VARIATIONS ON A THEME OF CHEVALLEY

ROBERT STEINBERG

1. Introduction. In this paper we use the methods of C. Chevalley to construct some simple groups and to gain for them the structural theorems of [3]. Among the groups obtained there are two new families of finite simple groups[1], not to be found in the list of E. Artin [1]. Whether the infinite groups constructed are new has not been settled yet.

Section 5 contains statements of the main results of [3]. In §§ 2, 3, 4 and 7, we define analogues of certain real forms of the Lie groups of type A_l, D_l and E_6 (in the usual notation), and extend to them the structural properties of the groups of Chevalley. Sections 6 and 9 treat some identifications, and § 8 deals with the question of simplicity. In §§ 10 and 11, using the extra symmetry inherent in a Lie algebra of type D_4, we consider two modifications of the first construction which are, perhaps, of more interest since they produce groups which have no analogue in the classical complex-real case: in fact, a basic ingredient of each of these variants is a field automorphism of order 3. In Sections 12 and 13, it is proved that new finite simple groups are obtained[1], and their orders are given. Section 14 deals with an application to the theory of group representations, and § 15 with some concluding observations.

The notation is cumulative. We denote by $|S|$ the cardinality of the set S, by K^* the multiplicative group of the field K, and by C the complex field. An introduction to the standard Lie algebra terminology together with statements of the principal results in the classical theory can be found in [3, p. 15–19]. (Proofs are available in [8] or [10]).

2. Roots and reflections. We first introduce some notations. Relative to a Cartan decomposition of a simple complex Lie algebra of rank l, let E be the real space generated by the roots, made into an Euclidean space in the usual way, and normalized as in [3, p. 17–18]. Relative to an ordering $\prec$ of the additive group generated by the roots, let Π be the set of positive roots, and $a(1), a(2), \cdots, a(l)$ the fundamental roots. For each root $r = \Sigma z_i a(i)$, set $\Sigma z_i = ht\ r$, the *height* of r. The ordering $\prec$ can always be chosen so that $ht\ r < ht\ s$ implies $r \prec s$ (see [3, p. 20, *l.* 35–40]); suppose this is done. Assume now the existence of an automorphism σ of E of order 2 such that $\sigma\Pi = \Pi$. This restricts the type of algebra to A_l, D_l $(l \geqq 4)$ or E_6 (see [3, p. 18]), and hence

Received October 2, 1958, in revised form January 8, 1959.

[1] Since the preparation of this paper, the author has learned that these groups have also been discovered by D. Hertzig [6], who has shown that they complete the list of finite simple algebraic groups.

implies that all roots have the same length. We also denote σr by $\bar{r}$. Clearly σ permutes the fundamental roots. Thus $ht\,\bar{r} = ht\,r$ for each root r. Finally, let W be the Weyl group, W^1 the subgroup of elements commuting with σ, and for each $w \in W$ denote by $n(w)$ the number of roots r for which $r \succ 0$ and $wr \prec 0$.

Consider now subsets S of Π of the following three types:

(1) S consists of one root r, which is self-conjugate ($\bar{r} = r$), and which can not be written as a sum of a conjugate pair of roots;

(2) S consists of a conjugate pair r, $\bar{r}$ such that $r + \bar{r}$ is not a root;

(3) S consists of three roots of the form r, $\bar{r}$, $r + \bar{r}$.

Note that in case (2) one has $r \perp \bar{r}$ because $ht\,r = ht\,\bar{r}$ implies that $r - \bar{r}$ is not a root. Shortly we prove the important fact:

2.1 LEMMA. *If Π^1 denotes the collection of sets of types* (1), (2) *and* (3) *above, then Π^1 is a partition of Π.*

In any case, the *fundamental sets* of Π^1 - those which contain fundamental roots - are disjoint because the fundamental roots are linearly independent. If w_r denotes the reflection in the hyperplane orthogonal to r, we set $w_s = w_r$, $w_r w_{\bar{r}}$ or $w_{r+\bar{r}} (= w_r w_{\bar{r}} w_r)$ according as S is of type (1), (2) or (3) above. Note that $w_s \in W^1$.

2.2 LEMMA. *For each fundamental $S \in \Pi^1$, w_s maps S onto -S and permutes the positive roots not in S. Hence $n(w_s) = |S|$.*

Proof. Since $n(w_a) = 1$ for each fundamental root a [8, p. 19-01, Lemma 1], and since w_s can be written as a product of $|S|$ such reflections, it follows that $n(w_s) \leqq |S|$. By direct verification one sees that $w_s S = -S$. Hence the lemma is proved.

2.3 LEMMA. *The group W^1 is generated by the w_s corresponding to fundamental $S \in \Pi^1$.*

Proof. Using induction on $n(w)$, we show that each $w \in W^1$ is a product of elements of the given form. If $n(w) = 0$, $w = 1$, the statement is clearly true. If $n(w) > 0$, $w \neq 1$, there is a fundamental root a such that $a \succ 0$ and $wa \prec 0$. Since $\bar{a} \succ 0$ and $w\bar{a} = \overline{wa} \prec 0$, it follows that $r \succ 0$, $wr \prec 0$ for each root r in the set $S \in \Pi^1$ which contains a. Hence $n(ww_s^{-1}) = n(w) - n(w_s)$ by 2.2, and the induction hypothesis can be applied to ww_s^{-1} to complete the proof.

2.4 LEMMA. *W is a normal subgroup of the group generated by W and σ.*

Proof. One has $\sigma w_r \sigma^{-1} = w_{\bar{r}}$ for each root r. Since σ permutes the roots, and the root reflections generate W, one gets $\sigma W \sigma^{-1} = W$, and hence 2.4.

2.5 LEMMA. *The element* w_0 *of* W *defined by* $w_0 \Pi = -\Pi$ *is in* W^1.

Proof. By 2.4, $\sigma w_0 \sigma^{-1} \in W$. Since $\sigma w_0 \sigma^{-1} \Pi = -\Pi$, one concludes that $\sigma w_0 \sigma^{-1} = w_0$ and that $w_0 \in W^1$.

2.6 LEMMA. *Each* $S \in \Pi^1$ *is congruent under* W^1 *to a fundamental set.*

Proof. Write the element w_0 of 2.5 in the form $w_0 = w_k \cdots w_2 w_1$ guaranteed by 2.3. Since $S \succ 0$ and $w_0 S \prec 0$, there is an index i such that $w_{i-1} \cdots w_1 S \succ 0$ and $w_i \cdots w_1 S \prec 0$. If $T \in \Pi^1$ corresponds to w_i, it follows from 2.2 that $w_{i-1} \cdots w_1 S \subseteq T$, and clearly equality must hold.

By using 2.6 and examinining the fundamental root systems for groups of type A_l, D_l and E_6 (see [3, p. 18] or [8, p. 13-08]), one sees that a set in Π^1 of type (3) can occur only in the case A_l (l even). This turns out to be the most troublesome case in the sequel. Note however that sets of types (1) and (3) do not occur simultaneously.

Proof of 2.1. This follows from 2.6 and the fact that the fundamental sets of Π^1 are non-overlapping.

We now associate with W^1 a reflection group. Let E^+ and E^- respectively denote the positive and negative subspaces of E under σ, and for each $w \in W^1$ let $\tilde{w}$ and $\tilde{W}^1$ denote the restrictions of w and W^1 to E^+. Also denote by $\tilde{S}$ the vector r, $r + \bar{r}$ or $r + \bar{r}$ in the respective cases (1), (2) or (3) of 2.1.

2.7 LEMMA. *The restriction of* W^1 *to* $\tilde{W}^1$ *is faithful.* $\tilde{W}^1$ *is a reflection group of type* $C_{[(l+1)/2]}$, B_{l-1} *or* F_4 *in the respective cases that* W *is of type* A_l, D_l *or* E_6, *and, to within a change of scale,* $\{\tilde{S} \mid S \in \Pi^1\}$ *is a corresponding system of positive root vectors.*

Proof. First if $w \in W^1$, $\tilde{w} = 1$, then w maps each positive root onto another one. Hence $w = 1$, and the restriction is faithful. Those $\tilde{S}$ which correspond to the fundamental $S \in \Pi^1$ form a new fundamental root system (to within a change of scale) of the listed type, as one sees by considering the separate cases (see [3, p. 18]). Becuse of 2.3 and 2.6, the proof is complete if it can be shown that, for each fundamental $S \in \Pi^1$, $\tilde{w}_s$ is the reflection in the hyperplane orthogonal to $\tilde{S}$. If

$|S| = 2$ and $S = \{a, \bar{a}\}$, then w_s has -1 as a characteristic value of multiplicity 2. Since $w_s(a + \bar{a}) = -(a + \bar{a})$, $w_s(a - \bar{a}) = -(a - \bar{a})$, $a + \bar{a} \in E^+$, and $a - \bar{a} \in E^-$, it follows that $\tilde{w}_s$ has -1 as a characteristic value of multiplicity 1, and then that $\tilde{w}_s$ is the required reflection. If $|S| = 1$ or $|S| = 3$, the result follows from the definitions.

2.8 COROLLARY. *Any two sets of the same type in the partition 2.1 are congruent under* W^1.

Proof. Since sets of types (1) and (3) do not occur simultaneously, and since $\tilde{W}^1$ is transitive on its root vectors of a given length, 2.8 follows from 2.7.

A new ordering $<$ of the positive roots is now introduced. First if $R, S \in \Pi^1$, then $R < S$ means that $\min r \in R \prec \min s \in S$. Then if $r, s \in \Pi$, define $r < s$ to mean that either r and s belong to distinct sets R and S of Π^1 and $R < S$, or r and s belong to the same set of Π^1 and $r \prec s$,

2.9 LEMMA. *The roots in each set* S *of* Π^1 *occur consecutively in the ordering of the roots of* Π *relative to* $<$. *If* r, s *and* $r + s$ *are positive roots, then* $r + s > \min(r, s)$.

Proof. The first statement follows from the definition. Since $\prec$ respects heights, the second assertion is true if $r + s$ has minimum height in the set S of Π^1 containing it. Thus one may assume that there is a root t such that $r + s = t + \bar{t}$, $r \neq t$, $r \neq \bar{t}$, and that W is of type A_l (l even). Then each positive root is a sum of a string of distinct fundamental roots, and the strings corresponding to r and s are necessarily of different lengths. Thus $ht\, t = ht\, \bar{t} > \min(ht\ r, ht\ s)$. Since $\prec$ respects heights, this implies that $r + s > \min(t, \bar{t}) > \min(r, s)$.

3. **Construction of an involution.** Suppose that $\mathfrak{g}$ is a simple complex Lie algebra with a generating system $(X_r, X_{-r}, H_r, r \in \Pi)$ chosen to satisfy the conditions of Theorem 1 of [3]. Assume also that $\mathfrak{g}$ is restricted to type A_l, D_l ($l \geqq 4$) or E_6 so that the results of § 2 can be applied. Set $r(H_s) = r(s)$. Then, all roots being of the same length, it follows that:

3.1 $$X_r X_s = N_{rs} X_{r+s}\,;\ N_{rs} = 0,\ \pm 1;\ r,\ s \in \Pi\ .$$

For the same reason $r(s) = s(r)$ and $r(r) = 2$. By the uniqueness theorem for a simple Lie algebra with a given root structure (see [8, p. 11-04] or [10, p. 94]), there exists an automorphism σ_C of $\mathfrak{g}$ such that $\sigma_C H_r = H_{\bar{r}}$ and $\sigma_C X_r = c_r X_{\bar{r}}$, $c_r \in C^*$, $r \in \Pi$ or $-\Pi$, with $c_a = 1$ for each fundamental root a. Then each $c_{-a} = 1$, and by induction on the height one gets each $c_r = \pm 1$. Next let K be a field on which an automorphism σ of order 2 acts, let K_0 be the fixed field, and write $\sigma k = \bar{k}$, $k \in K$. Then following the procedure of [3, p. 32], one can transfer the base field of $\mathfrak{g}$ from C to K, and thus gain a Lie algebra $\mathfrak{g}_K$ over K and a semi-automorphism σ of $\mathfrak{g}_K$ such that $\sigma(kH_r) = \bar{k}H_{\bar{r}}$ and $\sigma(kX_r) = \pm \bar{k}X_{\bar{r}}$, $k \in K$, $r \in \Pi$ or $-\Pi$. Note [3, p. 32] that the field is not transferred for roots (or weights) and that the expression $r(s)$ retains its original meaning.

3.2 Lemma. *The order of σ is 2. By appropriate sign changes of the X_r one can arrange things so that in the equations $\sigma X_r = k_r X_{\bar{r}}$, $r \in \Pi$, one has:*

(a) $k_{\bar{r}} = k_r$;

(b) *if $\bar{r} \neq r$, then $k_r = 1$;*

(c) *if $\bar{r} = r$, then k_r is 1 or -1 according as r belongs to an $S \in \Pi^1$ of 1 or 3 elements.*

Proof. One has $\sigma^2 X_a = X_a$, $\sigma^2 X_{-a} = X_{-a}$ for each fundamental root a. Thus $\sigma^2 = 1$, and this implies (a). If r, $\bar{r}$ is a conjugate pair in Π, if $r < \bar{r}$, and if $k_r = -1$, replace X_r by $-X_r$. Then (b) holds. If $|S| = 3$ in (c), there is a root s such that $r = s + \bar{s}$, and one gets (c) by applying σ to the equation $X_s X_{\bar{s}} = kX_r$. If $|S| = 1$, assume $ht\ r > 1$. Then there is either a self-conjugate fundamental root a such that $r - a$ is a root, or a conjugate pair of orthogonal fundamental roots b, $\bar{b}$ such that $r - b$, $r - \bar{b}$ and $r - b - \bar{b}$ are all roots. One then applies σ to the equation $X_{r-a} X_a = k_1 X_r$ or $(X_{r-b-\bar{b}} X_b) X_{\bar{b}} = k_2 X_r$, respectively, and completes the proof of (c) by induction on the height.

We assume henceforth that the normalization indicated by 3.2 has been made and that the corresponding treatment has been given to the negative roots, so that one has once again the equations of structure of Theorem 1 of [3] (in particular, $X_r X_{-r} = H_r$).

4. Some nilpotent groups. As in [3], we set $x_r(t) = \exp(t\ ad\ X_r)$, $t \in K$, $r \in \Pi$, denote by $\mathfrak{X}_r$ the one-parameter group $\{x_r(t) \mid t \in K\}$, and by $\mathfrak{U}$ the group generated by all $\mathfrak{X}_r$, $r \in \Pi$.

4.1 Lemma. *For r, $s \in \Pi$ and t_1, $t_2 \in K$, one has the commutator relation $(x_r(t_1), x_s(t_2)) = x_{r+s}(N_{rs} t_1 t_2)$.*

Proof. This follows from [3, p. 33, *l.* 22] and the fact that all roots have the same length.

A straightforward computation yields:

4.2 $$\sigma \exp(t\ ad\ X_r)\, \sigma^{-1} = \exp(\bar{t}\ ad\ \sigma X_r)\ .$$

4.3 LEMMA. *Let Σ be a subset of Π satisfying the condition*

4.4 $$r,\ s \in \Sigma,\ r + s \in \Pi \ \textit{imply}\ r + s \in \Sigma.$$

Then each $x \in \mathfrak{U}_\Sigma$, the group generated by all $\mathfrak{X}_r$, $r \in \Sigma$, can be written uniquely in the form $x = \prod x_r(t_r)$, the product being over the roots of Σ arranged in increasing order relative to $<$ (see § 2).

Proof. Using the formulas 4.1 repeatedly, one sees that the set of elements of the given form is closed under multiplication; thus each $x \in \mathfrak{U}_\Sigma$ has an expression of the given form. Uniqueness is proved by induction on $|\Sigma|$. If $|\Sigma| = 1$ and $\Sigma = \{r\}$, this follows from $x_r(t)X_{-r} = X_{-r} + tH_r - t^2X_r$ (see [3, p. 36, *l.* 15]). If $|\Sigma| > 1$, let r be the least element of Σ (relative to $<$), and set $\Sigma' = \Sigma - r$. Let $x \in \mathfrak{U}_\Sigma$ be written as $x = x_r(t_1)x_1$ and $x = x_r(t_2)x_2$ with $t_i \in K$ and $x_i \in \mathfrak{U}_{\Sigma'}$. Then $x_r(t_2 - t_1) = x_1x_2^{-1}$. Since $x_r(t_2 - t_1)X_{-r} = X_{-r} + (t_2 - t_1)H_r - (t_2 - t_1)^2X_r$, since $x_r(t_2 - t_1) \in \mathfrak{U}_{\Sigma'}$, and since r can not be written as a sum of roots larger than r by 2.9, it follows that the coefficient of H_r, namely $t_2 - t_1$, must be 0. Thus $x_1 = x_2$, and the induction hypothesis can be applied to Σ' to complete the proof.

The result 4.3 can be applied in the cases $\Sigma = \Pi$ and $\Sigma = S \in \Pi^1$. Because of 2.9, one gets:

4.5 COROLLARY. *Each $x \in \mathfrak{U}$ can be written uniquely in the form $x = \prod x_s$, $x_s \in \mathfrak{U}_s$, the product being over the sets S of Π^1 arranged in increasing order.*

Denote now by $\mathfrak{U}^1$, $\mathfrak{U}^1_s$, etc. the subgroups of elements of $\mathfrak{U}$, $\mathfrak{U}_s$, etc. commuting with σ.

4.6 LEMMA. *If $x \in \mathfrak{U}$ is written in the form 4.5, then $x \in \mathfrak{U}^1$ if and only if each $x_s \in \mathfrak{U}^1$. A necessary and sufficient condition for $x_s \in \mathfrak{U}_s$ to be in $\mathfrak{U}^1$ is that, in the cases (1), (2) or (3) of 2.1, x_s has the respective form (1) $x_r(t), \bar{t} = t$, (2) $x_r(t)x_{\bar{r}}(v)$, $v = \bar{t}$, or (3) $x_r(t)x_{\bar{r}}(v)x_{r+\bar{r}}(w)$, $v = \bar{t}$, $w + \bar{w} = N_{\bar{r}r}t\bar{t}$.*

Proof. If $x \in \mathfrak{U}^1$ commutes with σ, one has $x = \sigma x \sigma^{-1} = \prod(\sigma x_s \sigma^{-1})$. Since $\sigma x_s \sigma^{-1} \in \mathfrak{U}_s$ by 4.2, one gets $\sigma x_s \sigma^{-1} = x_s$ by the uniqueness in 4.5. Thus each $x_s \in \mathfrak{U}^1$. The converse is clear. In the cases listed in the second statement, one has

(1) $\sigma x_r(t)\sigma^{-1} = x_{\bar{r}}(\bar{t})$,

(2) $\sigma x_r(t)x_{\bar{r}}(v)\sigma^{-1} = x_r(\bar{v})x_{\bar{r}}(\bar{t})$, and

(3) $\sigma x_r(t)x_{\bar{r}}(v)x_{r+\bar{r}}(w)\sigma^{-1} = x_r(\bar{v})x_{\bar{r}}(\bar{t})x_{r+\bar{r}}(-\bar{w} + N_{r\bar{r}}\bar{t}\bar{v})$ by 3.2, 4.1 and 4.2. The required results now follow from 4.3.

4.7 LEMMA. *Let Π be the union of the disjoint sets Σ and Σ',* *each invariant under σ, and each satisfying* 4.4. *Then* $\mathfrak{U}^1 = \mathfrak{U}^1_\Sigma \mathfrak{U}^1_{\Sigma'}$ *and* $\mathfrak{U}^1_\Sigma \cap \mathfrak{U}^1_{\Sigma'} = 1$.

Proof. By [3, p. 41, Lemma 11], one can write $x \in \mathfrak{U}^1$ uniquely in the form $x = yy'$, $y \in \mathfrak{U}_\Sigma$, $y' \in \mathfrak{U}_{\Sigma'}$. The proof that y and y' are in $\mathfrak{U}^1$ is the same as that for the first part of 4.6.

If $\mathfrak{B}$ denotes the group generated by all $\mathfrak{X}_r$, $r < 0$, then one can define $\mathfrak{B}^1$, $\mathfrak{B}_s$, etc., and gain for these groups corresponding results.

5. Main results of Chevalley. For each simple complex Lie algebra $\mathfrak{g}$ (not necessarily one for which σ exists), consider the groups $\mathfrak{U}$ and $\mathfrak{B}$ and also the group G (denoted in [3] by G') which they generate. For each $w \in W$, if Σ consists of the roots r for which $r > 0$ and $wr < 0$, we set $\mathfrak{U}_\Sigma = \mathfrak{U}_w$ (denoted in [3] by $\mathfrak{U}''_w$). Let P_r and P, respectively, denote the additive groups generated by the roots and by the weights. Corresponding to each character χ of P_r into K^*, there is an automorphism $h = h(\chi)$ of $\mathfrak{g}_K$ defined by $hX_r = \chi(r)X_r$, $r \in \Pi$ or $-\Pi$. Let $\mathfrak{H}$ (denoted in [3] by $\mathfrak{H}'$) be the group generated by those automorphisms which correspond to characters which can be extended to P. For $h(\chi) \in \mathfrak{H}$, one has

5.1 $$hx_r(t)h^{-1} = x_r(\chi(r)t) \ .$$

The main results of [3] are as follows:

5.2 G contains $\mathfrak{H}$.

5.3 Corresponding to each $w \in W$ there is $\omega(w) \in G$ such that $\omega(w)X_r = c_rX_{wr}$, $\omega(w)H_r = H_{wr}$, $c_r \in K^*$, $r \in \Pi$ or $-\Pi$. The union of the sets $\mathfrak{H}\omega(w)$ is a group $\mathfrak{W}$ and the map $w \to \mathfrak{H}\omega(w)$ is an isomorphism of W on $\mathfrak{W}/\mathfrak{H}$.

Parenthetically, we remark that here one has:

5.4 $$\omega(w)\mathfrak{X}_r\omega(w)^{-1} = \mathfrak{X}_{wr} \ .$$

5.5 G is the union of the sets $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}_w$, $w \in W$. These sets are disjoint and each element of G has a unique expression of the indicated form.

5.6 G is simple if one excludes the case (1) $|K| = 2$ and $\mathfrak{g}$ of type A_1, B_2 or G_2, and (2) $|K| = 3$ and $\mathfrak{g}$ of type A_1.

Before proving corresponding results for the group G^1 generated by $\mathfrak{U}^1$ and $\mathfrak{B}^1$, we identify G^1 in the case that $\mathfrak{g}$ is of type A_l.

6. Some unitary groups. Consider the form

6.1 $$f(\alpha, \beta) = \sum_1^{l+1} (-1)^i \alpha_i \bar{\beta}_i$$

on a space of l dimensions over K. Let $U_{l+1}(f)$ denote the corresponding unimodular unitary group and $C_{l+1}(f)$ its center. Then one has:

6.2 *If* $\mathfrak{g}$ *is of type* A_l, $G^1 \cong U_{l+1}(f)/C_{l+1}(f)$.

Proof. *If* $\mathfrak{g}$ *is of type* A_l, one can identify $\mathfrak{g}_K$ with $\mathfrak{sl}_{l+1}(K)$, the algebra of $(l+1)$th order matrices of trace 0, in such a way that, for each fundamental root $a(i)$, $X_{a(i)} \in \mathfrak{g}_K$ corresponds to $E_{i,i+1}$, the matrix with 1 in the $(i, i+1)$ position and 0 elsewhere [7, p. 393]. If $m = ((-1)^i\delta_{i,l+2-j})$ is the matrix corresponding to f, one can then verify that σ is the product of the transformations $Y \to mYm^{-1}$ (matrix multiplication) and $Y \to -\overline{Y}^t$ (t = transpose). According to a recent identification of R. Ree [7], $\mathfrak{U}$ and $\mathfrak{V}$, respectively, consist of the superdiagonal matrices (0 below and 1 on the diagonal) and the subdiagonal matrices, acting on $\mathfrak{sl}_{l+1}$ via inner automorphisms, so that the group G of Chevalley is in this case the projective unimodular group. Now it follows from material in [4, p. 66-69] that $U_{l+1}(f)$ is generated by its superdiagonal and subdiagonal elements and that $C_{l+1}(f)$ consists of scalar matrices. Thus to prove 6.2 it is enough to prove:

6.3 Let x be a superdiagonal matrix. Then $x \in \mathfrak{U}^1$ if and only if $x \in U_{l+1}(f)$.

A simple calculation using the concrete form of σ given above shows that $x\sigma = \sigma x$ if and only if $\bar{x}^t m^{-1} x m$ commutes with each $Y \in \mathfrak{sl}_{l+1}$. This is equivalent to $xm\bar{x}^t = km$, $k \in K$. If x is superdiagonal, k must be 1, because the $(1, l+1)$ entries of the matrices $xm\bar{x}^t$ and m are both -1. Thus 6.3 and 6.2 are proved.

It is to be observed that the form f has index $[(l+1)/2]$.

7. Structure of G^1. Recall that G^1 is the group generated by $\mathfrak{U}^1$ and $\mathfrak{V}^1$. For each $w \in W^1$, set $\mathfrak{U}^1_w = \mathfrak{U}^1 \cap \mathfrak{U}_w$. For each $S \in \Pi^1$, let G^1_S be the group generated by $\mathfrak{U}^1_S$ and $\mathfrak{V}^1_S$. Denote by X^1 the group of those characters of P_r into K^* which can be extended to characters χ of P which are selfconjugate in the sense that $\chi(\bar{a}) = \overline{\chi(a)}$ for all $a \in P$, and by $\mathfrak{H}^1$ the corresponding subgroup of $\mathfrak{H}$. For $S \in \Pi^1$, set $\mathfrak{H}^1_S = \mathfrak{H}^1 \cap G_S$. Finally, for each root r and each $k \in K^*$, denote by $\chi_{r,k}$ the character on P_r defined by $\chi_{r,k}(s) = k^{s(r)}$.

It is assumed until further notice that $\mathfrak{g}$ is not of type A_l (l even). We aim to prove:

7.1 Lemma. *For each* $w \in W^1$, $\mathfrak{H}\omega(w) \cap G^1$ *is not empty.*

Once this is established, it can (and will) be assumed that $\omega(w) \in G^1$ for each $w \in W^1$. Then:

7.2 Theorem. G^1 *is the union of the sets* $\mathfrak{U}^1\mathfrak{H}^1\omega(w)\mathfrak{U}^1_w$, $w \in W^1$. *The sets are disjoint and each element of* G^1 *has a unique expression of the indicated form.*

The steps of the proof are quite analogous to those in the proof of 5.5 in view of the following:

7.3 LEMMA. *Assume $S \in \Pi^1$. Then* (1) *if $S = \{r\}$, there is a homomorphism φ_1 of $SL_2(K_0)$, the unimodular group, onto G^1_s such that*

$$\varphi_1\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} = x_r(t),\ \varphi_1\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} = x_{-r}(t),\ \varphi_1\begin{pmatrix}k & 0\\ 0 & k^{-1}\end{pmatrix} = h(\chi_{r,k}) ,$$

and

$$\varphi_1\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \equiv \omega(w_r) \pmod{\mathfrak{H}} ;$$

(2) *if $S = \{r, \bar{r}\}$, there is a homomorphism φ_2 of $SL_2(K)$ onto G^1_s such that*

$$\varphi_2\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} = x_r(t)x_{\bar{r}}(\bar{t}),\ \varphi_2\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} = x_{-r}(t)x_{-\bar{r}}(t),\ \varphi_2\begin{pmatrix}k & 0\\ 0 & k^{-1}\end{pmatrix} = h(\chi_{r,k}\chi_{\bar{r},\bar{k}}) ,$$

and

$$\varphi_2\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \equiv \omega(w_r w_{\bar{r}}) \pmod{\mathfrak{H}} .$$

Proof. The existence of φ_1 is established in [3, p. 29, p. 36]. Since $\mathfrak{X}_r$ and $\mathfrak{X}_{-r}$ commute elementwise with $\mathfrak{X}_{\bar{r}}$ and $\mathfrak{X}_{-\bar{r}}$, it is clear that φ_2 also exists.

Proof of 7.1. By 7.3, $\mathfrak{H}\omega(w_s) \cap G^1$ is non-empty for each $S \in \Pi^1$. Thus 7.1 follows from 2.3.

Now we choose $\omega(w) \in G^1$ for each $w \in W^1$, and denote by $\mathfrak{W}^1$ the union of the sets $\mathfrak{H}^1\omega(w)$. Then the analogue of 5.3 holds.

7.4 LEMMA. *G^1 contains $\mathfrak{H}^1$.*

Proof. G^1 contains all $h(\chi) \in \mathfrak{H}^1$ such that χ is of the form $\chi_{a,k}$, $\bar{a} = a$, $\bar{k} = k$, or $\chi_{a,j}\chi_{\bar{a},\bar{j}}$ by 7.3. These characters generate X^1 (see [3, p. 48, Lemma 2]). Thus $G^1 \supset \mathfrak{H}^1$.

7.5 LEMMA. *For each $S \in \Pi^1$, G^1_s is the the union of the sets $\mathfrak{U}^1_s\mathfrak{H}^1_s$ and $\mathfrak{U}^1_s\mathfrak{H}^1_s\omega(w_s)\mathfrak{U}^1_s$.*

Proof. Because of 7.3, this follows from the corresponding properties of the groups $SL_2(K_0)$ and $SL_2(K)$ (see [3, p. 34, Lemma 2]).

7.6 LEMMA. *G^1 is generated by the groups $\mathfrak{U}^1_s$ and $\mathfrak{V}^1_s$ which correspond to fundamental sets $S \in \Pi^1$.*

Proof. This follows from 7.1, 5.4 and 4.5.

7.7 LEMMA. $G^1 = \mathfrak{U}^1\mathfrak{W}^1\mathfrak{U}^1$.

Proof. This follows from 7.6, 7.5, 7.1 and 4.7 as in [3, p. 40, Lemma 10].

Proof of 7.2. That G^1 is the union of the given sets follows from 7.7 and 4.7 as in [3, p. 42, Theorem 2]. The disjointness and uniqueness follow from 5.5.

7.8 COROLLARY. $\mathfrak{H}^1 = \mathfrak{H} \cap G^1$.

Proof. Because of 7.2, this is clear.

7.9 COROLLARY. $\mathfrak{U}^1\mathfrak{H}^1$ *is the normalizer of* $\mathfrak{U}^1$ *in* G^1.

Proof. The normalizer contains $\mathfrak{U}^1\mathfrak{H}^1$ by 5.1, and equality follows from 7.2.

One also concludes from the preceding results:

7.10 COROLLARY. *The sets of* 7.2 *are the double cosets of* G^1 *relative to* $\mathfrak{U}^1\mathfrak{H}^1$.

7.11 COROLLARY. *If K is a finite field of characteristic p, then* $\mathfrak{U}^1$ *and* $\mathfrak{V}^1$ *are p-Sylow subgroups of* G^1.

In regard to 7.11, one sees from 4.5 and 4.6 that, if $|K| = q^2$ and $|\Pi| = N$, then $|\mathfrak{U}^1| = q^N$.

We now remove the restriction on $\mathfrak{g}$ and remark that the results of this section remain valid even if $\mathfrak{g}$ is of type A_l (l even). The key point here is that, if $S \in \Pi^1$ and $|S| = 3$, then there exists a homomorphism of $U_3(f)$ (see 6.1) onto G^1_S with properties like those of φ_1 and φ_2 in 7.3. We omit the proof which can be made to depend on the representation of G^1 by unitary matrices given in § 6.

8. Proof of simplicity.

Our aim here is to prove:

8.1 THEOREM. *If K_0 has at least* 5 *elements, then G^1 is simple.*

The simplicity of the group SL_2 over its center is assumed to be known. It is further assumed that $\mathfrak{g}$ is not of type A_l (l even) and that $l \geqq 3$. The proof to be given can be adapted with minor modifications to the missing groups, which are in any case adequately covered by 6.2 and [4, p. 70, Theorem 5].

8.2 LEMMA. *Assume R, $T \in \Pi^1$, $R \neq T$, and that r, t are elements of R, T, respectively. Then there is $\chi \in X^1$ such that $\chi(r) = 1$, $\chi(t) \neq 1$.*

Proof. Let $\tilde{R}$ (or more simply R) denote r or $r + \bar{r}$ in the cases $\bar{r} = r$ or $\bar{r} \neq r$, respectively, and then set $\chi_{R,k} = \chi_{r,k}$ or $\chi_{R,k} = \chi_{r,k}\chi_{\bar{r},\bar{k}}$ accordingly. Treat t and T similarly. If $R(T) = 0$, set $\chi = \chi_{T,k}$, $k \in K_0^*$, $k^2 \neq 1$. If $R(T) = \pm 1$, or if $R(T) = \pm 2$ and $|R| = |T| = 2$, set $\chi = \chi_{T,k}{}^2 \chi_{R,k}^{-r(T)}$, $k \in K_0^*$, $k^3 \neq 1$. In the other cases of $R(T) = \pm 2$, set $\chi = \chi_{t,k}\chi_{\bar{t},k}\chi_{R,k}^{-r(t)}$, $k \in K_0^*$, $k^2 \neq 1$. Finally if $R(T) = \pm 4$, set $\chi = \chi_{t,k}\chi_{\bar{t},\bar{k}}$, $k = \bar{k}_1/k_1$, $k_1 \in K$, $\bar{k}_1 \neq \pm k_1$. One can check that these cases are exhaustive and that $\chi(r) = 1$ and $\chi(t) \neq 1$ in each case.

8.3 LEMMA. *If $w \in W^1$ and $w \neq 1$, there is $h \in \mathfrak{H}^1$ such that $\omega(w)h \neq h\omega(w)$.*

Proof. We first show that there exist $\chi \in X^1$ and $r \in \Pi$ such that $\chi(wr) \neq \chi(r)$. If there is an $R \in \Pi^1$ such that $wR \neq \pm R$, then χ and r exist by 8.2. If $wR = \pm R$ for all $R \in \Pi^1$, then, since $w \neq 1$, one has $wR = -R$ for all $R \in \Pi^1$. Since $l \geqq 3$, one can readily choose $r, t \in \Pi$ so that $r \perp \bar{r}$, $t = \bar{t}$ and $r(t) < 0$. If $k \in K_0^*$, $k^2 \neq 1$, then $\chi = \chi_{t,k}$ and r have the required property. If $h = h(\chi)$, a simple calculation now shows that X_r has different images under $\omega(w)h$ and $h\omega(w)$.

Assume now that H is a normal subgroup of G^1 and that $|H| > 1$.

8.4 LEMMA. $|H \cap \mathfrak{U}^1\mathfrak{H}^1| > 1$.

Proof. By 7.2 there is $x \in H$ such that $x \neq 1$ and $x = uh_1\omega(w)$ with $u \in \mathfrak{U}^1$, $h_1 \in \mathfrak{H}^1$ and $w \in W^1$. If $w \neq 1$, then by 8.3 there is $h \in \mathfrak{H}^1$ such that $\omega(w)h \neq h\omega(w)$. Then $y = hxh^{-1}x^{-1} \in H \cap \mathfrak{U}^1\mathfrak{H}^1$, and we assert that $y \neq 1$. Indeed, if $y = 1$, then

$$x = hxh^{-1} = huh^{-1}(hh_1\omega(w)h^{-1}\omega(w)^{-1})\omega(w) ,$$

and by 7.2 one gets $h\omega(w)h^{-1}\omega(w)^{-1} = 1$, a contradiction. Thus the assertion and the lemma are proved.

8.5 LEMMA. $|H \cap \mathfrak{U}^1| > 1$.

Proof. By 8.4, there is $x \in H \cap \mathfrak{U}^1\mathfrak{H}^1$ such that $x \neq 1$. Write $x = uh$, $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$, and suppose $h \neq 1$. Then there is a fundamental root r such that $hX_r = cX_r$, $c \in K$, $c \neq 1$. If $r \in S \in \Pi^1$, let y be the commutator of x with $x_r(1)$ or $x_r(1)x_{\bar{r}}(1)$ according as $|S| = 1$ or 2. Then $y \in H \cap \mathfrak{U}^1$, and it remains to show that $y \neq 1$. If $y = 1$, then, for the case $|S| = 1$, one has $x_r(1) = uhx_r(1)h^{-1}u^{-1} = ux_r(c)u^{-1}$. Now it follows easily from 4.1 that the subgroup $\mathfrak{U}_2$ of $\mathfrak{U}$ generated by those $\mathfrak{X}_r$ for which $ht\ r > 1$ contains the commutator subgroup of $\mathfrak{U}$. Thus $x_r(1-c) = x_r(1)x_r(c)^{-1} \in \mathfrak{U}_2$, whence $1 - c = 0$ by 4.3. This contradiction establishes $y \neq 1$. The case $|S| = 2$ can be treated similarly.

8.6 LEMMA. *For some $R \in \Pi^1$, $|H \cap U^1_R| > 1$.*

Proof. Among all $x \in H \cap \mathfrak{U}^1$ with $x \neq 1$, choose one which maximizes the minimum $S \in \Pi^1$ for which $x_s \neq 1$ in the representation 4.5. If this minimum is R, we show $x = x_R$. Assuming the contrary, one can write $x = x_R x_T x_1$ with $x_R \neq 1$, $x_T \neq 1$, and x_1 denoting the remaining terms in 4.5. By 8.2, 5.1 and 4.6, there is $h \in \mathfrak{H}^1$ such that $hx_Rh^{-1} = x_R$ and $hx_Th^{-1} \neq x_T$. Thus $hxh^{-1} \neq x$ by 4.5. But then $y = x^{-1}hxh^{-1} \neq 1$, $y \in H \cap \mathfrak{U}^1$, and y provides a contradiction to the choice of x.

Using 8.6, one can deduce as in [3, p. 62, Lemma 15]:

8.7 LEMMA. *If $|H \cap \mathfrak{U}^1_R| > 1$ for $R \in \Pi^1$, then $H \supset \mathfrak{U}^1_R$.*

Proof of 8.1. As in 8.3 choose (fundamental) roots r, t such that $r \perp \bar{r}$, $t = \bar{t}$ and $r(t) < 0$. Since $r \perp \bar{r}$, this implies that $r + t$, $\bar{r} + t$ and $r + \bar{r} + t$ are all roots. Set $R = \{r, \bar{r}\}$, $T = \{t\}$, $U = \{r + t, \bar{r} + t\}$, $V = \{r + \bar{r} + t\}$, $x_R(1) = x_r(1)x_{\bar{r}}(1)$, $x_T(1) = x_t(1)$, etc.. Then by 4.1 (used several times), one gets:

8.8 $$(x_R(1),\ x_T(1)) = x_U(N_{rt})x_V(N_{rt}N_{r,\bar{r}+t})\ .$$

By 8.7, 5.4 and 2.8, either $x_R(1)$ or $x_T(1)$ is in H; hence so is their commutator. For the same reason one of the elements on the right of 8.8 is in H; hence so is the other. Thus, by 8.7, 5.4, 3.1 and 2.8, H contains all $\mathfrak{U}^1_S$, hence also $\mathfrak{U}^1$ by 4.5. Similarly H contains $\mathfrak{V}^1$, whence $H = G^1$. Thus G^1 is simple.

9. Some identifications. If $\mathfrak{g}$ is of type A_l, then G^1 has been identified in § 6 as a projective unitary group in $l + 1$ dimensions. Similarly, if $\mathfrak{g}$ is of type D_l ($l \geqq 4$), then using the representation of G given by Ree [7], one can show that G^1 is isomorphic to a projective orthogonal group corresponding to a form in $2l$ variables which has index $l - 1$ relative to K_0 and index l relative to K. The details in the complex-real case can be found in [2, p. 422]. If $\mathfrak{g}$ is of type E_6, then, again in the complex-real case, one can identify G^1 with a real form of E_6, the one characterized by Cartan [2, p. 493] by the fact that its Killing form, when written as a sum of real squares, contains a surplus of 2 positive terms. If $\mathfrak{g}$ is of type E_6 and K is finite, we show in § 12 that new groups are obtained[1], not isomorphic to any appearing in the list of finite simple groups given by Artin [1].

10. Second variation for D_4. A root system for D_4 has a fundamental basis consisting of roots a, b, c, d of the same length such that b, c, d are mutually orthogonal and each makes an angle of $2\pi/3$ with a. Let τ be the automorphism of order 3 of the underlying Euclidean space defined by $a, b, c, d \to a, c, d, b$, and let W^2 be the subgroup of elements of W commuting with τ. One can then obtain the analogues of the results of § 2 without essential change in the proofs. For example: W^2 is generated by the elements w_a and $w_b w_c w_d$, and is of type G_2. The roots are partitioned into sets of the types (1) $S = \{r\}$, $\tau r = r$, and (2) $S = \{r, \tau r, \tau^2 r\}$. Any 2 sets of the same type are congruent under W^2. One then introduces a field K on which an automorphism τ of order 3 acts, and defines a semi-automorphism τ of $\mathfrak{g}_K$ by $\tau(kX_r) = (\tau k)X_{\tau r}$. Then $\mathfrak{U}^2$ and $\mathfrak{V}^2$ are the subgroups of $\mathfrak{U}$ and $\mathfrak{V}$, respectively, made up of elements commuting with τ and G^2 is the group they generate. The whole previous developement goes through. It turns out that in the proof of simplicity it is enough to assume that the fixed field K_0 has at least 4 elements. In § 12, it is shown that once again new finite groups[1] are obtained.

11. Third variation for D_4. Assume now that K is a field admitting automorphisms σ and τ which are of orders 2 and 3 respectively, and which generate a group isomorphic to S_3, the symmetric group on 3 objects. Define corresponding semi-automorphisms σ and τ of the Lie algebra $\mathfrak{g}_K$ of type D_4 as in §§ 3 and 10. Then set $\mathfrak{U}^3 = \mathfrak{U}^1 \cap \mathfrak{U}^2$, $\mathfrak{V}^3 = \mathfrak{V}^1 \cap \mathfrak{V}^2$, and let G^3 be the group generated by $\mathfrak{U}^3$ and $\mathfrak{V}^3$. Again everything goes through. It need only be remarked that the present construction is possible only if K is infinite, and that all groups of type G^3 are simple.

12. Some new groups. The list L of known finite simple groups consists of the cyclic, alternating and Mathieu groups, and the "Lie groups", namely the groups G of Chevalley over A_l $(l \geqq 1)$, B_l $(l \geqq 2)$, C_l $(l \geqq 3)$, D_l $(l \geqq 4)$, E_6, E_7, E_8, F_4 and G_2, the groups G^1 over A_l $(l \geqq 2)$, D_l $(l \geqq 4)$ and E_6, and the groups G^2 over D_4, all constructed on a finite field. By the type of one of these latter groups we mean a combination consisting of the general mode of construction (G or G^1 or G^2), the underlying complex Lie algebra $\mathfrak{g}$, and the field K. We adopt the notation: $E_6^1(r)$ is the group of type G^1 over E_6 on a field of r elements. Our aim is to prove:

12.1 THEOREM. *If G is one of the groups $E_6^1(q^2)$ or $D_4^2(q^3)$, then $\hat{G}$*

is not isomorphic to a cyclic, alternating or Mathieu group, and two representations of $\hat{G}$ as Lie groups necessarily have the same type.

In other words the groups $E_6^1(q^2)$ and $D_4^2(q_1^3)$ are new[1] and distinct among themselves. We need some preliminary results. Let $\hat{G}$ be a Lie group over a field K of q, q^2 or q^3 elements in the cases G, G^1 or G^2, respectively, and set $\hat{W} = W$, W^1 or W^2 accordingly. The *Poincaré sequence* of $\hat{G}$ shall mean the list of numbers $q^{n(w)} (w \in \hat{W})$ arranged in non-decreasing order. Thus the first term is 1 and the last term is q^N, the integer N being the number of positive roots of $\mathfrak{g}$ (see 2.5, 4.5 and 4.6).

12.2 Lemma. *The Poincaré sequence of $A_l^1(q^2)$, $D_l^1(q^2)$, $E_6^1(q^2)$ or $D_4^2(q^3)$ is obtained by writing the respective polynomial* $\prod_1^{l+1} \frac{t^i - (-1)^i}{t - (-1)^i}$,

$$(t^l + 1) \prod_2^{l-1} \frac{t^{2i} - 1}{t - 1}, \quad \frac{t^2 - 1}{t - 1} \cdot \frac{t^5 + 1}{t + 1} \cdot \frac{t^6 - 1}{t - 1} \cdot \frac{t^8 - 1}{t - 1} \cdot \frac{t^9 + 1}{t + 1} \cdot \frac{t^{12} - 1}{t - 1} \text{ or}$$

$(t + 1)(t^3 + 1)(t^8 + t^4 + 1)$ *as a sum of non-decreasing powers of t and then replacing t by q in the individual terms.*

To avoid interruption of the present development we give the proof in the next section. We also need the polynomials for the groups of Chevalley. As one sees from considerations in [3, p. 44, p. 64], these polynomials take the form $\prod[(t^{a(i)} - 1)/(t - 1)]$, the $a(i)$ being given in [3, p. 64]. Since $q^{n(w)} = |\mathfrak{U}_w^1|$ by 4.6 and 4.7, one can use 12.2 in conjunction with 7.2 and the definition of $\mathfrak{H}^1$ to compute $|G^1|$. In the same way, one can find $|G^2|$. Thus:

12.3 Lemma. *If u is the g. c. d. of 3 and $q + 1$, the orders of $E_6^1(q^2)$ and $D_4^2(q^3)$ are $u^{-1}q^{36}(q^2 - 1)(q^5 + 1)(q^6 - 1)(q^8 - 1)(q^9 + 1)(q^{12} - 1)$ and $q^{12}(q^2 - 1)(q^6 - 1)(q^8 + q^4 + 1)$, respectively.*

The orders of the other Lie groups can be found in [1]. It is interesting to note that, if in the expressions in 12.2 and 12.3 which relate to the group $E_6^1(q^2)$ one replaces all plus signs by minus signs, then one obtains the corresponding properties of $E_6(q)$. A similar phenomenon occurs for each of the groups $A_l^1(q^2)$ and $D_l^1(q^2)$.

12.4 Lemma. *The Poincaré sequence of a finite Lie group $\hat{G}$ is determined by the abstract group and the characteristic p of the base field K. The type of a finite Lie group is determined by its Poincaré sequence except that $B_l(q)$ and $C_l(q)$ have the same sequence, as do $A_1(q^3)$ and $A_2^1(q)$ also.*

Proof. If $\hat{G}$ is of type G, then, to within an inner automorphism, G and p determine $\mathfrak{U}$ as a p-Sylow subgroup, then $\mathfrak{U}\mathfrak{H}$ as the normalizer of $\mathfrak{U}$, and finally the numbers $|\mathfrak{U} \cap x\mathfrak{U}x^{-1}|$ as x runs through a system of representatives of the double coset decomposition of G relative to $\mathfrak{U}\mathfrak{H}$. These latter numbers are just the terms of the Poincaré sequence by the analogue of 7.10, since $|\mathfrak{U} \cap \omega(w)\mathfrak{U}\omega(w)^{-1}| = q^{n(w_0w)}$ by 4.3. A similar proof of the first statement holds for groups of type G^1 or G^2. One proves the second statement by inspection of the Poincaré sequences for the various Lie groups.

By checking their orders, one sees that $A_1(q^3)$ and $A_2^1(q)$ can not be isomorphic. Thus the two statements of 12.4 can be combined to yield:

12.5. *The type of a finite Lie group is determined by the abstract group and the characteristic of the base field except that $B_l(q)$ and $C_l(q)$ may be isomorphic.*

This result has been obtained previously (for the previously known finite simple Lie groups) by Artin [1] and Dieudonné [5, p. 71–75] by different, more detailed methods. Artin actually draws the conclusion under the weak assumption that only $|\hat{G}|$ and p are known.

One also concludes from 12.4 the well-known fact that $A_2(4)$ and $A_3(2)$, both of order 20160, are not isomorphic.

An inspection of the results of 12.3 yields:

12.6 LEMMA. *Let $\hat{G}$ be either $E_6^1(q^2)$ or $D_4^2(q^3)$ over a field of characteristic p, and let Q be the largest power of p which divides $|\hat{G}|$. Let Q' be any prime power which divides $|\hat{G}|$. Then $Q^3 > |\hat{G}|$ and $Q \geqq Q'$.*

Proof of 12.1. Clearly $\hat{G}$ is not cyclic. Since $|\hat{G}| > 10^8$ and $Q^3 > |\hat{G}|$, it follows that $\hat{G}$ is not an alternating group (see [1]). $D_4^2(8)$ does not have the order of a Mathieu group and all other values of $|\hat{G}|$ are too large. $\hat{G}$ is not isomorphic to either of the groups $A_1(p_1)$ with $p_1 = 2^r - 1 =$ prime, or $A_1(2^s)$ with $2^s + 1 =$ prime, since in each case one has a prime p_2 such that p_2 divides $|\hat{G}|$ and $p_2^3 > |\hat{G}|$, and this is readily seen to be impossible by 12.3. But except for these two types, every simple finite Lie group verifies 12.6 (see [1] where the other groups are considered). Thus any representation of $\hat{G}$ as a Lie group must be over a field of characteristic p. An application of 12.4 completes the proof.

13. Proof of 12.2. By 2.2, 2.3 and 2.6, $n(w) = \sum |S|$, summed over those $S \in \Pi^1$ for which $wS < 0$. By 2.7, one can compute $n(w)$ within the framework of $\tilde{W}^1$ and its root system, but each root is to be counted with the right multiplicity (1, 2 or 3). Assume first that the group under consideration is $E_6^1(q^2)$. Then $\tilde{W}^1$ is of type F_4 and, in terms of coordinates relative to an orthonormal basis, its roots can be taken as $\pm x_i$, $(\pm x_1 \pm x_2 \pm x_3 \pm x_4)/2$, each of multiplicity 1, and $\pm x_i \pm x_j$ $(i \neq j)$, each of multiplicity 2 (see [8, p. 13-08]). The inequalities $x_1 - x_2 - x_3 - x_4 > 0$, $x_2 - x_3 > 0$, $x_3 - x_4 > 0$, and $x_4 > 0$ determine a fundamental region F of $\tilde{W}^1$ by [10, p. 160]. The last 3 inequalities determine a region L whose intersection with the unit sphere is lune-shaped with $(1, 0, 0, 0)$ as one of its vertices. The subgroup V of $\tilde{W}^1$ leaving $(1, 0, 0, 0)$ fixed is of type C_3 and has L as a fundamental region. Let $P(t)$ be the polynomial sought, let $P_1(t)$ be the corresponding polynomial for the group V, and let $P_2(t)$ be $\sum t^{n(w)}$, the sum being over those $w \in W^1$ for which $\tilde{w}F \subset L$. A simple geometric argument shows that $P = P_1P_2$. We next find P_2. The point $a = (16, 8, 4, 2)$ is in F. It has 24 transforms in L corresponding to the 24 elements $\tilde{w} \in \tilde{W}^1$ for which $\tilde{w}F \subset L$. These are a, $b = (15, 5, 3, 9)$, $c = (13, 11, 7, 1)$ and the points in L obtained from these by coordinate permutations. One can now find $n(w)$ for each of the 24 elements above. For example, if w maps a on b, then the roots positive at a and negative at b are $(x_1 - x_2 - x_3 - x_4)/2$, of multiplicity 1, and $x_2 - x_4$ and $x_3 - x_4$, each of multiplicity 2. Hence $n(w) = 5$. Thus P_2 is determined, and the original problem of rank 4 is reduced to one of rank 3. A similar reduction to rank 2 is possible, whence P can be determined. If one starts with $A_l^1(q^2)$ or $D_l^1(q^2)$ instead, the same inductive procedure can be carried through, and for $D_4^2(q^3)$ the polynomial P can be found rather quickly by enumerating $n(w)$ for the 12 elements of W^2. The results are those listed in 12.2.

14. Prime power representations. In [9], 14 assumptions on a finite group are made, and then some properties concerning the representations of the group are deduced. It is then verified that the groups of Chevalley satisfy the basic assumptions. The verification for G^1 or G^2 is virtually the same as for G because of the structure theorems of the present paper. Thus one gains the results of [9] (in particular Theorem 4) simultaneously for all known finite simple Lie groups.

15. Concluding remarks. We first note that it is possible to cover somewhat more ground than was indicated in the main development given here by allowing certain degeneracies to occur. For example, if σ on E is of order 2, if σ on K is of order 1, and if $\mathfrak{g}$ is of type A_{2l} or A_{2l-1}, then the construction of §§ 3, 4 and 5 yields a group of type B_l or C_l, respectively. Thus B_l, C_l and also A_m may be regarded as degenerate cases of A_m^1. Similarly D_l^1 degenerates to B_{l-1} and D_l; E_6^1 to F_4 and E_6; and D_4^2 to G_2, B_3, D_4, D_4^1 and D_4^2. It is easily verified that no other groups can be obtained by the present method of combining automorphisms of E and of K in various ways[1].

In regard to the construction given for G^1, it is to be noted that $\mathfrak{g}_K^1$, the set of fixed points of σ, is the Lie algebra (over K_0) of G^1 in many cases. We could have defined G^1 on $\mathfrak{g}_K^1$ in view of the easily proved facts that an automorphism x of $\mathfrak{g}_K$ commutes with σ if and only if $x\mathfrak{g}_K^1 = \mathfrak{g}_K^1$, and that, in this case, the restriction of x to $\mathfrak{g}_K^1$ is 1 only if $x = 1$; but this would have led to a much more complicated development. It is also to be noted that one can not define G^1 as the subgroup G^σ of G made up of elements which commute with σ. The difference, roughly speaking, lies in $\mathfrak{H}$: a self-conjugate character on P_r may be extendable to a character on P but not to a self-conjugate one, as is proved by the following example. Let $\mathfrak{g}$ be of type A_1, and let w and $a = 2w$ be fundamental weight and root, respectively. Then χ defined by $\chi(a) = k^2$, $k^2 \in K_0^*$, $\bar{k} \neq k$, has the given property. One sees rather easily, however, that G^σ/G^1 is always isomorphic to a subgroup of P/P_r.

The proof of simplicity given in §8 is considerably shorter than the one given in [3], but this is at the expense of the assumption that K has enough elements: left open is the question of simplicity for the groups $E_6^1(q^2)$ with $q \leqq 4$, and $D_4^2(q^3)$ with $q \leqq 3$. The answer quite likely requires rather detailed methods such as those of [3].

More important, perhaps, and probably more difficult is the identification of the infinite groups constructed. An infinite analogue of 12.4 would go a long way in this direction. Finally, it seems likely that there is some sort of description of D_4^2 and D_4^3 by Cayley numbers.

References

1. E. Artin, *Orders of classical simple groups*, Comm. Pure Appl. Math., **8** (1955), 455.
2. É. Cartan, *Oeuvres complètes*, Paris, 1952.
3. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J., (2) **7** (1955), 14.
4. J. Dieudonné, *Sur les groupes classiques*, Paris, 1948.
5. ———, *On the automorphisms of the classical groups*, Mem. Amer. Math. Soc. 2, 1955.
6. D. Hertzig, *On simple algebraic groups*, Short communications, Int. Congress of Math., Edinburgh, 1958.
7. R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392.
8. Séminaire "*Sophus Lie*", Paris, 1954–1955.
9. R. Steinberg, *Prime power representations of finite linear groups* II, Canad. J. Math., **9** (1957), 347.
10. H. Weyl, *The structure and representation of continuous groups*, I.A.S. notes, Princeton, 1934–35.

UNIVERSITY OF CALIFORNIA, LOS ANGELES