$. Now $G_X^+ x$ is closed and is also open since $[G_X : G_X^+] < \infty$ (in fact $< 2$) implies that $\dim G_X^+ x = \dim G_X x = \dim X^*$. Thus $G_X^+ x = X^*$ since $X^*$ is connected.

Now if $\dim G_X^+ x < \dim X^*$, $G_X^+$ is not transitive so neither is $G_X$. If $\dim G_X^+ x = \dim X^*$, then the argument above using the connectivity of $X^*$ yields $G_X^+ x = X^*$, hence $G_X x = X^*$.

**Theorem 8.** Suppose $G_X$ is transitive on $X^*$. Then $X$ is an isotypic $C$-module if $m = 3$, and is a simple $C$-module if $m \geq 4$.

**Proof.** $C(3) \cong H \oplus H$ and if $m \geq 4$, $C(4)$ is a matrix algebra which is not a division algebra or is the direct sum of two such algebras (see Table 1). Suppose $X$ is not isotypic when $m = 3$ or is not simple when $m \geq 4$. Then it contains nonzero vectors (and so also unit vectors, by scaling) with annihilators in $C$ of different
dimensions. The elements of $\Gamma$, being units in $C$, preserve the dimension of annihilators as they operate on $X$. The same is true of transformations in $U(h)$ since they are $C$-linear automorphisms of $X$. Thus $G_x^+$ is not transitive on $X^*$ by (7), so neither is $G_x$ by Lemma 2.

**Theorem 9.** $G_x$ is not transitive on $X^*$ if $m = 4$ or $m > 8$.

**Proof.** By Theorem 8 we may assume $X$ is simple so, by Table 1, $\dim X^* = 2^p - 1$ if $m \equiv 0, 6$ or $7 \pmod{8}$, while $\dim X^* = 2^{p+1} - 1$ if $m \equiv 1, 2, 3, 4$, or $5 \pmod{8}$. On the other hand, $\dim \Gamma^+ = \dim O^+(V) = \frac{1}{2}m(m-1)$ [4, Proposition 6, Chapter I, §1I]. Since $X$ is simple, $\text{Aut}_C X = R^\times, C^\times$ or $H^\times$ and so is a connected real algebraic group of dimension $< 4$. The subgroup $U(h)$ is a closed algebraic subgroup of $\text{Aut}_C X$ and is proper since, e.g. $U(h) \cap R^\times = \pm 1$. Thus $\dim U(h) < 3$ so $\dim G_x^+ = \dim \Gamma^+ U(h) < \frac{1}{2}m(m-1) + 3$. Thus any orbit of $G_x^+$ has dimension $< \frac{1}{2}m(m-1) + 3$ and it is straightforward to check that this in turn is $< \dim X^*$ when $m > 10$. Thus $G_x$ is not transitive on $X^*$ when $m > 10$ by Lemma 2.

Suppose that $m = 4, 8$ or $9$. Now $C^+(m) \simeq C(m - 1)$ by [8, Corollary 2.10, Chapter 5], so Table 1 shows that a simple $C^+$-module has half the dimension of a simple $C$-module and so $X$ is the direct sum of two simple $C^+$-modules. Each of the latter is stable under $\Gamma^+$ so $\Gamma^+$ has an orbit on $X^*$ of dimension $< \frac{1}{2}\dim X - 1$, so $G_x^+ = \Gamma^+ U(h)$ has an orbit of dimension $< \frac{1}{2}\dim X + 2$. Since $\dim X > 8$, this is $< \dim X^*$ so $G_x^+$ and $G_x$ are not transitive by Lemma 2.

**Theorem 10.** $G_x$ is transitive on $X^*$ if $m = 0, 1$ or $2$, or if $X$ is isotypic and $m = 3$.

**Remark.** When $m = 3$, $C \simeq H \oplus H$. Let $v_1, v_2, v_3$ be an orthonormal basis of $(V, f)$ and put $\gamma = v_1 v_2 v_3$ as usual. Then $\gamma^2 = 1$, and $X$ is isotypic iff $\gamma$ operates as $1$ or $-1$ on all of $X$, hence iff $u_1 u_2 u_3$ is a scalar transformation on $X$, where $u_1, u_2, u_3$ is an arbitrary orthogonal basis of $V$.

**Proof.** If $m = 0$, $G = \{1\} \times O(X)$ so $G_x = O(X)$ and is transitive on $X^*$ by Witt’s theorem. If $m = 1$, $C(1) \simeq C$ with $J =$ complex conjugation. Furthermore $\tau(a + bi) = a$ so it follows that $h$ is a (positive definite) complex hermitian form on $X$ with the same unit sphere as $f$. By Witt’s theorem, $U(h)$ is transitive on $X^*$, hence so is the larger group $G_x$. A similar argument works when $m = 2$ for then $C(2) \simeq H$ with $J =$ the usual conjugation and $\tau(a + bi + cj + dk) = a$; thus $h$ is a (positive definite) quaternionic hermitian form.

Finally suppose $m = 3$. Let $v_1, v_2, v_3$ be an orthonormal basis of $V$, $\gamma = v_1 v_2 v_3$, and let $C(2)$ be the Clifford algebra of the subspace $Ru_1 + Ru_2$. Then $C(3) = C(2)\epsilon_1 \oplus C(2)\epsilon_{-1}$ with $\epsilon_1 = \frac{1}{2}(1 + \gamma)$ and $\epsilon_{-1} = \frac{1}{2}(1 - \gamma)$ the orthogonal idempotents. Now $J$ fixes each $\epsilon_i$ and induces the standard involution on $C(2)$. Moreover $h$ can be considered as a hermitian form over one of the factors $C(2)e_i \approx H$ and since the 2-sphere of $h$ equals the unit sphere of $f$ (as is easily checked), $U(h)$ is once more transitive on $X^*$ by Witt’s theorem, hence also $G_x$.

**Theorem 11.** Let $m = 5, 6$ or $7$. Then $G_x$ is transitive on $X^*$ if and only if $\dim X = 8$. 

Proof. The necessity follows from Theorem 8 and Table 1. By Theorem 1 the sufficiency will be proved once we show that $\Gamma^+(5), \Gamma^+(6)$ and $\Gamma^+(7)$ are transitive on $X^* = S^7$. It is enough to do this for $\Gamma^+(5)$. Indeed we may suppose $C(5) \subset C(6) \subset C(7)$. Then $C(5)$ satisfies the adjointness condition (2) with respect to both $f(5)$ and $f(7)$ whence $f(7)$ is a scalar multiple of $f(5)$, so we can assume $f(7) = f(5)$ by Lemma 1. Similarly $f(6) = f(5)$ so the three unit spheres are identical. And $\Gamma^+(5) \subset \Gamma^+(6) \subset \Gamma^+(7)$.

What we must show then is that $\Gamma^+(5) (= \text{Spin}_5)$ is transitive on $S^7$ under the spin representation. This is evidently a well-known fact (cf. [10, Theorem IV]) but I have not been able to find a reference (with a proof). We sketch briefly an elementary proof (cf. [1, §§3, 4, Chapter VIII]). In $C_2$ define

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = iJ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and in $\otimes^3 C_2 \cong C_8$ define

$$V_1 = I \otimes E \otimes E, \quad V_2 = K \otimes I \otimes E, \quad V_3 = K \otimes K \otimes I, \quad V_4 = J \otimes E \otimes E, \quad V_5 = K \otimes J \otimes E.$$ 

The $V_i$ anticommute and satisfy $V_i^2 = -1$ so we obtain a representation $C(5) \rightarrow C_8$. Define

$$Y = \sum C(e_1 \otimes e_2 \otimes e_3) \subset \otimes^3 C^2 \cong C^8$$

where the sum runs over all choices of $e_1, e_2, e_3$ from $\{1, 0\}$ with exactly 0 or 2 of the three equal to $1$. It is easy to see that $Y$ is a $C$-module, and so since $\dim Y = 8$, we may take $X = Y$.

$\mathfrak{o}(5) = \sum_{j < k} \mathbf{R} V_j V_k$ is the image of the Lie algebra of $\Gamma^+$ in $C_8$. A calculation shows that $\mathfrak{o}(5)e$, where $e = (1) \otimes (1) \otimes (1)$, has (real) dimension 7, so the annihilator of $e$ in $\mathfrak{o}(5)$ has dimension $10 - 7 = 3$, so the stabilizer of $e$ in $\Gamma^+$ has dimension 3 (as a real Lie group) so the orbit $\Gamma^+e$ has dimension 7. Since some scalar multiple of $e$ is on $X^* = S^7$, the theorem follows by Lemma 2.

References


Department of Mathematical Sciences, McMaster University, Hamilton, Ontario L8S 4K1 Canada