AUTOMORPHISMS OF FINITE LINEAR GROUPS

ROBERT STEINBERG

1. Introduction. By the methods used heretofore for the determination of the automorphisms of certain families of linear groups, for example, the (projective) unimodular, orthogonal, symplectic, and unitary groups **(7, 8)**, it has been necessary to consider the various families separately and to give many case-by-case discussions, especially when the underlying vector space has few elements, even though the final results are very much the same for all of the groups. The purpose of this article is to give a completely uniform treatment of this problem for all the known finite simple linear groups (listed in §2 below). Besides the "classical groups" mentioned above, these include the "exceptional groups," considered over the complex field by Cartan and over an arbitrary field by Dickson, Chevalley, Hertzig, and the author **(3, 4, 5, 6, 10, 15)**. The automorphisms of the latter groups are given here for the first time. The unifying principles come from the theory of Lie algebras: each group is a group of automorphisms of a corresponding Lie algebra and this leads to structural properties shared by all of the groups. These centre around the so-called Bruhat decomposition (see **(2)** and 4.8 below), which, in case the underlying field is complex, reduces to the decomposition of the group into double cosets relative to a maximal solvable connected subgroup (see also **(13)** where much use is made of this decomposition). Stated roughly, the final result is that the outer automorphisms of these groups are generated by field automorphisms, graph automorphisms, which come from symmetries of the Schlaefli (or Coxeter) graph of the root structure of the corresponding Lie algebra, and diagonal automorphisms, a prototype of which is an automorphism of the unimodular group produced by conjugation by a (diagonal) matrix of determinant other than 1. Exact statements of these results (3.2 to 3.6 below) follow a description of the groups and automorphisms to be considered.

An introduction to the standard Lie algebra terminology together with statements of the principal results in the classification of the simple Lie algebras over the complex field can be found in **(4**, pp. 15–19**)**. (Proofs are available in **(3**: thesis**)**, **(9)**, **(14)**, or **(16)**.)

2. The groups. Let us start with a Cartan decomposition of a simple Lie algebra over the complex field and denote by Π and Σ respectively the sets of positive and fundamental roots relative to a fixed ordering of the additive group generated by the roots. Then, as in **(4)**, one can replace the complex field by an arbitrary base field K after choosing a generating set $\{X_r, X_{-r},$

Received July 7, 1959.

https://doi.org/10.4153/CJM-1960-054-6 Published online by Cambridge University Press

$H_r, r \in \Pi\}$ to fulfil the conditions of Theorem 1 of **(4)**, and then define: $x_r(k) = \exp(\text{ad}\, kX_r)$; $\mathfrak{X}_r = \{x_r(k), k \in K\}$; $\mathfrak{U}(\mathfrak{V})$ is the group generated by those $\mathfrak{X}_r$ for which r is positive (negative); and finally G (denoted G' in **(4)**) is the group generated by $\mathfrak{U}$ and $\mathfrak{V}$. The various groups G obtained in this way are A_l $(l \geqslant 1)$, B_l $(l \geqslant 2)$, C_l $(l \geqslant 3)$, and D_l $(l \geqslant 4)$, which are identified in **(11)** as suitable (projective) unimodular, orthogonal, symplectic, and orthogonal groups acting on spaces of $l + 1$, $2l + 1$, $2l$ and $2l$ dimensions respectively, as well as the exceptional groups E_6, E_7, E_8, F_4 and G_2. The groups G of this paragraph are called *normal types*.

If the additive group generated by the roots admits an automorphism $r \rightarrow \bar{r}$ of order 2 such that $\bar{\Sigma} = \Sigma$ and if the field K admits an automorphism $k \rightarrow \bar{k}$ of order 2, one can define an automorphism σ of the normal type of group such that $x_a(k)^\sigma = x_{\bar{a}}(\bar{k})$ for all $a \in \Sigma$ or $-\Sigma$, $k \in K$, then restrict each of $\mathfrak{U}$ and $\mathfrak{V}$ to the subgroup of elements invariant under σ, and finally restrict G to the group generated by these restrictions **(15)**. In this way one gets subgroups of A_l $(l \geqslant 2)$, D_l, and E_6 which we denote A_l^1 (unitary group in $l + 1$ dimensions), D_l^1 (a second orthogonal group in $2l$ dimensions), and E_6^1 respectively. Similarly, automorphisms of order 3 yield a second subgroup D_4^2 of D_4. The groups of this paragraph are called *twisted types* and are also denoted generically by G.

3. The automorphisms. Since each of the groups G above is centreless (to be proved in 4.4; actually with 5 exceptions the groups are all simple **(4, 15)**), we can identify G with its group of inner automorphisms.

For each normal type let $\hat{\mathfrak{H}}$ (this is essentially $\mathfrak{H}$ in **(4)**) denote the group of homomorphisms $r \rightarrow h(r)$ of the additive group generated by the roots into K^*, the multiplicative group of K, with multiplication in $\hat{\mathfrak{H}}$ defined by $(h_1h_2)(r) = h_1(r)h_2(r)$, and let $\mathfrak{H}$ (this is $\mathfrak{H}'$ in **(4)**) denote the subgroup consisting of those homomorphisms which can be extended to the group of weights. Each $h \in \hat{\mathfrak{H}}$ leads to an automorphism of the Lie algebra and then to one of G (also denoted h) such that:

3.1 $$x_r(k)^h = x_r(h(r)k) \qquad (r \in \Pi \text{ or } -\Pi, k \in K).$$

If G is a twisted type, then $\hat{\mathfrak{H}}$ is to be restricted to those elements which are self-conjugate in the sense that $h(\bar{r}) = \overline{h(r)}$ and $\mathfrak{H}$ to those which have self-conjugate extensions to the group of weights. The elements of $\hat{\mathfrak{H}}$ considered as acting on G are called *diagonal automorphisms*.

Each group G as a linear group admits *field automorphisms* induced by automorphisms of K (which must be restricted to commute with $k \rightarrow \bar{k}$ in the twisted cases).

Finally, symmetries of the corresponding graph lead to automorphisms of G. If $r \rightarrow \bar{r}$ is an automorphism of the group generated by the roots such that $\bar{\Sigma} = \Sigma$, there exists an automorphism σ of G such that $x_a(k)^\sigma = x_{\bar{a}}(k)$, $a \in \Sigma$ or $-\Sigma$, $k \in K$ (see **(14**, pp. 11–104**)** or **(16**, p. 94**)**). This yields extra automorphisms of A_l ($l \geqslant 2$), D_l and E_6 (5 extra for D_4 and 1 extra for each other group). Also if K is perfect and of characteristic 3 and if G is of type G_2 with fundamental roots a and b such that $2a + 3b$ is also a root, there is an automorphism σ of G such that $x_a(k)^\sigma = x_b(k)$, $x_b(k)^\sigma = x_a(k^3)$, $k \in K$, with similar equations for $-a$ and $-b$. If K is perfect and of characteristic 2 and if G is of type B_2 or F_4, a similar automorphism exists (**13**, Exposés 21 to 24). The automorphisms of this paragraph as well as the identity are called *graph automorphisms.* Note that distinct graph automorphisms effect distinct permutations of the groups $\mathfrak{X}_a$, $a \in \Sigma$.

Our aim is to prove first:

3.2. *If G is one of the groups defined in §2 and if G is finite, each automorphism σ of G can be written $\sigma = gfdi$, with i, d, f, and g being inner, diagonal, field and graph automorphisms respectively. In this representation f and g are uniquely determined by σ.*

Then denoting by $\hat{G}$ (this is G in (**4**)) the group of automorphisms of G generated by $\hat{\mathfrak{H}}$ and G, by $\hat{A}$ the group generated by $\hat{G}$ and the group of field automorphisms F, and by A the group of all automorphisms of G, and assuming that K has q^3, q^2, or q elements in the respective cases that G is of type D_4^2, one of the other twisted types, or a normal type, we show:

3.3. $G \subseteq \hat{G} \subseteq \hat{A} \subseteq A$ *is a normal sequence for* A.

3.4. *$\hat{G}/G$ is isomorphic to $\hat{\mathfrak{H}}/\mathfrak{H}$, hence is Abelian. Thus $\hat{G} = G$ for the groups E_8, F_4, G_2 and D_4^2; $\hat{G}/G$ has order $(l+1,\ q-1)$, $(2, q-1)$, $(2, q-1)$, $(4, q^l - 1)$, $(3, q-1)$, $(2, q-1)$, $(l+1, q+1)$, $(4, q^l + 1)$, or $(3, q+1)$ for the respective group A_l, B_l, C_l, D_l, E_6, E_7, A_l^1, D_l^1 or E_6^1; $\hat{G}/G$ is cyclic with the sole exception: G of type D_l (l even) and q odd.*

3.5. *$\hat{A}/\hat{G}$ is isomorphic to F, hence is cyclic if K is finite.*

3.6. *The graph automorphisms form a system of coset representatives of A over $\hat{A}$. Thus $A = \hat{A}$ with the exceptions: $A/\hat{A}$ has order 2 if G is A_l ($l \geqslant 2$), D_l ($l \geqslant 5$) or E_6, or if G is B_2 or F_4 and K has characteristic 2, or if G is G_2 and K has characteristic 3; $A/\hat{A}$ is isomorphic to the symmetric group on 3 objects if G is D_4.*

An immediate consequence of 3.3 to 3.6 is that each of the above groups which is simple verifies the Schreier conjecture (**12**, p. 303): *if A is the automorphism group of a finite simple non-Abelian group G, then A/G is solvable.*

Before starting the proofs of the above statements, we shall examine the groups under consideration a bit more closely.

4. Structure of the groups. In this section G need not be finite. However, until the last paragraph it is assumed that G is a normal type. Using the notation of §§2 and 3, one has:

4.1. *Each $x \in \mathfrak{U}$ can be written uniquely $x = \Pi x_r$, $x_r \in \mathfrak{X}_r$, the product being over the positive roots in increasing order.*

The proof of 4.1 as well as 4.2, 4.3, 4.5, 4.6, 4.7, 4.8, and 4.9 below can be found in **(4)**.

4.2. *$\mathfrak{H}$ is a subgroup of G, $\mathfrak{U}\mathfrak{H}$ is the normalizer of $\mathfrak{U}$ and $\mathfrak{U}\mathfrak{H} \cap \mathfrak{V} = 1$.*

4.3. *If K is finite and has characteristic p, then $\mathfrak{U}$ is a p-Sylow subgroup of G.*

4.4. *The centre of G is* 1.

Proof. If x is in the centre of G, then $x \in \mathfrak{U}\mathfrak{H}$ by 4.2. Similarly $x \in \mathfrak{V}\mathfrak{H}$, whence $x \in \mathfrak{H} = \mathfrak{U}\mathfrak{H} \cap \mathfrak{V}\mathfrak{H}$ by 4.2. But then 3.1 with $x = h$ yields $h(r) = 1$ for each $r \in \Pi$, whence $x = h = 1$.

Let W denote the Weyl group and w_r the reflection in W corresponding to the root r. One has:

4.5. *For each $w \in W$ there is $\omega(w) \in G$ such that $\omega(w)x_r(k)\omega(w)^{-1} = x_{wr}(\eta k)$, $r \in \Pi$ or $-\Pi$, with $\eta = \pm 1$ depending on w and r but not on k.*

4.6. *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 $\mathfrak{W}/\mathfrak{H}$.*

Next for each $w \in W$ define $\mathfrak{U}_w = \mathfrak{U} \cap \omega(w)^{-1}\mathfrak{V}\omega(w)$, $\mathfrak{U}_w' = \mathfrak{U} \cap \omega(w)^{-1}\mathfrak{U}\omega(w)$ so that $\mathfrak{U}_w$ ($\mathfrak{U}_w'$) is the group generated by those $\mathfrak{X}_r$ for which $r > 0$ and $wr < 0$ ($wr > 0$). Thus if $a \in \Sigma$ and $w = w_a$ one has $\mathfrak{U}_w = \mathfrak{X}_a$.

4.7. $\mathfrak{U} = \mathfrak{U}_w\mathfrak{U}_w' = \mathfrak{U}_w'\mathfrak{U}_w$.

4.8. *The sets $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}_w$, $w \in W$, are the distinct double cosets of G relative to $\mathfrak{U}\mathfrak{H}$, and each element of G has a unique expression of the indicated form.*

Analogous results hold with $\mathfrak{U}$ replaced by $\mathfrak{V}$.

4.9. *For each $r \in \Pi$ there is a homomorphism ϕ of $SL_2(K)$, the unimodular group, onto G_r, the group generated by $\mathfrak{X}_r$ and $\mathfrak{X}_{-r}$ such that*

$$\phi\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = x_r(k),$$

$$\phi\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = x_{-r}(k),$$

$$\phi\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv \omega(w_r) \bmod \mathfrak{H},$$

and $\phi^{-1}(\mathfrak{H} \cap G_r)$ consists of the diagonal matrices. The kernel of ϕ is contained in the centre of $SL_2(K)$.

We may (and do) normalize so that

$$\phi\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \omega(w_a)$$

for each $a \in \Sigma$ and then define each $\omega(w)$ to be a product of elements $\omega(w_a)$, $a \in \Sigma$. Then 4.9 implies:

4.10. *For each $a \in \Sigma$ the equation $x_a(1)x_a(k)x_a(1) = x_{-a}(k)x_a(1)x_{-a}(k)$ holds only if $k = -1$ and then both sides are equal to $\omega(w_a)$. Given $k, l \in K^*$, $a \in \Sigma$, then $x_a(k)x_{-a}(l)x_a(m)x_{-a}(t)$ is in $\mathfrak{H}\omega(w_a)$ only if $m = -l^{-1}$ and $t = l + kl^2$.*

4.11. *If $w = w_a$, $a \in \Sigma$, then* (1) *$T =$ union $\mathfrak{V}\mathfrak{H}$, $\mathfrak{V}\mathfrak{H}\omega(w)\mathfrak{V}_w$ is a group and* (2) *$T \cap \mathfrak{U} = \mathfrak{U}_w$.*

Proof. By 4.8, T is closed under right (or left) multiplication by $\mathfrak{V}\mathfrak{H}$. A consequence of 4.9 (see **(4**, p. 34, Lemma 2**)**) is $\omega(w)\mathfrak{V}_w\omega(w)^{-1} \subseteq$ union $\mathfrak{V}_w\mathfrak{H}$, $\mathfrak{V}_w\mathfrak{H}\omega(w)\mathfrak{V}_w$. Thus $T\omega(w)^{-1} \subseteq T$, hence $TT^{-1} \subseteq T$, and T is a group. Next write $\mathfrak{V} = \mathfrak{V}_w\mathfrak{V}_w'$. Then $\omega(w)\mathfrak{V}_w\omega(w)^{-1} = \mathfrak{U}_w$ and $\omega(w)\mathfrak{V}_w'\omega(w)^{-1} = \mathfrak{V}_w'$ by 4.5 so that $T = \omega(w)T\omega(w)^{-1} =$ union $\mathfrak{U}_w\mathfrak{V}_w'\mathfrak{H}$, $\mathfrak{U}_w\mathfrak{V}_w'\mathfrak{H}\omega(w)\mathfrak{U}_w$. Now $\mathfrak{U}_w\mathfrak{V}_w'\mathfrak{H} \cap \mathfrak{U} = \mathfrak{U}_w$ by 4.2; and if $w_0 \in W$ is defined by $w_0\Pi = -\Pi$, then $\mathfrak{U}\mathfrak{H}\omega(w_0w) \cap \omega(w_0)\mathfrak{U} = 0$ by 4.8, when left multiplication by $\omega(w_0)^{-1}$ yields $\mathfrak{V}\mathfrak{H}\omega(w) \cap \mathfrak{U} = 0$ and then $\mathfrak{U}_w\mathfrak{V}_w'\mathfrak{H}\omega(w)\mathfrak{U}_w \cap \mathfrak{U} = 0$. Thus $T \cap \mathfrak{U} = \mathfrak{U}_w$.

4.12. *Among the double cosets $\mathfrak{V}\mathfrak{H}\omega(w)\mathfrak{V}_w$ for which $w \neq 1$ and* (1) *of* 4.11 *holds, those for which w has the form $w = w_a$, $a \in \Sigma$, are characterized by the fact that $T \cap \mathfrak{U}$ is minimal.*

Proof. If w does not have the form $w = w_a$, $a \in \Sigma$, then $T \supseteq \omega(w)\mathfrak{V}_w\omega(w)^{-1} = \mathfrak{U}_{w^{-1}} \supset \mathfrak{X}_b$ for some $b \in \Sigma$, the last inclusion being proper; thus $T \cap \mathfrak{U}$ is not minimal by 4.11. If $a, b \in \Sigma, a \neq b$, then $\mathfrak{X}_a \not\supseteq \mathfrak{X}_b$; hence $T \cap \mathfrak{U}$ with $w = w_a$, $a \in \Sigma$, is minimal by 4.11.

Because of the results of **(15)**, the twisted types of groups have corresponding properties whose proofs are entirely analogous to those given above and in **(4)**.

5. Proof of 3.2 for the normal types. Throughout this section and the next assume that G is a normal type. The method of proof is as follows: we start with an arbitrary automorphism σ of G and multiply in turn by an inner, a diagonal, a graph and a field automorphism, referring at each stage to a normalization of σ; the final normalization yields $\sigma = 1$, whence 3.2 soon follows. Only in the first step is the finiteness of K used. Hence the rest of the argument is phrased so as to be applicable even if K is infinite.

5.1. *If K is finite, the automorphism σ can be normalized by an inner automorphism of G so that $\mathfrak{U}^\sigma = \mathfrak{U}$ and $\mathfrak{V}^\sigma = \mathfrak{V}$. If this is done, then $\mathfrak{H}^\sigma = \mathfrak{H}$ and there is a permutation ρ of the fundamental roots such that $\mathfrak{X}_a{}^\sigma = \mathfrak{X}_{\rho a}$ and $\mathfrak{X}_{-a}{}^\sigma = \mathfrak{X}_{-\rho a}$ for each fundamental root a.*

Proof. By 4.3, $\mathfrak{U}$, $\mathfrak{V}$, $\mathfrak{U}^\sigma$, and $\mathfrak{V}^\sigma$ are all p-Sylow subgroups of G, hence are conjugate. Thus one can normalize σ by an inner automorphism to fulfil $\mathfrak{U}^\sigma = \mathfrak{U}$. Now $\mathfrak{V}^\sigma = x^{-1}\mathfrak{U}x$ for some x in G; Thus $\mathfrak{V}^\sigma = u^{-1}\omega(w)^{-1}\mathfrak{U}\omega(w)u$

https://doi.org/10.4153/CJM-1960-054-6 Published online by Cambridge University Press

with $u \in \mathfrak{U}$, $w \in W$, by 4.8 and 4.2. Since $\mathfrak{V} \cap \mathfrak{U} = 1$ by 4.2, one has $\mathfrak{V}^\sigma \cap \mathfrak{U} = 1$, whence $w = w_0$ (defined by $w_0\Pi = -\Pi$) by 4.5, and then $\mathfrak{V}^\sigma = u^{-1}\mathfrak{V}u$ by 4.5. A second normalization, the inner automorphism effected by u, now yields $\mathfrak{V}^\sigma = \mathfrak{V}$. Then $\mathfrak{U}\mathfrak{H}$ and $\mathfrak{V}\mathfrak{H}$ are invariant under σ by 4.2, and so is $\mathfrak{H}$, since $\mathfrak{H} = \mathfrak{U}\mathfrak{H} \cap \mathfrak{V}\mathfrak{H}$ by 4.2. The double cosets of G relative to $\mathfrak{V}\mathfrak{H}$ ($\mathfrak{U}\mathfrak{H}$) are thus permuted by σ, and by 4.12 there exists a permutation ρ (a permutation τ) of the fundamental roots (of their negatives) such that $\mathfrak{X}_a{}^\sigma = \mathfrak{X}_{\rho a}$ and $\mathfrak{X}_{-a}{}^\sigma = \mathfrak{X}_{\tau(-a)}$ for each $a \in \Sigma$. If b and c are in Σ and $b \neq c$, then $b+(-c)$ is not a root, hence $X_bX_{-c} = 0$ (in the Lie algebra) and $\mathfrak{X}_b$ commutes with $\mathfrak{X}_{-c}$; if $b = c$, then $\mathfrak{X}_b$ does not commute with $\mathfrak{X}_{-c}$ by 4.9. Setting $b = \rho a$, $c = -\tau(-a)$, one concludes $\rho a = -\tau(-a)$. Thus 5.1 is proved.

5.2. *The normalization of σ attained in* 5.1 *can be refined by application of a diagonal automorphism of G so that in addition $x_a(1)^\sigma = x_{\rho a}(1)$ for each fundamental root a. It is then true that $x_{-a}(1)^\sigma = x_{-\rho a}(1)$, $\omega(w_a)^\sigma = \omega(w_{\rho a})$, and the orders of w_aw_b and $w_{\rho a}w_{\rho b}$ are equal for any fundamental roots a and b.*

Proof. Let $x_a(1)^\sigma = x_{\rho a}(k_a)$, $a \in \Sigma$. Then there exists a homomorphism h of the additive group generated by the roots into K^* such that $h(a) = k_a{}^{-1}$, $a \in \Sigma$. Application of the corresponding diagonal automorphism now yields the refinement $x_a(1)^\sigma = x_{\rho a}(1)$, $a \in \Sigma$, by 3.1. Applying σ to the first equation of 4.10, one then gets $x_{-a}(-1)^\sigma = x_{-\rho a}(-1)$ (so that $x_{-a}(1)^\sigma = x_{-\rho a}(1)$) and $\omega(w_a)^\sigma = \omega(w_{\rho a})$ for each $a \in \Sigma$. Lastly, the orders of w_aw_b and $w_{\rho a}w_{\rho b}$ are respectively equal to the orders of $\omega(w_a)\omega(w_b)$ and $\omega(w_{\rho a})\omega(w_{\rho b})$ mod $\mathfrak{H}$ by 4.6, hence are equal to each other because σ is an automorphism.

The last conclusion can be interpreted geometrically. If the order of w_aw_b is n, then the angle between a and b is $\pi - \pi/n$. Thus ρ effects an angle preserving permutation of the fundamental roots, hence is the identity unless the corresponding graph has extra "angular" symmetries (see (**3**, p. 18)).

5.3. *The normalization of σ in* 5.2 *can be refined by application of a graph automorphism of G so that ρ is the identity.*

Proof. Suppose first that G is of type F_4 or B_2 and that ρ is not the identity. Then there are a, $b \in \Sigma$ such that $a + b$ and $a + 2b$ are roots, $\rho a = b$ and $\rho b = a$, by the remarks above. Let α and β be the maps of K defined by $x_a(k)^\sigma = x_b(k^\alpha)$ and $x_b(l)^\sigma = x_a(l^\beta)$. One has $x_{a+b}(l) = \omega(w_a)x_b(l)\omega(w_a)^{-1}$ and $x_{a+2b}(k) = \omega(w_b)x_a(k)\omega(w_b)^{-1}$ by 4.5 (in which the normalization $\eta = 1$ is achieved by replacing X_{a+b} or X_{a+2b} by its negative if necessary). Applying σ to these equations, one gets $x_{a+b}(l)^\sigma = x_{a+2b}(l^\beta)$ and $x_{a+2b}(k)^\sigma = x_{a+b}(k^\alpha)$. Consider the commutator equation

5.4. $$(x_a(k), x_b(l)) = x_{a+b}(\delta kl)x_{a+2b}(\epsilon kl^2),$$

with each of δ and ϵ equal to ± 1 and independent of k and l by (**4**, p. 27, ll. 22–26). Apply σ to 5.4:

5.5. $$(x_b(k^\alpha), x_a(l^\beta)) = x_{a+2b}((\delta kl)^\beta)x_{a+b}((\epsilon kl^2)^\alpha).$$

https://doi.org/10.4153/CJM-1960-054-6 Published online by Cambridge University Press

Now let us replace k and l by l^β and k^α respectively in 5.4 and take inverses:

5.6. $$(x_b(k^\alpha), x_a(l^\beta)) = x_{a+2b}(-\epsilon l^\beta(k^\alpha)^2)x_{a+b}(-\delta l^\beta k^\alpha).$$

Comparing the $\mathfrak{X}_{a+2b}$ components of 5.5 and 5.6 with $l = 1$, one gets $\delta k^\beta = -\epsilon(k^\alpha)^2$ by 4.1 and 5.2. Setting first $k = 1$ and then $k = -1$, one gets $\delta = -\epsilon$ and $-\delta = -\epsilon$, whence $\delta + \delta = 0$, so that K is of characteristic 2. Then since β is onto, $k^\beta = (k^\alpha)^2$ implies that K is perfect. Hence (see the paragraph preceding 3.2) there exists a graph automorphism which normalizes σ so that $\rho a = a$ and $\rho b = b$. As is easily seen, ρ is now the identity. If G is of type G_2, one proceeds similarly and finds that a normalization is not required unless K is perfect and of characteristic 3. If G is of type A_l, D_l, or E_6 and K is arbitrary, then again there is a graph automorphism to normalize ρ to the identity. In all other cases, due to the lack of "angular" symmetry of the graph, ρ is already the identity. Thus 5.3 is proved.

5.7. *The normalization of σ in 5.3 can be refined to $\sigma = 1$ by application of a field automorphism of G.*

That is, if σ satisfies $\mathfrak{U}^\sigma = \mathfrak{U}$, $\mathfrak{V}^\sigma = \mathfrak{V}$, and $x_a(1)^\sigma = x_a(1)$ for each $a \in \Sigma$, then σ is a field automorphism.

Proof. Choose $a \in \Sigma$ and define α by $x_a(k)^\sigma = x_a(k^\alpha)$. We first show that α is an automorphism of K by the method of Schreier and van der Waerden (**12**, p. 318). By 5.2 we know that α maps K onto K and that $1^\alpha = 1$. The equation $x_a(k+l) = x_a(k)x_a(l)$ implies that $(k+l)^\alpha = k^\alpha + l^\alpha$. The equation 4.5 with $r = a$ and $w = w_a$ yields $x_{-a}(k)^\sigma = x_{-a}(k^\alpha)$, and then the second part of 4.10 implies $(l + kl^2)^\alpha = l^\alpha + k^\alpha(l^\alpha)^2$, whence $(kl^2)^\alpha = k^\alpha(l^\alpha)^2$ and $(l^2)^\alpha = (l^\alpha)^2$. If K is of characteristic 2, then $((kl)^\alpha)^2 = ((kl)^2)^\alpha = (k^2l^2)^\alpha = (k^2)^\alpha(l^\alpha)^2 = (k^\alpha)^2(l^\alpha)^2 = (k^\alpha l^\alpha)^2$, whence $(kl)^\alpha = k^\alpha l^\alpha$; if K is of characteristic other than 2, then polarization of the equation $(l^2)^\alpha = (l^\alpha)^2$ yields $(kl)^\alpha = k^\alpha l^\alpha$. Thus in either case α is an automorphism of K. Now choose a second root $b \in \Sigma$ (if one exists) such that $a + b$ is a root, and let β be the corresponding automorphism of K. By labelling appropriately a and b one may assume that $\omega(w_a)\mathfrak{X}_b\omega(w_a)^{-1} = \mathfrak{X}_{a+b}$. Then applying σ to the equation $(x_a(k), x_b(1)) = x_{a+b}(\delta k)\ldots$ as in 5.3 (but now with ρ the identity), one gets $k^\beta = k^\alpha$, whence $\alpha = \beta$. Since any 2 roots of Σ are the end terms of a sequence of roots of Σ such that the sum of each consecutive pair is a root (in other words, the graph is connected), it follows that there is a single automorphism γ of K such that $x_c(k)^\sigma = x_c(k^\gamma)$ for each c in Σ. Normalization of σ by the field automorphism of G corresponding to γ^{-1} now yields $x_c(k)^\sigma = x_c(k)$, $c \in \Sigma$. One has also $\omega(w_c)^\sigma = \omega(w_c)$, $c \in \Sigma$, by 5.3. However, since W is generated by the elements w_c, $c \in \Sigma$, and each root has the form wc with $w \in W$, $c \in \Sigma$, it follows from 4.5 that G is generated by the elements $x_c(k)$ and $\omega(w_c)$ with $k \in K$, $c \in \Sigma$. Hence $\sigma = 1$, and 5.7 is proved.

Let us now prove 3.2. Let σ be an automorphism of G and let i, d, g, and f' be the respective inner, diagonal, graph, and field automorphisms used in

https://doi.org/10.4153/CJM-1960-054-6 Published online by Cambridge University Press

5.1, 5.2, 5.3, and 5.7 to achieve the normalization of σ^{-1}. One has $f'gdi\sigma^{-1} = 1$, thus $\sigma = f'gdi$. Since $g^{-1}f'g = f$ is in F by 5.7, one gets $\sigma = gfdi$, and the first statement of 3.2 is proved. Now suppose $\sigma = g_1f_1d_1i_1$ is a second representation of σ in the indicated form. Then $d^{-1}f^{-1}g^{-1}g_1f_1d_1 = ii_1^{-1}$. The left side of this equation maps $\mathfrak{U}$ onto $\mathfrak{U}$ and $\mathfrak{V}$ onto $\mathfrak{V}$. Hence $ii_1^{-1} \in \mathfrak{U}\mathfrak{H} \cap \mathfrak{V}\mathfrak{H} = \mathfrak{H}$ by 4.2. Then $f^{-1}g^{-1}g_1f_1 = dii_1^{-1}d_1^{-1} \in \mathfrak{H}$. This element leaves fixed each $x_a(1)$, $a \in \Sigma$, hence $dii_1^{-1}d_1^{-1} = 1$ by 3.1; that is, $g^{-1}g_1 = ff_1^{-1}$. This implies that g and g_1 effect the same permutation of the groups $\mathfrak{X}_a$, $a \in \Sigma$. Hence $g = g_1$, then $f = f_1$, and 3.2 is proved completely.

6. Proof of 3.3 to 3.6 for the normal types. The group G of inner automorphisms is clearly a normal subgroup of each of $\hat{G}$, $\hat{A}$, and A. This implies $\hat{G} = \hat{\mathfrak{H}}G$. One has also $\hat{\mathfrak{H}} \cap G = \mathfrak{H}$ since $\mathfrak{H} \subseteq \hat{\mathfrak{H}} \cap G$ by 4.2, whereas $h \in \hat{\mathfrak{H}} \cap \mathfrak{G}$ implies $\mathfrak{U}^h = \mathfrak{U}$, $\mathfrak{V}^h = \mathfrak{V}$ and then $h \in \mathfrak{U}\mathfrak{H} \cap \mathfrak{V}\mathfrak{H} = \mathfrak{H}$ by 4.2. Thus $\hat{G}/G \cong \hat{\mathfrak{H}}/(\hat{\mathfrak{H}} \cap G) = \hat{\mathfrak{H}}/\mathfrak{H}$. The specific results of 3.4 can now be verified from the fact that the Cartan integers $2(a, b)/(a, a)$ $(a, b \in \Sigma)$, taken mod $(q - 1)$, build a relation matrix for $\hat{\mathfrak{H}}/\mathfrak{H}$ **(4**, p. 48, ll. 13–18**)**. It is easily verified (from the definitions) that $f\hat{\mathfrak{H}}f^{-1} = \hat{\mathfrak{H}}$ for each f in F. Hence $\hat{G}$ is normal in $\hat{A}$ and $\hat{A} = F\hat{\mathfrak{H}}G$, whence the uniqueness feature of 3.2 implies 3.5. Finally, if g is a graph automorphism, one verifies (by considering the effect on each $x_a(k)$) that $gFg^{-1} = F$ and $g\hat{\mathfrak{H}}g^{-1} = \hat{\mathfrak{H}}$, whence $\hat{A}$ is normal in A, and 3.3 is completely proved. The uniqueness feature of 3.2 then implies the first statement of 3.6; the last statement follows from the definition of graph automorphism given in the paragraph before 3.2.

7. The twisted types. The proofs of 3.2 to 3.6 for the twisted types are virtually the same as those given above for the normal types and to a large extent involve little more than a change of notation in view of the structural properties developed for the twisted types in **(15)**. A comparison of 4.1 and 5.4 with their analogues 4.5 and 8.8 in **(15)** should make completely clear what modifications are to be made, if G is not A_l^1 (l even), and even in the latter case if $l \geqslant 4$. This leaves the group A_2^1 to be considered. Although the proofs in this case are also of the same genre as those given above for the normal types, the details are sufficiently more complicated to warrant a separate exposition, especially since the case in which K has few elements has not been completely treated elsewhere.

Let us recall that A_2^1 is a subgroup of A_2 and may be identified with a 3-dimensional projective unimodular unitary group **(15)**. The positive roots of A_2 can be written as a, $\bar{a}$, and b (with $b = a + \bar{a}$), and then the elements of $\mathfrak{U}$ take the form $x_a(k)x_{\bar{a}}(\bar{k})x_b(l)$, subject to $k\bar{k} = l + \bar{l}$ **(15**, Lemma 4.6**)**. For given k this last equation is always solvable for l: choose m so that $m + \bar{m} \neq 0$, and then set $l = k\bar{k}m(m + \bar{m})^{-1}$. For convenience, we denote $x_a(k)x_{\bar{a}}(\bar{k})x_b(l)$ by $(k|l)$, so that the rule of multiplication is $(k|l)(m|n) = (k + m|l + n + \bar{k}m)$ (see **(4**, p. 27, ll. 22–26**)** or use the unitary identification). From this it follows that the elements $(0|t)$, subject to $t + \bar{t} = 0$, build the centre $\mathfrak{C}$ of $\mathfrak{U}$. Let us now turn to the proof of 3.2.

If σ is an automorphism of G, it can be normalized by an inner automorphism, just as before, so that $\mathfrak{U}^\sigma = \mathfrak{U}$ and $\mathfrak{V}^\sigma = \mathfrak{V}$; assume this is done. Then $\mathfrak{C}^\sigma = \mathfrak{C}$, and since $(k|l_1)^{-1}(k|l_2) \in \mathfrak{C}$, the map α defined by $(k|l)^\sigma = (k^\alpha|m)$ is single-valued; clearly α is also onto.

The normalization of σ can now be refined by application of a diagonal automorphism of G so that $1^\alpha = 1$, and the next thing to be proved is that α becomes an automorphism of K. If K has 4 elements, then α leaves fixed 0 and 1 and permutes the other 2 elements of K, hence is an automorphism. Thus in the rest of the proof we may assume that K has more than 4 elements. Because σ is an automorphism we have $(k + l)^\alpha = k^\alpha + l^\alpha$; k, $l \in K$. Next if $h \in \mathfrak{H}$ and $h(a) = k$, we have $h(l|*)h^{-1} = (kl|*)$, whence $h^\alpha(l^\sigma|*)(h^\sigma)^{-1} = ((kl)^\alpha|*)$. Setting $l = 1$, we get $h^\sigma(a) = k^\alpha$, and then from the equation, $(kl)^\alpha = k^\alpha l^\alpha$. Here l is arbitrary, but k is restricted to the set S of numbers of the form $m^2\bar{m}^{-1}$ (see the definition of $\mathfrak{H}$ in §3). The field K_0 of numbers left fixed by $k \to \bar{k}$ is contained in S, and this inclusion is proper: if K is of characteristic 3 and $m \notin K_0$, then $m^2\bar{m}^{-1} \notin K_0$; if K is of characteristic other than 3 and $k \notin K_0$, $r \in K_0$, $r \neq 0, 1$, then not all three of $m_1 = k$, $m_2 = 1 + k$, $m_3 = r + k$ can have cubes in K_0 because, in the contrary case, differencing yields $k + k^2$, $rk + k^2 \in K_0$ and then $k \in K_0$, a contradiction, and so $m_i^2\bar{m}_i^{-1} \notin K_0$ for some $i = 1, 2$, or 3. There is thus $k \in S$ such that $k \notin K_0$, and each element of K can be written as $rk + s$ $(r, s \in K_0)$, that is, as the sum of 2 elements of S. Since α is additive on K and multiplicative on S, this implies that α is multiplicative on all of K and hence is an automorphism.

Thus the normalization of σ can be refined by a field automorphism of G so that α is the identity, and what remains to be shown is that now $\sigma = 1$. Choose $k \notin K_0$, and set $j = k - \bar{k}$. Then σ applied to $((1|*), (k|*)) = (0|k - \bar{k}) = (0|j)$ yields $(0|j)^\sigma = (0|j)$, that is, σ leaves fixed $x_b(j)$. A slight extension of the first statement in 4.10 shows that $x_{-b}(-j^{-1})$ and $x_b(j)x_{-b}(-j^{-1})x_b(j)$ are also left fixed by σ, and that the latter element is in $\omega(w)\mathfrak{H}$ and so may be denoted $\omega(w)$ after a normalization. A final calculation shows that for given $(k|l)$, $l \neq 0$, one has $(k|l)\omega(w)(m|n) \in \mathfrak{V}\mathfrak{H}$ if and only if $m = \bar{j}k\bar{l}^{-1}$ and $n = j\bar{j}\bar{l}^{-1}$. If this condition is met, if $(k|l)^\sigma = (k|l_1)$ and if $(m|n)^\sigma = (m|n_1)$, then application of σ yields $m = \bar{j}k\bar{l}_1^{-1}$, whence $l_1 = l$ and $(k|l)^\sigma = (k|l)$. Thus $\sigma = 1$ on $\mathfrak{U}$. Since $\omega(w)^\sigma = \omega(w)$ and $\omega(w)\mathfrak{U}\omega(w)^{-1} = \mathfrak{V}$, we get $\sigma = 1$. The first statement of 3.2 is hereby proved, and the other statement as well as 3.3 to 3.6 follow from it, just as before.

8. Final observations. As we have already stated, the finiteness of K is used above only in the proof that an automorphism of G necessarily maps $\mathfrak{U}$ onto one of its conjugates. If K is algebraically closed, this fact is proved in **(13)** by rather advanced methods of topology and algebraic geometry. It is hoped that an elementary proof, along the lines of the present article, can be found to handle all fields K simultaneously. In regard to **(13)**, we also mention that the proof of existence of graph automorphisms for B_2, F_4, and G_2 is quite long and that a shortened self-contained treatment is desirable.

An interesting special case of such an automorphism occurs when G is $B_2(2)$, the group of type B_2 over a field K of 2 elements. This group is isomorphic to S_6, the only symmetric group which admits outer automorphisms: one of these shows up as a graph automorphism which owes its existence to the fact that K has characteristic 2. It is also interesting to compare the groups $A_2(4)$ and $A_3(2)$. For the first the order of A/G is 12 and for the second it is 2. Thus one has another proof of the well-known fact that these groups, both of order 20160, are not isomorphic.

Finally let us remark that a companion problem to that treated here, namely the determination of the isomorphisms among the various finite groups of §2 is handled in **(1)** by uniform number-theoretic methods. In this connection we also refer the reader to 12.5 of **(15)** which can be used to eliminate some of the computations of **(1)**.

References

1. E. Artin, *Orders of classical simple groups*, Comm. Pure Appl. Math., *8* (1955), 455.

2. F. Bruhat, *Représentations induites des groupes de Lie semi-simples connexes*, C. R. Acad. Sci. Paris, *238* (1954), 437.

3. E. Cartan, *Oeuvres complètes* (Paris, 1952).

4. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J., *7* (1955), 14.

5. L. E. Dickson, *Linear groups* (Leipzig, 1901).

6. ——— *A new system of simple groups*, Math. Ann., *60* (1905), 137.

7. J. Dieudonné, *On the automorphisms of the classical groups*, Mem. Amer. Math. Soc., *2* (1951).

8. ——— *La géométrie des groupes classiques*, Ergeb. der Math. u. i. Grenz. (1955).

9. E. B. Dynkin, *The structure of semi-simple algebras*, Amer. Math. Soc. Translation No. 17.

10. D. Hertzig, *On simple algebraic groups*, Short communications, Int. Congress of Math. (Edinburgh, 1958).

11. R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc., *84* (1957), 392.

12. O. Schreier and B. L. van der Waerden, *Die Automorphismen der projektiven Gruppen*, Abh. Math. Sem. Univ. Hamburg, *6* (1928), 303.

13. Séminaire C. Chevalley, *Classification des Groupes de Lie Algébriques* (Paris, 1956–8).

14. Séminaire "Sophus Lie" (Paris, 1954–1955).

15. R. Steinberg, *Variations on a theme of Chevalley*, Pac. J. Math., *9* (1959), 875.

16. H. Weyl, *The structure and representations of continuous groups*, I. A. S. notes (Princeton, 1934–1935).

University of California, Los Angeles