Czechoslovak Mathematical Journal

Hiroyuki Ishibashi

Generators of an orthogonal group over a finite field

Czechoslovak Mathematical Journal, Vol. 28 (1978), No. 3, 419–433

Persistent URL: http://dml.cz/dmlcz/101547

Czechoslovak Mathematical Journal, 28 (103) 1978, Praha

GENERATORS OF AN ORTHOGONAL GROUP OVER A FINITE FIELD

HIROYUKI ISHIBASHI, Sakado

(Received July 19, 1976)

In this paper we consider orthogonal groups over finite fields, and obtain a system of generators which consists of some symmetries. The number of the generators equals the dimension of the space on which the orthogonal group is defined. We shall easily observe that this system is a minimal one when we consider symmetries as generators.

1. INTRODUCTION

Let F be a finite field of characteristic not 2, V an n-dimensional vector space over F with a symmetric bilinear form B and an associated quadratic map Q, i.e. $Q(v) = B(v, v)$, $v \in V$. We suppose that V is non-singular, which means $\det \{B(v_i, v_j)\} \neq 0$ for a basis $\{v_i\}$ of V. For subspaces U and W of V, $U \perp W$ means $U \oplus W$ with $B(u, w) = 0$ for all $u \in U$ and $w \in W$. We know that V has an orthogonal basis $\{e_i\}$, i.e. $V = \overset{n}{\underset{i=1}{\perp}} Fe_i$, $e_i \in V$.

$O_n(V)$ is the orthogonal group on V, its elements are called *isometries*. A special isometry which fixes a hyperspace of V is called *a symmetry* and the set of all symmetries is denoted by $S(V)$. It is well known that $S(V)$ generates $O_n(V)$. However, this system of generators seems to me rather large, in other words it is not necessary to consider all symmetries to generate $O_n(V)$. In fact, we shall show that only n symmetries generate $O_n(V)$, which is our main result. Further, we see that $O_n^+(V)$ is generated by $n - 1$ rotations. In particular, $O_2^+(V)$ is cyclic.

The details will be stated in Theorems A and B in § 3, after we introduce the necessary notation and prove some lemmas in § 2.

Since $F^* = F - \{0\}$ is a multiplicative cyclic group, we can take a single generator ζ for F^*. By the assumption that char $F \neq 2$, $|F|$ is odd and $|F^*|$ is even. Hence $|F^*/(F^*)^2| = 2$. This implies that any element of F^* is 1 or ζ modulo $(F^*)^2$. Therefore we can take an orthogonal basis for V in which each basis element represents 1 or ζ, where we say that a vector v represents c if $Q(v) = c$. If V has an orthogonal basis $\{e_1, \ldots, e_n\}$ such that each e_i represents $a_i \in F$, $1 \leqq i \leqq n$, then we say that V is of the $(a_1, \ldots, a_n)$-type and denote it by

$$V \simeq \langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle$$

or simply

$$V \sim (a_1, \ldots, a_n) .$$

We wish to investigate relations between these types. We know that ord $\zeta = |F^*|$ is even, so put ord $\zeta = 2m$. Let $S_0 = \{\zeta^i \mid i \text{ is even}\}$ and $S_1 = \{\zeta^j \mid j \text{ is odd}\}$, i.e. $S_0 = (F^*)^2$ and $S_1 = F^* - (F^*)^2$. Clearly

$$F = S_0 \cup \{0\} \cup \{S_1\} \quad \text{(direct sum)} .$$

Define a permutation φ on F by $\varphi(a) = a + 1$, $a \in F$.

Lemma 2.1. $\varphi(S_0) \cap S_1 \neq \emptyset$.

Proof. Suppose $\varphi(S_0) \cap S_1 = \emptyset$. Then $\varphi(S_0) \subset \{0\} \cup S_0$. Since $\varphi(0) = 1 \in S_0$, we have $\varphi(\{0\} \cup S_0) = \{0\} \cup S_0$. Hence $\varphi(S_1) = S_1$. Take an element ζ^j in S_1. Then j is odd, $2m - j$ is also odd and $\zeta^{-j} = \zeta^{2m-j}$ is contained in S_1. So we have

$$\varphi(\zeta^j) = \zeta^j + 1 = \zeta^j(1 + \zeta^{-j}) = \zeta^j\, \varphi(\zeta^{-j}) = \zeta^j\, \varphi(\zeta^{2m-j}) .$$

This is a contradiction. Indeed, $\varphi(S_1) = S_1$ implies that the left hand side of the above equation belongs to S_1 while the right hand side belongs to S_0 as a product of two elements of S_1. Q.E.D

Lemma 2.2.

i) *If* $V \sim (1, \zeta)$, *then* $V \sim (\zeta, 1)$.

ii) *If* $V \sim (\zeta, \zeta)$, *then* $V \sim (1, 1)$.

iii) *If* $V \sim (1, \zeta)$, *then* $V \not\sim (1, 1)$.

Proof. Let $V = Fe_1 \perp Fe_2$. We suppose $Q(e_1) = 1$ and $Q(e_2) = \zeta$ to prove i). Then i) is obtained by permuting e_1 and e_2. Now we shall prove ii). Let $Q(e_1) = Q(e_2) = \zeta$. By the lemma, there exists $a \in F$ such that $a^2 + 1$ belongs to S_1. Putting $v = ae_1 + e_2$, we conclude that $Q(v) = a^2\zeta + \zeta = (a^2 + 1)\,\zeta$ is contained in S_0. So we put $Q(v) = \zeta^{2r}$ and take the following new basis $\{e_1', e_2'\}$ which will be the desired one:

$$e_1' = \zeta^{-r} v \quad \text{and} \quad e_2' = \zeta^{-r}(e_1 - ae_2).$$

Indeed,

$$Q(e_1') = \zeta^{-2r} Q(v) = 1,$$
$$Q(e_2') = \zeta^{-2r} Q(e_1 - ae_2) = \zeta^{-2r} Q(v) = 1$$

and

$$B(e_1', e_2') = B(\zeta^{-r}v, \zeta^{-r}(e_1 - ae_2)) =$$
$$= \zeta^{-2r} B(ae_1 + e_2, e_1 - ae_2) = 0.$$

Hence $V \sim (1, 1)$. Finally, iii) follows from the uniqueness of the discriminant dV of a quadratic space V. It is defined for any basis $\{e_i\}$ of V by det $B(e_i, e_j)$ modulo $(F^*)^2$, which is independent of the choice of the basis. Therefore if $V \sim (1, \zeta)$, then d$V \equiv \zeta$. If $V \sim (1. 1)$, then d$V \equiv 1$. But clearly $1 \not\equiv \zeta$ modulo $(F^*)^2$. Q.E.D.

Thus, according to the lemma there exist only two distinct types $(1, 1)$ and $(1, \zeta)$ for a binary space V. Consequently, applying the lemma successively, we have for an n-dimensional space V the following

Lemma 2.3. *$V \sim (\underbrace{1, 1, \ldots, 1}_{n})$ or $(\underbrace{1, 1, \ldots,}_{n-1} 1, \zeta)$.*

3. STATEMENT OF THE THEOREMS

Theorem A. a) *$O_n(V)$ is generated by n symmetries.*

b) *If $\{\tau_{y_i} \in S(V) \mid 1 \leqq i \leqq n\}$ are generators, then there are $r, s \in \{1, \ldots, n\}$ such that*

$$Q(y_r) \equiv 1 \quad \text{and} \quad Q(y_s) \equiv \zeta \quad \text{modulo} \quad (F^*)^2.$$

c) *τ_{y_1} may be arbitrarily chosen in $S(V)$.*

d) *$O_n(V)$ is not generated by less than n symmetries.*

Let ϱ be any isometry and M its matrix on a basis of V, then det $M = \pm 1$. If det $M = 1$, we call ϱ *a rotation* and the set of rotations is denoted by $O_n^+(V)$. ϱ is called *a reflexion*, if det $M = -1$.

$O_n^+(V)$ is a normal subgroup of $O_n(V)$ and $|O_n(V)/O_n^+(V)| = 2$.

Theorem B. *For $n \geqq 2$, $O_n^+(V)$ is generated by $n - 1$ rotations.*

In § 4 we shall prove Theorems A and B for $n = 2$. The general case of the theorems will be treated in § 5 and § 6, respectively.

4. PROOF OF THEOREMS A AND B FOR $n = 2$

In this section we shall show that $O_2(V)$ is generated by two symmetries and $O_2^+(V)$ is a cyclic group.

Put $V = Fe_1 \perp Fe_2$. Then we know from the preceding section that V is of the type $(1, 1)$ or $(1, \zeta)$. So we put

$$Q(e_1) = 1 \quad \text{and} \quad Q(e_2) = \varepsilon\,, \quad \varepsilon = 1 \quad \text{or} \quad \zeta\,.$$

Hence

$$V \sim (1, \varepsilon)\,.$$

Now we shall try to express isometries by matrices with respect to the above fixed basis $\{e_1, e_2\}$. Let $\varrho \in O_n(V)$ be an isometry.

Lemma 4.1. *ϱ is a rotation if and only if its matrix is expressed as*

$$\begin{pmatrix} a & -\varepsilon b \\ a & a \end{pmatrix} \quad \textit{with} \quad a^2 + \varepsilon b^2 = 1\,, \quad a, b \in F\,.$$

Proof. Let ϱ be a linear map on V defined by a matrix

$$\begin{pmatrix} a & -\varepsilon b \\ b & a \end{pmatrix}.$$

Then

$$\begin{aligned} Q(\varrho e_1) &= Q(ae_1 + be_2) = a^2 + \varepsilon b^2 = 1\,, \\ Q(\varrho e_2) &= Q(-\varepsilon b e_1 + ae_2) = \varepsilon^2 b^2 + \varepsilon a^2 = \varepsilon(\varepsilon b^2 + a^2) = \varepsilon\,, \\ B(\varrho e_1, \varrho e_2) &= B(ae_1 + be_2,\ -\varepsilon b e_1 + ae_2) = -\varepsilon ab + \varepsilon ab = 0 \end{aligned}$$

and

$$\det \begin{pmatrix} a & -\varepsilon b \\ b & a \end{pmatrix} = a^2 + \varepsilon b^2 = 1\,.$$

Hence ϱ is a rotation, i.e. $\varrho \in O_n^+(V)$.

Conversely, let ϱ be a rotation. Put $\varrho e_1 = ae_1 + be_2$, $a, b \in F$. Then we have $B(\varrho e_1, -\varepsilon b e_1 + ae_2) = 0$ as above. This means that $-\varepsilon b e_1 + ae_2$ is contained in $(F\varrho e_1)^\perp = F\varrho e_2$. Consequently ϱe_2 belongs to $F(-\varepsilon b e_1 + ae_2)$. Write

$$\varrho e_2 = c(-\varepsilon b e_1 + ae_2) \quad \text{for some} \quad c \in F\,,$$

The matrix of ϱ is given by

$$\begin{pmatrix} a & -\varepsilon bc \\ b & ac \end{pmatrix}.$$

Since ϱ is a rotation,

$$1 = \det\begin{pmatrix} a & -\varepsilon bc \\ b & ac \end{pmatrix} = a^2c + \varepsilon b^2 c =$$

$$= c(a^2 + \varepsilon b^2) = c\, Q(\varrho e_1) = c\, Q(e_1) = c\,.$$

Q.E.D.

From now we shall identify an isometry and its matrix with respect to the basis $\{e_1, e_2)$ of V.

Remark. ϱ is a reflexion if and only if its matrix is

$$\begin{pmatrix} a & \varepsilon b \\ b & -a \end{pmatrix} \quad \text{with} \quad a^2 + \varepsilon b^2 = 1\,.$$

By an easy computation, we have

$$\begin{pmatrix} a & -\varepsilon b \\ b & a \end{pmatrix}\begin{pmatrix} c & -\varepsilon d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - \varepsilon bd & -\varepsilon(ad + bc) \\ ad + bc & ac - \varepsilon bd \end{pmatrix} =$$

$$= \begin{pmatrix} c & -\varepsilon d \\ d & c \end{pmatrix}\begin{pmatrix} a & -\varepsilon b \\ b & a \end{pmatrix}, \quad a, b, c, d \in F\,.$$

This shows that $O_2^+(V)$ is a finite abelian group.

Lemma 4.2. *Let G be an abelian group and a an element which has the maximal order in G. Then for any b in G,* ord b *divides* ord a.

Proof. For any prime number p, let

$$\operatorname{ord} a = p^\lambda c\,, \quad 0 \leqq \lambda\,, \quad p \nmid c$$

and

$$\operatorname{ord} b = p^\mu d\,, \quad 0 \leqq \mu\,, \quad p \nmid d\,.$$

Then ord $a^{p^\lambda} = c$ and ord $b^d = p^\mu$. Hence we have ord $a^{p^\lambda} b^d = p^\mu c$. Therefore by the maximality of ord a,

$$p^\mu c \leqq p^\lambda c\,.$$

Hence $\mu \leqq \lambda$ and so $p^\mu \mid p^\lambda$. This implies the lemma, since p is any prime number.

Q.E.D.

Now, let us start with the proofs of the theorems for $n = 2$. Let σ be an element in $O_2^+(V)$ with the maximal order. We shall prove that σ generates $O_2^+(V)$, which is Theorem B for $n = 2$.

Since -1 is in $O_2^+(V)$ and its order is 2, by the preceding lemma, ord σ is even. So put

$$\operatorname{ord} \sigma = 2s\,.$$

We shall show that $|O_2^+(V)| = 2s$ which yields the desired result, $O_2^+(V) = \langle\sigma\rangle$. $|O_2^+(V)| \geqq 2s$ is clear, for $\sigma \in O_2^+(V)$. Therefore it suffices to show $O_2^+(V) \leqq 2s$.

Lemma 4.3. *Let x, y be indeterminants and r a natural number. Introduce a 2×2 matrix*

$$X = \begin{pmatrix} x & -\varepsilon y \\ y & x \end{pmatrix}.$$

Then there are polynomials h, k, h' and k' in two variables x^2 and y^2 such that

$$X^{2r} = \begin{pmatrix} h & -\varepsilon xyk \\ xyk & h \end{pmatrix} \tag{4.1}$$

and

$$X^{2r+1} = \begin{pmatrix} xh' & -\varepsilon yk' \\ yk' & xh' \end{pmatrix}. \tag{4.2}$$

The total degrees of h, xyk, h' and k' in x, y are obviously equal to or less than $2r$.

Proof. We prove the lemma by the induction on r. Since

$$X^2 = \begin{pmatrix} x & -\varepsilon y \\ y & x \end{pmatrix}^2 = \begin{pmatrix} x^2 - \varepsilon y^2 & -2\varepsilon xy \\ 2xy & x^2 - \varepsilon y^2 \end{pmatrix},$$

we have

$$X^{2(r+1)} = X^2 X^{2r} = \begin{pmatrix} x^2 - \varepsilon y^2 & -2\varepsilon xy \\ 2xy & x^2 - \varepsilon y^2 \end{pmatrix} \begin{pmatrix} h & -\varepsilon xyk \\ xyk & h \end{pmatrix} =$$

$$= \begin{pmatrix} (x^2 - \varepsilon y^2)\, h - 2\varepsilon x^2 y^2 k & -\varepsilon xy\{2h + (x^2 - \varepsilon y^2)\, k\} \\ xy\{2h + (x^2 - \varepsilon y^2)\, k\} & (x^2 - \varepsilon y^2)\, h - 2\varepsilon x^2 y^2 k \end{pmatrix}.$$

This proves (4.1). Applying (4.1), we obtain

$$X^{2r+1} = \begin{pmatrix} x & -\varepsilon y \\ y & x \end{pmatrix} \begin{pmatrix} h & -\varepsilon xyk \\ xyk & h \end{pmatrix} = \begin{pmatrix} x(h - \varepsilon y^2 k) & -\varepsilon y(h + x^2 k) \\ y(h + x^2 k) & x(h - \varepsilon y^2 k) \end{pmatrix},$$

which yields (4.2). Q.E.D.

In particular, we have the following

Corollary. *For suitable polynomials f and g in two variables x and y, we can write*

$$X^s = \begin{pmatrix} f & -\varepsilon g \\ g & f \end{pmatrix},$$

where $s = \frac{1}{2} \operatorname{ord} \sigma$.

Proof. If s is even, $s = 2r$, put $f = h$ and $g = xyk$. If s is odd, $s = 2r + 1$, put $f = xh'$ and $g = yk'$. Q. E. D.

Let ϱ be any element in $O_2^+(V)$ and let its matrix be

$$M = \begin{pmatrix} a & -\varepsilon b \\ b & a \end{pmatrix}, \quad a^2 + \varepsilon b^2 = 1\,, \quad a, b \in F$$

according to Lemma 4.1.

Then, substituting a, b for x, y, we obtain by the corollary

$$M^s = \begin{pmatrix} f(a, b) & -\varepsilon\, g(a, b) \\ g(a, b) & f(a, b) \end{pmatrix}.$$

By Lemma 4.2, $\varrho^{2s} = 1$ and so $M^{2s} = 1$.

Lemma 4.4. *Let*

$$N = \begin{pmatrix} c & -\varepsilon d \\ d & c \end{pmatrix} \quad \textit{with} \quad c^2 + \varepsilon d^2 = 1\,.$$

If $N^2 = 1$, *then* $N = \pm 1$. *So* $d = 0$.

Proof. Since

$$N^2 = \begin{pmatrix} c^2 - \varepsilon d^2 & -2\varepsilon cd \\ 2cd & c^2 - \varepsilon d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we have $c^2 - \varepsilon d^2 = 1$ and $2cd = 0$. By the assumption $c^2 + \varepsilon d^2 = 1$. So we obtain $2c^2 = 2$. Since char $F \neq 2$, $c^2 = 1$ and $c = \pm 1$. Hence $d = 0$. Thus we have $N = \pm 1$. Q.E.D.

By the lemma we have in M^s

$$g(a, b) = 0\,.$$

This means that (a, b) is a common solution in $F \times F$ of two polynomials $x^2 + \varepsilon y^2 = 1$ and $g(x, y) = 0$. Thus we conclude that any rotation in $O_2^+(V)$ corresponds to a common solution of these two polynomials. Let us put

$$t = \text{the number of common solutions of}$$

$$x^2 + \varepsilon y^2 = 1 \quad \text{and} \quad g(x, y) = 0 \quad \text{in} \quad F \times F\,.$$

Since distinct rotations correspond to distinct solutions of $x^2 + \varepsilon y^2 = 1$ by Lemma 4.1, we have

$$|O_2^+(V)| \leqq t\,.$$

We shall show $t \leqq 2s$. First, if s is odd, $s = 2r + 1$, then Lemma 4.3 and the identity $x^2 + \varepsilon y^2 = 1$ imply

$$g(x, y) = yk'(x^2, y^2) = yk'(1 - \varepsilon y^2, y^2) \quad \text{and} \quad \deg yk' \leqq s\,.$$

Hence g has at most s roots in F when we regard g as a polynomial in y. Further, for $y \in F$, $x^2 + \varepsilon y^2 = 1$ implies $x = \pm \sqrt{(1 - \varepsilon y^2)}$ in the algebraic closure $\bar{F}$ of F, which means that one root y of g gives 2 common solutions $(\pm \sqrt{(1 - \varepsilon y^2)}, y)$ in $\bar{F} \times F$. Hence t, the number of common solutions (x, y) in $F \times F$ is at most $2s$, i.e.

$$t \leqq 2s .$$

Now if s is even, $s = 2r$, then

$$g(x, y) = xyk(x^2, y^2) = xyk(1 - \varepsilon y^2, y^2)$$

and

$$\deg xyk \leqq s .$$

So the common solution (a, b) is a common solution of

$$\begin{cases} x = 0 \\ x^2 + \varepsilon y^2 = 1 \end{cases} \quad \text{or} \quad \begin{cases} yk(1 - y^2, y^2) = 0 , & \deg yk \leqq s - 1 \\ x^2 + \varepsilon y^2 = 1 . \end{cases}$$

The first system has at most 2 common solutions the second $2(s - 1)$, and so again

$$t \leqq 2 + 2(s - 1) = 2s .$$

Thus we have proved $t \leqq 2s$ for any s, i.e. we have proved that

$$O_2^+(V) = \langle \sigma \rangle .$$

Take any symmetry τ_u in $S(V)$. Then $\tau_u \notin O_2^+(V)$. Further, we know that $|O_2(V)/O_2^+(V)| = 2$. Hence

$$O_2(V) = \langle \tau_u, O_2^+(V) \rangle = \langle \tau_u, \sigma \rangle .$$

Put $\tau_v = \tau_u \sigma$. Then τ_v is also a symmetry and

$$O_2(V) = \langle \tau_u, \tau_v \rangle .$$

Thus $O_2(V)$ is generated by two symmetries, and one of them is arbitrarily chosen in $S(V)$. We shall conclude this section by the following lemma, which implies b) of Theorem A.

Lemma 4.5. *If $O_2(V) = \langle \tau_u, \tau_v \rangle$, then u represents* 1 *and v represents ζ modulo $(F^*)^2$, or vice versa.*

Proof. We suppose $Q(u) \equiv Q(v) \equiv \varepsilon$ modulo $(F^*)^2$, $\varepsilon = 1$ or ζ, and deduce a contradiction. Since any symmetry τ_y is a product of an odd number of τ_u, τ_v and $\tau_u^2 = \tau_v^2 = 1$, we have

$$\tau_y = \sigma \tau_u \sigma^{-1} \quad \text{or} \quad \varrho \tau_v \varrho^{-1}$$

for suitable σ, ϱ in $O_2(V)$. Hence

$$\tau_y = \tau_{\sigma u} \quad \text{or} \quad \tau_{\varrho v} .$$

Since

$$Q(\sigma u) = Q(u) = \varepsilon \quad \text{and} \quad Q(\varrho v) = Q(v) = \varepsilon ,$$

it holds for any $\tau_y \in S(V)$,

$$Q(y) \equiv \varepsilon \text{ modulo } (F^*)^2 .$$

But this is impossible. Indeed, by Lemma 2.1 there exists $a \in F$ with $a^2 + 1 \in S_1$, i.e. $a^2 + 1 = \zeta$ modulo $(F^*)^2$. Hence if we take $y = ae_1 + e_2$, then

$$Q(y) = a^2\varepsilon + \varepsilon = (a^2 + 1)\,\varepsilon \equiv \zeta\varepsilon \text{ modulo } (F^*)^2 .$$

So $\varepsilon = \zeta\varepsilon(F^*)^2$, which is a contradiction, for $1 \notin \zeta(F^*)$. Q.E.D.

The lemma shows that we may take the generators $\tau_{u'}$ and $\tau_{v'}$ of $O_2(V)$ with $Q(u') = 1$ and $Q(v') = \zeta$, by multiplying u, v by suitable scalars.

5. PROOF OF THEOREM A IN THE GENERAL CASE

In this section we shall prove Theorem A. First we prove a) and b) of the theorem, which will be done by induction on the dimension n of V. If $n = 2$, then a) and b) are true by § 4. Suppose $n \geqq 3$. Take a vector v_1 in V with

$$Q(v_1) = 1 \tag{5.1}$$

such a vector actually exists by Lemma 2.3. We split

$$V = Fv_1 \perp W . \tag{5.2}$$

The restrictions of B and Q to W make it a non-singular quadratic space. Hence by the inductive hypothesis for W, $O_{n-1}(W)$ is generated by $n - 1$ symmetries on W, say $\{\tau_{v_i} \mid 2 \leqq i \leqq n\}$, i.e. we have

$$O_{n-1}(W) = \langle \tau_{v_2}, \ldots, \tau_{v_n} \rangle \tag{5.3}$$

and we assume by b) of Theorem A

$$Q(v_2) = \zeta \quad \text{and} \quad Q(v_3) = 1 . \tag{5.4}$$

We divide the proof into the following two cases.

i) W is anisotropic or $|F| \neq 3$.

ii) W is isotropic and $|F| = 3$.

Case i). We put

$$H = Fv_1 \perp Fv_2 \quad \text{and} \quad J = Fv_1 \perp Fv_3 . \tag{5.5}$$

Then by § 4 we have two symmetries $\tau_{u_2} \in S(H)$ and $\tau_{u_3} \in S(J)$ such that

$$O_2(H) = \langle \tau_{v_1}, \tau_{u_2} \rangle \,, \tag{5.6}$$

$$O_2(J) = \langle \tau_{v_1}, \tau_{u_3} \rangle \,. \tag{5.7}$$

Definition. Let U be a non-singular subspace of V and ϱ in $O(U)$. Then $\varrho \perp 1_{U^\perp} \in O(V)$ is called *a natural extension of ϱ to V* and throughout this paper we shall denote it by ϱ'. For example, we write τ'_{v_i} for $\tau_{v_i} \perp 1_{Fv_1}$, $i \geqq 2$. It might be desirable to use the same notation for an isometry and its natural extension in order to simplify the proof. However, we are afraid of confusion. For this reason we shall distinguish them by the distinct notation as above.

Our purpose is to prove

$$O_n(V) = \langle \tau_{v_1}, \tau'_{u_2}, \tau'_{u_3}, \tau'_{v_4}, \ldots, \tau'_{v_n} \rangle \,, \tag{5.8}$$

which will directly yield a) of Theorem A. We note that we may write τ'_{v_1} for τ_{v_1} when we regard τ_{v_1} as an isometry on a non-singular subspace of V.

Since $O_n(V) = \langle S(V) \rangle$, it suffices to show that any symmetry $\tau_v \in S(V)$ is expressed by a product of some of the symmetries in (5.8). By (5.2) we write

$$v = av_1 + w \,, \quad a \in F \quad \text{and} \quad w \in W \,. \tag{5.9}$$

Proposition. *For v in (5.9) there exists ϱ in $O_2^+(H)$ such that if we express*

$$\varrho' v = a' v_1 + w' \,, \quad a' \in F \quad \textit{and} \quad w' \in W \,,$$

then $Q(w') \neq 0$.

Proof. If $Q(w) \neq 0$, then we can take $\varrho = 1$ in the expression (5.9), i.e. $v = av_1 + w$, and the proposition follows immediately. In particular, if W is anisotropic, then the proposition is true. So we suppose that W is isotropic and $Q(w) = 0$. Hence by (5.1)

$$Q(v) = a^2 \, Q(v_1) + Q(w) = a^2 \,.$$

Since

$$Q(\varrho' v) = (a')^2 \, Q(v_1) + Q(w') = (a')^2 + Q(w')$$

and

$$Q(v) = Q(\varrho' v) \,,$$

we have

$$a^2 = (a')^2 + Q(w') \,.$$

This shows that $Q(w') \neq 0$ if and only if $a^2 \neq (a')^2$. So we shall prove that such a ϱ actually exists in $O_2^+(H)$. Split

$$W = Fv_2 \perp Z$$

and write

$$w = bv_2 + z\,, \quad b \in F \quad \text{and} \quad z \in Z$$

Then

$$v = av_1 + bv_2 + z\,.$$

Let ϱ be a rotation in $O_2(H)$. Then ϱ' fixes z, since $V = H \perp Z$. Hence

$$\varrho' v = \varrho(av_1 + bv_2) + z\,.$$

Since H is of the $(1, \zeta)$ type by (5.5), Lemma 4.1 yields that ϱ is expressed as

$$\begin{pmatrix} c & -\zeta d \\ d & c \end{pmatrix} \quad \text{with} \quad c^2 + \zeta d^2 = 1\,, \quad c, d \in F$$

on the basis $\{v_1, v_2\}$. Hence

$$\varrho' v = (v_1, v_2)\begin{pmatrix} c & -\zeta d \\ d & c \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} + z = (ac - \varrho bd)\, v_1 + (ad + bc)\, v_2 + z\,.$$

This implies $a' = ac - \zeta bd$. Therefore $a^2 \neq (a')^2$ if and only if $a^2 \neq (ac - \zeta bd)^2$, i.e. it suffices that (c, d) is a solution of

$$x^2 + \zeta y^2 = 1$$

and

$$a^2 \neq (ax - \zeta by)^2\,.$$

On the other hand $a \neq 0$, since v is anisotropic. Hence the number of common solutions of the polynomials $x^2 + \zeta y^2 = 1$ and $a^2 = (ax - \zeta by)^2$ is at most 4. Thus if $x^2 + \zeta y^2 = 1$ has at least 5 solutions, then one of them does not satisfy $a^2 = (ax - \zeta by)^2$, and we obtain the desired $\varrho \in O_2^+(H)$. Moreover, we know that the solutions of $x^2 + \zeta y^2 = 1$ correspond one-to-one to the rotations of $O_2^+(H)$ by Lemma 4.1. Hence $x^2 + \zeta y^2 = 1$ has at least 5 solutions if and only if $|O_2^+(H)| \geqq 5$.

Lemma 5.1.

$$O_2^+(H) = \begin{cases} |F| + 1 & \textit{if} \quad H \quad \textit{is anisotropic}\,, \\ |F| - 1 & \textit{if} \quad H \quad \textit{is isotropic}\,. \end{cases}$$

Proof. Since $\dim H = 2$, reflexions are symmetries. Hence $|O_2^+(H)| = |S(H)|$. A symmetry is defined by an anisotropic line. So $|S(H)|$ equals the number of anisotropic lines of H. H has $|F| + 1$ lines $\{Fv_2, F(v_1 + cv_2)$ for all $c \in F\}$ and a line is isotropic if and only if $Q(v_1) + c^2\, Q(v_2) = 0$. Hence H is isotropic if and only if H has exactly 2 isotropic lines, otherwise H is anisotropic. Q.E.D.

By our assumption in the case i) $|F| \neq 3$ and throughout this paper char $|F| \neq 2$· So $|F| \neq 2, 4$. Therefore we have $|F| \geqq 5$. If $|F| \geqq 6$, then the lemma implies the desired result

$$|O_2^+(H)| \geqq |F| - 1 \geqq 5 .$$

When $|F| = 5$, the result is given by the following lemma.

Lemma 5.2. *If* $|F| = 5$, *then* $|O_2^+(H)| = 6$.

Proof. Since H is of the $(1, \zeta)$ type, the discriminant dV of H is ζ. On the other hand, if H were isotropic, then H would be a hyperbolic plane and its discriminant is -1. Hence

$$\zeta \equiv -1 \; (F^*)^2 .$$

This implies that ζ has an exponent $2 \times$ odd number. But this is a contradiction, since ord $\zeta = |F^*| = |F| - 1 = 4$. Hence H is anisotropic. Therefore by Lemma 5.1 we have $|O_2^+(H)| = 5 + 1 = 6$. O.E.D.

Thus we have completed the proof of the proposition.

Now, let us return to the situation mentioned before the statement of the proposition.

Let $\varrho \in O_2^+(H)$ be the isometry in the Proposition, i.e.

$$\varrho' v = a' v_1 + w' , \quad a' \in F , \quad w' \in W \quad \text{and} \quad Q(w') \neq 0 .$$

By $Q(w') \neq 0$, w' represents 1 or ζ modulo $(F^*)^2$. By (5.4), for $v_2, v_3 \in W$ we have $Q(v_2) = \zeta$ and $Q(v_3) = 1$. Hence taking a suitable $\sigma \in O(W)$, $\sigma w'$ is contained in Fv_2 or Fv_3 provided $Q(w') \equiv \zeta$ or 1, respectively. As usual, σ' is a natural extension of σ to V. Then

$$\sigma' \varrho' \tau_v (\varrho')^{-1} (\sigma')^{-1} = \tau_{\sigma' \varrho' v} = \tau_{\sigma'(a' v_1 + w')} = \tau_{a' v_1 + \sigma w'} \quad \text{for} \quad \sigma' = 1_{Fv_1} \perp \sigma .$$

Here by (5.5) and the choice of σ

$$a' v_1 + \sigma w' \in H \quad \text{or} \quad J .$$

On the other hand, (5.6) and (5.7) imply

$$O(H) = \langle \tau_{v_1}, \tau_{u_2} \rangle \quad \text{and} \quad O(J) = \langle \tau_{v_1}, \tau_{u_3} \rangle .$$

Therefore we may conclude

$$\tau_{a' v_1 + \sigma w'} \in \langle \tau'_{v_1}, \tau'_{u_2}, \tau'_{u_3} \rangle .$$

Hence

$$\tau_v = (\varrho')^{-1} (\sigma')^{-1} \tau_{a' v_1 + \sigma w'} \sigma' \varrho'$$

is contained in $\langle \tau'_{v_1}, \tau'_{u_2}, \tau'_{u_3}, \varrho', \sigma' \rangle$. However, ϱ belongs to $O_2^+(H)$ and $O_2^+(H) \subset O_2(H) = \langle \tau_{v_1}, \tau_{u_2} \rangle$, hence ϱ' is contained in $\langle \tau'_{v_1}, \tau'_{u_2} \rangle$. So

$$\tau_v \in \langle \tau'_{v_1}, \tau'_{u_2}, \tau'_{u_3}, \sigma' \rangle . \tag{5.10}$$

Moreover, the choice of σ together with (5.3) implies

$$\sigma \in O(W) = \langle \tau_{v_2}, \tau_{v_3}, \ldots, \tau_{v_n} \rangle .$$

However, by (5.6) and (5.7) we conclude

$$\tau_{v_2}, \tau_{v_3} \in \langle \tau_{v_1}, \tau_{u_2}, \tau_{u_3} \rangle .$$

Consequently

$$\sigma \in \langle \tau_{v_1}, \tau_{u_2}, \tau_{u_3}, \tau_{v_4}, \ldots, \tau_{v_n} \rangle .$$

So by (5.10) we have the desired result

$$\tau_v \in \langle \tau'_{v_1}, \tau'_{u_2}, \tau'_{u_3}, \tau'_{v_4}, \ldots, \tau'_{v_n} \rangle .$$

Thus we have proved that $O_n(V)$ is generated by n symmetries, which is the assertion a) of Theorem A. Since $Q(v_1) = 1$ and by (5.6) $O_2(H) = \langle \tau_{v_1}, \tau_{u_2} \rangle$, it is obviously $Q(u_2) \equiv \zeta\ (F^*)^2$ by Lemma 4.5. Therefore we have obtained b) of Theorem A. We have completed the proof of a) and b) in the case i).

Case ii). W is isotropic and $|F| = 3$.

Since $|F| = 3$, we have $F = \{0, \pm 1\}$ and $(F^*)^2 = \{1\}$. By (5.2)

$$V = Fv_1 \perp W, \quad Q(v_1) = 1 .$$

Take an isotropic vector $u \in W$ and a hyperbolic plane H such that

$$u \in H \subset W .$$

Split

$$H = Fe_2 \perp Fe_3 .$$

Then after multiplying e_1, e_2 by suitable scalars we may assume

$$u = e_2 + e_3 .$$

Clearly $Q(e_2) \neq 0$ and $Q(e_3) \neq 0$. Hence $Q(e_2)$ and $Q(e_3)$ are 1 or -1 for $F = \{0, \pm 1\}$.

Since

$$0 = Q(u) = Q(e_2) + Q(e_3) ,$$

we have $Q(e_2) = \pm 1$ and $Q(e_3) = \mp 1$. Thus we can suppose without loss of generality that

$$Q(e_2) = 1 \quad \text{and} \quad Q(e_3) = -1 .$$

Put

$$u_1 = v_1 + u .$$

By (5.3),

$$O(W) = \langle \tau_{v_2}, \tau_{v_3}, \ldots, \tau_{v_n} \rangle .$$

We denote

$$G = \langle \tau'_{v_2}, \tau'_{v_3}, \ldots, \tau'_{v_n} \rangle .$$

We shall prove

$$O_n(V) = \langle \tau_{u_1}, G \rangle = \langle \tau_{u_1}, \tau'_{v_2}, \ldots, \tau'_{v_n} \rangle$$

which implies a) of Theorem A. To do this, it suffices to show $S(V) \subset \langle \tau_{u_1}, G \rangle$.

Lemma 5.3.

$$\tau_{v_1+e_2} \in \langle \tau_{u_1}, G \rangle \, .$$

Proof. By the definition of symmetries,

$$\begin{aligned}
\tau_{u_1} e_3 &= e_3 - 2B(e_3, u_1)\, Q(u_1)^{-1}\, u_1 \\
&= e_3 + B(e_3, u_1)\, u_1 && (2 = -1 \text{ in } F \text{ and } Q(u_1) = 1.) \\
&= e_3 + B(e_3, v_1 + u)\, u_1 && (u_1 = v_1 + u.) \\
&= e_3 + B(e_3, v_1 + e_2 + e_3)\, u_1 && (u = e_2 + e_3.) \\
&= e_3 - u_1 && (B(e_3, v_1) = B(e_3, e_2) = 0 \quad \text{and} \\
& && Q(e_3) = -1.) \\
&= v_1 + e_2 \, .
\end{aligned}$$

Hence

$$\tau_{u_1} \tau_{e_3} \tau_{u_1} = \tau_{\tau_{u_1} e_3} = \tau_{v_1+e_2} \, .$$

So $\tau_{v_1+e_2}$ is in $\langle \tau_{e_3}, \tau_{u_1} \rangle$. On the other hand $e_3 \in H \subset W$, hence $\tau_{e_3} \in G$. Therefore $\tau_{v_1+e_2} \in \langle \tau_{u_1}, G \rangle$. Q.E.D.

Now, let τ_v be any symmetry in $S(V)$. We shall show that τ_v is contained in $\langle \tau_{u_1}, G \rangle$. Write

$$v = av_1 + w \, , \quad a \in F \quad \text{and} \quad w \in W \, .$$

If $a = 0$, then τ_v is contained in G. So we assume $a \neq 0$. Since $\tau_v = \tau_{a^{-1}v}$, we may suppose $a = 1$. Then

$$Q(v) = Q(v_1) + Q(w) = 1 + Q(w) \, .$$

Since $Q(v) \neq 0$, we have $Q(w) \neq -1$. So $Q(w) = 0$ or 1. Since for u, e_2 in W we have $Q(u) = 0$ and $Q(e_2) = 1$, we have

$$\lambda w = u \quad \text{or} \quad e_2$$

for some λ in $O(W)$. Hence

$$\lambda' \tau_v (\lambda')^{-1} = \tau_{\lambda' v} = \tau_{\lambda'(v_1+w)} = \tau_{v_1+\lambda w} = \tau_{u_1} \quad \text{or} \quad \tau_{v_1+e_2} \in \langle \tau_{u_1}, G \rangle \, .$$

Hence $O_n(V) = \langle \tau_{u_1}, G \rangle = \langle \tau_{u_1}, \tau_{v_2}, \ldots, \tau_{v_n} \rangle$, which was to be shown. Further, by (5.4) we have $Q(v_2) = \zeta$ and $Q(v_3) = 1$, so the assertion b) of Theorem A holds.

Thus we have proved a) and b) of Theorem A in both cases i) and ii). Finally, we prove c) and d) of Theorem A.

Proof of c).

Suppose $O_n(V) = \langle \tau_{y_i} \in S(V) \mid 1 \leqq i \leqq n \rangle$ with $Q(y_r) = 1$ and $Q(y_s) = \zeta$. Let τ_x be any symmetry in $S(V)$. Then $Q(x) \equiv 1$ or ζ modulo $(F^*)^2$. Hence for some $\mu \in O_n(V)$ we have

$$\mu y_r \quad \text{or} \quad \mu y_s \in Fx\,.$$

Therefore

$$\tau_x \in \{\tau_{\mu y_i} \mid 1 \leqq i \leqq n\} \quad \text{and} \quad O_n(V) = \langle \tau_{\mu y_i} \mid 1 \leqq i \leqq n \rangle\,.$$

This is nothing else but c).

Proof of d).

Suppose $O_n(V) = \langle \tau_i \mid 1 \leqq i \leqq r \rangle$ and $r < n$. We know that the fixed space of a symmetry is a hyperspace of V. So the intersection of the fixed spaces of all $\{\tau_i \mid 1 \leqq i \leqq r\}$ is not zero, since $r < n = \dim V$. Hence a certain non-zero vector is fixed by all $\{\tau_i\}$, which is a contradiction because $-1 \in O_n(V)$ reverses all vectors in V.

Thus Theorem A has been completely proved.

6. PROOF OF THEOREM B

Suppose $O_n(V)$ is generated by n symmetries, say $S = \{\tau_1, \ldots, \tau_n\}$. Putting $T = \{\tau_i\tau_n \mid 1 \leqq i \leqq n - 1\}$ we shall show $O_n^+(V) = \langle T \rangle$, which gives the theorem.

Take any ϱ in $O_n^+(V)$. Then ϱ is a product of an even number of elements of S. So we can write

$$\varrho = \prod_{i=1}^{\text{finite}} \lambda_i \mu_i\,, \quad \lambda_i \quad \text{and} \quad \mu_i \in S\,.$$

On the other hand by $\tau_n^2 = 1$, we have

$$\lambda_i \mu_i = \lambda_i \tau_n \tau_n \mu_i = \lambda_i \tau_n (\mu_i \tau_n)^{-1} \in \langle T \rangle\,.$$

Hence ϱ is contained in T and so

$$O_n^+(V) = \langle T \rangle\,.$$

Thus the proof of Theorem B is complete.

References

[1] *E. Artin:* Geometric Algebra, New York (1957).

[2] *J. Dieudonné:* Sur les groupes classiques, Hermann, Paris (1948).

[3] *O. T. O'Meara:* Introduction to Quadratic Forms, Springer-Verlag, Berlin (1966).

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