A THEOREM ON GENERATION OF FINITE ORTHOGONAL GROUPS

Dedicated to the memory of Hanna Neumann

W. J. WONG

(Received 11 July 1972)

Communicated by M. F. Newman

1. Introduction

Presentations in terms of generators and relations for the classical finite simple groups of Lie type have been given by Steinberg and Curtis [2, 4]. These presentations are useful in proving characterization theorems for these groups, as in the author's work on the projective symplectic groups [5]. However, in some cases, the application is not quite instantaneous, and an intermediate result is needed to provide a presentation more suitable for the situation in hand. In this paper we prove such a result, for the orthogonal simple groups over finite fields of odd characteristic. In a subsequent article we shall use this to give a characterization of these groups in terms of the structure of the centralizer of an involution.

Suppose F is a finite field of odd characteristic. By a quadratic space over F we mean a vector space V over F with a non-degenerate symmetric bilinear form $(\,,\,)$. If $\Omega(V)$ denotes the commutator subgroup of the orthogonal group of V, then the corresponding projective group $P\Omega(V)$ is simple if dim $V \geqq 5$. In this group, the centralizer of the involution corresponding to an involution of $\Omega(V)$ whose fixed-point subspace U has codimension 2 in V has a normal subgroup isomorphic with $\Omega(U)$. We shall give a presentation of $P\Omega(V)$ (or of $\Omega(V)$) in terms of generation by such a lower-dimensional orthogonal group, together with one additional element.

To state our result we need to set up some notation. Beginning with a quadratic space U, we set $M = \Omega(U)$, and write $\Omega(W)$ for the subgroup of M consisting of all elements which act as the identity on the orthogonal complement of a non-degenerate subspace W of U. The space U can be decomposed into an orthogonal direct sum.

Research partially supported by National Science Foundation grant at the University of Notre Dame.

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

$$U = V_0 \oplus V_1 \oplus \cdots \oplus V_{n-1},$$

where $V_1, \cdots, V_{n-1}$ are 2-dimensional subspaces of square discriminant, dim $V_0 \leqq 2$, and V_0 has non-square discriminant when dim $V_0 = 2$[3, p. 158]. We may choose isometries $z_i : V_1 \to V_i$, $i = 1, \cdots, n-1$, and write $v_i = vz_i$, for $v \in V_1$. If α is an element of the symmetric group Σ_{n-1} on $\{1, \cdots, n-1\}$, we obtain an orthogonal transformation $\sigma(\alpha)$ on U by setting

$$v_0\sigma(\alpha) = v_0,\ v_0 \in V_0,\ v_i\sigma(\alpha) = v_{i\alpha},\ v \in V_1,\ i = 1, \cdots, n-1.$$

Since $V_1, \cdots, V_{n-1}$ have square discriminant, $\sigma(\alpha)$ can be shown to have spinor norm 1, so that $\sigma(\alpha)$ lies in M, and we have an injective homomorphism

$$\sigma : \Sigma_{n-1} \to M.$$

THEOREM. *Let U be a quadratic space over a finite field F of odd characteristic, $M = \Omega(U)$, and let*

$$U = V_0 \oplus V_1 \oplus \cdots \oplus V_{n-1},\ \sigma : \Sigma_{n-1} \to M,$$

be as described above. Suppose G is a group generated by M and an element τ, such that

(i) $$\tau^2 = 1, (\tau\sigma((n-2, n-1)))^3 = 1, (\tau\sigma((i, i+1)))^2 = 1,$$

for $i = 1, \cdots, n-3$.

(ii) *τ normalizes $\Omega(V_0 \oplus V_i \oplus V_j)$, whenever $1 \leqq i < j \leqq n-2$.*

Suppose further that $n \geqq 5$ if $|F| \equiv 1 \pmod 4$, $n \geqq 8$ if $|F| \equiv -1 \pmod 4$. Then G is isomorphic with $\Omega(V)$ or $P\Omega(V)$, where V is a quadratic space over F, dim V = dim $U + 2$, and V has the same discriminant as U.

The remark concerning the discriminant is superfluous when dim $V_0 = 1$, since there is only one orthogonal group in each odd dimension. For even dimension there are two cases, depending on whether or not the discriminant is a square in F.

Our proof of the theorem requires that n be large enough for certain calculations to be carried out. By modifying the proof we shall also show that the theorem holds for three other cases. It seems likely that the theorem holds also for other cases with low values of n.

2

We begin by stating the Steinberg-Curtis results, as they apply to the orthogonal commutator groups over a finite field F of odd characteristic. There are three cases, which we label with the Lie notation.

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

Case ${}^2D_{n+1}$: Witt index n, dimension $2n+2$.

Case B_n: Dimension $2n+1$.

Case D_n: Witt index n, dimension $2n$.

Let V be a quadratic space over F, which can be decomposed into an orthogonal direct sum

$$V = W_0 \oplus W_1 \oplus \cdots \oplus W_n,$$

where $W_1, \cdots, W_n$ are 2-dimensional isotropic subspaces (hyperbolic planes) and W_0 is 2-dimensional anisotropic. We assume $n \geqq 3$. For $i = 1, \cdots, n$, we choose a hyperbolic basis e_i, e_{-i} of W_i, such that

$$(e_i, e_i) = (e_{-i}, e_{-i}) = 0, (e_i, e_{-i}) = 1,$$

and we choose a basis e_0, f_0 of W_0 such that

$$(e_0, e_0) = -2, (f_0, f_0) = 2\varepsilon, (e_0, f_0) = 0,$$

where ε is a non-square in F. Setting

$$V' = Fe_0 \oplus W_1 \oplus \cdots \oplus W_n,\ V'' = W_1 \oplus \cdots \oplus W_n,$$

we obtain groups $\Omega(V), \Omega(V'), \Omega(V'')$ which correspond to the three cases ${}^2D_{n+1}$, B_n, D_n. The group $\Omega(V')$ may be regarded as the subgroup of $\Omega(V)$ acting trivially on f_0, while $\Omega(V'')$ is the subgroup acting trivially on W_0. We shall give presentations for these groups.

For $i, j \in \{\pm 1, \cdots, \pm n\}$ with $|i| \neq |j|$, and $t \in F$, $\Omega(V)$ contains the element $x_{ij}(t)$ given by

$$x_{ij}(t) : e_i \to e_i + te_{-j}, e_j \to e_j - te_{-i},$$

with the action on the other basis elements being trivial. This element in fact lies in $\Omega(V'')$, and so in $\Omega(V')$.

Let E be the quadratic extension field $F(d)$, where $d^2 = \varepsilon$, and denote the automorphism of E of order 2 by $t \to \bar{t}$. For $i \in \{\pm 1, \cdots, \pm n\}$, $t \in E$, $\Omega(V)$ contains the element $x_i(t)$ given by

$$x_i(t) : e_0 \to e_0 + (t + \bar{t})e_{-i}, f_0 \to f_0 + d(t - \bar{t})e_{-i},$$

$$e_i \to e_i + \tfrac{1}{2}(t + \bar{t})e_0 + \tfrac{1}{2}d^{-1}(\bar{t} - t)f_0 + t\bar{t}e_{-i}.$$

This element lies in $\Omega(V')$ when $t \in F$.

These elements satisfy the following relations.

(A1) $$x_{ij}(t)x_{ij}(u) = x_{ij}(t+u).$$

(A2) $$x_i(t)x_i(u) = x_i(t+u).$$

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

(B1) $$[x_{ij}(t), x_{kl}(u)] = 1, \text{ if } i, j, -k, -l \text{ are distinct.}$$

$$[x_{ij}(t), x_{k,-j}(u)] = x_{ik}(-tu), \text{ if } |i| \neq |k|.$$

$$[x_{ij}(t), x_{-j,i}(u)] = 1.$$

(B2) $$[x_i(t), x_j(u)] = x_{ij}(\bar{t}u + t\bar{u}), \text{ if } |i| \neq |j|.$$

$$[x_{ij}(t), x_k(u)] = 1, \text{ if } i, j, -k \text{ are distinct.}$$

$$[x_{i,-k}(t), x_k(u)] = x_i(tu)x_{ik}(tu\bar{u}).$$

(C) $$(x_{12}(-1)x_{-1,-2}(1)x_{12}(-1))^2(x_{1,-2}(-1)x_{-1,2}(1)x_{1,-2}(-1))^2 = 1.$$

It may be noted that the relation $x_{ij}(t) = x_{ji}(-t)$ is implied by the second of the relations (B1), together with (A1).

Lemma 1. *The orthogonal commutator groups over F have the following presentations.*

Case $^2D_{n+1}$. *Generators*: $x_{ij}(t), t \in F$, $x_i(u), u \in E$.
Relations: $(A1), (A2), (B1), (B2), (C)$.

Case B_n. *Generators*: $x_{ij}(t), x_i(t), t \in F$.
Relations: $(A1), (A2), (B1), (B2), (C)$.

Case D_n. *Generators*: $x_{ij}(t), t \in F$.
Relations: $(A1), (B1), (C)$.

That this is simply a restatement of results of Steinberg and Curtis [2, 4] may be seen as follows. In Case D_n, the group $\Omega(V'')$ has a root system of type D_n, which may be considered as a subset of a real vector space with basis $\omega_1, \cdots, \omega_n$, consisting of the vectors $\omega_i + \omega_j$, where $i, j \in \{\pm 1, \cdots, \pm n\}$, $|i| < |j|$, and ω_{-i} stands for $-\omega_i$. In Cases $^2D_{n+1}$, B_n, the root system is of type B_n and is obtained from the root system of type D_n by adjoining the vectors $\omega_i, i \in \{\pm 1, \cdots, \pm n\}$. Now root elements $x_r(t)$ in the groups $\Omega(V), \Omega(V'), \Omega(V'')$ may be defined as follows.

$$x_{\omega_i + \omega_j}(t) = x_{ij}(t), \; |i| < |j|, \; x_{\omega_i}(t) = x_i(t).$$

Then the relations (A1), (A2) are the relations (A) of [4] and (B1), (B2) are the Chevalley commutator relations (B) of [4] (or their "twisted" analogues in Case $^2D_{n+1}$). The results of Steinberg and Curtis imply that, in the case of a finite ground field, these give presentations of the groups Spin (V), Spin (V'), Spin (V''). The left side of the relation (C) represents the element

$$h_{\omega_1 + \omega_2}(-1)h_{\omega_1 - \omega_2}(-1)$$

of the centre which must be factored out to obtain the groups $\Omega(V), \Omega(V'), \Omega(V'')$.

In fact the results of Curtis [2] indicate that it is necessary to take as generators only those root elements for which r is a linear combination of two fundamental roots, and as relations just those for which only such roots appear. Indeed, a commutator relation may be omitted unless there exists a pair of fundamental roots a, b such that all the roots appearing in the relation are linear combinations of a, b. The fundamental roots for Cases ${}^2D_{n+1}$, B_n may be taken as

$$-\omega_1, \omega_1 - \omega_2, \omega_2 - \omega_3, \cdots, \omega_{n-1} - \omega_n,$$

while those for D_n may be taken as

$$-\omega_1 - \omega_2, \omega_1 - \omega_2, \omega_2 - \omega_3, \cdots, \omega_{n-1} - \omega_n.$$

We thus obtain a refinement of Lemma 1.

Lemma 2. *In Lemma* 1, *it is necessary to take only the generators* $x_{ij}(t)$ *for which* $|i+j| \leqq 2$, *the generators* $x_{12}(t), x_{-1,-2}(t)$, *and the following additional generators.*

Cases ${}^2D_{n+1}$, B_n: $x_i(t), |i| \leqq 2$.

Case D_n: $x_{13}(t), x_{-1,-3}(t)$.

As relations it is necessary to take only the relations (A1), (A2) *which involve these elements alone, the relation* (C), *and certain of the relations* (B1), (B2) *which involve these elements alone. In particular, commutator relations for* $[x_{ij}(t), x_k(u)]$ *may be omitted unless* $|i|, |j|, |k| \leqq 2$, *or* $|i+j| = |k| = 1$.

3

We turn now to the proof of the theorem. We note first that, by Moore's presentation of the symmetric group [1, p. 464], the relations (i) in the hypothesis of the theorem are equivalent to the existence of an extension of σ to a homomorphism

$$\sigma : \Sigma_n \to G,$$

such that $\sigma((n-1, n)) = \tau$. Since σ is injective on Σ_{n-1}, it is injective on Σ_n also.

If A is a subset of $\{1, \cdots, n-1\}$ we write

$$\Omega(A) = \Omega\Big(\sum_{i \in A} V_i\Big), \Omega'(A) = \Omega\Big(V_0 \oplus \sum_{i \in A} V_i\Big),$$

then $\Omega(A)$ and $\Omega'(A)$ are subgroups of M.

Lemma 3. *If* $A, B \subsetneqq \{1, \cdots, n-1\}$, $\alpha \in \Sigma_n$, $A \doteq B\alpha$, *then* $\Omega(A) = \Omega(B)^{\sigma(\alpha)}$, $\Omega'(A) = \Omega'(B)^{\sigma(\alpha)}$.

Proof. We prove the last equation. Suppose first that A has two elements. If $\alpha \in \Sigma_{n-1}$, then the result holds, since $\sigma(\alpha)$ is an element of M transforming

$V_0 \oplus \sum_{j \in B} V_j$ into $V \oplus \sum_{i \in A} V_i$. If $\alpha \notin \Sigma_{n-1}$, then $\alpha = \beta(n-1)\gamma$, where $\beta, \gamma \in \Sigma_{n-1}$. Then

$$A\gamma^{-1} = B\beta(n-1, n)$$

and both $A\gamma^{-1}$, $B\beta$ are subsets of $\{1, \cdots, n-1\}$. Hence $B\beta \subseteqq \{1, \cdots, n-2\}$, and $A\gamma^{-1} = B\beta$. By the assumption (ii) of the theorem, $\sigma((n-1, n)) = \tau$ normalizes $\Omega'(B\beta)$, so that

$$\Omega'(A) = \Omega'(A\gamma^{-1})^{\sigma(\gamma)} = \Omega'(B\beta)^{\sigma((n-1,n))\sigma(\gamma)} = \Omega'(B)^{\sigma(\beta)\sigma((n-1,n))\sigma(\gamma)} = \Omega'(B)^{\sigma(\alpha)}.$$

Next suppose that A has only one element. Since $n \geqq 5$, we can find two 2-element sets B_1, B_2, such that $B_1, B_2, B_1\alpha, B_2\alpha$ are all subsets of $\{1, \cdots, n-1\}$ and $B_1 \cap B_2 = B$. Set $A_1 = B_1\alpha$, $A_2 = B_2\alpha$, so that $A = A_1 \cap A_2$. Using the 2-element case we have just proved, we see that

$$\Omega'(A_1) = \Omega'(B_1)^{\sigma(\alpha)}, \Omega'(A_2) = \Omega'(B_2)^{\sigma(\alpha)}.$$

Thus,

$$\Omega'(A) = \Omega'(A_1) \cap \Omega'(A_2) = (\Omega'(B_1) \cap \Omega'(B_2))^{\sigma(\alpha)} = \Omega'(B)^{\sigma(\alpha)}.$$

If A is the empty set ϕ, the same argument with B_1, B_2 suitable 1-element subsets of $\{1, \cdots, n-1\}$ gives the desired result.

If A has more than 2 elements, then $\Omega'(B)$ is generated by the subgroups $\Omega'(C)$ as C ranges over the 2-element subsets of B, while $\Omega'(A)$ is generated by the subgroups $\Omega'(C\alpha)$ [3, p. 161]. Thus the desired result in this case follows also from the 2-element case.

To prove the equation $\Omega(A) = \Omega(B)^{\sigma(\alpha)}$, we may assume $V_0 \neq 0$. If A has two elements, then we may find 1-element subsets $A_1 \subseteqq \{1, \cdots, n-1\} - A$, $B_1 \subseteqq \{1, \cdots, n-1\} - B$, such that $A_1 = B_1\alpha$. Then,

$$\Omega'(A \cup A_1) = \Omega'(B \cup B_1)^{\sigma(\alpha)}, \Omega'(A_1) = \Omega'(B_1)^{\sigma(\alpha)}.$$

Since $\Omega(A)$ is the commutator subgroup of the centralizer of $\Omega'(A_1)$ in $\Omega'(A \cup A_1)$ and $\Omega(B)$ is the commutator subgroup of the centralizer of $\Omega'(B_1)$ in $\Omega'(B \cup B_1)$, we find that

$$\Omega(A) = \Omega(B)^{\sigma(\alpha)}$$

in this 2-element case. The general case then follows as before. This proves the lemma.

We now extend the definition of the subgroups $\Omega(A)$, $\Omega'(A)$ to arbitrary proper subsets A of $\{1, \cdots, n\}$ as follows. Choose a subset B of $\{1, \cdots, n-1\}$ with the same number of elements as A, choose an element α of Σ_n such that $A = B\alpha$, and set

$$\Omega(A) = \Omega(B)^{\sigma(\alpha)}, \qquad \Omega'(A) = \Omega'(B)^{\sigma(\alpha)}.$$

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

By Lemma 3, this is consistent for subsets A of $\{1,\cdots,n-1\}$ with the earlier meaning for $\Omega(A),\Omega'(A)$.

LEMMA 4. (a) *If A is any proper subset of $\{1,\cdots,n\}$, then $\Omega(A),\Omega'(A)$ are well-defined.*

(b) *The result of Lemma 3 holds for arbitrary proper subsets A,B oj $\{1,\cdots,n\}$.*

(c) *If A,B are disjoint, then $[\Omega'(A),\Omega(B)]=1$.*

(d) *If $\alpha\in\Sigma_n$ and α fixes every element of a non-empty proper subset A of $\{1,\cdots,n\}$, then $\sigma(\alpha)$ centralizes $\Omega'(A)$.*

PROOF. (a) If $A=B\alpha=C\beta$, where $B,C\subseteqq\{1,\cdots,n-1\}$, $\alpha,\beta\in\Sigma_n$, then $B=C\beta\alpha^{-1}$, so that, by Lemma 3,

$$\Omega(B)^{\sigma(\alpha)}=\Omega(C)^{\sigma(\beta\alpha-1)\sigma(\alpha)}=\Omega(C)^{\sigma(\beta)}.$$

Thus $\Omega(A)$ is well-defined. Similarly $\Omega'(A)$ is well-defined.

(b) Suppose $A=B\alpha$. Choose $C\subseteqq\{1,\cdots,n-1\}$, $\beta\in\Sigma_n$, such that $B=C\beta$. Then $A=C\beta\alpha$. By definition,

$$\Omega(A)=\Omega(C)^{\sigma(\beta\alpha)}=\Omega(C)^{\sigma(\beta)\sigma(\alpha)}=\Omega(B)^{\sigma(\alpha)}.$$

Similarly, $\Omega'(A)=\Omega'(B)^{\sigma(\alpha)}$.

(c) Suppose A,B are disjoint. The result is clear if $A,B\subseteqq\{1,\cdots,n-1\}$. If $|A\cup B|\leqq n-1$, there is an element of Σ_n transforming $A\cup B$ into a subset of $\{1,\cdots,n-1\}$, and the result follows by applying (b). If $|A\cup B|=n$, then since $n\geqq 5$, $|A|\geqq 3$ or $|B|\geqq 3$. If $|B|\geqq 3$, then $\Omega(B)$ is generated by all the subgroups $\Omega(C)$, where C ranges over the 2-element subsets of B [3, p. 161], and we know already that $[\Omega'(A),\Omega(C)]=1$ for these C. Hence $[\Omega'(A),\Omega(B)]=1$. A similar argument applies if $|A|\geqq 3$.

(d) Let B be the set of elements of $\{1,\cdots,n\}$ which are not fixed by α. If $\alpha\in\Sigma_{n-1}$, then clearly $\sigma(\alpha)\in\Omega(B)$. An application of (b) gives the same result for any element α of Σ_n which has a fixed point, since α is conjugate to an element of Σ_{n-1}. Then (d) follows from (c). This proves the lemma.

The proof of the theorem now breaks into two cases. We take first the case that $|F|\equiv 1 \pmod 4$, so that -1 is a square in F. In this case the subspaces $V_1,\cdots,V_{n-1}$ are hyperbolic planes, and we can choose hyperbolic bases e_i,e_{-i} for V_i in such a way that

$$e_i\sigma(\alpha)=e_{i\alpha},\ e_{-i}\sigma(\alpha)=e_{-i\alpha},$$

for all $\alpha\in\Sigma_{n-1}$.

If $\dim V_0=1$, we may assume that V_0 has an element e_0 such that $(e_0,e_0)=-2$. If $\dim V_0=2$, we may take a basis e_0,f_0 of V_0 such that $(e_0,e_0)=-2$, $(f_0,f_0)=2\varepsilon$, $(e_0,f_0)=0$, where ε is a non-square in F. These vectors are fixed by $\sigma(\alpha)$, for all $\alpha\in\Sigma_{n-1}$.

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

As in the last section, we may now define elements $x_{ij}(t)$ in M, for $i,j \in \{\pm 1, \cdots, \pm(n-1)\}$, $|i| \neq |j|$, $t \in F$. If $V_0 \neq 0$, we also have elements $x_i(t)$ where $i \in 1\{\pm 1, \cdots, \pm(n-1)\}$, and t lies in F or the quadratic extension field E of F, according as dim $V_0 = 1$ or 2. Thus M is a group of type ${}^2D_n$, B_{n-1}, or D_{n-1}, according as dim $V_0 = 2, 1$ or 0. We have to show that G is of type ${}^2D_{n+1}, B_n$, or D_n respectively.

If $\alpha \in \Sigma_{n-1}$, we have the relations

$$(*) \qquad x_{ij}(t)^{\sigma(\alpha)} = x_{i\alpha,j\alpha}(t),\ x_i(t)^{\sigma(\alpha)} = x_{i\alpha}(t),$$

where the action of Σ_{n-1} is extended to $\{\pm 1, \cdots, \pm(n-1)\}$ by setting $(-i)\alpha = -(i\alpha)$. If the action of Σ_n is extended to $\{\pm 1, \cdots, \pm n\}$ in the same way, we can now define elements $x_{ij}(t)$ in G, for $i,j \in \{\pm 1, \cdots, \pm n\}$, $|i| \neq |j|$, $t \in F$, as follows. Choose $k, l \in \{\pm 1, \cdots, \pm(n-1)\}$ such that $|k| \neq |l|$, k has the same sign as i, and l has the same sign as j. Choose $\alpha \in \Sigma_n$ such that $i = k\alpha$, $j = l\alpha$, and set

$$x_{ij}(t) = x_{kl}(t)^{\sigma(\alpha)}.$$

Similarly, if $V_0 \neq 0$, we define $x_i(t)$, for $i \in \{\pm 1, \cdots, \pm n\}$, where $t \in F$ if dim $V_0 = 1$, $t \in E$ if dim $V_0 = 2$. By using Lemma 4 (d) and a similar argument to the proof of Lemma 4(a), (b), we see that these elements are well-defined, and further that the relations $(*)$ hold for $i,j \in \{\pm 1, \cdots, \pm n\}$, $\alpha \in \Sigma_n$.

It is now easy to check that the relations listed in Lemma 1 for the three cases ${}^2D_{n+1}, B_n, D_n$ are satisfied. Each of the relations (A1), (A2), (B1), (B2) involves at most 4 subscripts, and there exists an element α of Σ_n transforming these into elements of $\{\pm 1, \cdots, \pm(n-1)\}$, since $n \geqq 5$. Since the elements $x_{ij}(t)$, $x_i(t)$ with $i,j \in \{\pm 1, \cdots, \pm(n-1)\}$ do satisfy the requisite relations, application of $(*)$ shows that they are satisfied by all $x_{ij}(t)$, $x_i(t)$, with $i,j \in \{\pm 1, \cdots, \pm n\}$. The relation (C) is already known in M. It follows now from Lemma 1 that the group G_0 generated by all the $x_{ij}(t)$ (and the $x_i(t)$ if $V_0 \neq 0$) is isomorphic with $\Omega(V)$ or $P\Omega(V)$, where V is a quadratic space over F, dim $V =$ dim $U + 2$, and V has the same discriminant as U.

Since M is generated by the $x_{ij}(t)$ (and the $x_i(t)$ if $V_0 \neq 0$) having $i,j \in \{\pm 1, \cdots, \pm(n-1)\}$, G_0 contains M, and so G_0 contains $\sigma(\Sigma_{n-1})$. By $(*)$, G_0 is normalized by $\sigma(\Sigma_n)$. Since the only normal subgroup of Σ_n containing Σ_{n-1} is Σ_n itself, it follows that G_0 contains $\sigma(\Sigma_n)$, and, in particular, that G_0 contains τ. Since τ and M generate G, $G_0 = G$. This proves the theorem in the case $|F| \equiv 1 \pmod 4$.

We now assume that $|F| \equiv -1 \pmod 4$. Since $V_1, \cdots, V_{n-1}$ are not now hyperbolic planes, we need a somewhat more complicated argument. First we write

$$V_0 \oplus V_1 \oplus \cdots \oplus V_{n-8} = W_0 \oplus W_1 \oplus \cdots \oplus W_{m-8},$$

where $W_1, \cdots, W_{m-8}$ are hyperbolic planes, dim $W_0 \leqq 2$, and W_0 is anisotropic. Then $m = n-1$, n, or $n+1$. For simplicity of notation we shall assume that $m = n$. The argument in the other cases is not essentially different.

Setting

$$A_0 = \{1, \cdots, n-8\},\ A_1 = \{n-7,\ n-6\},$$
$$A_2 = \{n-5,\ n-4\},\ A_3 = \{n-3,\ n-2\},\ A_4 = \{n-1,\ n\},$$

we define a subgroup T_4 of Σ_n to consist of all elements which fix all elements of A_0, permute the sets A_1, A_2, A_3, A_4, and leave the set $\{n-6,\ n-4,\ n-2, n\}$ invariant. Such an element is essentially the product of a permutation on the set $\{n-6,\ n-4,\ n-2,\ n\}$ with the similar permutation on the set

$$\{n-7,\ n-5,\ n-3,\ n-1\}.$$

We write T_3 for the subgroup of T_4 fixing n (and so fixing $n-1$ also).

For $i = n-7,\ n-5,\ n-3$, we can write

$$V_i \oplus V_{i+1} = W_i \oplus W_{i+i},$$

where W_i, W_{i+i} are orthogonal hyperbolic planes, in such a way that

$$W_j\sigma(\alpha) = W_{j\alpha},$$

for $\alpha \in T_3$, $n-7 \leqq j \leqq n-2$. For $1 \leqq j \leqq n-2$ we can choose a hyperbolic basis e_j, e_{-j} of W_j, in such a way that

$$e_j\sigma(\alpha) = e_{j\alpha},\ e_{-j}\sigma(\alpha) = e_{-j\alpha},$$

for all $\alpha \in T_3$.

If $W_0 \neq 0$, we choose a basis e_0 or e_0, f_0 for W_0 in the usual way. If

$$N = \Omega(V_0 \oplus V_1 \oplus \cdots \oplus V_{n-2}) = \Omega(W_0 \oplus W_1 \oplus \cdots \oplus W_{n-2}),$$

we define elements $x_{ij}(t)$ in N, for $i,j \in \{\pm 1, \cdots, \pm(n-2)\}$, $|i| \neq |j|, t \in F$, as in the last section. If $W_0 \neq 0$, we also have elements $x_i(t)$, where

$$i \in \{\pm 1, \cdots, \pm(n-2)\},$$

and t lies in F or the quadratic extension field E of F, according as dim $W_0 = 1$ or 2. Thus N is a group of type ${}^2D_{n-1}$, B_{n-2}, or D_{n-2}, according as dim $W_0 = 2, 1$ or 0. We have to show that G is of type ${}^2D_{n+1}$, B_n or D_n respectively.

If $\alpha \in T_3$, we have relations

$$(*) \qquad x_{ij}(t)^{\sigma(\alpha)} = x_{i\alpha, j\alpha}(t),\ x_i(t)^{\sigma(\alpha)} = x_{i\alpha}(t),$$

where the action of Σ_n has been extended to $\{\pm 1, \cdots, \pm n\}$ in the usual way. If $i \in A_k$, $j \in A_l$, then $x_{ij}(t) \in \Omega(A_k \cup A_l)$. If an element α of T_4 fixes i and j, then it

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

fixes all elements of $A_k \cup A_l$, and so $\sigma(\alpha)$ centralizes $x_{ij}(t)$, by Lemma 4 (d). Similarly, if α fixes i then $\sigma(\alpha)$ centralizes $x_i(t)$.

We now define elements $x_{ij}(t)$ in G, for $i,j \in \{\pm 1, \cdots, \pm n\}$, $|i| \neq |j|$, $t \in F$, by choosing $\alpha \in T_4, k, l \in \{\pm 1, \cdots, \pm(n-2)\}$ such that $i = k\alpha$, $j = l\alpha$. This is possible, since T_4 acts as the symmetric group on A_1, A_2, A_3, A_4. We then set

$$x_{ij}(t) = x_{kl}(t)^{\sigma(\alpha)}.$$

Similarly, if $W_0 \neq 0$, we define $x_i(t)$, for $i \in \{\pm 1, \cdots, \pm n\}$, where $t \in F$ if dim $W_0 = 1$, $t \in E$ if dim $W_0 = 2$. By an argument similar to the proof of Lemma 4 (a), (b), we see that these elements are well-defined, and that the relations (∗) hold for $i,j \in \{\pm 1, \cdots, \pm n\}$, $\alpha \in T_4$.

The relations listed in Lemma 1 may now be verified. If one of the relations (A1), (A2), (B1), (B2) does not involve subscripts with absolute values from all four sets A_1, A_2, A_3, A_4, then there is an element of T_4 transforming the subscripts into elements of $\{\pm 1, \cdots, \pm(n-2)\}$, and the relation may be deduced from the corresponding relation in N, together with (∗). The only other type of relation involves $[x_{ij}(t), x_{kl}(u)]$, where $|i|, |j|, |k|, |l|$ lie in distinct sets A_a, A_b, A_c, A_d. Then,

$$[x_{ij}(t), x_{kl}(u)] \in [\Omega(A_a \cup A_b), \Omega(A_c \cup A_d)] = 1,$$

by Lemma 4 (c). The relation (C) is known in N. It follows now from Lemma 1 that the group G_0 generated by all the $x_{ij}(t)$ (and the $x_i(t)$ if $W_0 \neq 0$) is isomorphic with $\Omega(V)$ or $P\Omega(V)$, where V is a quadratic space over F, dim $V =$ dim $U + 2$, and V has the same discriminant as U.

The group G_0 contains $N = \Omega'(\{1, \cdots, n-2\})$ and is normalized by $\sigma(T_4)$. Since N contains $\sigma(T_3)$ and the only normal subgroup of T_4 containing T_3 is T_4 itself, it follows that G_0 contains $\sigma(T_4)$. If $\alpha = (n-3, n-1)(n-2, n)$, then we see that G_0 contains

$$\Omega(\{n-4, n-3\})^{\sigma(\alpha)} = \Omega(\{n-4, n-1\}).$$

From [3, p. 161], one sees easily that N and $\Omega(\{n-4, n-1\})$ generate M. Since M contains $\sigma(\Sigma_{n-1})$, and Σ_{n-1} and T_4 generate Σ_n, G_0 contains M and $\sigma(\Sigma_n)$. Thus $G_0 = G$, and the theorem is proved.

4

By modifying the proof, we can extend the theorem to a few other cases.

PROPOSITION. *The theorem holds also when $V_0 = 0$ and $n = 7$, and when dim $V_0 = 2$ and $n = 5$ or 7.*

PROOF. We may assume that $|F| \equiv -1 \pmod 4$. If $V_0 = 0$, we write

$$V_i \oplus V_{i+i} = W_i \oplus W_{i+i},$$

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

for odd $i \in \{1, \cdots, n-2\}$, where W_i, W_{i+i} are orthogonal hyperbolic planes. If $\dim V_0 = 2$, we write $V_1 \oplus V_2 = W_1 \oplus W_2$,

$$V_0 = W_3,\ V_i \oplus V_{i+1} = W_{i+1} \oplus W_{i+2}, \text{ for odd } i \in \{3, \cdots, n-2\},$$

where the W_j are orthogonal hyperbolic planes. Thus,

$$U = W_1 \oplus \cdots \oplus W_m,$$

where $m = n-1$ or n. Choosing hyperbolic bases for the W_j, we have elements $x_{ij}(t)$ defined in M, for $i, j \in \{\pm 1, \cdots, \pm m\}$, $|i| \neq |j|$, $t \in F$, as in Section 1. Thus M is a group of type D_m. We wish to show that G is of type ${}^2D_{m+1}$.

We have a decomposition

$$V_1 \oplus V_2 \oplus V_{n-1} = V_{n-1} \oplus W_1 \oplus W_2,$$

where W_1, W_2 are hyperbolic planes and V_{n-1} is anisotropic. Choosing a suitable basis of V_{n-1}, we may define elements $y_i(t)$ in $\Omega(\{1,2,n-1\})$ analogously to the $x_i(t)$ of Section 1, where $i \in \{\pm 1, \pm 2\}$ and t lies in the quadratic extension field E of F. We now set

$$x_i(t) = y_i(t)^\tau,$$

an element of $\Omega(\{1,2,n\})$.

The relations (A1), (B1), (C) of Section 1 are satisfied in M, and clearly the relations (A2) are satisfied by the $x_i(t)$, since they are satisfied by the $y_i(t)$, $i \in \{\pm 1, \pm 2\}$. For $|i| = 1$, $|j| = 2$, we have the relation

$$[y_i(t), y_j(u)] = x_{ij}(\bar{t}u + t\bar{u})$$

in $\Omega(\{1,2,n-1\})$. Conjugation by τ gives the relation

$$[x_i(t), x_j(u)] = x_{ij}(\bar{t}u + t\bar{u}).$$

If $|i| \geqq 3$, $|j| \geqq 3$, $|i| \neq |j|$, $|k| \leqq 2$, then $x_{ij}(t)$ lies in $\Omega'(\{3, \cdots, n-1\})$, while $x_k(u)$ lies in $\Omega(\{1,2,n\})$, so that $[x_{ij}(t), x_k(u)] = 1$, by Lemma 4(c). If $|i| \leqq 3$, $|j| \leqq 3$, $|i| \neq |j|$, then $x_{ij}(t)$ lies in $\Omega(\{1,2,3,4\})$ if $V_0 = 0$, and in $\Omega'(\{1,2,3\})$ if $\dim V_0 = 2$. In either case $x_{ij}(t)$ commutes with $\tau = \sigma((n-1,n))$, by Lemma 4(d) and our assumption on n. Hence, if $|k| \leqq 2$, the commutator relation for $[x_{ij}(t), x_k(u)]$ can be obtained from that for $[x_{ij}(t), y_k(u)]$ by conjugation by τ.

By Lemma 2, the group G_0 generated by the $x_i(t)$, $|i| \leqq 2$, the $x_{ij}(t)$, $|i+j| \leqq 2$, and the $x_{12}(t), x_{-1,-2}(t)$ is isomorphic to $\Omega(V)$ or $P\Omega(V)$, where V is a quadratic space over F, $\dim V = \dim U + 2$, and V has the same discriminant as U.

Since the $x_{ij}(t)$ mentioned above generate M, G_0 contains M. The $x_{ij}(t)$ with $|i|, |j| \leqq m-2$, together with the $y_k(t)$, generate $\Omega'(\{1, \cdots, n-3, n-1\})$. Conjugation by τ shows that $\Omega'(\{1, \cdots, n-3, n-1\})^\tau \subseteqq G_0$. Also, $\Omega(\{1, n-2\})^\tau$

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press

$= \Omega(\{1, n-2\}) \subseteqq G_0$. By [3, p. 161], $\Omega'(\{1, \cdots, n-3, n-1\})$ and $\Omega(\{1, n-2\})$ generate M, so that $M^\tau \subseteqq G_0$. Since Σ_{n-1} and its conjugate by $(n-1, n)$ generate Σ_n, G_0 contains τ also. Thus $G_0 = G$ and the proposition is proved.

5

We conclude by remarking that the proofs given above in fact show that not only is G isomorphic with $\Omega(V)$ or $P\Omega(V)$, but the isomorphism is such that the embedding of M in G is the natural one corresponding to an embedding of U as a non-degenerate subspace of codimension 2 in V.

References

[1] W. Burnside, *Theory of Groups of Finite Order*, (New York, Dover, 1955).

[2] C. W. Curtis, 'Central extensions of groups of Lie type', *Jour. für die reine u. angew. Math.*, 220 (1965), 174–185.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, (New York. Dover, 1958).

[4] R. Steinberg, *Générateurs, relations et revêtements de groups algébriques*, Colloque sur la Théorie des Groupes Algébriques, (Bruxelles, 1962, 113–127).

[5] W. J. Wong, 'Characterization of the finite simple groups $PSp_{2n}(q)$', *Jour. of Algebra* 14 (1970), 531–551.

University of Notre Dame
Notre Dame, Indiana, U. S. A.

https://doi.org/10.1017/S1446788700015470 Published online by Cambridge University Press