ON THE STRUCTURE OF UNITARY GROUPS

BY
JEAN DIEUDONNÉ

1. Let $K$ be an arbitrary sfield with an involution $J$, that is, a one-to-one mapping $\xi \rightarrow \xi'$ of $K$ onto itself, distinct from the identity, such that $(\xi + \eta)' = \xi' + \eta'$, $(\xi \eta)' = \eta' \xi'$, and $(\xi')' = \xi$. Let $E$ be an $n$-dimensional right vector space over $K$ $(n \geq 2)$; an hermitian (resp. skew-hermitian) form over $E$ is a mapping $(x, y) \rightarrow f(x, y)$ of $E \times E$ into $K$ which, for any $x$, is linear in $y$, and such that $f(y, x) = f(x, y)'$ (resp. $f(y, x) = -f(x, y)'$). This implies that $f(x, y)$ is additive in $x$ and such that $f(xa, y) = \lambda f(x, y)$. The values $f(x, x)$ are always symmetric (resp. skew-symmetric) elements of $K$, that is, elements $\alpha$ such that $\alpha = 0$ (resp. $\alpha' = -\alpha$). The orthogonality relation $f(x, y) = 0$ relative to $f$ is always symmetric.

We shall always suppose that the form $f$ is nondegenerate, or in other words that there is no vector in $E$ other than 0 orthogonal to the whole space. Moreover, when the characteristic of $K$ is 2, the distinction between hermitian and skew-hermitian forms disappears, and $f(x, x)$ is symmetric for every $x \in E$; in that case we shall make the additional assumption that $f(x, x)$ has always the form $\xi + \xi' = f(x, x)$ ("trace" of $\xi$) for a convenient $\xi \in K$; this assumption is automatically verified when the restriction of $J$ to the center $Z$ of $K$ is not the identity, but not necessarily in the other cases.

A unitary transformation $u$ of $E$ is a one-to-one linear mapping of $E$ onto itself such that $f(u(x), u(y)) = f(x, y)$ identically; these transformations constitute the unitary group $U_n(K, f)$. In a previous paper [5, pp. 63–82]¹, I have studied the structure of that group in the two simplest cases, namely those in which $K$ is commutative, or if is a reflexive sfield and the form $f$ is hermitian; the present paper is devoted to the study of $U_n(K, f)$ in the general case.

2. We shall need the following lemma:

LEMMA 1. If the sfield $K$ is not commutative, it is generated by the set $S$ of the symmetric elements, except when $K$ is a reflexive sfield of characteristic $\neq 2$, and $S$ is identical with the center $Z$ of $K$.

Let $L$ be the subsfield of $K$ generated by $S$; we are going to prove that if $L$ is not contained in $Z$, then $L = K$. Suppose the contrary, and let $\alpha$ be an element in $K$ not belonging to $L$; let $M$ be the 2-dimensional right vector space over $L$ having 1 and $\alpha$ as a basis; we are going to prove that $M$ is a sfield. We first notice that $L$ is identical with the subring of $K$ generated by $S$;

¹ Numbers in square brackets refer to the bibliography at the end of the paper.

Received by the editors August 14, 1951.
for if $\xi \neq 0$ is an element of that subring, it is clear that $\xi'$ also belongs to it; but $\xi'\delta^0 = \delta$ is in $S$, hence $\xi^{-1} = \xi'^{-1} \delta^{-1}$ belongs to the ring generated by $S$, which proves that $L$ is identical with that ring. We next notice that $\alpha \delta = \beta \in S \subseteq L$, and $\alpha \delta = -\alpha^2 + \alpha \beta = \gamma \in L$ and therefore $\alpha^2 = \alpha \beta - \gamma$. On the other hand, if $\xi$ is any element in $S$, $\alpha \xi + (\alpha \xi)\delta = \alpha \xi + \xi \delta$ is in $L$, and therefore $\alpha \xi - \xi \alpha$ is in $L$; by induction on $k$, it follows that if $\xi = \xi_1 \xi_2 \cdots \xi_k$, the element $\alpha \xi - \xi \alpha$ is in $L$. These remarks prove that $M$ is a subring of $K$, invariant by the involution $J$, and the same argument as the one made for $L$ proves that $M$ is a subfield. Now for any $\xi \in L$, $\alpha \xi + (\alpha \xi)\delta = \alpha \xi + \xi \delta$ is in $S \subseteq L$, and replacing $\delta$ by its value shows that $\alpha \xi - \xi \alpha$ is in $L$; but as $\xi'\alpha - \alpha \xi'$ also belongs to $L$, we see that $\alpha (\xi - \xi')$ is in $L$; this is of course possible only when $\xi = \xi'$. In other words, we come to the conclusion that $L = S$; in particular, if $\xi$ and $\eta$ are any two elements of $S$, $\xi \eta$ is in $S$, and therefore $(\xi \eta)\delta = \eta \xi' = \eta \xi$ is equal to $\xi \eta$; this means that $L$ is a commutative field.

To go on with the argument, let us first suppose that the characteristic of $K$ is $\neq 2$; then, as $\alpha = (\alpha + \alpha')/2 + (\alpha - \alpha')/2$, $\alpha - \alpha'$ is not in $L$, and we can replace $\alpha$ by $\alpha - \alpha'$ in the preceding sequence of arguments. We then have $\alpha' = -\alpha$, and $\alpha^2 = -\gamma \in L$. The mapping $\xi \mapsto \alpha \xi - \xi \alpha$ is a derivation of the field $L$; if we put $D\xi = \alpha \xi - \xi \alpha$, we have $D^2\xi = \alpha^2 \xi - 2\alpha \xi^2 \xi + \xi^2 \xi \xi \in L$ for every $\xi \in L$, which gives $\alpha \xi \alpha \in L$, since the characteristic of $L$ is $\neq 2$. But we may write $\alpha \xi$ and as $\alpha^2 \xi \in L$, this gives $\alpha \cdot D\xi \in L$, which is possible only if $D\xi = 0$ for every $\xi \in L$. This proves that every element $\alpha \in K$ commutes with every element of $L$, in other words, that $L$ is in the center of $K$, contrary to assumption.

We next take up the case in which the characteristic of $K$ is 2. From the relation $\alpha^2 = \alpha \beta - \gamma \alpha = \alpha \beta - \alpha \gamma$, one derives immediately $D\beta = D\gamma = 0$, in other words, $\beta$ and $\gamma$ commute with $\alpha$; replacing $\alpha$ by $\beta^{-1} \alpha$, we can therefore suppose that $\alpha^2 = \alpha + \gamma$, with $D\gamma = 0$. Let $N$ be the subfield of $L$ defined by the equation $D\xi = 0$ (commuting subfield of $\alpha$ or center of $M$). The relation $\alpha^2 = \alpha + \gamma$ implies that $D^2\xi = D\xi$ for every $\xi \in L$, or in other words, that $\xi + D\xi \in N$ for all $\xi \in L$. On the other hand, $D(\xi^2) = 2\xi \cdot D\xi = 0$ because the characteristic is 2, hence $\xi^2 \in N$ for $\xi \in L$. Now, if $\xi = \alpha \xi + \eta$ is any element of $M$, with $\xi \in L$ and $\eta \in L$, an easy computation shows that $\xi' = \gamma \xi^2 + \xi^2 \xi + D(\xi \eta) + \eta^2$ and therefore $\xi' \in N$; on the other hand $\xi + \xi' = \xi + D\xi$ is also in $N$. If $N \neq L$, this means that $M$ is a reflexive sfield over its center $N$ [5, p. 72]. But in a reflexive sfield of characteristic 2, the symmetric elements constitute a 3-dimensional subspace over the center, whilst here they are the elements of $L$, which is only 2-dimensional over $N$; the assumption $N \neq L$ is therefore untenable. But if $N = L$, $\alpha$ commutes again with every element of $L$, in other words, $L$ is again the center of $K$, contrary to assumption.

We have still to examine the exceptional case in which $S$ is contained in $Z$. For every element $\xi \in K$, $\xi + \xi'$ and $\xi \xi'$ are then in the center $Z$, and therefore, as $\xi^2 - (\xi + \xi')\xi + \xi \xi' = 0$, every element of $K$ has degree 2 over the center.
Z. It is well known that this is possible only if \( K \) has rank 4 over \( Z \). Moreover if \( \gamma \in Z \) and \( \gamma' \) is not in \( Z \), \( \gamma' + (\gamma')^\prime = \gamma (\gamma + \gamma') + (\gamma' - \gamma)\gamma' \) is in \( Z \), which implies \( \gamma' = \gamma \); this shows that \( K \) is a reflexive field [5, p. 72], and \( S = Z \); but this is possible only when \( K \) has a characteristic \( \neq 2 \) (loc. cit.), and that completes the proof of Lemma 1.

3. From the involution \( J \), we can deduce other involutions \( T \) of \( K \) by the general process of setting \( \xi^T = p^{-1} p' \xi p \), where \( p \) is a symmetric or skew-symmetric element of \( K \) (with respect to \( J \)); if \( p' = \epsilon p \) (\( \epsilon = 1 \) or \( \epsilon = -1 \)), the relation \( \xi^T = \xi \) is then equivalent to \( p\xi = \epsilon (p\xi)^T \); in other words, the \( T \)-symmetric elements of \( K \) are of the form \( p^{-1} \eta \), where \( \eta \) is \( J \)-symmetric if \( \epsilon = 1 \) and \( \eta \) is \( J \)-skew-symmetric if \( \epsilon = -1 \). This enables one to reduce to each other the hermitian and skew-hermitian forms, by a change of the involution (when the characteristic of \( K \) is not 2). Indeed, if \( f(y, x) = -(f(x, y))^T \), consider the form \( g(x, y) = p^{-1} f(x, y) \), where \( p \) is skew-symmetric; then \( g \) is linear in \( y \), and one has \( g(y, x) = -p^{-1} (f(x, y))^T = -p^{-1} (pg(x, y))^T = g(x, y)^T \). For the sake of convenience, we shall always suppose in the following that the form \( f \) is skew-hermitian for \( J \).

The notions of orthogonal basis, of isotropic vector, of isotropic and totally isotropic subspaces of \( E \) are defined as usual (see [5]); the index \( v \) of \( f \) is the maximum dimension of the totally isotropic subspaces, and one has \( 2v \leq n \). When a plane \( P \subset E \) is not totally isotropic but contains an isotropic vector \( a \neq 0 \), then there exists in \( P \) a second isotropic vector \( b \) such that \( f(a, b) = 1 \); \( P \) is then said to be a hyperbolic plane, and the restrictions of \( f \) to any two hyperbolic planes are equivalent. Moreover, Witt's theorem is still valid (see [6, pp. 8–9]); in the case of characteristic 2, this, as well as the preceding property, is due to the restrictive assumption on \( f \) to be "trace-valued"); we shall formulate it in the following form: if \( V \) and \( W \) are any two subspaces of \( E \) such that the restrictions of \( f \) to \( V \) and \( W \) are equivalent, then there is a unitary transformation \( u \) such that \( u(V) = W \).

4. Let us recall that a transvection is a linear transformation of the type \( x \rightarrow x + a \rho(x) \), where \( \rho \) is a linear form, not identically 0, and such that \( \rho(a) = 0 \). If we write that such a transformation is unitary, we get

\[(\rho(x))^T f(a, y) + f(x, a) \rho(y) + (\rho(x))^T f(a, a) \rho(y) = 0\]

identically in \( x \) and \( y \); with \( x = a \) this gives \( f(a, a) \rho(y) = 0 \), hence \( f(a, a) = 0 \), the vector \( a \) must be isotropic; then we get

\[(\rho(x))^T f(a, y) + f(x, a) \rho(y) = 0\]

which, for fixed \( x \) such that \( \rho(x) \neq 0 \), shows that \( f(x, a) \neq 0 \), and \( \rho(y) = \lambda f(a, y) \); finally, we have

\[(f(a, x))^T \lambda f(a, y) + f(x, a) \lambda f(a, y) = 0\]

identically, and as \( f(a, x) = -(f(x, a))^T \), this yields \( \lambda' = \lambda \). In other words,
unitary transvections exist only if $\nu \geq 1$, and then are of the form $x \rightarrow x + a\lambda f(a, x)$, where $a$ is an arbitrary isotropic vector, and $\lambda$ an arbitrary symmetric element in $K$; the hyperplane of points of $E$ invariant by the transvection is the hyperplane orthogonal to $a$.

Let $H$ be a nonisotropic hyperplane, $a$ a vector orthogonal to $H$. Then every unitary transformation $u$ leaving invariant every element of $H$ is such that $u(a) = \alpha u$, with $\mu'\alpha u = \alpha$, where $\alpha = f(a, a)$; we shall say that such a transformation is a quasi-symmetry. There always exist quasi-symmetries of hyperplane $H$, not reduced to the identity; this is obvious if $K$ has a characteristic $\neq 2$, for then the ordinary symmetry ($\mu = -1$) has that property. If $K$ has characteristic 2, one has by assumption $\alpha = \beta + \beta'$, with $\beta \neq \beta'$; then $\mu = \beta^{-1}\beta'$ satisfies $\mu'\alpha u = \alpha$, and $\mu \neq 1$.

These remarks already enable us to determine the center $Z_n$ of the group $U_n(K, f)$. Indeed, a transformation $v$ belonging to the center must permute with every quasi-symmetry, hence leave invariant every nonisotropic line; and if there are isotropic lines, $v$ must permute with every unitary transvection, hence leave invariant every isotropic line as well. Therefore $v$ leaves invariant every line, which means that it is a homothetic mapping $x \rightarrow xy$, with $y$ in the center $Z$ of $K$ and $\neq 0$; moreover, in order that such a mapping be unitary, it is necessary and sufficient that $\gamma'\gamma = 1$.

5. From now on, we are going to suppose that $\nu \geq 1$. Let $T_n$ be the subgroup of $U_n(K, f)$ generated by unitary transvections; as a transform $vuv^{-1}$ of a transvection $u$ is again a transvection, it is clear that $T_n$ is a normal subgroup of $U_n$. Let $W_n$ be the center of $T_n$ (we shall determine its structure in §11). We shall now prove the following theorem.

**Theorem 1.** If the sfield $K$ has more than 25 elements\(^{(2)}\), the group $T_n/W_n$ is simple for $n \geq 2$ and $\nu \geq 1$.

Our proof will be modeled after that of [5, Theorem 4, p. 55], and will proceed in several steps.

1°. We first prove that *if a normal subgroup $G$ of $T_n$ contains all transvections of $U_n$ having the same vector $a$, then $G = T_n$.* In order to do this, we shall prove the following lemma.

**Lemma 2.** If $a$ and $b$ are any two noncollinear isotropic vectors, there exists a transformation $u \in T_n$ such that $u(a) = bu$ for a convenient scalar $\mu \in K$.

If we suppose the lemma proved, and consider an arbitrary transvection $x \rightarrow v(x) = x + a\alpha f(a, x)$, it is readily verified that $vuv^{-1}$ is the transvection $x \rightarrow x + b\mu v f(b, x)$; but as $\alpha$ can take any value in the set $S$ of symmetric elements, so can $\mu v f$. Therefore $G$ contains all transvections of $b$, and in consequence is identical to $T_n$, since $b$ is an arbitrary isotropic vector.

\(^{(2)}\) The theorem is still true when $K$ has at most 25 elements, except when $K = F_n$, $n = 2$ and $n = 3$, and $K = F_n$, $n = 2$ [5, p. 70].
To prove the lemma, let us first suppose that \( f(a, b) \neq 0 \); then there is a scalar \( \mu \neq 0 \) such that \( a + b \mu = c \) is isotropic. Indeed, the relation \( f(a + b \mu, a + b \mu) = 0 \) gives the condition \( \mu^2 f(b, a) + f(a, b) \mu = 0 \) which is satisfied by taking \( \mu = (f(a, b))^{-1} \), owing to the relation \( f(b, a) = -f(a, b) \). The transvection \( x \rightarrow u(x) = x + cf(c, x) \) sends then \( a \) into \( -b \mu \), for \( f(c, a) = \mu^2 f(b, a) = -1 \).

Suppose next that \( f(a, b) = 0 \); this means that the plane containing \( a \) and \( b \) is totally isotropic, hence \( n \geq 3 \). Therefore there exists a vector \( z \) such that \( f(a, z) \neq 0 \) and \( f(b, z) \neq 0 \); the plane containing \( a \) and \( z \) is hyperbolic, and contains therefore a vector \( a_1 \) not collinear to \( a \) and isotropic; moreover \( a_1 \) cannot be orthogonal to \( b \), otherwise \( z \) would also be orthogonal to \( b \); therefore one has \( f(a, a_1) \neq 0 \) and \( f(a_1, b) \neq 0 \); applying the preceding result, there is a transvection \( u_1 \) transforming \( a \) into a scalar multiple of \( a_1 \), and a transvection \( u_2 \) transforming \( a_1 \) into a scalar multiple of \( b \); the transformation \( u = u_2 u_1 \) satisfies the conditions of the lemma.

6. Our next step will be to prove that:

2°. Theorem 1 is true for \( n = 2, \upsilon \geq 1 \). The assumption implies that there is a basis of \( E \) consisting of 2 isotropic vectors \( e_1, e_2 \) such that \( f(e_1, e_2) = 1 \). If \( u \) is a unitary transformation,

\[
U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}
\]

its matrix with respect to the basis \((e_1, e_2)\), the elements of \( U \) satisfy the following conditions

(1) \( \alpha^T \gamma - \gamma^T \alpha = 0, \quad \beta^T \delta - \delta^T \beta = 0, \quad \alpha^T \delta - \gamma^T \beta = 1, \)

and conversely, the matrices satisfying these relations are unitary. We observe that from (1) one deduces the following relations

(2) \( \alpha \beta^T - \beta \alpha^T = 0, \quad \gamma \delta^T - \delta \gamma^T = 0. \)

Indeed, let

\[
A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},
\]

and let \( U^* \) be the transposed matrix of \( U^* \); then (1) is equivalent to the matrix relation \( U^* A U = A \), whence \( A^{-1} = U^{-1} A^{-1} (U^*)^{-1} \), and therefore \( U A^{-1} U^* = A^{-1} \); but as \( A^{-1} = -A \), the last relation implies (2) (this short derivation of (2) from (1) was indicated by the referee). The transvections of vector \( e_2 \) have matrices of the type

\[
B(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\]
where \( \lambda \in S \); the transvections of vector \( e_i \) have matrices of the type

\[
C(\mu) = \begin{pmatrix}
1 & \mu \\
0 & 1
\end{pmatrix},
\]

with \( \mu \in S \). We want to prove that if a normal subgroup \( G \) of \( T_2 \) contains a transformation \( u \) not in the center \( W_2 \), then \( G = T_2 \); it will be enough, by virtue of part 1°, to show that all matrices \( C(\mu) \) belong to \( G \).

Let us first suppose that the matrix \( U \) is such that \( \beta \neq 0 \). Then the matrix

\[
(B(\lambda))^{-1}UB(\lambda) = B \begin{pmatrix} \alpha + \beta \lambda & \beta \\ \gamma' & \delta' \end{pmatrix}
\]

belongs to \( G \), for any \( \lambda \in S \). It follows from the first relation (2) that \( \beta^{-1} \alpha \in S \); taking \( \lambda = -\beta^{-1} \alpha \), we see that we can always limit ourselves to the case in which \( \alpha = 0 \); the third relation (1) then yields \( \gamma = -(\beta^{-1})' \).

Supposing therefore that \( \alpha = 0 \), we next determine a linear transformation \( v \) of \( S \) such that \( u(v(e_i)) = e_i \xi \), and \( v(u(e_i)) = e_i \eta \), \( \xi \) and \( \eta \) being at first arbitrary elements \( \neq 0 \) in \( K \). An easy computation shows that the matrix of \( v \) with respect to \( e_1, e_2 \) is equal to

\[
V = \begin{pmatrix}
\gamma^{-1} \partial^{-1} \xi & \eta \gamma^{-1} \\
\beta^{-1} \xi & 0
\end{pmatrix}.
\]

We now want \( v \) to be in the group \( T_2 \); this, by the third condition (1), is possible only if we have

\[
(\eta \gamma^{-1})' \beta^{-1} \xi = -1.
\]

Conversely, if \( \xi \) and \( \eta \) satisfy (3) and \( \beta^{-1} \xi \in S \), then \( v \in T_2 \). To prove this, we first remark that there is \( \sigma \in S \) such that

\[
VB(\sigma) = \begin{pmatrix}
0 & -(\gamma^{-1})' \\
\xi & 0
\end{pmatrix},
\]

with \( \xi = \beta^{-1} \xi \); indeed, this relation is equivalent to \( \sigma = \gamma \eta^{-1} \gamma^{-1} \delta \beta^{-1} \xi \); but it follows from the second relation (2) that \( \gamma^{-1} \delta \xi \in S \), and on the other hand, (3) shows that \( \gamma \eta^{-1} = -(\beta^{-1} \xi)' \); therefore, the element \( \sigma \) is in \( S \).

Further, we have, for \( \xi \in S \),

\[
C(\xi)B(\xi)C(\xi^{-1}) = \begin{pmatrix}
0 & -\xi^{-1} \\
\xi & 0
\end{pmatrix},
\]

hence \( VB(\sigma) \) is in \( T_2 \), which proves that \( V \) is in \( T_2 \).

The transformation \( u_1 = u^{-1}vu \) is then in \( G \), and its matrix has the form
where \( \rho = \beta' \xi \beta \xi \). Finally the matrix \( W = U_1 C(\theta) U_1^{-1} C(-\theta) \) is in \( G \) for every \( \theta \in S \), and is equal to

\[
\begin{pmatrix}
1 & \rho \rho' - \theta \\
0 & 1
\end{pmatrix}
\]

in other words, it is a matrix \( C(\mu) \) with \( \mu = \rho \rho' - \theta \).

7. We first want to prove that it is possible to choose \( \xi \) and \( \theta \) in the set \( S \) of symmetric elements such that \( \mu \neq 0 \). This will certainly be the case if \( \rho \rho' \neq 1 \), with \( \theta = 1 \). We have therefore to show that, under the assumptions of Theorem 1, it is impossible that \( \rho \rho' = 1 \) for every \( \xi \in S \). This is immediate if the subfield \( Z_0 \) of the center \( Z \), which consists of the symmetric elements of \( Z \) (and is such that \( Z \) is a separable quadratic extension of \( Z_0 \), or identical to \( Z_0 \)), has more than 5 elements; for if \( \xi \in Z_0 \), the relation \( \rho \rho' = 1 \) reduces to \( \xi^4 (\beta' \beta)^2 = 1 \), which can be verified by at most 4 different elements of \( Z_0 \). We are therefore reduced to the case in which \( Z_0 \) has at most 5 elements, which means that \( Z \) has at most 25 elements; moreover, we can suppose that \( K \) is noncommutative, and therefore infinite. In the identity \( \rho \rho' = 1 \), if we replace \( \xi \) by 1, we get \( (\beta' \beta)^2 = 1 \), hence \( \beta' = \beta^{-1} \) or \( \beta' = -\beta^{-1} \); in any case, \( \beta' \) and \( \beta \) commute. If \( \beta' + \beta = 0 \), we have \( \beta^4 = 1 \); if \( \beta + \beta' \neq 0 \), we can replace \( \beta \) by \( \beta + \beta' \), and we get \( (\beta + \beta')^4 = 1 \). In every case, \( \beta \) is a root of an algebraic equation with coefficients in \( Z \), and as \( Z \) is finite, so is the commutative field \( Z(\beta) \).

Let \( L \) be the subsfield of \( K \) consisting of the elements of \( K \) which commute with \( \beta \); as \( Z(\beta) \) has finite degree over \( Z \), \( K \) has finite degree over \( L \), and therefore \( L \) is an infinite field [2, p. 104]; moreover, as \( Z(\beta') = Z(\beta) \), \( L \) is invariant under the involution \( J \). Now, if we take \( \xi \) in \( S \cap L \), the relation \( \rho \rho' = 1 \) reduces to \( \xi^4 = 1 \), in other words \( \xi^2 = 1 \) or \( \xi^2 = -1 \). If we apply this to \( \xi = \xi + \eta \), where \( \xi \) and \( \eta \) are arbitrary in \( S \cap L \), we conclude that \( \xi \eta + \eta \xi \) is in the center \( Z \) of \( K \), from which it immediately follows that the field \( M \) generated by \( \xi \) and \( \eta \) over \( Z \) has at most rank 4 over \( Z \); as \( Z \) is finite, this field must be commutative. In other words, any two elements of \( S \cap L \) commute; it then follows from Lemma 1 that either \( L \) is commutative, or is a reflexive field, and then has necessarily an infinite center which is identical to \( S \cap L \). In any case, the relation \( \xi^4 = 1 \), valid for \( \xi \in S \cap L \) (and \( \xi \neq 0 \)) shows that \( S \cap L \) must be finite; this is possible only when \( L \) is commutative; but then \( S \cap L \) is a subfield of \( L \) such that \( L \) has degree 2 over \( S \cap L \), and as \( L \) is infinite, \( S \cap L \) would also have to be infinite; we thus have reached a contradiction, which ends this part of the argument.

8. We now have proved that there exists in \( S \) an element \( \mu_0 \neq 0 \) such that \( C(\mu_0) \) belongs to \( G \). We want to show next that \( C(1) \) also belongs to \( G \). In order to do this, we repeat the whole argument of §§6 and 7, starting with
the matrix \( C(\mu_0) \) instead of \( U \), and, therefore, this time the element \( \beta = \mu_0 \) is symmetric. If we can take \( \xi \) in the center \( Z \), we thus get an element \( \rho \) which is symmetric and such that \( \rho^2 \neq 1 \). If not, which is the case only when \( Z_0 \) has at most 5 elements, the commutative field \( Z(\beta) \) is either finite or infinite. If it is infinite, we can again take a symmetric \( \xi \) in \( Z(\beta) \) such that \( \rho \) is symmetric and \( \rho^2 \neq 1 \). If on the contrary \( Z(\beta) \) is finite, an argument similar to that of §7, where \( Z(\beta) \) replaces \( Z \), proves that in the subfield \( L \) of \( K \) commuting with \( \beta \) it is possible to find a symmetrical element \( \xi \) such that \( \xi^4 \beta^4 \neq 1 \), and then \( \rho = \beta^2 \xi^2 \) is again symmetric and such that \( \rho^2 \neq 1 \). Now, in the method of §6, we can take \( \theta = (\rho^2 - 1)^{-1} \); then \( \rho \) and \( \theta \) commute, and the matrix we obtain in that way is \( C(1) \).

Finally, let \( \mu \) be any symmetric element \( \neq 0 \), and consider the subfield \( N \) of \( K \) commuting with \( \mu \); we are going to prove that there exists in \( N \) a symmetric element \( \xi \) such that \( \xi^4 \neq 1 \). This is certainly the case if the center of \( N \) (which contains the commutative field \( Z(\mu) \)) is infinite (or has more than 25 elements). On the other hand, if the center of \( N \) is finite and is distinct from \( N \), in particular \( Z(\mu) \) is finite, and then \( N \) is necessarily infinite; but then the argument of §7 shows that it is impossible that \( \xi^4 = 1 \) for every symmetric element in \( N \). The symmetric element \( \xi \) being thus chosen, we apply again the procedure of §6, starting this time from the matrix \( C(1) \) instead of \( U \); we take then \( \rho = \xi^4 \), and \( \rho \) is symmetric and such that \( \rho^2 \neq 1 \). Moreover, \( \rho \) commutes with \( \mu \) and with \( \xi \) (which commute together); therefore, if we take this time \( \theta = \mu(\xi^4 - 1)^{-1} \), \( \theta \) is symmetric, and we have \( \rho \theta \rho^T = \theta = \mu \).

9. To end the proof of step 2°, we still have to consider the cases in which \( \beta = 0 \) in the matrix \( U \). Suppose first that \( \gamma \neq 0 \); then, if

\[
Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},
\]

we notice that \( Q = C(-1)B(1)C(-1) \) belongs to \( T_2 \) and that

\[
QUQ^{-1} = \begin{pmatrix} \delta & -\gamma \\ 0 & \alpha \end{pmatrix},
\]

and we are reduced to the preceding case. Finally, if \( \beta = \gamma = 0 \), we have \( \delta = (\alpha^{-1})^T \) by the third relation (1); then the matrix \( C(\mu)UC(-\mu) \) belongs to \( G \), and it is equal to

\[
\begin{pmatrix} \alpha & \mu(\alpha^{-1})^T - \alpha \mu \\ 0 & (\alpha^{-1})^T \end{pmatrix}.
\]

We are therefore reduced to the former case if there is a symmetric \( \mu \) such that \( \mu(\alpha^{-1})^T - \alpha \mu \neq 0 \). If not, \( U \) commutes with every matrix \( C(\mu) \), and it is easily verified that it also commutes with every matrix \( B(\lambda) \). But this is
possible only if $U$ is in the center $W_2$ of $T_2$, owing to the following lemma:

**Lemma 3.** The group $T_2$ is generated by the transvections $B(\lambda)$ and $C(\mu)$.

To prove that lemma, consider an arbitrary isotropic vector $x = e_2\alpha + e_2\beta$ in $E$; one has then $\alpha'\beta - \beta'\alpha = 0$. Suppose $\beta \neq 0$; then $\alpha\beta^{-1}$ is a symmetric element. But then the transvection $C(\mu)$, with $\mu = -\alpha\beta^{-1}$, transforms $x$ into a vector collinear with $e_2$, and this shows that every transvection of vector $x$ is transformed by $C(\mu)$ into a transvection of vector $e_2$, that is, a transvection $B(\lambda)$. This of course proves the lemma, and ends the proof of step 2° of Theorem 1.

10. It is now easy to prove that Theorem 1 is true for any $n \geq 3$. Let $G$ be a normal subgroup of $T_n$, and $u$ a transformation in $G$ which does not belong to the center $W_n$. Then $u$ does not belong to $Z_n$, in other words it is not a homothetic mapping. From that, we shall deduce that there exists an isotropic vector $x$ such that $u(x)$ and $x$ are not collinear. This will be proved if we show that when $u$ leaves invariant every isotropic line, it leaves invariant every line (and is therefore a homothetic mapping), according to the following lemma:

**Lemma 4.** For $n \geq 3$ and $v \geq 1$, every nonisotropic line in $E$ is the intersection of two hyperbolic planes.

To prove the lemma, let $x$ be a nonisotropic vector, and $y$ an isotropic vector. Let $z$ be a vector which is orthogonal neither to $x$ nor to $y$ and is not in the plane determined by $x$ and $y$. Then the plane $P$ determined by $y$ and $z$ is a hyperbolic plane, and it contains therefore a second isotropic vector $y_1$ such that $f(y, y_1) = 1$. Moreover, any vector $y_2 = y\alpha + y_1\beta$ is isotropic if $\alpha'\beta - \beta'\alpha = 0$, and therefore there exists such a vector $y_2$ which is collinear with neither of $y$ and $y_1$ (take for instance $\alpha = \beta = 1$). Among the three isotropic vectors $y$, $y_1$, $y_2$, two at least are not orthogonal to $x$, since $x$ is not orthogonal to $P$. Therefore two of the three planes $Q$, $Q_1$, $Q_2$ determined by $x$ and the vectors $y$, $y_1$, $y_2$, respectively, are hyperbolic planes, which proves the lemma.

We can now resume the end of the proof of Theorem 1. Let $x$ be an isotropic vector such that $x$ and $u(x)$ are not collinear. Suppose first that $f(x, u(x)) = 0$. Then there exists a vector $z$ which is orthogonal to $u(x)$ but not to $x$. The plane $P$ determined by $x$ and $z$ is a hyperbolic plane, hence contains an isotropic vector $y$ which is not collinear to $x$. From Lemma 2, there exists a transvection $v \in T_n$ transforming $x$ into a scalar multiple $\gamma y$ of $y$; moreover the vector of that transvection is in $P$, hence orthogonal to $u(x)$, and therefore $v(u(x)) = u(x)$. The transformation $u_1 = vu^{-1}v^{-1}u$ belongs to $G$, and one has $u_1(x) = y$. This proves that we can always suppose that $u \in G$ is such that $f(x, u(x)) \neq 0$.

Let then $w$ be a transvection of vector $x$; $uwu^{-1}$ is a transvection of vector
u(x), and as x and u(x) are not collinear, these two transvections do not commute. Let Q be the hyperbolic plane determined by x and u(x); the transformation \( u_2 = w^{-1}uwu^{-1} \) belongs to G, and leaves invariant every vector in the subspace \( Q^* \) orthogonal to Q. It therefore belongs to the subgroup \( \Gamma \) of \( U_n(K, f) \) which leaves invariant every vector of \( Q^* \), and is obviously isomorphic to the unitary group \( U_2(K, f_1) \), where \( f_1 \) is the restriction of f to the plane Q; we shall identify \( \Gamma \) with that group. Moreover, \( u_2 \) is the product of two transvections, hence belongs to the group \( T_2(K, f_1) \); finally, it is not in the center of that group, since it does not commute with w. Now step 2° of the proof shows that G contains every transformation of \( T_2(K, f_1) \), in particular every transvection of vector x. Applying step 1° of the proof, we see that \( G = T_n \), and Theorem 1 is completely proved.

11. We can supplement Theorem 1 by proving the following theorem.

**THEOREM 2.** Under the same assumptions as in Theorem 1, the center \( W_n \) of the group \( T_n \) is the intersection \( T_n \cap Z_n \).

Indeed, if \( n \geq 3 \), every transformation \( u \in W_n \) must commute with every transvection, hence leave invariant every isotropic line. It then follows from Lemma 4 that \( u \) leaves invariant every line, hence is a homothetic mapping.

For \( n = 2 \), if \( e_1 \) and \( e_2 \) are two isotropic vectors constituting a basis of \( E \) such that \( f(e_1, e_2) = 1 \), the matrix \( U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \) of \( u \) with respect to that basis must commute with every one of the matrices \( B(\lambda) \) and \( C(\mu) \) (notations of §6); this, as is readily seen, means that

\[
U = \begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^T \end{pmatrix},
\]

where \( \alpha \) is such that \( \alpha \lambda = \lambda (\alpha^{-1})^T \) for every symmetric element \( \lambda \in K \). Taking \( \lambda = 1 \) gives \( \alpha^T = \alpha^{-1} \), and therefore \( \alpha \) must commute with every symmetric element. From Lemma 1, we deduce therefore that \( \alpha \) is in the center \( Z \) of \( K \) (and therefore that \( u \in T_2 \cap Z_2 \)) with the possible exception of the case in which \( K \) is a reflexive sfield of characteristic \( \neq 2 \), and \( Z \) is identical to the set \( S \) of symmetric elements. But in that case we remark that the matrices \( B(\lambda) \) and \( C(\mu) \) have their elements in \( Z \), and from Lemma 3 it follows that the same is true for every matrix of the group \( T_2 \); hence if the matrix \( U \) belongs to \( T_2 \), \( \alpha \) is again in \( Z \), and this ends the proof of Theorem 2.

12. The remainder of this paper is devoted to the study of the quotient group \( U_n/T_n \); the results we obtained in that direction are far from complete, and part of them are valid only under the additional assumption that the sfield \( K \) has finite rank over its center \( Z \).
We begin by proving a lemma which is valid for any field \( K \). A plane rotation is a transformation \( u \in U_n \) which leaves invariant every element of a nonisotropic \((n-2)\)-dimensional subspace \( Q \); the plane \( Q^* \) orthogonal to \( Q \) is then called the plane of the rotation \( u \). A hyperbolic rotation is a plane rotation whose plane is hyperbolic. We then prove the following lemma.

**Lemma 5.** For \( n \geq 1 \), every unitary transformation is a product of hyperbolic rotations.

The lemma being obvious for \( n = 2 \), we prove it by induction on \( n \), as in [5, p. 66]. Let \( u \) be any unitary transformation, and let \( x \) be a nonisotropic vector such that the hyperplane \( H \) orthogonal to \( x \) contains isotropic vectors. If \( u(x) = x \), \( u \) leaves \( H \) invariant, and we can apply induction to its restriction to \( H \), since the index of the restriction of the form \( f \) to \( H \) is \( \geq 1 \) by assumption; the lemma is then proved. If \( u(x) \neq x \), there is always a hyperbolic plane \( P \) containing the vector \( u(x) - x \): indeed, if \( a = u(x) - x \) is not isotropic, there is an isotropic vector \( b \) not orthogonal to \( a \) (Lemma 4), and then the plane \( P \) determined by \( a \) and \( b \) is hyperbolic; if on the contrary \( a \) is isotropic, there is a nonisotropic vector \( c \) not orthogonal to \( a \), and the plane \( P \) determined by \( a \) and \( c \) is hyperbolic. Now, as \( u(x) - x \) is in \( P \), we can write \( x = z + y \), \( u(x) = z + y' \), where \( y \) and \( y' \) are in \( P \), and \( z \) in the \((n-2)\)-dimensional subspace \( P^* \) orthogonal to \( P \). Moreover, as \( f(u(x), u(x)) = f(x, x) \), we have also \( f(y, y) = f(y', y') \). From Witt's theorem applied to the restriction of \( f \) to the plane \( P \), it follows that there exists a plane rotation \( v \) of plane \( P \) such that \( v(y) = y' \), hence also \( v(x) = u(x) \), since \( v(z) = z \). But then \( v^{-1}u \) leaves \( x \) invariant, and we are reduced to the first case: \( v^{-1}u \) is thus a product of hyperbolic rotations, and so is therefore \( u \).

13. We shall use Lemma 5 to prove that in certain cases the subgroup \( T_n \) is identical to \( U_n \): Lemma 5 shows that this will be done if we can prove that every hyperbolic rotation is a product of transvections. In particular, we shall have proved that \( U_n = T_n \) for every dimension \( n \) if we can prove that \( U_2 = T_2 \) (for \( n \geq 1 \), of course). We therefore begin by investigating the relations between the group \( U_2 \) and its subgroup \( T_2 \).

As in §6, we consider a basis of \( E \) consisting of two isotropic vectors \( e_1, e_2 \) such that \( f(e_1, e_2) = 1 \); let

\[
U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}
\]

be the matrix of a unitary transformation \( u \) with respect to that basis; the relations (1) and (2) are then satisfied. As \( \alpha \) and \( \beta \) are not both 0, there is a \( \sigma \in S \) such that in

\[
UB(\sigma) = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix},
\]
$\alpha' = \alpha + \beta \sigma \neq 0$; we can therefore already suppose that $\alpha \neq 0$; then it follows from the first relation (2) that $\mu = \alpha^{-1} \beta$ and from the first relation (1) that $\lambda = \gamma \alpha^{-1}$ are both symmetric. But then the matrix

$$B(-\lambda)UC(-\mu) = \begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^T \end{pmatrix}$$

(owing to the third relation (1)). If we observe that $T_2$ is a normal subgroup of $U_2$, and that $T_2$ is generated by the matrices $B(\xi)$ and $C(\eta)$ (Lemma 3), we finally see that every matrix $U$ in the group $U_2$ can be written as a product $VW$, where $W$ belongs to the group $T_2$, and $V$ has the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^T \end{pmatrix}.$$

In order that $T_2 = U_2$, it is therefore necessary and sufficient that every matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^T \end{pmatrix}$$

belong to $T_2$. Now, for every pair of elements $\lambda, \mu$ in $S$, we have

$$C(\mu)B(\lambda) = \begin{pmatrix} 1 + \mu \lambda & \mu \\ \lambda & 1 \end{pmatrix};$$

if we apply the preceding method to that matrix, we see that every matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^T \end{pmatrix}$$

with $\alpha = 1 + \mu \lambda = (\lambda^{-1} + \mu) \lambda$ belongs to $T_2$.

This proves that $T_2 = U_2$ if every element $\neq 0$ in $K$ is a product of elements of $S$.

14. Let us suppose in this section that $K$ has finite rank $m^2$ over its center $Z$. We recall that $K$ is said to be of the first kind if $J$ leaves invariant every element of $Z$, of the second kind if the restriction of $J$ to $Z$ is not the identity (it is then an involution in $Z$). Moreover, when $K$ is of the first kind and of characteristic $\neq 2$, the dimension of $S$ over $Z$ is equal to $m(m+1)/2$ or $m(m-1)/2$ [7]; the easiest way to see this is to extend $Z$ to a splitting field $L$ of $K$; the involution $J$ is extended to $K_{(L)}$ in an obvious way (the elements of $L$ being invariant by $J$), and by taking a basis of $K$ over $Z$ consisting of symmetric or skew-symmetric elements, one sees readily that the dimension over $L$ of the space of symmetric elements of $K_{(L)}$ is equal to the dimension over $Z$ of the space of symmetric elements of $K$. But $K_{(L)}$ is the algebra of matrices of order $m$ over $L$, and an involution of that algebra leaving in-
variant the elements of $L$ is known, namely the mapping $X \rightarrow X^t$, where $X^t$ is the transposed matrix of $X$; therefore [1, p. 896], one has $X^t = P^{-1} X^t P$, where $P$ is either a symmetric or a skew-symmetric matrix. Hence, the relation $X^t = X$ means that $PX$ is symmetric (resp. skew-symmetric) if $P$ is symmetric (resp. skew-symmetric); this proves at once our assertion. Similarly, it is shown that when the characteristic of $K$ is 2, the dimension of $S$ over $Z$ is always $m(m+1)/2$ when $K$ is of the first kind.

We can now prove the following theorem.

**Theorem 3.** When $K$ is a skewfield of the first kind, of finite rank $m^2$ over its center $Z$ and of characteristic $\neq 2$, and such that the space $S$ of symmetric elements in $K$ has dimension $m(m-1)/2$ over $Z$, then $U_n = T_n$ for every $n \geq 2$.

All we have to prove (according to the final remark of §13) is that, for every $\xi \in K$, there exist two elements $\xi, \eta$ in $S$ such that $\xi = \eta^t \eta$. If $\theta = \eta^{-1}$, this amounts to saying that there exists an element $\theta \in S$ such that $\theta \theta = 0$. But the mapping $\theta \rightarrow \xi^t \theta - \theta \xi^t$ of $S$ into $K$ is linear with respect to $Z$, and maps $S$ into the space $A$ of skew-symmetric elements, which is supplementary to $S$ in $K$, hence has a dimension equal to $m(m-1)/2$; as $m(m+1)/2 > m(m-1)/2$, the kernel of the linear mapping $\theta \rightarrow \xi^t \theta - \theta \xi^t$ is not reduced to 0, and this ends our proof.

As a corollary, we obtain Theorem 6 of [5] when $K$ is a reflexive skewfield of characteristic $\neq 2$: the passage from an hermitian to a skew-hermitian form over $K$, explained in §3, replaces the involution $\xi \rightarrow \eta$ in $K$ by an involution for which the symmetric elements are the skew-symmetric elements of $\xi \rightarrow \eta$, hence form a subspace of dimension 3 over the center $Z$.

15. Turning now to the case in which the skewfield $K$, of finite rank $m^2$ over $Z$, is a skewfield of the first kind but such that $S$ has dimension $m(m-1)/2$ over $Z$ (this property implying that $K$ has a characteristic $\neq 2$), we have to set aside the case $m = 2$, in which $S = Z$, and therefore $S$ cannot generate the group $K^*$ of elements $\neq 0$ in $K$. When $m > 2$, it seems likely (due to Lemma 1) that $S$ generates $K^*$, but I have not been able to prove that conjecture, and in the absence of any further assumptions, the structure of the group $U_n/T_n$ remains unknown in that case. I shall therefore consider only the case $m = 2$; in other words, $K$ is then a skewfield of generalized quaternions over $Z$, and the involution $J$ is the (unique) involution of $K$ for which the elements of $Z$ are the only symmetric elements.

Let us first consider the case $n = 2$; then $T_2$ is simply the unimodular group $SL_2(Z)$ [4, p. 30]. Moreover, as every element $\alpha \in K$ is such that $(\alpha^{-1})^t = \alpha \cdot (N(\alpha))^{-1}$, where $N(\alpha) = \alpha \alpha^t Z$, it follows from §13 that every matrix $U$ in the group $U_2$ can be written $\alpha X$, where $X$ is an arbitrary matrix in $GL_2(Z)$ such that $\det(X) = (N(\alpha))^{-1}$, and $\alpha$ is an arbitrary element in $K^*$. We observe in addition that $\alpha$ and $X$ are permutable, and that $\alpha$ is determined by $U$ up to a factor $\lambda \in Z^*$ (the matrix $X$ being then multiplied
by $\lambda^{-1}$). We can therefore describe the structure of the group $U_2$ in the following way: consider in the direct product $K^* \times GL_2(Z)$ the subgroup $\Gamma$ consisting of the pairs $(\alpha, X)$ such that $N(\alpha) \cdot \det(X) = 1$, and let $\Delta$ be the subgroup of $\Gamma$ consisting of the pairs $(\lambda, \lambda^{-1})$, where $\lambda \in Z^*$; then $U_2$ is isomorphic to the factor group $\Gamma/\Delta$. We observe that $U_2$ contains as a normal subgroup the multiplicative group $U_1$ of elements of norm 1 in $K$, and that $U_1$ and $T_2$ commute and have as their intersection the two elements 1 and $-1$, which constitute the center $W_2$ of $T_2$; the quotient group $U_2/T_2$ contains $U_1/W_2$ as a subgroup, hence $T_2$ is certainly not the commutator subgroup of $U_2$.

16. There are reasons to believe that the preceding structure of the group $U_2(K, f)$ when $K$ is a subfield of generalized quaternions and $f$ a skew-hermitian form is exceptional among the corresponding groups $U_n(K, f)$ for $n > 2$, much as the 4-dimensional orthogonal groups among the orthogonal groups of other dimensions. The evidence I can supply in favor of that view is summed up in the following theorem:

**Theorem 4.** If $K$ is a subfield of characteristic $\neq 2$, and the index $\nu$ of the form $f$ is at least 2 (which implies $n \geq 4$), then $T_\nu$ is the commutator subgroup of $U_n(K, f)$.

To prove that theorem, we shall establish two lemmas.

**Lemma 6.** Let $P$ be a hyperbolic plane, $\Gamma$ the group of hyperbolic rotations of plane $P$. Then (for $\nu \geq 2$) the factor group $\Gamma/(\Gamma \cap T_\nu)$ is abelian.

Let $e_1, e_2$ be two isotropic vectors forming a basis of $P$, with $f(e_1, e_2) = 1$; it is then possible to find two other isotropic vectors $e_3, e_4$ orthogonal to $P$ and such that $f(e_3, e_4) = 1$ (because $\nu \geq 2$). Let $Q$ and $R$ be the totally isotropic planes determined by $e_1, e_3$ and $e_2, e_4$ respectively; if $u \subseteq U_n$ leaves invariant both planes $Q$ and $R$, and $V$ and $W$ are the matrices of the restrictions of $u$ to $Q$ and $R$, with respect to the bases $e_1, e_3$ and $e_2, e_4$ respectively, one has $W = (V')^T$, $V'$ being the contragredient of $V$. We are going to prove that there are transformations $u \subseteq T_\nu$ of the preceding type, and such that $V = B(\lambda)$, where $\lambda$ is any element of $K$. Let $a = e_6 + e_7$ be any vector in the totally isotropic plane determined by $e_2$ and $e_3$, and consider the transvection $w$ such that $w(x) = x + af(a, x)$; it leaves invariant $e_2$ and $e_3$, and is such that

$$w(e_1) = e_1 - e_2 e_3 a_1 - e_3 e_2 a_1^T,$$  
$$w(e_4) = e_4 + e_2 e_3 a_1 + e_3 e_2 a_1^T.$$

Let $a_1 = e_6 a_1 + e_7 a_1$ be a second isotropic vector, $w_1$ the transvection such that $w_1(x) = x - a_1 f(a_1, x)$; then $u = w_1 w$ leaves invariant $e_2$ and $e_3$ and is such that

$$u(e_1) = e_1 + e_2 (c_1 a_1 - a_2 a_1^T) + e_3 (c_2 a_1 - a_2 a_1^T),$$  
$$u(e_4) = e_4 + e_2 (c_2 a_1 - a_2 a_1^T) + e_3 (c_2 a_1 - a_2 a_1^T).$$
If we take $\alpha_1 = \alpha$ and $\beta_1 = -\beta$, $u$ leaves invariant $Q$ and $R$, and is such that $u(e_i) = e_i - 2e_i \beta a_i^j$; as the characteristic of $K$ is not 2, it is possible to take $\alpha$ and $\beta$ such that $-2\beta a_i^j = \lambda$, for any element $\lambda \in K$, and the matrix of the restriction of $u$ to $Q$ is then $B(\lambda)$. Similarly, it can be proved that $u \in T_n$ exists such that $V = C(\mu)$ for any $\mu \in K$. Therefore $T_n$ contains all the transformations $u \in U_n$ leaving invariant $Q$ and $R$ and such that the matrix of the restriction of $u$ to $Q$ is any matrix $V$ in the unimodular group $SL_2(K)$ [4, p. 30]; in particular, for any element $\gamma$ in the commutator subgroup of $K^*$, $u \in T_n$ exists such that

$$V = \begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix},$$

[4, p. 29], which means that $u$ is a hyperbolic rotation of plane $P$, such that its matrix in $P$ is

$$\begin{pmatrix} \gamma & 0 \\ 0 & (\gamma^{-1})^j \end{pmatrix}.$$

Now we have seen in §13 that every hyperbolic rotation of plane $P$ has a matrix (with respect to $e_1, e_2$) which can be written as the product of a matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^j \end{pmatrix}$$

(with $\alpha \in K^*$) and a matrix of $\Gamma \cap T_n$. If, to every $\alpha \in K^*$, we associate the class of the matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^j \end{pmatrix},$$

modulo the subgroup $\Gamma \cap T_n$, we define a homomorphism of $K^*$ onto $\Gamma/(\Gamma \cap T_n)$, and the preceding result shows that the kernel of that homomorphism contains the commutator subgroup $C$ of $K^*$; hence $\Gamma/(\Gamma \cap T_n)$ is isomorphic to a quotient group of the abelian group $K^*/C$.

17. Lemma 7. Let $P_1$ and $P_2$ be any two hyperbolic planes. Then (for $\nu \geq 2$) there exists a transformation $w \in T_n$ such that $w(P_1) = P_2$.

It follows from Lemma 2 that there exists a transformation in $T_n$ sending an isotropic vector in $P_1$ into an isotropic vector in $P_2$; we can therefore assume in the following proof that there exists a common isotropic vector $e_2$ in $P_1$ and $P_2$. We now consider separately several cases.

(a) The dimension $n = 4$. Let $e_1$ be a second isotropic vector in $P_1$ such that $f(e_1, e_2) = 1$, and let $e_3, e_4$ be determined as in the proof of Lemma 6. There exists in $P_2$ an isotropic vector $e'_2$ such that $f(e'_2, e_2) = 1$; we can write $e'_2 = e_1$.
+e_2\beta + e_3\gamma + e_4\delta$, and the condition $f(e_1', e_1') = 0$ is equivalent to

$$\beta - \beta' + \gamma'\delta - \delta'\gamma = 0$$

which can be written $\beta + \gamma'\delta = (\beta + \gamma\delta)'$, and means therefore that the expression $\beta + \gamma'\delta$ is a symmetric element $\lambda$. Now, it has been proved in the proof of Lemma 6 that the transformation $w_1$ leaving invariant $e_2$ and $e_3$, and such that

$$w_1(e_1) = e_1 + e_2\gamma, \quad w_1(e_4) = e_4 - e_2\gamma',$$

belongs to $T_n$. Similarly (exchanging the parts played by $e_3$ and $e_4$), the transformation $w_2$ leaving invariant $e_2$ and $e_4$, and such that

$$w_2(e_1) = e_1 + e_4\delta, \quad w_2(e_3) = e_3 - e_2\delta',$$

belongs to $T_n$. The transformation $w_1w_2$, which belongs to $T_n$, is such that $w_1w_2(e_2) = e_2$, and $w_1w_2(e_1) = e_1 + e_2\gamma + e_3\delta - e_2\gamma'\delta$. Let finally $v$ be the translation $x \rightarrow x - e_2\lambda f(e_2, x)$, which leaves invariant $e_2, e_3, e_4$ and is such that $v(e_1) = e_1 + e_2\lambda$; the transformation $w = vw_1w_2$ belongs to $T_n$, leaves $e_2$ invariant, and is such that

$$w(e_1) = e_1 + e_2(\lambda - \gamma'\delta) + e_3\gamma + e_4\delta = e_1'.$$

Therefore $w(P_1) = P_2$, and the lemma is proved in that case.

(b) $n > 4$ and the 3-dimensional subspace $M = P_1 + P_2$ is isotropic. This means that there exists in $M$ at least an isotropic vector $c$ orthogonal to $M$; such a vector cannot be in $P_1$, since $P_1$ is not isotropic. Therefore the three vectors $c, e_1, e_2$ ($e_1$ being defined as in (a)) constitute a basis for $M$, such that $f(e_1, e_2) = 1, f(e_1, c) = f(e_2, c) = 0$. There exists then in $E$ a fourth isotropic vector $d$ such that $f(c, d) = 1, f(e_1, d) = f(e_2, d) = 0$ [5, p. 18], and the four vectors $e_1, e_2, c, d$ form the basis of a nonisotropic 4-dimensional subspace $N$ of $E$ containing $P_1$ and $P_2$ and such that the restriction of the form $f$ to $N$ has an index equal to 2. The result of case (a) proves then the lemma.

(c) $n > 4$ and the space $M$ is not isotropic. There exists then in $M$ a nonisotropic vector $c$ orthogonal to $P_1$. As the index $\nu \geq 2$, the restriction of $f$ to the $(n - 2)$-dimensional subspace $P_1^\perp$ orthogonal to $P_1$ has an index $\geq 1$, by Witt's theorem. Therefore (Lemma 4), there exists a hyperbolic plane $Q$ contained in $P_1^\perp$ and containing $c$. The subspace $N = P_1 + Q$ is then a nonisotropic 4-dimensional subspace of $E$, such that the restriction of $f$ to $N$ has index 2, and $N$ contains $P_1$ and $P_2$. The proof of the lemma then follows as in case (b).

18. To end the proof of Theorem 4, let us consider a fixed hyperbolic plane $P$. We are going to show that every unitary transformation $v$ can be written $su$, where $s$ is a hyperbolic rotation of plane $P$, and $u$ belongs to $T_n$. The result is true if $v$ is a hyperbolic rotation of plane $P'$, for by Lemma 7 there exists $t \in T_n$ such that $t(P) = P'$, and therefore $v = tst^{-1}$, where $s$ is a
rotation of plane $P$; but we can also write $v = s^{-1}ts^{-1}$, and as $T_n$ is a normal subgroup, $s^{-1}ts^{-1} \in T_n$. Suppose now that $v$ is a product of $p$ hyperbolic rotations (Lemma 5), and use induction on $p$. Let $v = w_1w_2$, where $w_1$ is a hyperbolic rotation and $w_2$ is a product of $p-1$ hyperbolic rotations; we can write by assumption $w_1 = s_1u_1$, $w_2 = s_2u_2$, hence $v = s_1u_1s_2u_2 = s_1s_2(s_2^{-1}u_1s_2)u_2$, and this proves our contention. We have thus shown that the group $U_n/T_n$ is isomorphic to $\Gamma/(\Gamma \cap T_n)$, hence abelian (and isomorphic to a quotient group of $K^*/C$). Theorem 4 then follows from the fact that $T_n/W_n$ is a simple group (Theorem 1).

19. In special cases it is possible to obtain more precise information. Let us suppose for instance that $K$ is the skewfield of ordinary quaternions over a Euclidean ordered field $Z$ (i.e., an ordered field in which every positive element has a square root in $Z$). The usual theory of quaternions can then be carried out exactly as when $Z$ is the field $R$ of real numbers; we know therefore that every quaternion $\xi \neq 0$ can be written in one and only one way $\xi = \rho \gamma$, where $\rho \in Z$, $\rho > 0$, and $\rho^2 = N(\xi)$, hence $N(\xi) = 1$; moreover, every quaternion of norm 1 is a commutator; finally, if $\xi$ and $\eta$ are two quaternions of norm 1 and scalar 0, there is a third quaternion $\alpha$ of norm 1 such that $\xi = \alpha \eta \alpha^{-1}$. We suppose as usual that $J$ is the only involution in $K$ leaving invariant the elements of $Z$, and that $f$ is skew-hermitian. We can then show that there exists an orthogonal basis in $E$ with respect to which $f(x, y) = \sum_{k=1}^{n} \xi_k \overline{\xi}_k$. Indeed, there exists an orthogonal basis $(e_k)$ for $f$, and with respect to that basis, $f(x, y) = \sum_{k=1}^{n} \xi_k \alpha_k \overline{\xi}_k$, with $\alpha_k = -\alpha_k$, which means that the scalar of the quaternion $\alpha_k$ is 0. We can write $\alpha_k = \rho_k \beta_k$, with $\rho_k > 0$, $N(\beta_k) = 1$, and $\beta_k = -\beta_k$, and therefore $\alpha_k = \rho_k \gamma_k \gamma_k^{-1}$, where $N(\gamma_k) = 1$, hence $\gamma_k = \gamma_k^{-1}$. If we replace $e_k$ by $e_k (\rho_k^{-1}) \gamma_k$, we obtain for $f(x, y)$ the canonical expression $\sum_{k=1}^{n} \xi_k \overline{\xi}_k$. This proves that all nondegenerate skew-hermitian forms over $E$ are equivalent, hence their index is $[n/2]$. In particular, for $n \geq 4$, $\nu \geq 2$, and therefore Theorem 4 applies. But here every matrix

$$
\begin{pmatrix}
\alpha & 0 \\
0 & (\alpha^{-1})^J
\end{pmatrix}
$$

can be written

$$
\begin{pmatrix}
\gamma & 0 \\
0 & (\gamma^{-1})^J
\end{pmatrix}
\begin{pmatrix}
\rho & 0 \\
0 & \rho^{-1}
\end{pmatrix},
$$

where $N(\gamma) = 1$, hence $\gamma$ is a commutator, and $\rho \in Z$; as the matrix

$$
\begin{pmatrix}
\rho & 0 \\
0 & \rho^{-1}
\end{pmatrix}
$$

belongs to $SL_2(Z)$, the proof of Lemma 6 shows that we have here $\Gamma = \Gamma \cap T_n$, hence $U_n = T_n$. When $Z = R$, this is equivalent to one of E. Cartan's theorems.
on the real forms of the simple Lie groups [3, p. 286].

20. We end by mentioning some relations between our results and the properties of the commutator subgroup $C$ of a sfield $K$ with involution.

**Theorem 5.** Let $K$ be a sfield of characteristic $\neq 2$, of finite rank over its center $Z$, and let $J$ be an involution in $K$ leaving invariant the elements of $Z$. Then, for every $\xi \in K^*$, $\xi$ and $\xi^J$ are in the same class modulo the commutator subgroup $C$ of $K^*$.

Let $m^2$ be the rank of $K$ over its center, and let us suppose first that the set $S$ of symmetric elements in $K$ has dimension $m(m+1)/2$ over $Z$. Then we have seen in §14 that every element $\xi \in K^*$ can be written $\xi = \alpha \beta$, where $\alpha$ and $\beta$ are in $S$; accordingly $\xi^J = \beta^J \alpha^J = \beta \alpha$, hence $\xi^J \xi^{-1} = \beta \alpha^{-1} \beta^{-1}$, which proves our contention in that case. If on the contrary $S$ has dimension $m(m-1)/2$ over $Z$, and $\rho$ is a skew-symmetric element of $K$, then $\xi \rightarrow \xi^\rho = \rho^{-1} \xi^J \rho$ is an involution in $K$ for which the symmetric elements form a space of dimension $m(m+1)/2$ over $Z$ (§3); therefore $\xi$ and $\xi^\rho$ are in the same class modulo $C$, and the same is true for $\xi$ and $\xi^J$, since $\xi$ and $\rho^{-1} \xi \rho$ are in the same class modulo $C$.

The situation is reversed when $K$ is a sfield of the second kind:

**Theorem 6.** Let $K$ be a sfield of finite rank over its center $Z$, and let $J$ be an involution in $K$ which does not leave invariant every element of $Z$. Then there exist elements $\xi$ in $K^*$ such that $\xi$ and $\xi^J$ are not in the same class modulo $C$.

The theorem being obvious when $K$ is commutative, we can suppose that $K$ is not commutative, hence that $Z$ is an infinite field. The theorem will be proved if we exhibit a homomorphism $\phi$ of $K^*$ onto an abelian group, such that $\phi(\xi^J) \neq \phi(\xi)$ for some $\xi \in K^*$. Let $N(\xi)$ be the norm of an element $\xi$ in the regular representation of $K$ (considered as an algebra over its center $Z$); $\xi \rightarrow N(\xi)$ is then a homomorphism of $K^*$ into $Z^*$. If $r = m^2$ is the rank of $K$ over $Z$, we have $N(\xi) = \xi^r$ for every $\xi \in Z^*$; we have only therefore to verify that if the element $\omega \in Z$ constitutes with the identity a basis of $Z$ over the subfield $Z_0$ of $J$-invariant elements, then the elements $(x+y\omega)^r$ and $(x+y\omega^J)^r$ cannot be identical for all values of $x$ and $y$ in $Z_0$. But as $\omega^J \neq \omega$, this follows at once from the fact that $Z_0$ is an infinite field.

Theorem 6 has as a consequence that when $K$ is a sfield of the second kind, the groups $U_n$ and $T_n$ (for \( n \geq 1 \)) are always distinct. To prove this, we have only to verify that the determinant [4] of some unitary matrix is not the identity element in $K^*/C$; but this is obvious for the matrix

$$
\begin{pmatrix}
\alpha & 0 \\
0 & (\alpha^{-1})^J
\end{pmatrix}
$$

if $\alpha$ and $\alpha^J$ are not in the same class modulo $C$.  

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Bibliography


University of Nancy,
Nancy, France.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use