GENERATORS FOR SIMPLE GROUPS

ROBERT STEINBERG

1. Introduction. The list of known finite simple groups other than the cyclic, alternating, and Mathieu groups consists of the classical groups which are (projective) unimodular, orthogonal, symplectic, and unitary groups, the exceptional groups which are the direct analogues of the exceptional Lie groups, and certain twisted types which are constructed with the aid of Lie theory (see §§ 3 and 4 below). In this article, it is proved that each of these groups is generated by two of its elements. It is possible that one of the generators can be chosen of order 2, as is the case for the projective unimodular group **(1)**, or even that one of the generators can be chosen as an arbitrary element other than the identity, as is the case for the alternating groups. Either of these results, if true, would quite likely require methods much more detailed than those used here.

As a model on which the construction for all groups is based, the situation is now described for the group G of $(n+1)$th order unimodular matrices taken modulo the scalar multiples of the identity. Let k be a generator of the multiplicative group K^* of the finite field K; h the diagonal matrix with entries $k, k^{-1}, 1, 1, \ldots$; x the matrix with 1 in all diagonal positions and the (1, 2) position and 0 in all other positions; and w the matrix with 1 in the $(i, i+1)$ position for $1 \leqslant i \leqslant n$, $(-1)^n$ in the $(n+1, 1)$ position, and 0 elsewhere. Then if K has more than three elements, G is generated by the elements represented by h and xw, while if K has two or three elements, x and w will do.

The two-element generation of all of the above groups is covered by 3.11, 3.13, 3.14 and 4.1 below.

With the exception of the complex field, all fields considered in this paper are assumed to be finite.

2. Roots and reflections. Let $\sum = \{a_1, a_2, \ldots, a_n\}$ be a simple (also called fundamental) system of roots corresponding to a simple Lie algebra over the complex field. Throughout the paper we assume that the elements of $\sum$ for the various possible root systems are so labelled that $(a, a) = 2$ and $(a, b) = 0$ for each pair of roots in $\sum$ with the following exceptions:

A_n: $(a_i, a_{i+1}) = -1$ for $1 \leqslant i \leqslant n-1$
B_n: $(a_1, a_1) = 1$, $(a_i, a_{i+1}) = -1$ for $1 \leqslant i \leqslant n-1$
C_n: $(a_i, a_i) = 1$ and $(a_i, a_{i+1}) = -1/2$ for $1 \leqslant i \leqslant n-2$,
$\quad (a_{n-1}, a_{n-1}) = -(a_{n-1}, a_n) = 1$

Received January 10, 1961.

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press

D_n: $(a_1, a_3) = (a_i, a_{i+1}) = -1$ for $2 \leqslant i \leqslant n-1$
E_n: $(a_i, a_{i+1}) = (a_{n-3}, a_n) = -1$ for $1 \leqslant i \leqslant n-2$
F_4: $(a_1, a_1) = (a_2, a_2) = 1$, $(a_1, a_2) = -1/2$, $(a_2, a_3) = (a_3, a_4) = -1$
G_2: $(a_1, a_1) = 2/3$, $(a_1, a_2) = -1$.

Whenever it is convenient, the notation $a, b, \ldots$ is also used for $a_1, a_2, \ldots$. The reflections w_r reversing the various roots r generate a finite group W (the Weyl group) which is at the same time generated by the reflections w_i corresponding to the simple roots a_i. As is well known, any two roots of the same length are congruent under W.

2.1 *Let* $w = w_1 w_2 \ldots w_n$ (*operations from right to left*). (a) *W is generated by w and w_1 with the exceptions: type B_n $(n \geqslant 3)$ or D_n (n even) when w, w_1 and w_2 will do, C_n $(n \geqslant 3)$ when w, w_{n-1} and w_n will do, F_4 when w, w_2 and w_3 will do.* (b) *W contains the central reflection -1 (defined by $(-1)r = -r$ for each r in $\sum$) if W is not of type A_n $(n \geqslant 2)$, D_n (n odd) or E_6.* (c) *If -1 is in W, it is a power of w.*

Proof. Let V be the subgroup of W generated by the given elements. If W is of type A_n, then V contains each $w_i = w^{i-1}w_1w^{1-i}$, hence all of W. If W is of type B_2 or G_2, then V contains w_1 and $w_2 = w_1 w$, hence all of W. If W is of type B_n $(n \geqslant 3)$, V contains w_1 and each $w_i = w^{i-2}w_2w^{2-i}$ for $2 \leqslant i \leqslant n$, hence all of W. If W is of type C_n $(n \geqslant 3)$, the situation is similar. If W is of type D_n, V contains w_2 even if n is odd since then $w_2 = w^{n-1}w_1w^{1-n}$; thus V contains $w_3 = w_2ww_1w^{-1}w_2$, $w_i = w^{i-3}w_3w^{3-i}$ for $3 \leqslant i \leqslant n$, hence all of W. If W is of type E_n, V contains $w_i = w^{i-1}w_1w^{1-i}$ for $1 \leqslant i \leqslant n-3$, then $w_{n-2} = w_{n-3}w^{-2}w_1w^2w_{n-3}$, $w_{n-1} = ww_{n-2}w^{-1}$ and $w_n = w_{n-1} \ldots w_2w_1w$, hence all of W. Finally, if W is of type F_4, V contains w_2, $w_1 = w^{-1}w_2w$, w_3 and $w_4 = ww_3w^{-1}$, hence all of W. Thus (a) is true. Now if w_0 is the element of W such that $w_0 \sum = -\sum$, then $-w_0$ is an orthogonal transformation which permutes the roots of $\sum$. If $\sum$ is not of type A_n, D_n or E_6, the only possibility is that $-w_0$ is the identity, whence $-1 = w_0$ is in W. If W is of type D_n (n even), one can verify that $w^{n-1}a_i = -a_i$ for each i, whence $-1 = w^{n-1}$ is in W. Thus (b) is proved. For the proof of (c), see 4.1 and 4.5 of **(6)**.

3. The normal types. Following Chevalley, let us consider a Cartan decomposition of a simple Lie algebra over the complex field, choose a generating set $\{X_r, H_r | r = \text{root}\}$ to fulfil the conditions of Theorem 1 of **(2)** (so that the structural constants are all integers), transfer the base field to a finite field K, and then define $x_r(k) = \exp(\text{ad } kX_r)$ for each root r and each k in K, $\mathfrak{X}_r = \{x_r(k) | k \text{ in } K\}$, and G as the group generated by all $\mathfrak{X}_r$. Excluding the cases in which the corresponding simple system of roots $\sum$ is of type A_1, B_2 or G_2 and K has two elements and the case in which $\sum$ is of type A_1 and K has three elements, we obtain a simple group G and call it a *normal type.* Henceforth we also exclude explicit mention of the group G of type C_n con-

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press

structed over a field of characteristic 2 since it is isomorphic to the corresponding group of type B_n.

The following properties are shared by the normal types.

3.1. *G is generated by those $\mathfrak{X}_r$ for which $\pm r$ is in $\sum$.*

3.2. *If r and s are roots such that $r + s$ is not a root, then $\mathfrak{X}_r$ and $\mathfrak{X}_s$ commute elementwise.*

3.3. *Let r and s be roots such that $r + s$ is a root and $(r + s, r + s) = e(r, r) = e(s, s)$ with $e \geqslant 1$. Then there holds the commutator relation $(x_r(k), x_s(l)) = x_{r+s}(\epsilon ekl)$ with $\epsilon = \pm 1$ depending only on r and s.*

3.4. *For each root r and each k in K^*, the multiplicative group of K, there exists $h = h_{r,k}$ in G such that $hx_s(l)h^{-1} = x_s(k^{2(s,r)/(r,r)}l)$ for each root s and each l in K. The elements $h_{r,k}$ generate an Abelian subgroup $\mathfrak{H}$.*

For each h in $\mathfrak{H}$, we also use h to denote the character on the roots defined by $hx_s(1)h^{-1} = x_s(h(s))$. Thus $hx_s(l)h^{-1} = x_s(h(s)l)$ for every root s and every l in K.

3.5. *For each w in W, there is $\omega(w)$ in G such that $\omega(w)x_r(k)\omega(w)^{-1} = x_{wr}(\epsilon k)$ for each k in K and each root r with $\epsilon = \pm 1$ independent of k.*

3.6. *$\mathfrak{H}\omega(W)$ is a group $\mathfrak{W}$ which contains $\mathfrak{H}$ as a normal subgroup and $\omega(W)$ as a system of coset representatives relative to $\mathfrak{H}$. Further, the map $w \to \mathfrak{H}\omega(w)$ is an isomorphism of W on $\mathfrak{W}/\mathfrak{H}$.*

3.7. *For each positive root r, we can (and do) choose $\omega(w_r) = x_r(1)x_{-r}(-1)x_r(1)$.*

For the proof of these results, see **(2)**.

3.8. *If G is a normal type, then G is generated by any system of coset representations for $\mathfrak{W}$ over $\mathfrak{H}$ together with $\mathfrak{X}_a$ except when G is of type B_n over a field of characteristic 2, or of type F_4 over a field of characteristic 2, or of type G_2 over a field of characteristic 3, in which case "$\mathfrak{X}_a$" is to be replaced by "$\mathfrak{X}_a$ and $\mathfrak{X}_b$", or "$\mathfrak{X}_b$ and $\mathfrak{X}_c$", or "$\mathfrak{X}_a$ and $\mathfrak{X}_b$", respectively.*

Proof. Since W is transitive on roots of the same length, the result is clear from 3.4, 3.5 and 3.6 if all roots have the same length. For the same reason if G is of type B_n, a system of representatives for $\mathfrak{W}$ over $\mathfrak{H}$ and $\mathfrak{X}_a$ and $\mathfrak{X}_b$ generate G. But if the characteristic is not 2 in the latter case, then $\mathfrak{X}_b$ may be omitted since the other elements generate $\mathfrak{X}_{-a}$, $\mathfrak{X}_{a+b}$ and then $(\mathfrak{X}_{-a}, \mathfrak{X}_{a+b}) = \mathfrak{X}_b$ by 3.3 with $e = 2$. The argument is similar in the other exceptional cases.

3.9. *Let r be a root, l in K^*, and h in $\mathfrak{H}$ such that $h(r)$ is either a generator or the square of a generator of K^*. Then h and $x_r(l)$ generate $\mathfrak{X}_r$.*

Proof. By repeated conjugation by h, we get from $x_r(l)$ all elements of the form $x_r(lk^2)$, and then by multiplication, $x_r(l \sum k_i^2)$. The numbers inside the

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press

last brackets form an additive subgroup which contains more than half the elements of K, hence must be K.

3.10. *Let r be a root, w in W, and h in $\mathfrak{H}$ such that $h(r)$ and $h(w^{-1}r)$ are generators or squares of generators of K^* and different from 1. Then h and $x_r(1)\ \omega(w)$ generate $\mathfrak{X}_r$ and $\omega(w)$.*

Proof. Set $h(r) = k$, $h((w^{-1}r) = l$, $x_r(1)\ \omega(w) = x$. Then $y = xhx^{-1} = x_r(1-l)h_1$ with h_1 in $\mathfrak{H}$ by 3.4 and 3.5. Since $(y, h) = x_r(1-l)\ (1-k)) = x_r(m)$ with $m \neq 0$, the desired result follows from 3.9.

We can now prove our first principal result.

3.11. *Let G be a normal type, but assume that G is not of type D_n (n even), or of type B_n or F_4 if the underlying field K is of characteristic 2, or of type G_2 if K is of characteristic 3. Let k be a generator of K^*, $a = a_1$, $h = h_{a,k}$ except that for type B_n $h = h_{r,k}$ with $r = 2a_1 + a_2 + \ldots + a_n$, and $w = w_1 w_2 \ldots w_n$. Then G is generated by h and $x_a(1)\ \omega(w)$ if K has more than three elements and by $x_a(1)$ and $\omega(w)$ if K has not.*

Proof. Let F be the group generated by the given elements. By 3.10, F contains $\mathfrak{X}_a$ and $\omega(w)$. By 2.1, 3.5, 3.6 and 3.8, it suffices to prove that F also contains an element congruent to $\omega(w_1)$ mod $\mathfrak{H}$, unless G is of type B_n, C_n, or F_4 in which respective cases elements must be produced which are congruent to $\omega(w_1)$ and $\omega(w_2)$, to $\omega(w_{n-1})$ and $\omega(w_n)$, or to $\omega(w_2)$ and $\omega(w_3)$. If G is of type A_n, F contains $\mathfrak{X}_a$, $\mathfrak{X}_b = \omega(w)\mathfrak{X}_a\omega(w)^{-1}, \ldots$, and then by commutation, $\mathfrak{X}_r$ with $r = a + b + \ldots$ and $\mathfrak{X}_{-a} = \omega(w)\mathfrak{X}_r\omega(w)^{-1}$, hence also $\omega(w_a) = \omega(w_1)$ by 3.7. If G is of type B_n, F contains $\mathfrak{X}_a$, $\mathfrak{X}_{a+b} = \omega(w)\mathfrak{X}_a\omega(w)^{-1}$, $\mathfrak{X}_{2a+b} = (\mathfrak{X}_a, \mathfrak{X}_{a+b})$ by 3.3, and $\mathfrak{X}_{-a}$ and $\mathfrak{X}_{-2a-b}$ by 2.1 and 3.5, thus also $\omega(w_a)$ and $\omega(w_{2a+b})$ by 3.7, and $\omega(w_a)\omega(w_{2a+b})\omega(w_a)^{-1}$ which is congruent to $\omega(w_b)$ mod $\mathfrak{H}$. If G is of type C_n, set $s = a_1 + a_2 + \ldots + a_{n-1}$, $t = a_{n-1}$, $u = a_n$. Then F contains $\mathfrak{X}_r$ for $r = a_1, a_2, \ldots, a_{n-1}$ and then for $r = s$, the first by conjugation of $\mathfrak{X}_a$ by $\omega(w)$ and the second by commutation. Thus F also contains $\omega(w)^{-1}\mathfrak{X}_s\omega(w) = \mathfrak{X}_{-t-u}$, $\mathfrak{X}_{-u} = (\mathfrak{X}_t, \mathfrak{X}_{-t-u})$, $\mathfrak{X}_{-t}$ and $\mathfrak{X}_u$ by 2.1 and 3.5, and then $\omega(w_t) = \omega(w_{n-1})$ and $\omega(w_u) = \omega(w_n)$ by 3.7. If G is of type D_n (n odd), F contains $\mathfrak{X}_a$, $\mathfrak{X}_{b+c} = \omega(w)\mathfrak{X}_a\omega(w)^{-1}$, $\mathfrak{X}_{-b} = \omega(w)^{n-1}\mathfrak{X}_a\omega(w)^{1-n}$, $\mathfrak{X}_{-a-c} = \omega(w)\mathfrak{X}_{-b}\omega(w)^{-1}$, $\mathfrak{X}_c = (\mathfrak{X}_{b+c}, \mathfrak{X}_{-b})$, $\mathfrak{X}_{-a} = (\mathfrak{X}_c, \mathfrak{X}_{-a-c})$, hence also $\omega(w_a)$ by 3.7. If G is of type E_6, F contains $\mathfrak{X}_a$ and $\mathfrak{X}_{-a} = (\omega(w)^4\mathfrak{X}_a\omega(w)^{-4}, \omega(w)^8\mathfrak{X}_a\omega(w)^{-8})$, hence also $\omega(w_a)$ by 3.7. If G is of type E_7 or E_8, F contains $\mathfrak{X}_{-a}$ by 2.1 and 3.5, hence also $\omega(w_a)$ by 3.7. If G is of type F_4, F contains $\mathfrak{X}_b = \omega(w)\mathfrak{X}_a\omega(w)^{-1}$, $\mathfrak{X}_{a+b+c} = \omega(w)\mathfrak{X}_b\omega(w)^{-1}$, $\mathfrak{X}_{-a}$ and $\mathfrak{X}_{-b}$ by 2.1 and 3.5, $\mathfrak{X}_{-a-b} = (\mathfrak{X}_{-a}, \mathfrak{X}_{-b})$, $\mathfrak{X}_c = (\mathfrak{X}_{a+b+c}, \mathfrak{X}_{-a-b})$ by 3.3 with $e = 2$, $\mathfrak{X}_{-c}$ by 2.1 and 3.5, and then $\omega(w_b)$ and $\omega(w_c)$ by 3.7. Finally, if G is of type G_2, F contains $\mathfrak{X}_a$ and $\mathfrak{X}_{-a}$ by 2.1 and 3.5, and then $\omega(w_a)$ by 3.7.

In order to treat the normal types excluded by 3.11, we require the following statement.

3.12. *Assume that r and s are roots such that $\mathfrak{X}_r$ and $\mathfrak{X}_s$ commute elementwise,*

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press

and that w in W and h in $\mathfrak{H}$ are such that $h(r) = 1$ and, setting $h(s) = k$, $h(w^{-1}r) = l$, $h(w^{-1}s) = m$, $h(wr) = n$, that each of k, l, m, n is either a generator or the square of a generator of K^* and different from 1. Then h and $x = x_r(1)x_s(1)\omega(w)$ generate $\mathfrak{X}_r$, $\mathfrak{X}_s$ and $\omega(w)$.

Proof. If F is the subgroup generated by h and x, then F contains $y = xhx^{-1} = x_r(1-l)x_s(1-m)h_1$ with h_1 in $\mathfrak{H}$, then also $(y, h) = x_s((1-m)(1-k))$ and all of $\mathfrak{X}_s$ by 3.9. Thus F contains $t = x_r(1)\omega(w)$, $h_2 = t^{-1}ht = \omega(w)^{-1}h\omega(w)$ with $h_2(r) = h(wr) = n$ by 3.4 and 3.5, $u = tht^{-1} = x_r(1.-.l)h_1$, and $x_r((1-l)(1.-.n)) = (u, h_2)$, thus all of $\mathfrak{X}_r$ by 3.9 (with h replaced by h_2).

We can now give two-element generations for the remaining normal types.

3.13. *Let G be of normal type D_n (n even), k a generator of K^*, and set $h = h_{b,k}$ and $w = w_1w_2 \ldots w_n$. Then h and $x_{-a}(1)x_c(1)\omega(w)$ generate G if K has more than 2 elements, while $x_a(1)x_c(1)$ and $\omega(w)$ do if K has not.*

Proof. Let F be the group generated by the given elements. If K has two elements, then F contains $x_{a+c}(1) = (x_a(1)x_c(1))^2$, $x_b(1) = \omega(w)^{-1}x_{a+c}(1)\omega(w)$, $x_{b+c}(1) = ((x_a(1)x_c(1))^{-1}, x_b(1))$, $x_a(1) = \omega(w)^{-1}x_{b+c}(1)\omega(w)$, hence $x_{-b}(1)$ and $x_{-a}(1)$ by 2.1 and 3.5, $\omega(w_a)$ and $\omega(w_b)$ by 3.7, and all of G by 2.1, 3.5 and 3.8. If K has more than two elements, F contains $\mathfrak{X}_{-a}$, $\mathfrak{X}_c$ and $\omega(w)$ by 3.12 with $r = -a$ and $s = c$, hence also $\mathfrak{X}_{-b-c} = \omega(w)\mathfrak{X}_{-a}\omega(w)^{-1}$, $\mathfrak{X}_{-b} = (\mathfrak{X}_{-b-c}, \mathfrak{X}_c)$, and then all of G just as before.

3.14. *Let G be of normal type B_n, F_4, G_2, and in these respective cases let K be of characteristic 2, 2, 3, and define $r = b + c + \ldots$, $s = -a$; $r = c$, $s = -b$; $r = b$, $s = -a$. Let k be a generator of K^*, $t = r - 2s$, $h = h_{t,k}$ and $w = w_1w_2 \ldots w_n$. Then G is generated by h and $x_r(1)x_s(1)\omega(w)$ if K has more than two elements and by $x_r(1)x_s(1)$ and $\omega(w)$ if it has not.*

Proof. Let F be the group generated by the given elements. If K has more than two elements, F contains $\mathfrak{X}_r$, $\mathfrak{X}_s$ and $\omega(w)$ by 3.12. Thus if G is of type F_4 or G_2, F contains $\mathfrak{X}_{-r}$, $\mathfrak{X}_{-s}$, $\omega(w_r)$ and $\omega(w_s)$ by 2.1, 3.5 and 3.7, thus all of G by 3.5 and 3.8; whereas if G is of type B_n, F contains $\mathfrak{X}_{-a}$, then $\omega(w_a)$ by 2.1, 3.5 and 3.7, then $\mathfrak{X}_{-b} = \omega(w_a)\omega(w)\mathfrak{X}_r\omega(w)^{-1}\omega(w_a)^{-1}$, thus all of G as before. If K has two elements, and G is of type B_n, then $n \geqslant 3$, and F contains $x = x_r(1)x_s(1)$, $x_b(1) = (x, (\omega(w)^n x\omega(w)^{-n}, (x, \omega(w)^{n+1}x\omega(w)^{-n-1})))$, thus $x_c(1) = \omega(w)x_b(1)\omega(w)^{-1}, \ldots$, by commutation $x_r(1)$, then $x_s(1) = x_{-a}(1)$ and again all of G by 2.1, 3.5 and 3.8; whereas if G is of type F_4, F contains $x = x_{-b}(1)x_c(1)$, $y = x_{c+d}(1) = (x, (\omega(w)^{-2}x\omega(w)^2, \omega(w)x\omega(w)^{-1}))$, $x_c(1) = (\omega(w)^2y\omega(w)^{-2}, \omega(w)^{-3}y\omega(w)^3)$, $x_{-b}(1) = xx_c(1)$ and all of G once again.

4. The twisted types. Each of the groups yet to be considered occurs as a subgroup of a normal type and will be treated as such. Let the simple root system $\sum$ possess a permutation $r \to \bar{r}$ such that $(\bar{r}, \bar{s}) = (r, s)$ for each pair r, s in $\sum$, and let the field K possess an automorphism $k \to \bar{k}$ of the same

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press

period. Then the normal type G constructed from $\sum$ and K has an automorphism α such that $x_a(k)^\alpha = x_{\bar{a}}(\bar{k})$ whenever $\pm a$ is in $\sum$ and k is in K. We then define: $\mathfrak{U}$ (respectively $\mathfrak{V}$) is the subgroup of G generated by those $\mathfrak{X}_r$ for which r is positive (respectively negative), $\mathfrak{U}^1$ (respectively $\mathfrak{V}^1$) is the subgroup of $\mathfrak{U}$ (respectively $\mathfrak{V}$) consisting of the elements invariant under α, and G^1 is the group generated by $\mathfrak{U}^1$ and $\mathfrak{V}^1$. If the period of α is 2, the groups G^1 obtained in this way are A_n^1 $(n \geqslant 2)$, D_n^1 $(n \geqslant 4)$ and E_6^1 (in the notation of **(7)** and **(8)**; see also **(3)**, **(11)**, **(12)**, while if it is 3, one obtains D_4^2, a second subgroup of D_4; these groups are all simple except for the type A_2^1 over a field of four elements. Next, the normal type C_2 over a field of $2^{2f+1} = 2e^2$ elements has an automorphism α such that $x_a(k)^\alpha = x_b(k^{2e})$ and $x_b(k)^\alpha = x_a(k^e)$ with similar equations for $-a$ and $-b$ (**5**, Exposés 21 to 24), and one constructs as before a subgroup G^1 (see also **(10)**). A similar construction is possible if the normal type is F_4 over a field of 2^{2f+1} elements or G_2 over a field of 3^{2f+1} elements (see **4**). If $f \geqslant 1$, we get simple groups C_2^1, F_4^1 and G_2^1 in this way and call them, as well as the other simple groups constructed in this paragraph, *twisted types.*

For each twisted type, a *simple set* (of roots) is one which contains a simple root, is closed under addition and the permutation $a \to \bar{a}$ used in the construction, and is minimal relative to these properties. We label the various simple sets S_i thus:

A_{2n}^1: $S_1 = \{a_n, a_{n+1}, a_n + a_{n+1}\}$, $S_i = \{a_{n+1-i}, a_{n+i}\}$, $2 \leqslant i \leqslant n$
A_{2n-1}^1: $S_i = \{a_i, a_{2n-i}\}$, $S_n = \{a_n\}$, $1 \leqslant i \leqslant n-1$
D_n^1: $S_1 = \{a_1, a_2\}$, $S_i = \{a_{i+1}\}$, $2 \leqslant i \leqslant n-1$
E_6^1: $S_1 = \{a_1, a_5\}$, $S_2 = \{a_2, a_4\}$, $S_3 = \{a_3\}$, $S_4 = \{a_6\}$
D_4^2: $S_1 = \{a_1, a_2, a_4\}$, $S_2 = \{a_3\}$
C_2^1: $S_1 = \{a, b, a+b, 2a+b\}$
F_4^1: $S_1 = \{b, c, b+c, 2b+c\}$, $S_2 = \{a, d\}$
G_2^1: $S_1 = \{a, b, a+b, 2a+b, 3a+b, 3a+2b\}$.

For each simple set S_i, let w_i^1 be the unique element of W which maps S_i on $-S_i$ and is in the group generated by those w_r for which r is in S_i (cf. **7**, 2.2), and then set $w = w_1^1 w_2^1 \ldots$. Further, define h thus: if k is a generator of K^* and r is a simple root in S_1, then $h = h_{r,k} h_{r,k}^{\alpha}$ unless the type is D_4^2 in which case $h = h_{r,k} h_{r,k}^{\alpha} h_{r,k}^{\alpha\alpha}$. Finally, define x thus: for type A_{2n-1}^1, D_n^1 or E_6^1, $x = x_a(1) x_a(1)^\alpha$ with $a = a_1$; for type D_4^2, $x = x_a(1)x_a(1)^\alpha x_a(1)^{\alpha\alpha}$ with $a = a_1$; for type A_{2n}^1, $x = x_r(1)x_s(1)x_{r+s}(k)$ with $r = a_n$, $s = a_{n+1}$ and $k + \bar{k} = 1$ (this is $(1|k)$ in **(9)**); for type C_2^1, $x = x_a(1)x_b(1)x_{2a+b}(1)$ (this is $S(1, 0)$ in **(10)**); for type F_4^1, $x = x_b(1)x_c(1)x_{2b+c}(1)$; for type G_2^1, $x = x_a(1)$ $x_b(1)x_{a+b}(1)x_{2a+b}(1)$ (this is $\alpha(1)$ in **(4)**). We can now state our results on the generation of the twisted types.

4.1. *Let G^1 be a twisted type and let w, h and x be defined as in the preceding paragraphs. Then G^1 is generated by h and $x\omega(w)$.*

The properties 2.1 and 3.1 to 3.7 for the normal types have analogues for the twisted types (see **7** and **4**). For this reason, a proof of 4.1 can be patterned after that of 3.11. The details are omitted.

Added in proof. Since the preparation of this paper, I have learned that the symplectic groups (groups of type C_n in the above notation) have been considered by several other authors. In **(13)** and **(14)** a two element generation is given in case the underlying field has a prime number of elements, and in **(15)** the general case is dealt with.

References

1. A. A. Albert and J. Thompson, Illinois J. Math., *3* (1959), 421.
2. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J., *7* (1955), 14.
3. D. Hertzig, *On simple algebraic groups*, Short communications, Int. Cong. Math. (Edinburgh, 1958).
4. R. Ree, *A family of simple groups associated with the simple Lie algebra of type* G_2, Bull. Amer. Math. Soc., *66* (1960), 508.
5. Séminaire C. Chevalley, *Classification des groupes de Lie algébriques* (Paris, 1956–8).
6. R. Steinberg, *Finite reflection groups*, Trans. Amer. Math. Soc., *91* (1959), 493.
7. ——— *Variations on a theme of Chevalley*, Pacific J. Math., *9* (1959), 875.
8. ——— *The simplicity of certain groups*, Pacific J. Math., *10* (1960), 1039.
9. ——— *Automorphisms of finite linear groups*, Can. J. Math., *12* (1960), 606.
10. M. Suzuki, *A new type of simple groups of finite order*, Proc. Nat. Acad. Sci., *46* (1960), 868.
11. J. Tits, *Les "formes réelles" des groupes de type* E_6, Séminaire Bourbaki, Exposé 162 (Paris, 1958).
12. ——— *Sur la trialité et certains groupes qui s'en déduisent*, Publ. Math. Inst. Hautes Etudes Sci., *2* (1959), 14.
13. T. G. Room and R. J. Smith, *A generation of the symplectic group*, Quart. J. Math., *9* (1958), 177.
14. T. G. Room, *The generation by two operators of the symplectic group over* $GF(2)$, J. Austr. Math. Soc., *1* (1959), 38.
15. P. F. G. Stanek, *Two element generation of the symplectic group*, Bull. Amer. Math. Soc., *67* (1961), 225.

University of California

https://doi.org/10.4153/CJM-1962-018-0 Published online by Cambridge University Press