Can. J. Math., Vol. XXXIII, No. 1, 1981, pp. 116–128

GENERATORS OF ORTHOGONAL GROUPS OVER VALUATION RINGS

HIROYUKI ISHIBASHI

Introduction. Let $\mathfrak{o}$ be a valuation ring with unit element, i.e., $\mathfrak{o}$ is a commutative ring such that for any a and b in $\mathfrak{o}$, either a divides b or b divides a. We assume 2 is a unit of $\mathfrak{o}$. V is an n-ary nonsingular quadratic module over $\mathfrak{o}$, $O(V)$ or $O_n(V)$ is the orthogonal group on V, and S is the set of symmetries in $O(V)$. We define $l(\sigma)$ to be the minimal number of factors in the expression of σ of $O(V)$ as a product of symmetries on V. For the case where $\mathfrak{o}$ is a field, $l(\sigma)$ has been determined by P. Scherk [**6**] and J. Dieudonné [**1**]. In [**3**] I have generalized the results of Scherk to orthogonal groups over valuation domains. In the present paper I generalize my results of [**3**] to orthogonal groups over valuation rings.

Since $\mathfrak{o}$ is a valuation ring, it is a local ring with the maximal ideal A which consists of all nonunits of $\mathfrak{o}$.

Let σ be in $O_n(V)$. V_σ denotes the fixed module of σ in V, i.e., $V_\sigma = \{x \in V | \sigma x = x\}$ and d is the dimension of V_σ modulo A. Then our result is

$$l(\sigma) = n - d \quad \text{or} \quad n - d + 2.$$

In this paper the set theoretic difference of P and Q will be written $P - Q$.

1. Statement of the theorem. We use π or $-$ to denote the canonical homomorphism from $\mathfrak{o}$ onto $\mathfrak{o} = \bar{\mathfrak{o}}/A$. We use the same notation π or $-$ to denote the canonical homomorphism from V onto $\bar{V} = V/AV$.

V is an n-ary nonsingular quadratic space over $\mathfrak{o}$. Nonsingular means that the homomorphism ψ: $V \to V^\circ$ of V into its dual V° which is given by $\psi(y)(x) = xy$ is an isomorphism.

We define canonically $\bar{x} + \bar{y} = \overline{x + y}$, $\bar{a}\bar{x} = \overline{ax}$ and $\bar{x}\bar{y} = \overline{xy}$ for a in $\mathfrak{o}$ and x, y in V. Hence $\bar{V}$ is also an n-ary nonsingular quadratic space over $\bar{\mathfrak{o}}$.

If U is a nonempty subset of V, then $U^\perp$ denotes its orthogonal complement (in V), i.e., $U^\perp = \{x \in V | xU = 0\}$. For submodules U and W, $U \perp W$ means $U \oplus W$ with $UW = \{0\}$.

Now we state our theorem. For σ in $O_n(V)$ we put $d = \dim \overline{V_\sigma}$ and $d_0 = \dim \operatorname{rad} \overline{V_\sigma}$, where $\operatorname{rad} \overline{V_\sigma}$ denotes the radical of $\overline{V_\sigma}$, i.e., $\overline{V_\sigma} \cap \overline{V_\sigma}^\perp$.

Received July 11, 1979 and in revised form March 28, 1980.

THEOREM. *Let* $1 \neq \sigma$ *be in* $O_n(V)$.
i) *If* $n - d - d_0 \neq 0$, *then* $l(\sigma) = n - d$.
ii) *If* $n - d - d_0 = 0$, *then* $l(\sigma) = n - d + 2$.

Note. Since $\mathfrak{o}$ is a valuation ring, for any vector x in V there exist a in $\mathfrak{o}$ and x' in $V - AV$ such that $x = ax'$.

2. Symmetries and preliminary lemmas.

LEMMA 2.1. *For* n *vectors* $v_1, \ldots, v_n$ *of* V *and submodules* U, W *of* V *we have*
(a) $U = V$ *if and only if* $\bar{U} = \bar{V}$.
(b) $V = \bigoplus_{i=1}^n \mathfrak{o}v_i$ *if and only if* $\bar{V} = \bigoplus_{i=1}^n \bar{\mathfrak{o}}\bar{v}_i$.
(c) *If* $V = U \oplus W$, *then* U *is free with* rank $U = \dim \bar{U}$, *and* $\bar{V} = \bar{U} \oplus \bar{W}$.

Proof. (a) It is clear that $U = V$ implies $\bar{U} = \bar{V}$. So we show the converse. We write $V = \bigoplus_{i=1}^n \mathfrak{o}x_i$ for x_i in V. Since $\bar{U} = \bar{V}$, we can take the u_i's in U with $\bar{x}_i = \bar{u}_i$ for $i = 1, 2, \ldots, n$. Hence for $1 \leqq i \leqq n$, $x_i - u_i$ is contained in AV. Write

$$x_i = u_i + \sum_{j=1}^n a_{ij}x_j, \quad a_{ij} \in A.$$

Put $M = \{a_{ij}\}$. Then we have

$${}^t(u_1, \ldots, u_n) = {}^t(x_1, \ldots, x_n)(E - M).$$

E is the identity matrix. Since $\{1 - a_{ii} | 1 \leqq i \leqq n\}$ are units in $\mathfrak{o}$, $E - M$ is an invertible matrix, whence $\{x_1 \ldots, x_n\} \subset U$. Therefore $U = V$.

(b) It is clear that $V = \bigoplus_{i=1}^n \mathfrak{o}v_i$ implies $\bar{V} = \bigoplus_{i=1}^n \bar{\mathfrak{o}}\bar{v}_i$. So we show the converse. Let $\bar{V} = \bigoplus_{i=1}^n \bar{\mathfrak{o}}\bar{v}_i$. Then by (a) we have

$$V = \sum_{i=1}^n \mathfrak{o}v_i.$$

Hence we show the linear independence of $\{v_i\}$ over $\mathfrak{o}$. Suppose $a_1v_1 + \ldots + a_nv_n = 0$, $a_i \in \mathfrak{o}$, with at least one nonzero coefficient. Since $\mathfrak{o}$ is a valuation ring, we may assume a_1 divides all a_i's. So let

$$a_1(v_1 + e_2v_2 + \ldots) = 0, \quad e_i \in \mathfrak{o}.$$

Since $\bar{V} = \bigoplus_{i=1}^n \bar{\mathfrak{o}}\bar{v}_i$ is non-singular, we have a vector v in V with $\bar{v}_1\bar{v} = 1$ and $\bar{v}_i\bar{v} = 0$ for $i \neq 1$. Put

$$b = (v_1 + e_2v_2 + \ldots)v.$$

Then $b \notin A$, i.e., b is a unit, and $a_1b = 0$. This implies $a_1 = 0$, a contradiction.

(c) Since $V = U \oplus W$, we have $\bar{V} = \bar{U} + \bar{W}$. Write $\bar{U} = \oplus\, \bar{\mathfrak{o}}\bar{u}_i$ for $\{u_i\}$ in U and $\bar{V} = \bar{U} \oplus (\oplus\, \mathfrak{o}\bar{w}_j)$ for $\{w_j\}$ in W. Then by (b) we have

$$V = (\oplus\, \mathfrak{o}\, u_i) \oplus (\oplus\, \mathfrak{o} w_j).$$

Since $\oplus\, \mathfrak{o} u_i \subset U$, $\oplus\, \mathfrak{o} w_j \subset W$ and $V = U \oplus W$, we have $\oplus\, \mathfrak{o} u_i = U$ and $\oplus\, \mathfrak{o} w_j = W$. This gives (c).

By (c) of Lemma 2.1, we call a direct summand U of V a *subspace* of V and call its rank the *dimension* of U. For a subspace U of V we say U is a *line*, a *plane* or a *hyperplane* if $\dim U = 1, 2$ or $n - 1$ respectively.

LEMMA 2.2. *Let E be a hyperplane of V. Then for any submodule U of V we have*

$$\dim \bar{U} - 1 \leqq \dim \overline{U \cap E}.$$

Proof. Split $V = \mathfrak{o}x \oplus E$, $x \in V$. Express $\bar{U} = \bigoplus_{i=1}^{r} \bar{\mathfrak{o}}\bar{x}_i$, $x_i \in U$. Then we may write for each $i = 1, \ldots, r$, $x_i = a_i x + z_i$, $a_i \in \mathfrak{o}$ and $z_i \in E$. If all a_i's are zero then $\{x_1, \ldots, x_r\} \subset E$ and the lemma is clear. So, let at least one a_i be different from zero. Since $\mathfrak{o}$ is a valuation ring, we may assume a_1 divides all a_i's. Put $a_i = a_1 b_i$, $b_i \in \mathfrak{o}$. Then,

$$\{x_i - b_i x_1 | 2 \leqq i \leqq r\} \subset U \cap E$$

which gives the lemma.

Definition. For any ρ in $O_n(V)$ we define

$$V_\rho = \{x \in V | \rho x = x\}.$$

LEMMA 2.3. $((\rho - 1)V)V_\rho = \{0\}$.

Proof. This is easy so we leave it to the reader.

LEMMA 2.4. *Let ρ be in $O_n(V)$. If $x^2 \notin A$ and $\rho x = ax$ for some a in $\mathfrak{o}$, then $a = 1$ or -1.*

Proof. We have $x^2 = (\rho x)^2 = a^2 x^2$. Since $x^2 \notin A$, i.e., x^2 is a unit, we have $a^2 = 1$. Hence $(a + 1)(a - 1) = 0$. If $a + 1 \in A$ and $a - 1 \in A$, then $2 = (a + 1) - (a - 1) \in A$, a contradiction. So, either $a + 1 \notin A$ or $a - 1 \notin A$, i.e., $a + 1$ or $a - 1$ is a unit. Therefore $(a + 1)(a - 1) = 0$ implies $a - 1 = 0$ or $a + 1 = 0$.

LEMMA 2.5. *Let x be a vector in V. If $x^2 \notin A$, then we can split $V = \mathfrak{o}x \perp x^\perp$.*

Proof. Let $ax \in x^\perp$ for a in $\mathfrak{o}$. Then $ax^2 = 0$. Since $x^2 \notin A$, this implies $a = 0$. Thus we have $\mathfrak{o}x \cap x^\perp = \{0\}$.

Next, for any v in V, we can take b in $\mathfrak{o}$ with $vx = bx^2$. This means $v - bx \in x^\perp$. Hence $V = \mathfrak{o}x + x^\perp$ and so $\mathfrak{o}x \perp x^\perp$.

LEMMA 2.6. *If* $V = \mathfrak{o}x \perp x^{\perp}$, *then* $\dim x^{\perp} = n - 1$ *and* $x^{\perp}$ *is nonsingular.*

Proof. Put $U = x^{\perp}$. By (c) of Lemma 2.1, we know U is a hyperplane. Write $U = \bigoplus_{i=2}^{n} \mathfrak{o}x_i$. Put $x = x_1$. Then we have $V = \bigoplus_{i=1}^{n} \mathfrak{o}x_i$. Since V is nonsingular, we may take in V a dual base $\{f_i\}$ of the base $\{x_i\}$. Write

$$f_i = a_i x_1 + g_i, \quad a_i \in \mathfrak{o} \quad \text{and} \quad g_i \in U.$$

Since $x_1 x_i = 0$ for $2 \leqq i \leqq n$, we see $\{g_2, \ldots, g_n\}$ is a dual base of $\{x_2, \ldots, x_n\}$. Thus, $U = x^{\perp}$ is nonsingular.

We have defined S to be the set of symmetries on V, i.e.,

$$S = \{\tau \in O_n(V) | \dim V_\tau = n - 1\}.$$

Let $x^2 \notin A$ for x in V. Then by Lemma 2.5 we have $V = \mathfrak{o}x \perp x^{\perp}$ and by Lemma 2.6 $x^{\perp}$ is a hyperplane of V. Hence a linear mapping τ_x which carries x to $-x$ and is the identity on $x^{\perp}$ is clearly a symmetry, i.e., $\tau_x \in S$.

Conversely, take any τ in S. We show τ is expressed as τ_y for some y in V. First, we have a hyperplane V_τ of V. Put $V_\tau = U$. Split $V = \mathfrak{o}x \oplus U$ for some x in V. Put

$$U = \mathfrak{o}u_2 + \ldots + \mathfrak{o}u_n.$$

Since V is non-singular, considering a dual base of the base $\{x, u_2, \ldots, u_n\}$, we may take a vector y in V with $xy = 1$, $y^{\perp} = U$ and $U^{\perp} = \mathfrak{o}y$.

On the other hand we know by Lemma 2.3 that $(\tau - 1)x \in U^{\perp}$. So, we can write $(\tau - 1)x = ay$ for $0 \neq a$ in $\mathfrak{o}$, i.e., $\tau x = x + ay$. Then

$$0 = (\tau x)^2 - x^2 = (x + ay)^2 - x^2 = a(2xy + ay^2) = a(2 + ay^2).$$

Hence if y^2 were in A, then $2 + ay^2 \notin A$, i.e., $2 + ay^2$ is a unit, which implies $a = 0$, a contradiction. Therefore $y^2 \notin A$. Then by Lemma 2.5 we have

$$V = \mathfrak{o}y \perp y^{\perp} = \mathfrak{o}y \perp U = \mathfrak{o}y \perp V_\tau.$$

Finally we show $\tau y = -y$. By $\tau U = U$ we have $\tau \mathfrak{o}y = \mathfrak{o}y$. Let $\tau y = by$ for b in $\mathfrak{o}$. Then, by Lemma 2.4, $b = 1$ or -1. Since $\tau \neq 1$ we have $b = -1$. Hence $\tau = \tau_y$ with $y^2 \notin A$.

Thus, we have shown $S = \{\tau_y | y \in V \text{ and } y^2 \notin A\}$.

LEMMA 2.7. *For any* ρ *in* $O_n(V)$ *we have*

$$n - \dim \overline{V}_\rho \leqq l(\rho).$$

Proof. Let $\rho = \tau_1 \tau_2 \ldots \tau_r$, $\tau_i \in S$. Since each τ_i fixes a hyperplane, by Lemma 2.2 we have $n - r \leqq \dim \overline{V}_\rho$.

https://doi.org/10.4153/CJM-1981-011-3 Published online by Cambridge University Press

3. Proof for i) **of the theorem.** We take $\sigma \neq 1$ in $O_n(V)$ and fix it throughout this section. To simplify the notations we put

$$d = \dim \overline{V_\sigma}, \quad d_0 = \dim \operatorname{rad} \overline{V_\sigma} \quad \text{and} \quad d_1 = d - d_0.$$

By Lemma 2.7 we know $l(\sigma) \geqq n - d$. Hence it suffices to show $l(\sigma) \leqq n - d$. Our proof will proceed by induction on n and $n - d$.

Step A. Let $n = 1$. We write $V = \mathfrak{o}x$ for x in V and $\sigma x = ax$ for a in $\mathfrak{o}$. Then $x^2 = a^2x^2$. Since V is nonsingular, $x^2 \notin A$. Hence by Lemma 2.4, we have $a = \pm 1$. Since $\sigma \neq 1$, we have $a = -1$. This means $\sigma = \tau_x$ and $d = 0$. Thus, $l(\sigma) \leqq 1 = n - d$.

Definition. For any nonsingular subspace U of V and ρ in $O(U)$ we define

$$k(\rho) = \dim \bar{U} - \dim \overline{U_\rho} - \dim \operatorname{rad} \overline{U_\rho}.$$

LEMMA 3.1. $0 \leqq k(\rho)$.

Proof. This is easy (see Theorem 3.8 of E. Artin's book on Geometric Algebra).

By our assumption of i) of the theorem we have

$$k(\sigma) = n - d - d_0 \neq 0.$$

Hence by Lemma 3.1 we have

(1) $\quad 0 < k(\sigma)$.

Step B. Let $d_1 \neq 0$. Then there exists x in $\overline{V_\sigma}$ with $x^2 \notin A$. By Lemma 2.5 we can split $V = \mathfrak{o}x \perp x^\perp$. Put $x^\perp = U$. By Lemma 2.6, $\dim U = n - 1$ and U is nonsingular. Write $\rho = \sigma|_U$. Then,

$$\rho \in O_{n-1}(U),$$
$$\dim \overline{U_\rho} = \dim \overline{V_\sigma \cap U} = d - 1 \quad \text{and}$$
$$\dim \operatorname{rad} \overline{U_\rho} = \dim \operatorname{rad} \overline{V_\sigma} = d_0.$$

Hence

$$k(\rho) = (n-1) - (d-1) - d_0 = k(\sigma) \neq 0.$$

So, by the induction on n, we have

$$l(\rho) = (n-1) - (d-1) = n - d.$$

Since $\sigma = 1_{\mathfrak{o}x} \perp \rho$, we have $l(\sigma) \leqq l(\rho)$ and so $l(\sigma) \leqq n - d$.

Step C. By Step A and B, we may assume

(2) $\quad 2 \leqq n$,

(3) $\quad d_1 = 0, \quad$ i.e., $\overline{V_\sigma{}^2} = \{0\}$.

https://doi.org/10.4153/CJM-1981-011-3 Published online by Cambridge University Press

Hence

(4) $\quad d = d_0$ and $k(\sigma) = n - 2d.$

PROPOSITION 1. *There exists τ_y in S such that*

$$\dim \overline{V_{\tau_y \sigma}} = d + 1 \quad \textit{and} \quad k(\tau_y \sigma) \neq 0.$$

Suppose this has been proved, then by the inductive hypothesis on $n - d$ we have

$$l(\tau_y \sigma) = n - \dim \overline{V_{\tau_y \sigma}} = n - (d + 1).$$

Hence $l(\sigma) \leqq n - (d + 1) + 1 = n - d$, which completes our proof for i) of the theorem.

Therefore if suffices to prove the above proposition.

From now on we put $n - d = e$. Split

$$\bar{V} = \overline{V_\sigma} \oplus \left(\bigoplus_{i=1}^{e} \bar{\mathfrak{o}} \bar{x}_i \right) \quad \text{and} \quad \overline{V_\sigma} = \bigoplus_{i=e+1}^{n} \bar{\mathfrak{o}} \bar{x}_i$$

for $\{x_1, \ldots, x_e\}$ in V and $\{x_{e+1}, \ldots, x_n\}$ in V_σ. Then $V = \bigoplus_{i=1}^{n} \mathfrak{o} x_i$ by Lemma 2.1. Let $\{f_i\} \subset V$ be a dual base of $\{x_i\}$. Write

$$D = \bigoplus_{i=e+1}^{n} \mathfrak{o} x_i, \quad E = \bigoplus_{i=1}^{e} \mathfrak{o} x_i, \quad F = \bigoplus_{i=1}^{e} \mathfrak{o} f_i.$$

Then

(5) $\quad V = D \oplus E, d = \dim D, e = \dim E$ and $n = d + e,$

(6) $\quad D \subset V_\sigma$ and $\bar{D} = \overline{V_\sigma},$

(7) $\quad F = D^\perp$ and $(\sigma - 1)V \subset F$ (by Lemma 2.3).

Thus we have subspaces D, E, F of V. For $1 \leqq i \leqq e$ we may express

(8) $\quad (\sigma - 1)x_i = a_i y_i, \quad a_i \in \mathfrak{o}$ and $y_i \in F - AF.$

We note $a_i \neq 0$ for each i by (5) and (6). Hence by a suitable numbering we may assume a_i divides a_{i+1} for each i in $\{1, \ldots, e\}$, say,

(9) $\quad a_{i+1} = p_i a_i$ for p_i in $\mathfrak{o}$.

LEMMA 3.2. *We may choose $\{a_i, x_i, y_i\}$ in (8) such that $\{y_1, \ldots, y_e\}$ is a base for F.*

Proof. Suppose that we have

$$F = \mathfrak{o} y_1 \oplus \ldots \oplus \mathfrak{o} y_{j-1} \oplus U$$

and

$$\{y_j, \ldots, y_e\} \subset U$$

for some subspace U of F (if $j = 1$ then the first equation means $F = U$).

https://doi.org/10.4153/CJM-1981-011-3 Published online by Cambridge University Press

Since y_j is in $F - AF$, y_j is a basis element of F. Split $U = \mathfrak{o}y_j \oplus W$. We write for $j < i \leqq e$

$$y_i = b_i y_j + w_i, \quad b_i \in \mathfrak{o} \quad \text{and} \quad w_i \in W.$$

Since by (9) a_j divides all a_i's, we can write $a_i = q_i a_j$, $q_i \in \mathfrak{o}$. Put $x'_i = x_i - b_i q_i x_j$. Then $\{x_1, \ldots, x_j, x'_{j+1}, \ldots, x'_e\}$ is a base for E and $(\sigma - 1)x'_i \in W$ for $j < i \leqq e$. Write $(\sigma - 1)x'_i = a'_i y'_i$ for a'_i in $\mathfrak{o}$ and y'_i in $W - AW$ for $j < i \leqq e$. Then we have

$$F = \mathfrak{o}y_1 \oplus \ldots \oplus \mathfrak{o}y_j \oplus W$$

and

$$\{y'_{j+1}, \ldots, y'_e\} \subset W.$$

Further, by (5) and (6) we have each $a'_i \neq 0$.

Thus repeating this method, we obtain the desired base $\{y_1, \ldots, y_e\}$ for F.

By the lemma we may assume $F = \bigoplus_{i=1}^{e} \mathfrak{o}y_i$ for $\{y_i\}$ in (8).

LEMMA 3.3. *For some a in $\mathfrak{o}$, x in E and y in F we have*
(a) $\sigma x - x = ay$ *with* $a \neq 0$,
(b) $y^2 \notin A$,
(c) $x \in E - AE$,
(d) $(\sigma x + x)y = 0$.

Proof. By (1) and (4) we have $0 < k(\sigma) = n - 2d$. Hence $d < n/2$. So $n/2 < e$, since $n = d + e$ by (5). Thus $n/2 < \dim F$. Since $\dim F = \dim \bar{F}$ by (c) of Lemma 2.1, we obtain $n/2 < \dim \bar{F}$. Since $\bar{V}$ is non-singular this implies that there exists a vector w in F with $\bar{w}^2 \neq 0$, i.e., $w^2 \notin A$.

Since $F = \bigoplus_{i=1}^{e} \mathfrak{o}y_i$, we may write

$$w = \sum_{i=1}^{e} b_i y_i, \quad b_i \in \mathfrak{o}.$$

Let r be the maximal number in $\{1, \ldots, e\}$ such that $b_r \notin A$. Put

$$y = \sum_{i=1}^{r} b_i y_i.$$

Then clearly $y^2 \notin A$ by the choice of r. By (8) we have

$$(\sigma - 1)x_i = a_i y_i \quad \text{for} \quad i = 1, \ldots, r$$

and by (9) a_i divides a_{i+1}. So for each $i = 1, \ldots, r$ we can express $a_r = c_i a_i$, $c_i \in \mathfrak{o}$ and $c_r = 1$. Write

$$a = a_r \quad \text{and} \quad x = \sum_{i='}^{r} b_i c_i x_i.$$

Then $x \in E - AE$, because $E = \bigoplus_{i=1}^{e} \mathfrak{o}x_i$, $r \leqq e$ and $b_r c_r = b_r \notin A$. Further we have $(\sigma - 1)x = ay$ and $a \neq 0$. Thus we have (a), (b), (c) of the lemma for $\{a, x, y\}$ above.

Further we show that (d) holds for a suitable choice of y. Put $z = \sigma x + x$ and $b = zy$. Then

$$ab = azy = zay = (\sigma x + x)(\sigma x - x) = 0.$$

Hence if $a \notin A$, then we have $b = 0$, i.e., (d) holds. So let $a \in A$. On the other hand, we have $z = 2x + ay$ by (a). Since $2x \in E - AE$ and F is the dual space of E, we have u in F with $2xu = 1$. Hence $zu = 1 + ayu$ and so $zu \notin A$.

Put $c = zu$ and $v = y - bc^{-1}u$. Since $ab = 0$ and $a \neq 0$, we have $b \in A$. Hence $v^2 \notin A$. Further

$$\sigma x - x = ay = av$$

(note $ab = 0$) and

$$zv = z(y - bc^{-1}u) = b - b = 0.$$

Thus if we take v for y we have (d).

We take $\{a, x, y\}$ of the Lemma. Then, by $y^2 \notin A$, we can define a symmetry τ_y in S and the following lemma holds.

LEMMA 3.4. *$D \oplus \mathfrak{o}x \subset V_{\tau_y\sigma}$, $\bar{D} \oplus \bar{\mathfrak{o}}\bar{x} = \overline{V_{\tau_y\sigma}}$ and so*

$$\dim \overline{V_{\tau_y\sigma}} = d + 1.$$

Proof. We write $\tau = \tau_y$. We use (5), (6), (7) to prove the lemma. Since $D \subset V_\sigma$, σ fixes D. Next since y belongs to F and $F = D^\perp$, we have $Dy = \{0\}$. Hence τ fixes D. Therefore $\tau\sigma$ fixes D.

By (d) of Lemma 3.3 we have $(\sigma x + x)y = 0$. Hence τ fixes $\sigma x + x$. Since τ reverses y, it also reverses $ay = \sigma x - x$. Hence

$$\begin{aligned}\tau\sigma x &= \tau(2^{-1}((\sigma x + x) + (\sigma x - x))) \\ &= 2^{-1}((\sigma x + x) - (\sigma x - x)) = x,\end{aligned}$$

i.e., $\tau\sigma$ fixes x.

Thus we have $D + \mathfrak{o}x \subset V_{\tau\sigma}$. In fact $D + \mathfrak{o}x = D \oplus \mathfrak{o}x$, because $V = D \oplus E$ by (5) and $x \in E$. Hence

$$\bar{D} \oplus \bar{\mathfrak{o}}\bar{x} \subset \overline{V_{\tau\sigma}}.$$

Here we consider the dimensions of both sides. First, $V = D \oplus E$ implies $\bar{V} = \bar{D} \oplus \bar{E}$ by (c) of Lemma 2.1. Since $x \in E - AE$ by (c) of Lemma 3.3, we have $\bar{x} \neq 0$, and so

$$\dim(\bar{D} + \bar{\mathfrak{o}}\bar{x}) = d + 1.$$

On the other hand, since $\tau\sigma$ fixes $V_{\tau\sigma}$ and τ fixes $y^\perp$, we see σ fixes

$V_{\tau\sigma} \cap y^{\perp}$, i.e., $V_{\tau\sigma} \cap y^{\perp} \subset V_{\sigma}$. Hence

$$\dim \overline{V_{\tau\sigma} \cap y^{\perp}} \leqq \dim \overline{V_{\sigma}}.$$

By (6) $\dim \overline{V_{\sigma}} = d$. Hence

$$\dim \overline{V_{\tau\sigma} \cap y^{\perp}} \leqq d.$$

We know $y^{\perp}$ is a hyperplane by Lemmas 2.5 and 2.6. Hence by Lemma 2.2 we have

$$\dim \overline{V_{\tau\sigma}} - 1 \leqq \dim \overline{V_{\tau\sigma} \cap y^{\perp}}.$$

Therefore $\dim \overline{V_{\tau\sigma}} \leqq d + 1$. Thus we have

$$\bar{D} \oplus \bar{\mathfrak{o}}\bar{x} = \overline{V_{\tau\sigma}} \quad \text{and} \quad \dim \overline{V_{\tau\sigma}} = d + 1.$$

By Lemma 3.4 we have $\dim \overline{V_{\tau_y\sigma}} = d + 1$. Hence if $k(\tau_y\sigma) \neq 0$, then Proposition 1 holds.

Now let

(10) $k(\tau_y\sigma) = 0.$

Under the assumption (10), we shall find a new triple $\{a, x, y\}$ which satisfies the additional condition $k(\tau_y\sigma) \neq 0$. Namely we prove the following:

PROPOSITION 2. *There are a in* $\mathfrak{o}$, *x in E, and y in F satisfying* (a) *to* (d) *of Lemma* 3.3 *and in addition*

(e) $k(\tau_y\sigma) \neq 0$.

By Lemma 3.4 we get $\dim \overline{V_{\tau_y\sigma}} = d + 1$. Hence we see Proposition 2 implies Proposition 1. Now, let us prove the above proposition.

We write $N = V_{\tau_y\sigma}$. Then by the definition of $k(\rho)$ and (10) we have

(11) $k(\tau_y\sigma) = n - \dim \bar{N} - \dim \operatorname{rad} \bar{N} = 0$

and by Lemma 3.4

(12) $D \oplus \mathfrak{o}x \subset N, \quad \bar{D} \oplus \bar{\mathfrak{o}}\bar{x} = \bar{N} \quad \text{and} \quad \dim \bar{N} = d + 1.$

Since $n - \dim \bar{N} = \dim \bar{N}^{\perp}$ and $\dim \operatorname{rad} \bar{N} = \dim \operatorname{rad} (\bar{N}^{\perp})$, by (11) we have $\dim \bar{N}^{\perp} - \dim \operatorname{rad} (\bar{N}^{\perp}) = 0$. Hence

(13) $\bar{N}^{\perp} = \operatorname{rad} (\bar{N}^{\perp}) \quad (= \operatorname{rad} \bar{N}).$

LEMMA 3.5. (10) *implies* $\bar{D}\bar{x} = \{0\}$ *and* $\bar{y}\bar{x} \neq 0$.

Proof. Since $F = D^{\perp}$ and $y \in F$, we have $Dy = \{0\}$. Hence if $\bar{y}\bar{x} = 0$, then by (12) we have $\bar{y} \in \bar{N}^{\perp}$. So by (13), $\bar{y} \in \operatorname{rad} \bar{N}$ and so $\bar{y}^2 = 0$, which contradicts (b) of Lemma 3.3. Thus $\bar{y}\bar{x} \neq 0$.

Next, we show $\bar{D}\bar{x} = \{0\}$. So we may assume $\bar{D} \neq \{0\}$. If $\bar{D}\bar{x} \neq \{0\}$,

https://doi.org/10.4153/CJM-1981-011-3 Published online by Cambridge University Press

then by (12) $\bar{N}$ would contain a nonsingular plane, because $\bar{D}^2 = \{0\}$ by (3). Hence

$$\dim \operatorname{rad} \bar{N} \leqq \dim \bar{N} - 2.$$

Therefore by (11) and (12) we have

$$0 = k(\tau_y\sigma) \geqq n - \dim \bar{N} - (\dim \bar{N} - 2) = n - 2 \dim \bar{N} + 2$$
$$= n - 2(d + 1) + 2 = n - 2d = k(\sigma)$$

by (4), which contradicts (1). Thus $\bar{D}\bar{x} = \{0\}$.

We have $\sigma x - x = ay$ with $a \neq 0$ by (a) of Lemma 3.3.

LEMMA 3.6. $\bar{a} \neq 0$ *if and only if* $\bar{x}\bar{y} \neq 0$.

Proof. We have

$$0 = (\sigma x)^2 - x^2 = (x + ay)^2 - x^2$$
$$= 2axy + a^2y^2 = a(2xy + ay^2).$$

Let $\bar{a} \neq 0$, i.e., $a \notin A$. Then a is a unit. Hence by multiplying the above equation by a^{-1}, we have $0 = 2xy + ay^2$. Since $y^2 \notin A$ by Lemma 3.3, we get $xy \notin A$, i.e., $\bar{x}\bar{y} \neq 0$.

Conversely let $\bar{x}\bar{y} \neq 0$, i.e., $xy \notin A$. If a were in A, then, $2xy + ay^2 \notin A$. Therefore the above equation $0 = a(2xy + ay^2)$ would imply $a = 0$, a contradiction.

Now, we prove Proposition 2. First we treat the case $D = \{0\}$. As before we denote $N = V_{\tau_y\sigma}$. By (12) we have $\bar{N} = \bar{\mathfrak{o}}\bar{x}$. Hence

$$\dim \bar{N} = 1 \quad \text{and} \quad \dim \operatorname{rad} \bar{N} \leqq 1.$$

Therefore (11) implies $n - 2 \leqq 0$, i.e., $n \leqq 2$. Since by (2) we have $2 \leqq n$, we conclude $n = 2$. Then again (11) implies $\dim \operatorname{rad} \bar{N} = 1$, whence $\bar{N} = \operatorname{rad} \bar{N} = \bar{\mathfrak{o}}\bar{x}$. This means $\bar{x}^2 = 0$ and $\bar{V} = \bar{\mathfrak{o}}\bar{x} \oplus \bar{\mathfrak{o}}\bar{y}$. So $V = \mathfrak{o}x \oplus \mathfrak{o}y$ by Lemma 2.1.

We show $\bar{\sigma}\bar{y} = -\bar{y}$. Write $\rho = \tau_y\sigma$. Put $\rho y = px + qy$. We know $\bar{\rho}$ fixes $\bar{x}$ by (12). Hence

$$\bar{y}\bar{x} = (\bar{\rho}\bar{y})(\bar{\rho}\bar{x}) = (\bar{\rho}\bar{y})\bar{x} = (\bar{p}\bar{x} + \bar{q}\bar{y})\bar{x} = \bar{q}\bar{y}\bar{x},$$

which implies $\bar{q} = 1$, because $\bar{y}\bar{x} \neq 0$ by Lemma 3.5. Further

$$0 = (\bar{\rho}\bar{y})^2 - \bar{y}^2 = (\bar{p}\bar{x} + \bar{y})^2 - \bar{y}^2 = 2\bar{p}\bar{x}\bar{y},$$

which implies $\bar{p} = 0$. Thus we see $\bar{\rho}$ fixes $\bar{y}$, i.e., $\overline{\tau_y\sigma}\bar{y} = \bar{y}$. This implies $\bar{\sigma}\bar{y} = \bar{\tau}_y\bar{y} = -\bar{y}$. Let $a = 1$, $u = y$ and $v = \sigma u - u$.

We shall show that if we take $\{1, u, v\}$ for $\{a, x, y\}$ in Proposition 2 then the conditions (a)–(e) in the proposition are all satisfied. Since $D = \{0\}$, we have $V = E = F$. From this and by $a = 1$, (a), (c), (d) of

Proposition 2 are obvious. As for (b),

$$\overline{v^2} = \bar{v}^2 = \overline{\sigma u - u^2} = \overline{\sigma y - y^2} = (\bar{\sigma}\bar{y} - \bar{y})^2 = (-2\bar{y})^2 \neq 0$$

by Lemma 3.3, i.e., $v^2 \notin A$. Finally we show (e). Put $W = V_{\tau_v \sigma}$. Since $D = \{0\}$, we have $\bar{W} = \bar{\sigma}\bar{u}$ by the same way as for (12). Since $\bar{u}^2 = \bar{y}^2 \neq 0$, we have rad $\bar{W} = \{0\}$. Hence by the same equation as (11) we have

$$k(\tau_v \sigma) = 2 - 1 - 0 = 1 \neq 0.$$

Thus Proposition 2 holds.

Next we treat the case $D \neq \{0\}$. Since $\bar{D}$ is totally isotropic by (3), we can take z in E with $\bar{D}\bar{z} \neq \{0\}$. Write $w = \sigma z - z$.

Let $w^2 \notin A$. Then, taking $\{1, z, w\}$ for $\{a, x, y\}$ in Proposition 2, the proposition holds because (a), (b), (d) are clear. Since $\bar{D}\bar{z} \neq \{0\}$, we have $z \in E - AE$, i.e., (c). If $k(\tau_v \sigma)$ were zero, then we would have $\bar{D}\bar{z} = \{0\}$ by the same way as in Lemma 3.5, a contradiction. Thus Proposition 2 holds.

Let $w^2 \in A$. By (10) and Lemmas 3.5, 3.6, we have $\bar{a} \neq 0$, i.e., a is a unit. Hence there exists $\epsilon = 1$ or -1 such that

$$(y + a^{-1}\epsilon w)^2 \notin A \quad \text{since} \quad y^2 \notin A.$$

Put $u = x + \epsilon z$ and $v = y + a^{-1}\epsilon w$. We show that if we take $\{a, u, v\}$ for $\{a, x, y\}$ in Proposition 2 then the proposition holds. (a) and (b) are clear by the choice of u and v. Since $\bar{D}\bar{x} = \{0\}$ by Lemma 3.5 and $\bar{D}\bar{z} \neq \{0\}$, we have

$$\bar{D}\bar{u} = \bar{D}(\overline{x + z}) \neq 0.$$

Hence $u \in E - AE$, i.e., (c) holds. Since a is a unit,

$$(\sigma u + u)av = (\sigma u + u)(\sigma u - u) = 0$$

implies

$$(\sigma u + u)v = 0,$$

which is (d). Finally if $k(\tau_v \sigma)$ were zero, then by Lemma 3.5 we would have $\bar{D}\bar{u} = \{0\}$, a contradiction, whence $k(\tau_v \sigma) \neq 0$. Thus Proposition 2 holds and we have completed the proof for i) of the theorem.

4. Proof for (ii) **of the theorem.** In this section we write $M = V_\sigma$. Hence

$$d = \dim \bar{M} \quad \text{and} \quad d_0 = \dim \operatorname{rad} \bar{M}.$$

By the assumption of (ii) of the theorem we have $k(\sigma) = n - d - d_0 = 0$.

LEMMA 4.1. $\bar{M}^\perp = \operatorname{rad}(\bar{M}^\perp) = \operatorname{rad} \bar{M}$.

Proof. We have

$$0 = k(\sigma) = (n - d) - d_0 = \dim \bar{M}^{\perp} - \dim \operatorname{rad} \bar{M}$$
$$= \dim \bar{M}^{\perp} - \dim \operatorname{rad} (\bar{M}^{\perp}).$$

This gives the lemma.

LEMMA 4.2. *Let* τ_y *be in* S *and write* $N = V_{\tau_y \sigma}$. *Then we have* $N \subset M$ *and* $\dim \bar{N} \subseteq d - 1$.

Proof. We note $\bar{y}^2 \neq 0$, since τ_y defines a symmetry. Suppose $N \not\subset M$. Take x in $N - M$. Then $\tau_y \sigma x = x$. Since $\tau_y{}^2 = 1$, we have $\sigma x = \tau_y x = x + ay$ for some a in $\mathfrak{o}$ and y in $V - AV$. Since $x \notin M$, we have $a \neq 0$. On the other hand by Lemma 2.3 we have $May = \{0\}$. Hence $My \subset A$. Therefore $\bar{M}\bar{y} = \{0\}$, i.e., $\bar{y} \in \bar{M}^{\perp}$. But this is impossible, since $\bar{y}^2 \neq 0$ and $\bar{M}^{\perp}$ is totally isotropic by Lemma 4.1. Thus $N \subset M$.

Next we show $\bar{N} \neq \bar{M}$. Write

$$\bar{N} = \bigoplus_{i=1}^{t} \bar{\mathfrak{o}}\bar{x}_i, \quad x_i \in N.$$

Then, by $\tau_y \sigma x_i = x_i$, we have $\sigma x_i = \tau_y x_i$. Since $x_i \in N \subset M$, we have $\sigma x_i = x_i$. Hence $\tau_y x_i = x_i$. This means $x_i y = 0$ for $i = 1, \ldots, t$. Hence $\bar{N}\bar{y} = 0$. Therefore if $\bar{N} = \bar{M}$ then we would have $\bar{M}\bar{y} = 0$, i.e., $\bar{y} \in \bar{M}^{\perp} = \operatorname{rad} \bar{M}$, a contradiction.

Let $\sigma = \tau_1 \tau_2 \ldots \tau_r$, $\tau_i \in S$. Write $\tau = \tau_1$. Then, since $\tau^2 = 1$, we have $\tau\sigma = \tau_2 \ldots \tau_r$. By the lemma we have

$$\dim \overline{V_{\tau\sigma}} \leqq d - 1.$$

Hence by Lemma 2.7, we have

$$n - (d - 1) \leqq r - 1,$$

i.e., $n - d + 2 \leqq r$. Thus we have

$$n - d + 2 \leqq l(\sigma).$$

So, we show $l(\sigma) \leqq n - d + 2$. Take any τ_y in S. As before, $M = V_\sigma$ and $N = V_{\tau_y \sigma}$. Since σ fixes M and τ_y fixes $y^{\perp}$, $\tau_y \sigma$ fixes $M \cap y^{\perp}$. That is, we have $M \cap y^{\perp} \subset N$. Hence $\overline{M \cap y^{\perp}} \subset \bar{N}$. By Lemma 4.2 we know

$$\dim \bar{N} \leqq d - 1$$

and by Lemma 2.2 we have

$$d - 1 \leqq \dim \overline{M \cap y^{\perp}}.$$

Therefore we obtain $\overline{M \cap y^{\perp}} = \bar{N}$ and $\dim \bar{N} = d - 1$. From this and $\operatorname{rad} \bar{M} \neq \{0\}$ it is possible to choose τ_y in S with $\operatorname{rad} \bar{N} \subsetneq \operatorname{rad} \bar{M}$. For such τ_y we have

$$k(\tau_y\sigma) = n - \dim \bar{N} - \dim \operatorname{rad} \bar{N}$$
$$> n - (d - 1) - d_0 = k(\sigma) + 1 = 1.$$

Hence, applying i) of the theorem, we see

$$l(\tau_y\sigma) = n - (d - 1)$$

and so

$$l(\sigma) \leqq n - d + 2.$$

Thus we have completed the proof for ii) of the theorem.

Acknowledgment. I would like to express my thanks to the referee for his suggestions to revise the original paper.

REFERENCES

1. J. Dieudonné, *Sur les generateurs des groupes classiques*, Summa Brasil. Math. *3* (1955), 149–179.
2. E. W. Ellers, *Decomposition of orthogonal, symplectic, and unitary isometries into simple isometries*, Abh. Math. Sem. Univ. Hamburg *46* (1977), 97–127.
3. H. Ishibashi, *Generators of an orthogonal group over a local valuation domain*, J. Algebra *55* (1978), 302–307.
4. ——— *Generators of $O_n(V)$ over a quasi-semilocal semihereditary domain*, Comm. in Alg. *7* (1979), 1043–1064.
5. O. T. O'Meara, *Introduction to quadratic forms* (Springer-Verlag, Berlin, Göttingen, Heidelberg, 1963).
6. P. Scherk, *On the decomposition of orthogonalities into symmetries*, Proc. Amer. Math. Soc. *1* (1950), 481–491.

Josai University,
Sakado, Saitama, Japan