Hiroyuki Ishibashi

Decomposition of isometries of isotropic $U_n(V)$ over finite fields into simple isometries

Czechoslovak Mathematical Journal, Vol. 31 (1981), No. 2, 301–305

Czechoslovak Mathematical Journal, 31 (106) 1981, Praha

DECOMPOSITION OF ISOMETRIES OF $U_n(V)$ OVER FINITE FIELDS INTO SIMPLE ISOMETRIES

HIROYUKI ISHIBASHI, Sakado

(Received November 7, 1979)

1. INTRODUCTION

Let K be a finite field with an involution $*$. We assume char $K \neq 2$. Let V be an n-dimensional right vector space over K with a λ-hermitian form $f : V \times V \to K$. Thus λ is a fixed element of K with $\lambda\lambda^* = 1$ and f is a sesquilinear form satisfying $f(y, x) = \lambda^* f(x, y)^*$ for all x, y in V. We assume f is non-singular, that is, the mapping $V \to \mathrm{Hom}_K(V, K)$ given by $x \mapsto f(\cdot, x)$ is an isomorphism. We shall write in this paper xy for $f(x, y)$. For a vector u in V if $u^2 = 0$, then u is called *isotropic*. A vector space having an isotropic vector is also said isotropic. We assume $i(V) \geqq 1$. Namely we can fix an orthogonal splitting $V = H \perp L$ with $H = uK + vK$ a hyperbolic plane with $uv = 1$ and $u^2 = v^2 = 0$. The unitary group $U_n(V)$, or simply $U(V)$, is the set of isometries φ, i.e., φ in $\mathrm{Aut}_K(V)$ with $\varphi x \varphi y = xy$ for all x, y in V. An isometry which fixes a hyperplane of V is called *a quasi symmetry or unitary transvection* according as the hyperplane is nonsingular or not (resp.).

If $* = 1$ and $\lambda = 1$, then the unitary group is called an *orthogonal group* and denoted by $O_n(V)$ or $O(V)$. If $* = 1$ and $\lambda = -1$, then we say it a symplectic group and denote it by $\mathrm{Sp}_n(V)$ or $\mathrm{Sp}(V)$.

By Ishibashi [3] we know $O_n(V)$ is generated by n symmetries either K is isotropic or not but with char $K \neq 2$. In [4] I have shown $\mathrm{Sp}_n(V)$ is generated by n symplectic transvections and one isometry Δ_α without the assumption char $K \neq 2$.

In the present paper we consider the analogous problem for $U_n(V)$. Our purpose is to prove the following theorem.

Theorem. *Let V be an n dimensional nonsingular λ-hermitian space over a finite field of characteristic not 2. Suppose V can be splitted a hyperbolic plane H. S denotes the set of quasi symmetries and unitary transvections:*

(i) *$U_2(H)$ is generated by 2 or 3 elements of S.*

(ii) *$U_n(V)$ is generated by $U_2(H)$ and $n - 2$ elements of S.*

(iii) *$O_n(V)$ is generated by n symmetries (this is true either V is isotropic or not by Ishibashi [3]).*

(iv) *$\mathrm{Sp}_n(V)$ is generated by $n + 1$ symplectic transvections.*

2. GENERATORS AND RELATIONS

We introduce the isometries used in the generation of $U(V)$. We put $C = \{c \in K \mid c + \lambda c^* = 0\}$.

Δ is defined by $u \to v$, $v \to u\lambda$ and $\Delta = 1$ on L.

$\Phi(a)$ is defined for $a \neq 0$ in K by $u \to ua$, $v \to v(a^*)^{-1}$ and $\Phi(a) = 1$ on L.

$T(u, c)$ is defined for any c in C by $T(u, c)\, z = z + u \,.\, c \,.\, uz$, $z \in V$.

$E(u, x)$ is defined for any x in L by $E(u, x).z = z + u \,.\, xz - x \,.\, \lambda \,.\, uz - u \,.\, \frac{1}{2} \,.\, \lambda \,.\, x^2 \,.\, uz$, $z \in V$.

$T(u, C) = \{T(u, c) \mid c \in C\}$ and $E(u, Y) = \{E(u, y) \mid y \in Y\}$ for any subset Y of L.

Similarly we define $T(v, c)$ and $E(v, x)$. Let x, y be vectors in V with $xy \neq 0$. Then we have $V = y^\perp \oplus xK$ where $y^\perp = \{z \in V \mid yz = 0\}$. So, if $x^2 = (x + y)^2$, then a linear map τ on V which defined by $\tau = 1$ on $y^\perp$ and $\tau x = x + y$ is an isometry on V. We write $\tau_{x,y}$ for τ. τ is called a *quasi symmetry* if $y^2 \neq 0$, and a unitary transvection if $y^2 = 0$. Therefore $T(u, c)$ above is a unitary transvection.

The following identities can be easily verified:

$$T(u, a)\, T(u, b) = T(u, a + b)\,. \tag{1}$$

$$\Phi(a)\, T(u, c)\, \Phi(a)^{-1} = T(u, aca^*)\,. \tag{2}$$

$$E(u, x)^r = E(u, xr)\,, \quad r \in Z\,. \tag{3}$$

$$\Phi(a)\, E(u, x)\, \Phi(a^{-1}) = E(u, xa^*)\,. \tag{4}$$

$$[E(u, x\, 2^{-1}), E(u, y)]^{-1}\, E(u, x)\, E(u, y) = E(u, x + y)\,. \tag{5}$$

3. PRELIMINARY LEMMAS

We have a splitting $V = H \perp L$. $U(H)$ denotes the subgroup of $U(V)$ which consists of all isometries φ with $\varphi = 1$ on L. Let $X = \{x_1, \ldots, x_{n-2}\}$ be a fixed base for L.

Lemma 3.1. $U(V) = \langle U(H), E(u, L)\rangle$ (see James [5], Theorem 2.2.).

Proof. We wirte $G = \langle U(H), E(u, L)\rangle$ and show $U(V) = G$. Note $E(v, L) \subset G$, since for Δ in $U(H)$ we have $\Delta E(u, L)\, \Delta^{-1} = E(v, L)$.

Take any φ in $U(V)$. We have a base $X = \{x_1, \ldots, x_{n-2}\}$ for L. Assume φ fixes $x_1, \ldots, x_{i-1}$ and not x_i, $i \leqq n-2$. Define $D = \{\sigma \in G \mid \sigma \text{ fixes } x_1, \ldots, x_{i-1}\}$. We shall show there exists σ in D with $\sigma\varphi x_i = x_i$. The proof will proceed step by step. First, to simplify the notations we write x for x_i and express $\varphi x = ua + vb + z$, $a, b \in K$ and $z \in L$.

Step i). For some σ_1 in D we have $\sigma_1\varphi x = uc + vd + z$, $c, d \in K$ and $c \neq 0$.

Because, if $a \neq 0$ then let $\sigma_1 = 1$. If $a = 0$ and $b \neq 0$ then let $\sigma_1 = \Delta$. Assume $a = b = 0$, i.e., $\varphi x = z$. Then, considering a dual base of $\varphi X = \{x_1, \ldots, x_{i-1}, z, \ldots\}$, we may choose w in L with $wx_1 = \ldots = wx_{i-1} = 0$ and $wz = 1$. Then $E(u, w)\, z = z + u$, so let $\sigma_1 = E(u, w)$.

Step ii). For some σ_2 in D we have $\sigma_2\sigma_1\varphi x = uc + ve + x$, $e \in K$.

Because, put $t = z - x$. Then $t \in L$ and for $j = 1, \ldots, i-1$ we have $x_j x = (\sigma_1\varphi x_j)(\sigma_1\varphi x) = x_j z = x_j x + x_j t$. Hence $x_j t = 0$ for $j = 1, \ldots, i-1$. Therefore $\sigma_2 = E(v, tc^{-1})$ is the desired one.

Step iii). For some σ_3 in D we have $\sigma_3\sigma_2\sigma_1\varphi x\ uc + x$.

Because, by $x^2 = (uc + ve + x)^2$, we have $(uc + ve)^2 = 0$. Let $\sigma_3 = \tau_{u, -vc^{-1}e}$.

Step iv). For some σ_4 in D we have $\sigma_4\sigma_3\sigma_2\sigma_1\varphi x = x$.

Because, we have y in L with $yx_1 = \ldots = yx_{i-1} = 0$ and $yx = 1$. So, let $\sigma_4 = E(u, -yc^*)$.

Thus if we take $\sigma = \sigma_4\sigma_3\sigma_2\sigma_1$, then $\sigma\varphi x_j = x_j$ for $j = 1, \ldots, i$. Now by induction on i, we have ϱ in G with $\varrho\varphi = 1$ on L, i.e., $\varrho\varphi$ is in $U(H)$ and so φ is in G. Q.E.D.

Lemma 3.2. $U(V) = \langle U(H), E(u, X)\rangle$.

Proof. By the previous lemma it suffices to show $E(u, L) \subset \langle \Phi(\alpha), E(u, X)\rangle$. This inclusion is given by the identities in § 2. By (4) we have $E(u, x_iK) \subset \langle \Phi(\alpha), E(u, x_i)\rangle$ and by (3), (5) we have $E(u, x + y) \subset \langle E(u, x), E(u, y)\rangle$ for any x, y in L. Thus we have the lemma. Q.E.D.

Lemma 3.3. $U(H) = \langle \Phi(\alpha), \Delta, T(u, C)\rangle$.

Proof. We note $\Delta T(u, C)\, \Delta^{-1} = T(v, C)$. Take any φ in $U(H)$. Put $\varphi u = ua + vb$, $a, b \in K$. We may assume $a \neq 0$. Because, if $a = 0$, then $b \neq 0$, consider $\Delta\varphi$ for φ. Since α generates $K - \{0\}$, we may write $a = \alpha^i$ for some i. Then $\Phi^{-i}(\alpha) \,.\, T(v, -\lambda ba^{-1})\, \varphi$ is in $T(u, C)$. Q.E.D.

Definition. $K_0 = \{a \in K \mid a^* = a\}$.

K_0 is a subfield of K. Let $\beta = \alpha^m$ be a generator of the multiplicative cyclic group $K_0 - \{0\}$. We note $\beta \neq 1$. Because, if $\beta = 1$, then $K_0 = \{0, 1\}$ which implies char $K = 2$, a contradiction.

Suppose $c \neq 0$ exists in C. Take any b in C. By $c + \lambda c^* = 0$ and $b + \lambda b^* = 0$, we have $bc^{-1} = -\lambda b^*(-\lambda c^*)^{-1} = (bc^{-1})^*$. This means bc^{-1} is in K_0. Thus we see $C \subset cK_0$. The converse $cK_0 \subset C$ is clear. Therefore, for any $c \neq 0$ in C, we have $C = cK_0$ and $cK_0 - \{0\} = \{c\beta^i \mid i = 1, 2, \ldots\} = \{c\alpha^{mi} \mid i = 1, 2, \ldots\}$.

Lemma 3.4. *For some even numbers r and s, it holds* $\beta^r + \beta^s = \beta$ *or* $\beta^r - \beta^s = \beta$.

Proof. Since $\beta \neq 1$, we have $\beta - 1 \neq 0$. Write $\beta - 1 = \beta^s$. If s is even, then the lemma is clear (put $r = 0$). If s is odd, then $\beta^2 - \beta = \beta^{s+1}$ gives the lemma.

Q.E.D.

Lemma 3.5. $U(H) = \langle \Phi(\alpha), \Delta, T(u, c) \rangle$ *for any c in* $C - \{0\}$.

Proof. By Lemma 3.3 it suffices to show $T(u, C) = \langle \Phi(\alpha), T(u, c) \rangle$. We know $C = \{c\beta^i \mid i = 1, 2, \ldots\}$. Hence $T(u, C) = \{T(u, c\beta^i) \mid i = 1, 2, \ldots\}$. Since $\beta = \alpha^m$ and $\beta \in K_0$, for any i we have $\Phi(\alpha)^{mi}\, T(u, c)\, \Phi(\alpha)^{-mi} = T(u, c\beta^{2i})$. By Lemma 3.4, for some even r and s we can express $\beta = \beta^r \pm \beta^s$. From this we have $\Phi(\alpha)^{mi} \,.\, T(u, c\beta^r)\, T(u, c\beta^s)^{\pm 1}\, \Phi(\alpha)^{-mi} = T(u, c\beta^{2i+1})$. Q.E.D.

4. PROOF OF THE THEOREM

(a) Proof of (i).

Define $\tau_1 = \tau_{v,u-v}$ and $\tau_2 = \tau_{u,v\alpha-u}$. Therefore, $\tau_1 : v \to u,\ u \to u(1 - \lambda^*) + v\lambda^*$ and $\tau_2 : u \to v\alpha,\ v \to u\lambda\alpha^{*-1} + v(1 - \lambda\alpha\alpha^{*-1})$.

First let $C = \{0\}$. It is easy to see that $a\lambda - a^*$ is in C for any a in K. Hence it must be $\lambda = 1$ and $* = 1$. Namely $U(H) = O(H)$ and $\tau_1 = \Delta$, $\tau_1\tau_2 = \Phi(\alpha)$. Thus by Lemma 3.5 we have $U(H) = \langle \tau_1, \tau_2 \rangle$.

Next let $C \neq \{0\}$. For above τ_1 and τ_2 we write $\tau = \tau_1\tau_2$. Take any $0 \neq c$ in C. We note $\tau u = u\alpha = \Phi(\alpha)\, u$. Hence by the same way as the proof of Lemma 3.5, we have $T(u, C) \subset \langle \tau, T(u, c) \rangle$. Further, since $\Delta^{-1} = T(u, 1 - \lambda)\, \tau_1$ and $\Phi(\alpha) = \Delta^{-1} T(v, \alpha\lambda - \alpha^*)\, \tau_2$, we have $U(H) = \langle \tau_1, \tau_2, T(u, c) \rangle$.

(b) Proof of (ii).

Let x be any nonzero vector of L. Take y in L with $xy = 1$. Then $V = x^\perp \oplus yK$. By an direct computation we see $\tau_{y,x+u}^{-1}\, \Phi(2^{-1})\, \tau_{y,x+u}\, E(u, x)$ is in $U(H)$, because it is the identity map on L. Thus $E(u, x)$ is in $\langle U(H), \tau_{y,x+u} \rangle$. Now, running x in the base $X = \{x_1, \ldots, x_{n-2}\}$ for L, we can choose $\{\tau_1, \ldots, \tau_{n-2}\}$ in S such that $E(u, x_i) \in \langle U(H), \tau_i \rangle$. Thus, Lemma 3.2 gives $U(V) = \langle U(H), \tau_1, \ldots, \tau_{n-2} \rangle$.

(c) Proof of (iii) and (iv).

If $U(V) = O(V)$, then $C = \{0\}$. Hence $O(H)$ is generated by 2 symmetries by the case (a) above. So, we have (iii). If $U(V) = \mathrm{Sp}(V)$, then $C = K$. Hence $\mathrm{Sp}(H)$ is generated by 3 symplectic transvections by (a). This implies (iv). Thus we have completed the proof of the theorem.

References

[1] *J. Dieudonné:* On the structure of unitary groups, Trans. Amer. Math. Soc. *72* (1952), 367—385.

[2] *J. Dieudonné:* La Géométrie des groupes classiques, 3rd ed., Springer-Verlag, Berlin/New York, 1971.

[3] *H. Ishibashi:* Generators of an orthogonal group over a finite field, Czechoslovak Math. J. *28* (1978), 419—433.

[4] *H. Ishibashi:* Minimal sets of generators of symplectic groups over finite fields (preprint).

[5] *D. G. James:* Unitary Groups over Local Rings*, J. Algebra *52* (1978), 354—363.

Author's address: Department of Mathematics, Josai University, Sakado, Saitama, Japan.