(12) Proof of Theorem 26. We write (11) as $(t^N - (-1)^{|\Pi|})/P(t) = \sum_{\pi \subsetneq \Pi} (-1)^{\pi}/P_{\pi}(t)$ and (4) as $(t^N - (-1)^{|\Pi|})/W(t) = \sum_{\pi \subsetneq \Pi} (-1)^{\pi}/W_{\pi}(t)$. Then, by induction on $|\Pi|$, $W(t) = P(t)$.

Remark: Step (7), the geometric step, represents the only simplification of Solomon's original proof.

§10. Isomorphisms and automorphisms. In this section we discuss the isomorphisms and automorphisms of Chevalley groups over perfect fields. This assumption of perfectness is not strictly necessary but it simplifies the discussion in one or two places. We begin by proving the existence of certain automorphisms related to the existence of symmetries of the underlying root systems.

Lemma 55: Let Σ be an abstract indecomposable root system with not all roots of one length. Let $\Sigma^* = \{\alpha^* = 2\alpha/(\alpha,\alpha) | \alpha \in \Sigma\}$ be the abstract system obtained by inversion. Then:

(a) Σ^* is a root system.

(b) Under the map $*$ long roots are mapped onto short roots and vice versa. Further, angles and simple systems of roots are preserved.

(c) If $p = (\alpha_o,\alpha_o)/(\beta_o,\beta_o)$ with α_o long, β_o short then the map $\alpha \longrightarrow \begin{cases} p\alpha^* & \text{if } \alpha \text{ is long,} \\ \alpha^* & \text{if } \alpha \text{ is short,} \end{cases}$

extends to a homothety.

Proof: (a) holds since $\langle\alpha^*,\beta^*\rangle = \langle\beta,\alpha\rangle$. (b) and (c) are clear.

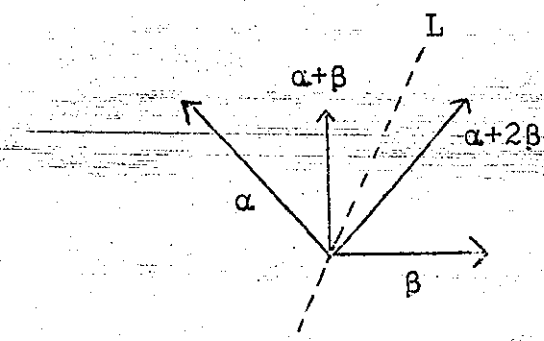
The root system Σ^* obtained in this way from Σ is called the root system dual to Σ.

Exercise: Let $\alpha = \Sigma n_i\alpha_i$ be a root expressed in terms of the simple ones. Prove that α is long if and only if $p|n_i$ whenever α_i is short.

Examples: (a) For $n \geq 3$, B_n and C_n are dual to each other.

B_2 and F_4 are in duality with themselves (with $p = 2$) as is G_2 (with $p = 3$).

(b) Let $\alpha, \beta, \alpha + \beta, \alpha + 2\beta$ be the positive roots for Σ of type B_2. Then those for Σ^* are $\alpha^*, \beta^*, (\alpha + \beta)^* = 2\alpha^* + \beta^*$, and $(\alpha + 2\beta)^* = \alpha^* + \beta^*$. If we identify α^* with β and β^* with α we get a map of B_2 onto itself. $\alpha \longrightarrow \beta$, $\beta \longrightarrow \alpha$, $\alpha + \beta \longrightarrow \alpha + 2\beta$, $\alpha + 2\beta \longrightarrow \alpha + \beta$. This is the map given by reflecting in the line L in the diagram below (L is the bisector of $\angle(\alpha,\beta)$) and adjusting lengths.



Theorem 28: Let Σ, Σ^* and p be as above, k a field of characteristic p (p is either 2 or 3), G, G^* universal Chevalley groups constructed from (Σ,k) and (Σ^*,k) respectively. Then there exists a homomorphism φ of G into G^* and signs ε_α for all $\alpha \in \Sigma$ such that $\varphi(x_\alpha(t)) = \begin{cases} x_\alpha^*(\varepsilon_\alpha t) & \text{if } \alpha \text{ is long,} \\ x_\alpha^*(\varepsilon_\alpha t^p) & \text{if } \alpha \text{ is short.} \end{cases}$

If k is perfect then φ is an isomorphism of abstract groups.

Examples: (a) If k is perfect of characteristic 2 then Spin_{2n+1}, SO_{2n+1} (split forms), and Sp_{2n} are isomorphic.

(b) Consider C_2, $p = 2$, $\varepsilon_\alpha = 1$. The theorem asserts that on U we have an endomorphism (as before we identify Σ and Σ^*) such that (1) $\varphi(x_\alpha(t)) = x_\beta(t)$, $\varphi(x_\beta(t)) = x_\alpha(t^2)$, $\varphi(x_{\alpha+\beta}(t)) = x_{\alpha+2\beta}(t^2)$, $\varphi(x_{\alpha+2\beta}(t)) = x_{\alpha+\beta}(t)$. The only non-trivial relation of type (B) on U is (2) $(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(tu)x_{\alpha+2\beta}(tu^2)$ by Lemma 33. Applying φ to (2) gives

(3) $(x_\beta(t), x_\alpha(u^2)) = x_{\alpha+2\beta}(t^2u^2)x_{\alpha+\beta}(tu^2)$.

This is valid, since it can be obtained from (2) by taking inverses and replacing t by u^2, u by t.

(c) The map φ in (b) is outer, for if we represent G as Sp_4 and if $t \neq 0$, $x_\alpha(t) - 1$ has rank 1 while $x_\beta(t) - 1$ has rank 2.

(d) If in (b) $|k| = 2$, φ leads to an outer automorphism of S_6 since, in fact, $Sp_4(2) \cong S_6$. To see this represent S_6 as the Weyl group of type A_5. This fixes a bilinear form with matrix

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

relative to a basis of simple roots. This is so because, up to multiplication by a scalar, the form is just $\Sigma\, x_i x_j(\alpha_i, \alpha_j) = |\Sigma\, x_i\alpha_i|^2$. Reduce mod 2. The line through $\alpha_1 + \alpha_3 + \alpha_5$ becomes invariant and the form becomes skew and nondegenerate on the quotient space. Hence we have a homomorphism $\psi : S_6 \longrightarrow Sp_4(2)$. It is easily

seen that $\ker \Psi \not\supseteq a_6$ so $\ker \Psi = 1$. Since $|S_6| = 6! = 720 = 2^4(2^2 - 1)(2^4 - 1) = |Sp_4(2)|$, Ψ is an isomorphism.

Ψ^{-1} may be described as follows. $Sp_4(2)$ acts on the underlying projective space P^3 which contains 15 points. Given a point p there are 8 points not orthogonal to p. These split into two four point sets S_1, S_2 such that each of $\{p\} \cup S_1$ and $\{p\} \cup S_2$ consists of mutually nonorthogonal points and these are the only five element sets containing p with this property. There are $15 \cdot 2/5 = 6$ such 5 element sets. $Sp_4(2)$ acts faithfully by permutation on these 6 sets, so $Sp_4(2) \longrightarrow S_6$ is defined. Under the outer automorphism the stabilizers of points and lines are interchanged. Each of the above five point sets corresponds to a set of five mutually skew isotropic lines.

Proof of Theorem 28: If $p = 2$ each $\varepsilon_\alpha = 1$. We must show that φ as defined on the $x_\alpha(t)$ by the given equations preserves (A), (B), and (C). Here (A) and (C) follow at once. The nontrivial relations in (B) are:

$$(x_\alpha(t), x_\beta(u)) = \begin{cases} x_{\alpha+\beta}(\pm tu) & \text{if } |\alpha| = |\beta| \text{ and } \langle(\alpha,\beta) = 120^\circ, \\ x_{\alpha+\beta}(\pm 2tu) & \text{if } \alpha,\beta \text{ are short, orthogonal, and } \alpha+\beta \in \Sigma, \\ x_{\alpha+\beta}(\pm tu)\, x_{\alpha+2\beta}(\pm tu^2) & \text{if } |\alpha| > |\beta| \text{ and } \langle(\alpha,\beta) = 135^\circ. \end{cases}$$

(The last equation follows from Lemma 33. In the others the right hand side is of the form $x_{\alpha+\beta}(N_{\alpha,\beta} tu)$.) If $p = 2$ the second equation can be omitted and there are no ambiguities in sign. Becuase of the calculations in Example (b) above φ preserves

these relations. Thus φ extends to a homomorphism.

There remains only the case G_2, $p = 3$. The proof in that case depends on a sequence of lemmas.

Lemma 56: Let G be a Chevalley group. Let α, β be distinct simple roots, n the order of $w_\alpha w_\beta$ in W, so that $w_\alpha w_\beta w_\alpha \ldots = w_\beta w_\alpha w_\beta \ldots$ (n factors on each side) in W. Then: (a) $w_\alpha(1)w_\beta(1)w_\alpha(1) \ldots = w_\beta(1)w_\alpha(1)w_\beta(1) \ldots$ (n factors on each side) in G.

(b) Both sides map X_α to $-X_{w\alpha}$ (where $w = w_\alpha w_\beta \ldots$).

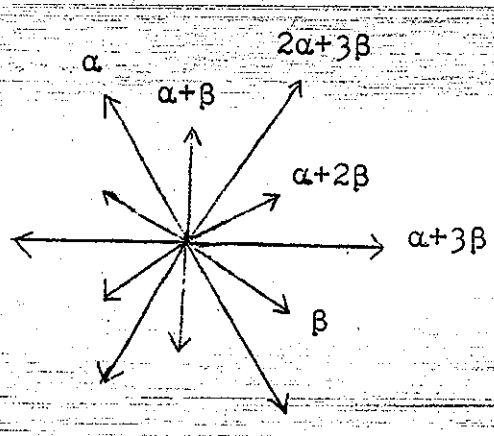
Proof: We may assume G is universal. For simplicity of notation we assume $n = 3$. Consider $x = w_\alpha(1)w_\beta(1)w_\alpha(1)w_\beta(-1)w_\alpha(-1)w_\beta(-1)$. Let $G_\alpha = \langle X_\alpha, X_{-\alpha} \rangle$. Then the product of the first five factors of x is in $w_\alpha(1)w_\beta(1)G_\alpha w_\beta(-1)w_\alpha(-1) = G_{w_\alpha w_\beta \alpha} = G_\beta$ and hence $x \in G_\beta$. Similarly $x \in G_\alpha$. By the uniqueness in Theorem 4', $x \in H$. By the universality of G, $x = 1$. Let $y = w_\alpha(1)w_\beta(1)w_\alpha(1)$. Then $yX_\alpha = cX_{-\beta}$ where $c = \pm 1$. Since $[X_\alpha, X_{-\alpha}] = H_\alpha$ is preserved by y, $yX_{-\alpha} = cX_\beta$ (same c as above). Exponentiating and using $w_\alpha(1) = x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1)$ we obtain $yw_\alpha(1)y^{-1} = w_{-\beta}(c) = w_\beta(-c)$. By (a) $yw_\alpha(1)y^{-1} = w_\beta(1)$, so $c = -1$, proving (b).

Lemma 57: If a, b are elements of an associative algebra over a field of characteristic 0, if both commute with $[a,b]$ and if exp makes sense then $\exp(a + b) = \exp a \exp b \exp(-[a,b]/2)$.

Proof: Consider $f(t) = \exp(-(a+b)t)\exp at \exp bt \exp(-[a,b]t^2/2)$,

a formal power series in t. Differentiating we get $f'(t)$ $= (-(a+b) + a - [b,a]t + b - [a,b]t)f(t) = 0$. Hence $f(t)$ $= f(0) = 1$.

Now assume G is a Chevalley group of type G_2 over a field of characteristic 0, and that the corresponding root system is as shown.



(1) Let $y = w_\alpha(1)w_\beta(1)$ be an element of G corresponding to $w = w_\alpha w_\beta$ (rotation through 60° (clockwise)). Then the Chevalley basis of $\mathcal{L}$ can be adjusted by sign changes so that $yX_\gamma = -X_{w\gamma}$ for all γ.

Proof: Let $yX_\gamma = c_\gamma X_{w\gamma}$, $c_\gamma = \pm 1$. Then (*) $c_\gamma = c_{-\gamma}$, and (**) $c_\gamma c_{w\gamma} c_{w^2\gamma} = -1$ (by Lemma 56(b)). Adjust the signs of $X_{w\alpha}$ and $X_{w^2\alpha}$ so that $c_\alpha = c_{w\alpha} = -1$, and adjust the signs of $X_{-w\alpha}$ and $X_{-w^2\alpha}$ in the same way. It is clear from (*) and (**) that $c_\gamma = -1$ for all γ in the w-orbit through α. Similarly we may make $c_\gamma = -1$ for all γ in the w-orbit through β.

(2) (a) In (1) we have $N_{w\gamma,w\delta} = -N_{\gamma,\delta}$ for all γ, δ.

(b) We may arrange so that $N_{\alpha,\beta} = 1$ and $N_{\alpha+\beta,\beta} = 2$. It then follows that $N_{\beta,\alpha+2\beta} = N_{\alpha+\beta,\alpha+2\beta} = 3$ and $N_{\alpha,\alpha+3\beta} = 1$.

Proof: (a) follows from applying y to $[X_\gamma, X_\delta]$ and using (1). In the proof of (b) we use (*) if γ, δ are roots and $\{\gamma + i\delta \mid -r \leq i \leq q\}$ is the δ-string through γ, then $N_{\gamma,\delta} = \pm(r+1)$, and $N_{\gamma,\delta}$ and $N_{\gamma+\delta,-\delta}$ have the same sign (for their product is $q(r+1)$). By changing the signs of all X_γ for γ in a w-orbit we can preserve the conclusion of (1) and arrange that $N_{\alpha,\beta} = 1$, $N_{\alpha+\beta,\beta} = 2$. By (a) and (*) we have $N_{\beta,\alpha+2\beta} = N_{\alpha+\beta,\alpha+2\beta} = 3N_{-\alpha-\beta,2\alpha+3\beta} = -3N_{\beta,\alpha} = 3$. Now $[X_\alpha[X_{\alpha+2\beta},X_\beta]] = [X_{\alpha+2\beta},[X_\alpha,X_\beta]]$, so that $N_{\alpha+2\beta,\beta}N_{\alpha,\alpha+3\beta} = N_{\alpha,\beta}N_{\alpha+2\beta,\alpha+\beta}$. Hence $N_{\alpha,\alpha+3\beta} = N_{\alpha,\beta} = 1$.

(3) If (1) and (2) hold then:

(a) $(x_\alpha(t),x_\beta(u)) = x_{\alpha+\beta}(tu)x_{\alpha+3\beta}(-tu^3)x_{\alpha+2\beta}(-tu^2)x_{2\alpha+3\beta}(t^2u^3)$

(b) $(x_{\alpha+\beta}(t),x_\beta(u)) = x_{\alpha+2\beta}(2tu)x_{\alpha+3\beta}(-3tu^2)x_{2\alpha+3\beta}(3t^2u)$.

(c) $(x_\alpha(t),x_{\alpha+3\beta}(u)) = x_{2\alpha+3\beta}(tu)$.

(d) $(x_{\alpha+2\beta}(t),x_\beta(u)) = x_{\alpha+3\beta}(-3tu)$.

(e) $(x_{\alpha+\beta}(t),x_{\alpha+2\beta}(u)) = x_{2\alpha+3\beta}(3tu)$.

Proof: (a) By (2) $x_\beta(u)X_\alpha = (\exp \operatorname{ad} uX_\beta)X_\alpha = X_\alpha - uX_{\alpha+\beta} + u^2X_{\alpha+2\beta} + u^3X_{\alpha+3\beta}$. Multiplying by $-t$ and exponentiating we get $x_\beta(u)x_\alpha(-t)x_\beta(-u) = \exp(-tX_\alpha - tu^3X_{\alpha+3\beta})\exp(tuX_{\alpha+\beta} - tu^2X_{\alpha+2\beta})$ $= x_\alpha(-t)x_{\alpha+3\beta}(-tu^3)x_{2\alpha+3\beta}(-t^2u^3/2)x_{\alpha+\beta}(tu)x_{\alpha+2\beta}(-tu^2)x_{2\alpha+3\beta}(3t^2u^3/2)$, by Lemma 57, which yields (a). The proof of (b) is similar. In

(c) - (e) the term on the right hand side corresponds to the only root of the form $i\gamma + j\delta$. The coefficient is $N_{\gamma,\delta}$. We have taken the opportunity of working out all of the nontrivial relations of U explicitly. However, we will only use them in characteristic 3 when they simplify considerably.

(4) (a) There exists an automorphism θ of G such that if w is rotation through 60° then $\theta x_\gamma(t) = x_{w\gamma}(-t)$ for all $\gamma \in \Sigma$, $t \in k$.

(b) If characteristic $k = 3$, then there exists an endomorphism φ of G such that if r is the permutation of the roots given by rotation through 30° then

$$\varphi x_\alpha(t) = \begin{cases} x_{r\gamma}(-t) & \text{if } \gamma \text{ is long,} \\ x_{r\gamma}(t^3) & \text{if } \gamma \text{ is short.} \end{cases}$$

Proof: (a) Take θ to be the inner automorphism by the element y of (1).

(b) The relations (A) and (C) are clearly preserved. Now on the generators $\varphi^2 = \theta \circ \psi$, where $\psi: x_\alpha(t) \longrightarrow x_\alpha(t^3)$, hence φ^2 extends to an endomorphism of G . This implies that in verifying that the relations (B) are preserved by φ it suffices to show this for one pair of roots (γ,δ) with $\angle(\gamma,\delta) =$ each of the angles 30°, 60°, 90°, 120°, 150°. For if $R(\gamma,\delta)$ is the relation $(x_\gamma(t),x_\delta(u)) = \prod x_{i\gamma+j\delta}(c_{ij}t^iu^j)$, if $\angle(\gamma',\delta') = \angle(\gamma,\delta)$, and if φ preserves $R(\gamma,\delta)$ then φ preserves $R(\gamma',\delta')$. To show this it is enough to show that φ preserves $R(r\gamma,r\delta)$. If φ does not preserve $R(r\gamma,r\delta)$ then

φ^2 does not preserve $R(\gamma,\delta)$, a contradiction since $\varphi^2 = \theta \circ \psi$ extends to an endomorphism. It remains to verify $R(\gamma,\delta)$ for pairs of roots (γ,δ) with $<(\gamma,\delta) = 30^\circ, 60^\circ, 90^\circ, 120^\circ, 150^\circ$. For $<(\gamma,\delta) = 30^\circ; 60^\circ, 90^\circ$ we take $\gamma = \alpha$, $\delta = \alpha + \beta$, $2\alpha + 3\beta$, $\alpha + 2\beta$ respectively. Here we have commutativity both before and after applying φ (since (e) becomes trivial since characteristic $k = 3$). For $<(\gamma,\delta) = 120^\circ$ take $(\gamma,\delta) = (\alpha, \alpha + 3\beta)$. Then φ converts (c) to $(x_{\alpha+\beta}(-t), x_\beta(-u)) = x_{\alpha+2\beta}(-tu)$ which is (b), a valid relation. For $<(\gamma,\delta) = 150^\circ$ we take $(\gamma,\delta) = (\alpha,\beta)$. We compare the constants $N_{\gamma,\delta}$ for the positive root system relative to (α,β) and the positive root system relative to $(-\alpha, \alpha + \beta)$. Corresponding to $N_{\alpha,\beta} = 1$ we have $N_{-\alpha,\alpha+\beta} = 1$ and corresponding to $N_{\alpha+\beta,\beta} = 2$ we have $N_{\beta,\alpha+\beta} = -2$. By changing the sign of X_γ for all short roots γ we return to the original situation. Since w_α maps the first system onto the second, $\eta : x_\gamma(t) \longrightarrow \begin{cases} x_{w_\alpha\gamma}(-t) & \text{if } \gamma \text{ is short,} \\ x_{w_\alpha\gamma}(t) & \text{if } \gamma \text{ is long} \end{cases}$ extends to an automorphism of G, and so to prove that φ preserves $R(\gamma,\delta)$ it is sufficient to prove that $\eta \circ \varphi$ does, i.e. that (a) is preserved by $x_\gamma(t) \longrightarrow \begin{cases} x_{w_\alpha r\gamma}(t) & \text{if } \gamma \text{ is long,} \\ x_{w_\alpha r\gamma}(t^3) & \text{if } \gamma \text{ is short.} \end{cases}$

(Note that $w_\alpha r$ is the reflection in the line bisecting $<(\alpha,\beta)$). I.e., that the following equations are consistent:

(a) $(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(tu)x_{\alpha+3\beta}(-tu^3)x_{\alpha+2\beta}(-tu^2)x_{2\alpha+3\beta}(t^2u^3)$,

(a') $(x_\beta(t), x_\alpha(u^3)) = x_{\alpha+3\beta}(t^3u^3)x_{\alpha+\beta}(-tu^3)x_{2\alpha+3\beta}(-t^3u^6)x_{\alpha+2\beta}(t^2u^3)$

(a') follows from (a) by replacing t by u^3, u by t, and taking inverses. This proves (4).

We now complete the proof of Theorem 28. The only remaining case of the first statement is G of type G_2, $p = 3$. If $G = G^*$ this follows from (4) above. In fact, whether $G = G^*$ or not is immaterial because (*) a universal Chevalley group is determined by Σ and k independently of $\mathcal{L}$ or the Chevalley basis of $\mathcal{L}$. (*) follows from Theorem 29 below.

Assume now that k is perfect. Then φ maps one set of generators one to one onto the other so that φ^{-1} exists on the generators. Since φ preserves (A), (B), and (C) so does φ^{-1}. Hence φ^{-1} exists on G^*, i.e. φ is an isomorphism.

Remark: If k is not perfect, and $\varphi: G \longrightarrow G$, then φG is the subgroup of G in which X_α is paramaterized by k if α is long, by k^p if α is short. Here k^p can be replaced by any field between k^p and k to yield a rather weird simple group.

Theorem 29: Let G and G' be Chevalley groups constructed from $(\mathcal{L}, \mathcal{B} = \{X_\alpha, H_\alpha \mid \alpha \in \Sigma\}, L, k)$ and $(\mathcal{L}', \mathcal{B}' = \{X_{\alpha'}, H_{\alpha'} \mid \alpha' \in \Sigma'\}, L', k)$, respectively. Assume that there exists an isomorphism of Σ onto Σ' taking $\alpha \longrightarrow \alpha'$ such that L maps onto L'. Then there exists an isomorphism $\varphi: G \longrightarrow G'$ and signs $\varepsilon_\alpha (\alpha \in \Sigma)$ such that $\varphi x_\alpha(t) = x_{\alpha'}(\varepsilon_\alpha t)$ for all $\alpha \in \Sigma$, $t \in k$. Furthermore we may take $e_\alpha = +1$ if α or $-\alpha$ is simple.

Proof: By the uniqueness theorem for Lie algebras with a given root system there exists an isomorphism $\psi: \mathcal{L} \longrightarrow \mathcal{L}'$ such that $\psi X_\alpha = \varepsilon_\alpha X_{\alpha'}$, $\psi H_\alpha = H_{\alpha'}$ with $\varepsilon_\alpha \varepsilon$ base field for $\mathcal{L}$ (of characteristic 0) and $\varepsilon_\alpha = 1$ if α or $-\alpha$ is simple. (For this see, e.g. Jacobson, Lie Algebras.) By Theorem 1, $N_{\alpha,\beta} = \pm(r+1) = N_{\alpha',\beta'}$. By induction on heights every $\varepsilon_\alpha = \pm 1$. Let ρ be a faithful representation of $\mathcal{L}'$ used to construct G'. Then $\rho \circ \psi$ is a representation of $\mathcal{L}$ which can be used to construct G. Then $x_\alpha(t) = x_{\alpha'}(\varepsilon_\alpha(t))$, so that $\varphi = id.$ meets our requirements.

Remarks: (a) Suppose k is infinite and we try to prove Theorem 28 with t^p replaced by t. Then we must fail. For then the transpose of $\varphi|H$, mapping characters on H^* to those on H, maps Σ^* onto Σ in the inversional manner of Lemma 55, hence can not be a homomorphism. This explains the relative treatment of long and short roots.

(b) If k is algebraically closed and we view G and G^* as algebraic groups then φ is a homomorphism of algebraic groups and an isomorphism of abstract groups, but not an isomorphism of algebraic groups (for taking p^{th} roots (which is necessary for the inverse map) is not a rational operation).

(c) For type G_2, characteristic $k = 3$ (a similar result holds for C_2 and F_4, characteristic $k = 2$), in $\mathcal{L}^k$ there is an endomorphism $\mathfrak{A}\varphi$ such that

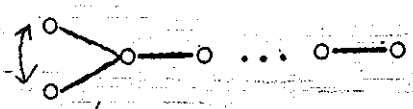
$$d\varphi : X_\alpha \longrightarrow \begin{cases} -X_{r\alpha} & \text{if } \alpha \text{ is long} \\ 3X_{r\alpha} = 0 & \text{if } \alpha \text{ is short.} \end{cases}$$

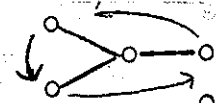
Thus $\mathcal{L} \xrightarrow{d\varphi} \mathcal{L}_{\text{short}} \xrightarrow{d\varphi} 0$ is exact, where $\mathcal{L}_{\text{short}}$ is the 7-dimensional ideal spanned by all X_γ and H_γ for γ short. This leads to an alternate proof of the existence of φ.

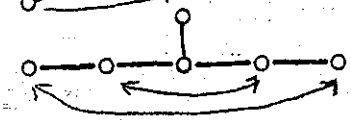
Corollary: (a) Let Σ be an indecomposable root system, σ an angle preserving permutation of the simple roots, $\sigma \neq 1$. If all roots are equal in length then σ extends to an automorphism of Σ. If not, and if p is defined as above, then σ must interchange long and short roots and σ extends to a permutation σ of all roots which also interchanges long and short roots and is such that the map $\alpha \longrightarrow \sigma\alpha$ if α is long, $\alpha \longrightarrow p\sigma\alpha$ if α is short is an isomorphism of root systems. The possibilities for σ are:

(i) 1 root length:

$A_n (n \geq 2)$:  $\sigma^2 = 1$

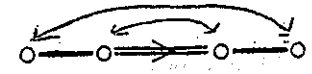
$D_n (n \geq 4)$:  $\sigma^2 = 1$

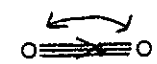
D_4:  $\sigma^3 = 1$

E_6:  $\sigma^2 = 1$

(ii) 2 root lengths, $\sigma^2 = 1$ in all cases.

C_2  $p = 2$

F_4  $p = 2$

G_2  $p = 3$

(b) Let k be a field and G a Chevalley-group constructed from (Σ,k). Let σ be as in (a). If two root lengths occur assume k is perfect of characteristic p. If G is of type D_{2n}, and characteristic $k \neq 2$, assume $\sigma L = L$. Then there exists an automorphism φ of G and signs ε_α ($\varepsilon_\alpha = 1$ if α or $-\alpha$ is simple) such that

$$\varphi x_\alpha(t) = \begin{cases} x_{\sigma\alpha}(\varepsilon_\alpha t) & \text{if } \alpha \text{ is long or all roots are of one length,} \\ x_{\sigma\alpha}(\varepsilon_\alpha t^p) & \text{if } \alpha \text{ is short.} \end{cases}$$

Proof: (a) is clear. (b) If G is universal the existence of φ follows from Theorems 28 and 29. If G is not universal let $\pi: G' \longrightarrow G$ be the universal covering. To show that φ can be dropped from G' to G it is necessary to show that $\varphi \ker \pi \subseteq \ker \pi$. Now $\ker \pi \subseteq$ center G' and unless G is of type D_{2n} with characteristic $k \neq 2$ the center of G' is cyclic, so the result follows. Now suppose G is of type D_{2n} and characteristic $k \neq 2$. If C' = center of G', then C' is canonically isomorphic to $\mathrm{Hom}(L_1/L_0, k^*) = (L_1/L_0)^*$, giving a correspondence between subgroups C of C' and lattices L between L_0 and L_1 such that $\varphi C \subseteq C$ if and only if $\sigma L \subseteq L$. Since $\ker \pi$ corresponds to L and $\sigma L = L$, the result follows.

Remark: The preceeding argument shows that for D_{2n} in characteristic $k \neq 2$ an automorphism of G fixing H and permuting the $\mathcal{X}_\alpha$'s according to σ can exist only if $\sigma L = L$.

Remark: Automorphisms of G of this type as well as the identity are called graph automorphisms.

Exercise: (a) Prove φ above is outer.

(b) By imbedding A_2 in G_2 as the subgroup generated by all χ_α such that α is long, show that its graph automorphisms can be realized by inner automorphisms of G_2. Similarly for D_4 in F_4, D_n in B_n, and E_6 in E_7.

Lemma 58: Let G be a Chevalley group over k, $f_\alpha \in k^*$ for all simple α. Let f be extended to a homomorphism of L_0 into k^*. Then there exists a unique automorphism φ of G such that $\varphi x_\alpha(t) = x_\alpha(f_\alpha t)$ for all $\alpha \in \Sigma$.

Proof: Consider the relations (B), $(x_\alpha(t), x_\beta(u))$ $= \prod x_{i\alpha+j\beta}(c_{ij}t^i u^j)$. Applying φ we get the same thing with t replaced by $f_\alpha t$, u replaced by $f_\beta u$ (for $f_{i\alpha+j\beta} = f_\alpha^i f_\beta^j$). The relations (A) and (C) are clearly preserved. The uniqueness is clear.

Remark: Automorphisms of this type are called diagonal automorphisms.

Exercise: Prove that every diagonal automorphism of G can be realized by conjugation of G in $G(\bar{k})$ by an element in $H(\bar{k})$.

Example: Conjugate SL_n by a diagonal element of GL_n.

If G is realized as a group of matrices and γ is an automorphism of k then the map $\gamma: x_\alpha(t) \longrightarrow x_\alpha(t^\gamma)$ on generators extends to an automorphism of G. Such an automorphism is called a field automorphism.

Theorem 30: Let G be a Chevalley group such that Σ is

indecomposable and k is perfect. Then any automorphism of G can be expressed as the product of an inner, a diagonal, a graph and a field automorphism.

Proof: Let σ be any automorphism of G.

(1) The automorphism σ can be normalized by multiplication by an inner automorphism so that $\sigma U = U$, $\sigma U^- = U^-$. If this is done then $\sigma H = H$ and there exists a permutation ρ of the simple roots such that $\sigma \mathcal{X}_\alpha = \mathcal{X}_{\rho\alpha}$ and $\sigma \mathcal{X}_{-\alpha} = \mathcal{X}_{-\rho\alpha}$ for all simple α.

Proof: If k is finite, U is a p-Sylow subgroup (p = characteristic k) by the corollary of Theorem 25, so by Sylow's Theorem we can normalize σ by an inner automorphism so that $\sigma U = U$. If k is infinite the proof of the corresponding statement is more difficult and will be given at the end of the proof (steps (5) - (12)). For now we assume $\sigma U = U$.

U^- is conjugate to U, so $\sigma U^- = uwUwu^{-1}$ for some $w \in W$, $u \in U$. Since $U^- \cap U = 1$, $uwUwu^{-1} \cap U = 1$ and hence $wUw^{-1} \cap U = 1$. Thus $w = w_o$ so $\sigma U^- = uU^-u^{-1}$. Normalizing σ by the inner automorphism corresponding to u^{-1} we get $\sigma U = U$, $\sigma U^- = U^-$. Now $B = UH$ = normalizer of U, $B^- = U^-H$ = normalizer of U^-. Hence σ fixes $B \cap B^- = H$. Also σ permutes the (B,B) double cosets. Now $B \cup BwB$ $(w \neq 1)$ is a group if and only if $w = w_\alpha$, α simple. Therefore σ permutes these groups. Now $(B \cup Bw_\alpha B) \cap U^- = \mathcal{X}_{-\alpha}$. Since for $B \cup Bw_\alpha B = Bw_\alpha^{-1} \cup Bw_\alpha Bw_\alpha^{-1} = Bw_\alpha^{-1} \cup B\mathcal{X}_{-\alpha}$, and

$B \cap U^- = 1$, $B\mathfrak{X}_{-\alpha} \cap U^- = \mathfrak{X}_{-\alpha}$, we must show $Bw_\alpha^{-1} \cap U^-$ is empty. Thus it suffices to show $Bw_\alpha^{-1}w_o \cap U^-w_o = Bw_\alpha^{-1}w_o \cap w_oU$ is empty. This holds by Theorem 4. Therefore the $\mathfrak{X}_{-\alpha}$'s, α simple, are permuted by σ and similarly for the $\mathfrak{X}_\alpha$'s. The permutation in both cases is the same since $\mathfrak{X}_\alpha$ and $\mathfrak{X}_{-\beta}$ commute (α, β simple) if and only if $\alpha \neq \beta$.

(2) The automorphism σ can be further normalized by a diagonal automorphism so that $\sigma x_\alpha(1) = x_{\rho\alpha}(1)$ for all simple α. It is then true that $\sigma x_{-\alpha}(1) = x_{-\rho\alpha}(1)$ and $\sigma w_\alpha(1) = w_{\rho\alpha}(1)$. Further ρ preserves angles.

In the proof of (2) we use:

Lemma 59: Let α be a root, $t \in k^*$, $u \in k$. Then $x_\alpha(t)x_{-\alpha}(u)x_\alpha(t) = x_{-\alpha}(u)x_\alpha(t)x_{-\alpha}(u)$ if and only if $u = -t^{-1}$, in which case both sides equal $w_\alpha(t)$.

Proof: It suffices to verify this in SL_2, where it is immediate.

Proof of (2): We can achieve $\sigma x_\alpha(1) = x_{\rho\alpha}(1)$ for all simple roots α by a diagonal automorphism. By Lemma 59 with $t = 1$ $\sigma x_{-\alpha}(-1) = x_{-\rho\alpha}(-1)$ and hence $\sigma w_\alpha(1) = w_{\rho\alpha}(1)$. Suppose α and β are simple roots. Then $<(\alpha,\beta) = \pi - \pi/n$ where $n =$ order of $w_\alpha w_\beta$ in $W =$ order of $w_\alpha(1)w_\beta(1)$ mod $H =$ order of $\sigma(w_\alpha(1)w_\beta(1))$ mod $H =$ order of $w_{\rho\alpha}w_{\rho\beta}$ in W. Hence $<(\alpha,\beta) = <(\rho\alpha,\rho\beta)$.

(3) σ can be further normalized by a graph automorphism so that $\rho = 1$.

Proof: By the Corollary to Theorem 28 a graph automorphism exists corresponding to ρ provided that $p = 2$ if Σ is of type C_2 or F_4, or $p = 3$ if Σ is of type G_2, or $\rho L = L$ if Σ is of type D_{2n} and char $k \neq 2$, in the notation there. Suppose Σ is of type C_2 or F_4 and $\rho \neq 1$. Then there exist simple roots α and β, α long, β short, such that $\alpha + \beta$ and $\alpha + 2\beta$ are roots, $\rho\alpha = \beta$, $\rho\beta = \alpha$, and $w_\alpha(1)\chi_\beta w_\alpha(-1) = \chi_{\alpha+\beta}$. Applying σ we get $\sigma\chi_{\alpha+2\beta} = \chi_{\alpha+\beta}$, $\sigma\chi_{\alpha+\beta} = \chi_{\alpha+2\beta}$. Since χ_α and $\chi_{\alpha+2\beta}$ commute so do χ_β and $\chi_{\alpha+\beta}$. Hence $0 = N_{\alpha+\beta,\beta} = \pm 2$. Hence characteristic $k = 2$ so the required graph automorphism exists. Similarly it exists if Σ is of type G_2. Finally, if Σ is of type D_{2n}, characteristic $k \neq 2$, and ρ is extended in the obvious way, then $\rho L = L$ by the remark after Corollary (b) to Theorem 28, so that the graph automorphism exists by the corollary itself.

(4) σ can now be normalized by a field automorphism so that $\sigma = 1$ (i.e. if σ satisfies $\sigma U = U$, $\sigma U^- = U^-$, $\sigma x_\alpha(1) = x_\alpha(1)$ for all simple roots α then σ is a field automorphism).

Proof: Fix a simple root α and define $f: k \longrightarrow k$ by $\sigma x_\alpha(t) = x_\alpha(f(t))$. We will show that f is an automorphism of k. We have f additive, onto, $f(1) = 1$ and by Lemma 59 $\sigma w_\alpha(t) = w_\alpha(f(t))$. Therefore $\sigma h_\alpha(t) = h_\alpha(f(t))$. Since the kernel of the map $t \longrightarrow h_\alpha(t)$ is contained in $\{\pm 1\}$ and $h_\alpha(t)$ is multiplicative, f is multiplicative up to sign.

Assume $f(tu) = af(t)f(u)$ (where $a = a(t,u) = \pm 1$ and $t, u \neq 0$). We must show $a = 1$. Then $af(t)f(u) + f(u) = f(tu) + f(u)$ $= f((t + 1)u) = bf(t + 1)f(u)$ (where $b = b(t + 1,u) = \pm 1$) $= b(f(t) + 1)f(u) = bf(t)f(u) + bf(u)$. Hence $(b - a)f(t)$ $= 1 - b$. Thus if $a = b$, then $a = b = 1$. If $a \neq b$, then $b \neq 1$ so that $a = 1$ again. Hence f is an automorphism.

Let β be another simple root connected to α in the Dynkin diagram (β if one exists). Let g be the automorphism of k corresponding to β. Then σ fixes $\chi_{\alpha+\beta}$. Consider $(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(\pm tu)\cdots$ (+ or - is independent of t,u). Applying σ, first with $u = 1$ then with $t = 1$, u replaced by t we get

$\sigma(x_\alpha(t), x_\beta(1)) = (x_\alpha(f(t)), x_\beta(1)) = x_{\alpha+\beta}(\pm f(t))\cdots$

$\sigma(x_\alpha(1), x_\beta(t)) = (x_\alpha(1), x_\beta(g(t)) = x_{\alpha+\beta}(\pm g(t))\cdots$. In either case the $\chi_{\alpha+\beta}$ term on the right is $\sigma x_{\alpha+\beta}(\pm t)$. Hence $f(t) = g(t)$.

Since Σ is indecomposable there is a single automorphism f of k so that $\sigma x_\alpha(t) = x_\alpha(f(t))$ for all simple α. Applying the field automorphism f^{-1} to G we get the normalization $f = 1$, i.e. σ fixes every $x_\alpha(t)$, $w_\alpha(t)$ for α simple. These elements generate G so $\sigma = 1$.

We now assume k is infinite and consider the normalization $\sigma U = U$ of (1).

(5) Assume that k is infinite, that A and M are its additive and multiplicative groups, that A_o and M_o are infinite

subgroups such that A/A_o is finite and M/M_o is a torsion group. If $M_oA_o \subseteq A_o$ then $A_o = A$.

Proof: Let F be the additive group generated by M_o. Then F is a field for it is closed under multiplication and addition and if $f \in F$, $f \neq 0$ then $f^{-r} \in F$ for some $r > 0$ so $f^{-1} = f^{r-1}f^{-r} \in F$. Now for $a \in A$, $a \neq 0$, $Fa \cap A_o$ is nontrivial since Fa is infinite and A/A_o is finite. Thus $fa \in A_o$ for some $f \neq 0$. Hence $a \in FA_o \subseteq A_o$.

(6) If B, U are as usual, k is infinite and B_o is a subgroup of finite index in B, then $\mathcal{D}B_o = U$.

Proof: Fix α and identify $\mathfrak{X}_\alpha$ with A (the additive subgroup of k) and $\mathfrak{X}_\alpha \cap B_o$ with A_o in (5). Set $M_o = \{t^2 | h_\alpha(t) \in \mathfrak{h}_\alpha \cap B_o\}$. Now (*) $h_\alpha(t)x_\alpha(u)h_\alpha(t)^{-1} = x_\alpha(t^2u)$ so $M_oA_o \subseteq A_o$. M_o is infinite and M/M_o is torsion so by (5) $\mathfrak{X}_\alpha \cap B_o = \mathfrak{X}_\alpha$, i.e. $\mathfrak{X}_\alpha \subseteq B_o$. By (*) $\mathcal{D}B_o \supseteq \mathfrak{X}_\alpha$. Thus $\mathcal{D}B_o \supseteq U$. Since B_o/U is abelian $\mathcal{D}B_o \subseteq U$.

(7) If A is a connected solvable algebraic group then $\mathcal{D}A$ is a connected unipotent group.

This follows from:

Theorem (Lie-Kolchin): Every connected solvable algebraic group A is reducible to superdiagonal form.

Proof: We use induction on the dimension of the underlying space V and thus need only to find a common eigenvector and may assume V is irreducible. Let $A_1 = \mathcal{D}A$. By induction on the length

of the derived series of A there exists $v \in V$, $v \neq 0$ such that $x_1 v = \chi(x_1)v$ for all $x_1 \in A_1$, χ a rational character on A_1. Let V_χ be the space of all such v. A normalizes A_1 and hence permutes the V_χ, which are finite in number. Since A is connected this is the identity permutation. Since V is irreducible there is only one V_χ and it is all of V, i.e., A_1 acts by scalars. Since $A_1 = \mathcal{D}A$ each element of A_1 has determinant 1 so there are only finitely many scalars. Since A_1 is connected all scalars are 1, that is A_1 acts trivially. Thus A/A_1 is abelian and acts on V_1 and hence has a common eigenvector.

An algebraic variety is <u>complete</u> if whenever it is imbedded densely in another variety it is the entire variety. (For a more exact definition see Mumford, <u>Algebraic Geometry</u>).

<u>Examples:</u> The affine line is not complete. It can be imbedded in the projective line. The following are complete:

(a) All projective spaces.

(b) All flag spaces.

(c) $\overline{B}\backslash\overline{G}$ where $\overline{G}$ is a connected linear algebraic group and $\overline{B}$ is a maximal connected solvable subgroup. (See Seminaire Chevalley, Exp 5 - 10.)

We now state, without proof, two results about connected algebraic groups acting on complete varieties.

(8) <u>Borel's Theorem:</u> A connected solvable algebraic group acting on a complete variety fixes some point. This is an extension

of the Lie-Kolchin theorem, which may be restated: every connected solvable algebraic group fixes some flag on the underlying space. We need a refinement of a special case of it.

Theorem: (Rosenlicht, Annali, 1957.) If A is a connected unipotent group acting on a complete variety V, if everything is defined over a perfect field k, and if V contains a point over k, then it contains one fixed by A.

Notation: Let G be a Chevalley group over an infinite field k, $\bar{k}$ the algebraic closure of k, $\bar{G}$, $\bar{B}$ constructed over $\bar{k}$, and $\bar{G}_k$ the set of elements in $\bar{G}$ whose coordinates lie in k.

(9) The map $\bar{G}_k \longrightarrow (\bar{B}\backslash\bar{G})_k$ is onto.

Proof: Assume $\bar{B}x$ is defined over k, $x = wu$ as in Theorem 4'. We can take w a product of $w_\alpha(1)$'s defined over k. Therefore $\bar{B}u^-$ is defined over k where $u^- = wuw^{-1} \varepsilon U^-$. Now U^- is defined over k. Since $u^- = \bar{B}u^- \cap U^-$, u^- is defined over k and hence x is defined over k also.

(10) $\bar{G}_k = \bar{H}_k G$

Proof: See the proof of Theorem 7, Corollary 3.

(11) If A is a connected unipotent subgroup of $\bar{G}$ defined over k, it is G-conjugate to a subgroup of $\bar{U}$.

Proof: We make A act on $\bar{B}\backslash\bar{G}$ by right multiplication. By (8) there exists $\bar{B}x$ defined over k fixed by A. By (9) we can choose $x \varepsilon \bar{G}_k$, and then by (10) $x \varepsilon G$. We have $\bar{B}xa = \bar{B}x$ for all $a \varepsilon A$, i.e., $xax^{-1} \varepsilon \bar{B}$ for all $a \varepsilon A$, so that

$xAx^{-1} \subseteq \overline{B}$. Since A is unipotent $xAx^{-1} \subseteq \overline{U}$.

(12) If k is infinite and perfect, the normalization $\sigma U = U$ of (1) can be attained.

Proof: σB is solvable so $\overline{\sigma B}$ (the smallest algebraic subgroup of $\overline{G}$ containing σB) is solvable. Hence $(\overline{\sigma B})_o$, the connected component of the identity, is solvable and of finite index in $\overline{\sigma B}$. $(\overline{\sigma B})_o = \overline{\sigma(B_o)}$ for some B_o of finite index in B . Let $A = \mathcal{D}\overline{\sigma B_o}$. By (7) A is connected, unipotent and defined over k . By (6) $\sigma U \subseteq A$. By (11) there exists $x \in G$ such that $xAx^{-1} \subseteq \overline{U}$. Hence $x\sigma Ux^{-1} \subseteq U$, i.e., the normalization $\sigma U \subseteq U$ has been attained. Then $U \subseteq \sigma^{-1}U$. But U is maximal with respect to being nilpotent and containing no elements of the center of G . (Check this.) Therefore $\sigma^{-1}U = U$ so $\sigma U = U$.

Corollary: If k is finite Aut G/Int G is solvable.

Exercise: Let D be the group of diagonal automorphisms modulo those which are inner. Prove:

(a) $D \cong \mathrm{Hom}(L_o, k^*)/\{\text{Homomorphisms extendable to } L_1\}$.
$\cong \prod k^*/k^{*e_i}$ where the e_i are the elementary divisors of L_1/L_0 .

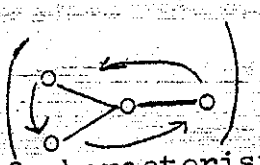
(b) If k is finite, $D \cong C$, the center of the corresponding universal group.

(c) $D = 1$ if k is algebraically closed or if all $e_i = 1$.

Examples: (a) SL_n . Every automorphism can be realized by a

semilinear mapping of the underlying space composed with either the identify or the inverse transpose. I.e., every automorphism is induced by a collineation or a correlation of the underlying projective space.

(b) Over $\mathbb{R}$ or $\mathbb{Q}$ every automorphism of E_8, F_4, or G_2 is inner.

(c) The triality automorphism  exists for $Spin_8$ and PSO_8, but not for SO_8 if characteristic $k \neq 2$.

(d) Aside from triality every automorphism of SO_n or PSO_n (split form) is induced by a collineation of the underlying projective space P which fixes the basic quadric Q: $\Sigma\, x_i x_{n+1-i} = 0$. If n is even, there exist two families of $(n-2)/2$ dimensional subspaces of P entirely within Q (e.g., if $n = 4$ the two families of lines in the quadric surface $x_1x_4 + x_2x_3 = 0$). The graph automorphism occurs because these two families can be interchanged.

Theorem 31: Let G, G' be Chevalley groups relative to (Σ,k), (Σ',k') with Σ, Σ' indecomposable, k, k' perfect. Assume G and G' are isomorphic. If k is finite, assume also characteristic k = characteristic k'. Then k is isomorphic to k', and either Σ is isomorphic to Σ' or else Σ, Σ' are of type B_n, $C_n (n \geq 3)$ and characteristic k = characteristic $k' = 2$.

Proof: As in (1) and (2) of the proof of Theorem 30 we can

normalize σ so that $\sigma U = U'$, $\sigma x_\alpha(1) = x_{\rho\alpha}(1)$, where now ρ is an angle preserving map of Σ onto Σ'. Hence $\Sigma \cong \Sigma'$ or else Σ, Σ' are B_n, $C_n (n \geq 3)$. As in (3) characteristic k = characteristic k' = 2 in the second case. As in (4) $k \cong k'$.

Corollary: Over a field of characteristic $\neq 2$ the Chevalley groups of type B_n, $C_n (n \geq 3)$ are not isomorphic.

* Exercise: If rank Σ, rank $\Sigma' \geq 2$ then the assumption characteristic k = characteristic k' can be dropped in Theorem 31. (Hint: if p = characteristic k and rank $\Sigma \geq 2$ then p makes the largest prime power contribution to $|G|$. If you get stuck see Artin, Comm. Pure and Appl. Math., 1955). (There are exceptions in case rank Σ, rank $\Sigma' \geq 2$ fails, e.g., $SL_2(4) \cong PSL_2(5)$, $SL_3(2) \cong PSL_2(7)$.)

§ 11. Some twisted Groups. In this section we study the group G_σ of fixed points of a Chevalley group G under an automorphism σ. We consider only the simplest case, in which σ fixes U, H, U^-, N, hence acts on $W = N/H$ and permutes the $\mathcal{H}_\alpha$'s. Before launching into the general theory, we consider some examples:

(a) $G = SL_n$. If σ is a nontrivial graph automorphism, it has the form $\sigma x = ax^{t-1}a^{-1}$ (where x^t is the transpose of x and $a = \begin{bmatrix} \epsilon_1 & & \\ & \epsilon_2 & \\ & & \ddots \end{bmatrix}$, $\epsilon_i = \pm 1$). We see that σ fixes x if and only if $xax^t = a$. If a is skew, we get $G_\sigma = Sp_n$. If a is symmetric, we get $G_\sigma = SO_n$ (split form). The group SO_{2n} in characteristic 2 does not arise here, but it can be recovered as a subgroup of SO_{2n+1}, namely the one "supported" by the long roots.

Let $t \to \bar{t}$ be an involutory automorphism of k having k_0 as fixed field. If σ is now modified so that $\sigma x = ax^{t-1}a^{-1}$, then $G_\sigma = SU_n$ (split form). This last result holds even if k is a division ring provided $t \to \bar{t}$ is an anti-automorphism.

If V is the vector space over $\mathbb{R}$ generated by the roots and W is the Weyl group, then σ acts on V and W and has fixed point subspaces V_σ and W_σ. W_σ is a reflection group on V_σ with the corresponding "roots" being the projection on V_σ of the original roots. To see these facts, we write $n = 2m + 1$ or

$n = 2m$ and use the indices $-m, -(m-1), \ldots, m-1, m$ with the index 0 omitted in case $n = 2m$. If ω_i is the weight on H defined by $\omega_i : \mathrm{diag}(a_{-m}, \ldots, a_m) \longrightarrow a_i$, then the roots are $\omega_i - \omega_j (i \neq j)$ and $\sigma\omega_i = -\omega_{-i}$. V_σ is thus spanned by $\{\omega_i' = \omega_{-i} - \omega_i \mid i > 0\}$. Now $w \in W_\sigma$ if and only if w commutes with σ, i.e., if and only if $w(\omega_i - \omega_j) = \omega_k - \omega_\ell$ implies $w(\omega_{-i} - \omega_{-j}) = \omega_{-k} - \omega_{-\ell}$. We see that W_σ is the octahedral group acting on V_σ by all permutations and sign changes of the basis $\{\omega_i'\}$. The projection of $\omega_i - \omega_j (i, j \neq 0)$ on V_σ is $\frac{1}{2}(\omega_i - \omega_{-i} - \omega_j + \omega_{-j}) = \frac{1}{2}(\pm\omega_k' \pm\omega_\ell')$ $(k, \ell > 0)$ or $= \pm\omega_k'$ $(k > 0)$. If either $i = 0$ or $j = 0$, the projection of $\omega_i - \omega_j$ is $\pm\frac{1}{2}\omega_k' (k > 0)$. The projected system is of type C_m if $n = 2m$ or BC_m (a combination of B_m and C_m) if $n = 2m + 1$.

(b) $G = SO_{2n}$ (split form, char $k \neq 2$). We take the group defined by the form $f = 2\sum_{i=1}^{n} x_i x_{-i}$. We will take the graph automorphism to be $\sigma x = a_1 a x' {}^{-1} a^{-1} a_1^{-1}$ $\left(a = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}, a_1 = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & 0 & 1 \\ & & 1 & 0 & \\ & & & & \ddots \\ & & & & & 1 \end{bmatrix} \right)$. The corresponding form fixed by elements of G_σ is $f' = 2\sum_{i=2}^{n} x_i x_{-i} + x_1^2 + x_{-1}^2$. Thus, G_σ fixes $f' - f = (x_1 - x_{-1})^2$ and hence the hyperplane $x_1 - x_{-1} = 0$. G_σ on this hyperplane is the group SO_{2n-1}.

If we now combine σ with $t \longrightarrow \bar{t}$ as in (a), the form f' is replaced by $f'' = \sum_{i=2}^{n} (x_i \bar{x}_{-i} + x_{-i} \bar{x}_i) + x_1 \bar{x}_1 + x_{-1} \bar{x}_{-1}$.

If we make the change of coordinates x_1 replaced by $x_1 + tx_{-1}$ x_{-1} replaced by $x_1 + \bar{t}x_{-1}$ $(t \in k, t \neq \bar{t})$, we see that f is replaced by $2\sum_{i=2}^{n} x_i x_{-i} + 2(x_1^2 + ax_1x_{-1} + bx_{-1}^2)$ and f' is replaced by $\sum_{i=2}^{n} (x_i\bar{x}_{-i} + x_{-i}\bar{x}_i) + (2x_1\bar{x}_1 + a(x_1\bar{x}_{-1} + x_{-1}\bar{x}_1) + 2bx_{-1}\bar{x}_{-1})$, where $a = t + \bar{t}$ and $b = t\bar{t}$. Since these two forms have the same matrix, G_σ is SO_{2n} over k_o re the new version of f. That is, G_σ is $SO_{2n}(k_o)$ for a form of index $n - 1$ which has index n over k.

Example: If $n = 4$, $k = \mathbb{C}$, and $k_o = \mathbb{R}$, G_σ is the Lorentz group (re $f = x_1^2 - x_2^2 - x_3^2 - x_4^2$). If we observe that D_2 corresponds to $A_1 \times A_1$, we see that $SL_2(\mathbb{C})$ and the 0-component of the Lorentz group are isomorphic over their centers. Thus, $SL_2(\mathbb{C})$ is the universal covering group of the connected Lorentz group.

Exercise: Work out $D_3 \sim A_3$ in the same way.

For other examples see E. Cartan, Oeuvres Complètes, No. 38, especially at the end.

Aside from the specific facts worked out in the above examples we should note the following. In the single root length case, the fixed point set of a graph automorphism yields no new group, only an imbedding of one Chevalley group in another (e.g. Sp_n or SO_n in SL_n). To get a new group (e.g. SU_n) we must use a field automorphism as well.

Now to start our general development we will consider first

the effect of twisting abstract reflection groups and root systems.

Let V be a finite dimensional real Euclidean vector space and let Σ be a finite set of nonzero elements of V satisfying

(1) $\alpha \in \Sigma$ implies $c\alpha \notin \Sigma$ if $c > 0$, $c \neq 1$.

(2) $w_\alpha \Sigma = \Sigma$ for all $\alpha \in \Sigma$ where w_α is the reflection in the hyperplane orthogonal to α.

(See Appendix I). We pick an ordering on V and let P (respectively $\prod$) be the positive (respectively simple) elements of Σ relative to that ordering. Suppose σ is an automorphism of V which permutes the positive multiples of the elements of each of Σ, P, and $\prod$. It is not required that σ fix Σ, although it will if all elements of Σ have the same length. Let ρ be the corresponding permutation of the roots. Note that σ is of finite order and normalizes W. Let V_σ and W_σ denote the fixed points in V and W respectively. If $\bar{\alpha}$ i the average of the elements in the σ-orbit of α, then $(\beta, \bar{\alpha}) = (\beta, \alpha)$ for all $\beta \in V_\sigma$. Hence the projection of α on V_σ is $\bar{\alpha}$.

Theorem 32: Let Σ, P, $\prod$, σ etc. be as above.

(a) The restriction of W_σ to V_σ is faithful.

(b) $W_\sigma | V_\sigma$ is a reflection group.

(c) If Σ_σ denotes the projection of Σ on V_σ, then Σ_σ is the corresponding "root system"; i.e., $\{w_{\bar{\alpha}} | V_\sigma, \bar{\alpha} \in \Sigma_\sigma\}$ generates $W_\sigma | V_\sigma$ and $w_{\bar{\alpha}} \Sigma_\sigma = \Sigma_\sigma$. However, (1) may fail for Σ_σ.

(d) If Π_σ is the projection of Π on V_σ, then Π_σ is the corresponding "simple system"; i.e. if multiples are cast out (in case (1) fails for Π_σ), then Π_σ is linearly independent and the positive elements of Σ_σ are positive linear combinations of elements of Π_σ.

Proof: Denote the projection of V on V_σ by $v \to \bar{v}$. This commutes with σ and with all elements of W_σ.

(1) If $\alpha \in \Sigma$, then $\bar{\alpha} \neq 0$; indeed $\alpha > 0$ implies $\bar{\alpha} > 0$. If α is positive, so are all vectors in the σ-orbit of α. Thus, their average $\bar{\alpha}$ is also positive. If $\alpha < 0$, then $\bar{\alpha} = -(-\bar{\alpha}) < 0$.

(2) Proof of (a). If $w \in W_\sigma$, $w \neq 1$, then $w\alpha < 0$ for some root $\alpha > 0$. Thus, $w\bar{\alpha} = \overline{w\alpha} < 0$ and $\bar{\alpha} > 0$. So $w|V_\sigma \neq 1$.

(3) Let π be a ρ-orbit of simple roots, let W_π be the group generated by all $w_\alpha (\alpha \in \pi)$, let P_π be the corresponding set of positive roots, and let w_π be the unique element of W_π so that $w_\pi P_\pi = -P_\pi$. Then $w_\pi \in W_\sigma$ and $w_\pi|V_\sigma = w_{\bar{\alpha}}|V_\sigma$ for any root $\alpha \in P_\pi$. To see this, first consider $\sigma w_\pi \sigma^{-1} \in W_\pi$. Since $\sigma w_\pi \sigma^{-1} P_\pi = P_\pi$, then $\sigma w_\pi \sigma^{-1} = w_\pi$ by uniqueness, and $w_\pi \in W_\sigma$. Since ρ permutes the elements of π in a single orbit, the projections on V_σ of the elements of P_π are all positive multiples of each other. It follows that if α is any element of P_π, then $w_\pi \bar{\alpha} = -\bar{\alpha}$. If $v \in V_\sigma$ with $(v,\bar{\alpha}) = 0$, then $0 = (v,\bar{\beta}) = (v,\beta)$ for $\beta \in \pi$. Hence $w_\pi v = v$. Thus $w_\pi|V_\sigma = w_{\bar{\alpha}}|V_\sigma$.

(4) If ν is a ρ-orbit of roots and $w \in W_\sigma$ then all elements of $w\nu$ have the same sign. This follows from $w\sigma\alpha = \sigma w\alpha$ for $\alpha \in \Sigma$, $w \in W_\sigma$.

(5) $\{w_\pi | \pi$ a ρ-orbit of simple roots$\}$ generates W_σ. Let $w \in W_\sigma$ with $w \neq 1$ and let α be a simple root such that $w\alpha < 0$. Let π be the ρ-orbit containing α. By (4), $wP_\pi < 0$ (i.e., $w\beta < 0$ for all $\beta \in P_\pi$). Now $ww_\pi P_\pi > 0$ and w_π permutes the elements of $P - P_\pi$. Hence, $N(ww_\pi) = N(w) - N(w_\pi)$ (see Appendix II.17). Using induction on $N(w)$, we may thus show that w is a product of w_π's.

(6) If w_o is the element of W such that $w_o P = -P$, then $w_o \in W_\sigma$. This follows from $\sigma w_o \sigma^{-1} P = -P$ and the uniqueness of w_o.

(7) $\{wP_\pi | w \in W_\sigma, \pi$ a ρ-orbit of simple roots$\}$ is a partition of Σ. If the wP_π's are called parts, then α, β belong to the same part if and only if $\overline{\alpha} = c\overline{\beta}$ for some $c > 0$. To prove (7), we consider $\alpha \in \Sigma$, $\alpha > 0$. Now $w_o\alpha < 0$ and $w_o = w_1 w_2 \cdots w_r$ where each $w_i = w_\pi$ for some ρ-orbit of simple roots π (by (5) and (6)). Choose i so that $w_{i+1} \cdots w_r \alpha > 0$ and $w_i w_{i+1} \cdots w_r \alpha < 0$. If $w_i = w_\pi$, then $w_{i+1} \cdots w_r \alpha \in P_\pi$; i.e., α is in some part. Similarly, if $\alpha < 0$, α is in some part. Now assume α, β belong to the same part, say to wP_π. We may assume $\alpha, \beta \in P_\pi$. Then $\overline{\alpha}$ and $\overline{\beta}$ are positive multiples

of each other, as has been noted in (3). Conversely, assume

(8) Σ_0 consists of all $w\bar{\alpha}$ such that $w \in W_0$ and α is a root whose support lies in a simple ρ-orbit."

Now $\bar{\beta}$ has its support in π and hence so does β since σ maps simple roots not in π to positive multiples of simple roots not in π. We see then that $\beta \in P_\pi$, and that any part containing α also contains β. The parts are just the sets of β such that $\bar{\beta} = c\bar{\alpha}$, $c > 0$ and hence form a partition.

(8) $\{w\bar{\alpha} | w \in W_\sigma$, α has support in a ρ-orbit of simple roots$\} = \Sigma_\sigma$.

(9) Parts (b) and (c) follow from (3), (5), and (8).

(10) Proof of (d). We select one root α from each ρ-orbit and form $\{\alpha\}$. This set, consisting of elements whose supports in Π are disjoint, is independent since Π is. If $\alpha > 0$ then it is a positive linear combination of the elements of Π. Hence $\bar{\alpha}$ is a positive linear combination of the elements of Π_σ.

Remark: To achieve condition (1) for a root system, we can stick to the set of shortest projections in the various directions.

Examples:

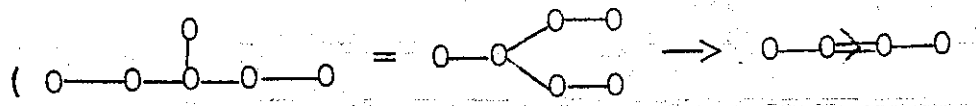
(a) For σ of order 2, W of type A_{2n-1}, we get W_σ of type C_n. For W of type A_{2n}, we get W_σ of type BC_n.

(b) For σ of order 2, W of type D_n, we get W_σ of type B_{n-1}.

(c) For σ of order 3, W of type D_4, we get W_σ of type G_2. To see this let α, β, γ, δ be the simple roots with δ connected with α, β, and γ. Then $\overline{\alpha} = 1/3\,(\alpha + \beta + \gamma)$, $\overline{\delta} = \delta$ and $\langle \overline{\alpha}, \overline{\delta} \rangle = -1$, $\langle \overline{\delta}, \alpha \rangle = -3$, giving W_σ of type G_2.

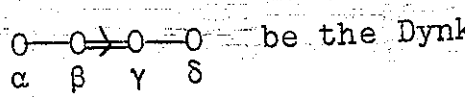
(Schematically: )

(d) For σ of order 2, W of type E_6, we get W_σ of type F_4.

()

(e) For σ of order 2, W of type C_2, we get W_σ of type A_1.

(f) For σ of order 2, W of type G_2, we get W_σ of type A_1.

(g) For σ of order 2, W of type F_4, we get W_σ of type $\mathcal{D}_{16}$ (the dihedral group of order 16). To see this let  be the Dynkin diagram of F_4, and $\sigma\alpha = \sqrt{2}\,\delta$, $\sigma\beta = \sqrt{2}\,\gamma$. Since $\overline{\alpha} = 1/2(\alpha + \sqrt{2}\,\delta)$, $\overline{\beta} = 1/2(\beta + \sqrt{2}\,\gamma)$, we have $\langle \overline{\beta}, \overline{\alpha} \rangle = -1$, $\langle \overline{\alpha}, \overline{\beta} \rangle = -(2 + \sqrt{2})$. This corresponds to an angle of $7\pi/8$ between $\overline{\alpha}$ and $\overline{\beta}$. Hence W_σ is of type $\mathcal{D}_{16}$. Alternatively, we note that $w_{\overline{\alpha}} w_{\overline{\beta}}$ makes six positive roots negative and that there are 24 positive roots in

all, so that $w_o = (w_{\bar{\alpha}} w_{\bar{\beta}})^4$. Hence, $w_{\bar{\alpha}}^2 = w_{\bar{\beta}}^2$ $= (w_{\bar{\alpha}} w_{\bar{\beta}})^8 = 1$ and W_σ is of type $\mathcal{D}_{16}$. Note that this is the only case of those we have considered in which W_σ fails to be crystallographic (See Appendix V).

In (e), (f), (g) we are assuming that multiples have been cast out.

The partition of Σ in (7) above can be used to define an equivalence relation R on Σ by $\alpha \equiv \beta$ if and only if $\bar{\alpha}$ is a positive multiple of $\bar{\beta}$ where $\bar{\alpha}$ is the projection of α on V_σ. Letting Σ/R denote the collection of equivalence classes we have the following:

Corollary: If Σ is crystallographic and indecomposable, then an element of Σ/R is the positive system of roots of a system of one of the following types:

(a) A_1^n $n = 1, 2,$ or 3 .

(b) A_2 (this occurs only if Σ is of type A_{2n}) .

(c) C_2 (this occurs if Σ is of type C_2 or F_4).

(d) G_2 .

Now let G be a Chevalley group over a field k of characteristic p . Let σ be an automorphism of G which is the product of a graph automorphism and a field automorphism θ of k and

such that if ρ is the corresponding permutation of the roots then

(1) if ρ preserves lengths, then order θ = order ρ.

(2) if ρ doesn't preserve lengths, then $p\theta^2 = 1$ (where p is the map $x \to x^p$).

Condition (1) focuses our attention on the only interesting case. Observe that $\rho = id.$, $\theta = id.$ is allowed.

Condition (2) could be replaced by $\theta^2 = p$ thereby extending the development to follow, suitably modified, to imperfect fields k.) We know that $p = 2$ if G is of type C_2 or F_4 and $p = 3$ if G is of type G_2. Recall also that $\sigma x_\alpha(t)$

$$= \begin{cases} x_{\rho\alpha}(\epsilon_\alpha t^\theta) & \text{if } |\alpha| \geq |\rho\alpha| \\ x_{\rho\alpha}(\epsilon_\alpha t^{p\theta}) & \text{if } |\alpha| < |\rho\alpha| \end{cases}$$

where $\epsilon_\alpha = \pm 1$ and $\epsilon_\alpha = 1$ if $\pm\alpha$ is simple. (See the proof of Theorem 29.)

Now σ preserves U, H, B, U^-, and N, and hence $N/H \cong W$. The action thus induced on W is concordant with the permutation ρ of the roots. Since ρ preserves angles, it agrees up to positive multiples with an isometry on the real space generated by the roots. Thus the results of Theorem 32 may be applied. Also we observe that if n is the order of ρ, then $n = 1$, 2, or 3, so that the length of each ρ-orbit is 1 or n.

Lemma 60: $\prod \epsilon_\alpha = 1$ over each ρ-orbit of length n.

Proof: Since σ^n acts on each χ_α ($\pm\alpha$ simple) as a field automorphism, it does so on all of G, whence the lemma.

Lemma 61: If $a \in \Sigma/R$, then $\chi_{a,\sigma} \neq 1$.

Proof: Choose $\alpha \in a$ so that no $\beta \in a$ can be added to it to yield another root. If the orbit of α has length 1, set $x = x_\alpha(1)$ if $\epsilon_\alpha = 1$, $x = x_\alpha(t)$ with $t \in k$, $t \neq 0$ and $t + t^\theta = 0$ if $\epsilon_\alpha \neq 1$. Then $x \in \chi_{a,\sigma}$. If the length is n, we set $y = x_\alpha(1)$, then $x = y \cdot \sigma y \cdot \sigma^2 y \cdots$ over the orbit, and use Lemma 60.

Theorem 33: Let G, σ, etc. be as above.

(a) For each $w \in W_\sigma$, the group $U_w = U \cap w^{-1}U^-w$ is fixed by σ.

(b) For each $w \in W_\sigma$, there exists $n_w \in N_\sigma$, indeed $n_w \in \langle U_\sigma, U_\sigma^- \rangle$, so that $n_w H = w$.

(c) If n_w ($w \in W_\sigma$) is as in (b), then $G_\sigma = \bigcup_{w \in W_\sigma} B_\sigma n_w U_{w,\sigma}$ with uniqueness of expression on the right.

Proof:

(a) This is clear since U and $w^{-1}U^-w$ are fixed by σ.

(b) We may assume that $w = w_\pi$ for some ρ-orbit of simple roots π. By Lemma 61, choose $x \in \chi_{-a,\sigma}$ $x \neq 1$, where $a \in \Sigma/R$

corresponds to π. Using Theorem 4' we may write $x = un_w v$ for some $w \in W$ where $u \in U$, $v \in U_w$, and $n_w H = w$. Now $x = \sigma x = \sigma u \cdot \sigma n_w \sigma v$ and by Theorem 4 and the uniqueness in Theorem 4', we have $\sigma w = w$, $\sigma n_w = n_w$, $\sigma u = u$, and $\sigma v = v$. Thus, $n_w \in \langle U_\sigma, U_\sigma^- \rangle$. Since $w \neq 1$, $w \in W_\sigma$, and $w \in W_\pi$, we have $w\alpha < 0$ for some $\alpha \in \pi$, $w\pi < 0$, and $w = w_\pi$.

(c) Let $x \in G_\sigma$, say $x \in BwB$. Since $\sigma(BwB) = B\sigma wB$ we have $w \in W_\sigma$. Choose n_w as in (b) and write $x = bn_w v$ with $b \in B$ and $v \in U_w$. Applying σ we get $b \in B_\sigma$ and $v \in U_{w,\sigma}$. Uniqueness follows from Theorem 4'.

Corollary: The conclusions of Theorem 33 are still valid if G_σ and B_σ are replaced by $G'_\sigma = \langle U_\sigma, U_\sigma^- \rangle$ and $B'_\sigma = G'_\sigma \cap B_\sigma$. Also since $B_\sigma = U_\sigma H_\sigma$, we can replace H_σ by $H'_\sigma = G'_\sigma \cap H_\sigma$.

Lemma 62: Let a generically denote a class in Σ/R. Let S be a union of classes in Σ/R which is closed under addition and such that if $a \subseteq S$ then $-a \notin S$. Then $\mathcal{X}_{S,\sigma} = \prod_{a \subseteq S} \mathcal{X}_{a,\sigma}$ with the product taken in any fixed order and there is uniqueness of expression on the right. In particular, $U_\sigma = \prod_{a>0} \mathcal{X}_{a,\sigma}$ and $U_{w,\sigma} = \prod_{\substack{a>0 \\ wa \leq 0}} \mathcal{X}_{a,\sigma}$ for all $w \in W_\sigma$.

Proof: We arrange the positive roots in a manner consistent with the order of the a's; i.e., those roots in the first a are first, etc. Now $\mathcal{X}_S = \prod_{\alpha>0} \mathcal{X}_\alpha$ in the order just described and with

uniqueness of expression on the right by Lemma 17. Hence $\mathcal{X}_S = \prod_{a>0} \mathcal{X}_a$ in the given order and again with uniqueness of expression on the right. The lemma follows by considering the fixed points of σ on both sides of the last equation.

Corollary: If a, b are classes in Σ/R with $a \neq \pm b$, then $(\mathcal{X}_a, \mathcal{X}_b) \subseteq \prod \mathcal{X}_c$, where the roots on the right are in the closed subsystem generated by a and b, those of a and b excluded. The condition on c can be stated alternately, in terms of Σ_σ, that $\bar{c}$ is in the interior of the (plane) convex cone generated by $\bar{a}$ and $\bar{b}$.

Remark: The exact relations in the above corollary can be quite complicated but generally resemble those in the Chevalley group whose Weyl group is W_σ. For example, if G is of type A_3 and σ is of order 2, say $\overset{\alpha}{\circ}\!\!-\!\!\overset{\beta}{\circ}\!\!-\!\!\overset{\gamma}{\circ}$, $a = \{\beta\}$, $b = \{\alpha, \gamma\}$, $c = \{\alpha + \beta, \beta + \gamma\}$, $d = \{\alpha + \beta + \gamma\}$, and if we set $x_a(t) = x_\beta(t)$ $(t \in k_\theta)$, $x_b(u) = x_\alpha(u)x_\gamma(u^\theta)$ $(u \in k)$, and similarly for c and d, we get $(x_a(t), x_b(u)) = x_c(\pm tu)x_d(\pm t\, uu^\theta)$. In C_2, the corresponding relation is

$$(x_a(t), x_b(u)) = x_{a+b}(\pm tu)\, x_{a+2b}(\pm tu^2).$$

If G is of type X and σ is of order n, we say G_σ is of type ${}^nX$. E.g., the group considered in the above remark is of type ${}^2A_3$. The group of type ${}^2C_2$ is called the Suzuki group and the groups of type ${}^2G_2$ and ${}^2F_4$ are called Ree groups. We

write $G \sim X$ and $G_\sigma \sim {}^nX$.

Lemma 63: Let a be a class in Σ/R , then $\mathcal{X}_{a,\sigma}$ has the following structure:

(a) If $a \sim A_1$, then $\mathcal{X}_{a,\sigma} = \{x_a(t) | t \in k_\theta\}$

(b) If $a \sim A_1^n$, then $\mathcal{X}_{a,\sigma} = \{x \cdot \sigma x \cdots | x = x_\alpha(t),\ \alpha \in a,\ t \in k\}$

(c) If $a \sim A_2$, $a = \{\alpha, \beta, \alpha + \beta\}$, then $\theta^2 = 1$ and

$$\mathcal{X}_{a,\sigma} = \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+\beta}(u) | tt^\theta + u + u^\theta = 0\}$$

If (t,u) denotes the given element, then

$$(t,u)(t',u') = (t + t',\ u + u' - t^\theta t') .$$

(d) If $a \sim C_2$, $a = \{\alpha, \beta, \alpha + \beta, \alpha + 2\beta\}$, then $2\theta^2 = 1$ and $\mathcal{X}_{a,\sigma} = \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+2\beta}(u)x_{\alpha+\beta}(t^{1+\theta} + u^\theta) | t,u \in k\}$.

If (t,u) denotes the given element, $(t,u)\ (t',u')$ $= (t + t',\ u + u' + t^{2\theta}t')$.

(e) If $a \sim G_2$, $a = \{\alpha, \beta, \alpha + \beta, \alpha + 2\beta, \alpha + 3\beta, 2\alpha + 3\beta\}$, then $3\theta^2 = 1$ and $\mathcal{X}_{a,\sigma} = \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+3\beta}(u)x_{\alpha+\beta}(u^\theta - t^{1+\theta})$

$x_{2\alpha+3\beta}(v)x_{\alpha+2\beta}(v^\theta - t^{1+2\theta}) | t,u,v \in k\}$. If

(t,u,v) denotes the given element then

$$(t,u,v)(t',u',v') = (t + t',\ u + u' + t't^{3\theta},\ v + v' - t'u + t'^2t^{3\theta}) .$$

Note that in (a) and (b), $\mathcal{X}_{a,\sigma}$ is a one parameter group for the fields k_θ and k respectively.

Proof: (a) and (b) are easy and we omit their proofs. For (c), normalize the parametrization of $\mathcal{X}_{\alpha+\beta}$ so that $N_{\alpha,\beta} = 1$. Then $\sigma x_\alpha(t) = x_\beta(t^\theta)$, $\sigma x_\beta(t) = x_\alpha(t^\theta)$, and $\sigma x_{\alpha+\beta}(u) = x_{\alpha+\beta}(-u^\theta)$. Write $x \in \mathcal{X}_{a,\sigma}$ as $x = x_\alpha(t)x_\beta(v)x_{\alpha+\beta}(u)$ and compare the coefficients on both sides of $x = \sigma x$ to get (c). The proof of (d) is similar to that of (c). For (e), first normalize the signs as in Theorem 28, and then complete the proof as in (c) and (d).

Exercise: Complete the details of the above proof.

Remark: The role of the group SL_2 in the untwisted case is taken by the groups $SL_2(k_\theta)$, $SL_2(k)$, $SU_3(k,\theta)$(split form), the Suzuki group, and Ree group of type G_2.

Exercise: Determine the structure of H_σ in the case G is universal.

Lemma 64: If G is universal, then G_σ is generated by U_σ and U_σ^- except perhaps for the case $G_\sigma \sim {}^2G_2$ with k infinite.

Proof: Let $G'_\sigma = \langle U_\sigma, U_\sigma^- \rangle$ and let $H'_\sigma = H_\sigma \cap G'_\sigma$. By the corollary to Theorem 33, it suffices to show $H_\sigma \subseteq G'_\sigma$; i.e., (*) $H'_\sigma = H_\sigma$. Since G is universal, H is a direct product of $\{h_\alpha | \alpha \text{ simple}\}$ (see the corollary to Lemma 28). These groups are permuted by σ exactly as the roots are. Hence it is enough to prove (*) when there is a single orbit; i.e., when G_σ is one of the types SL_2, ${}^2A_2$, ${}^2C_2$, or ${}^2G_2$. For SL_2, this is clear.

(1) For $x \in U_\sigma^- - \{1\}$, write $x = u_1 n u_2$ with $u_i \in U_\sigma^-$, $i = 1,2$ and $n = n(x) \in N \cap G'_\sigma$. Then H'_σ is generated by $\{n(x)n(x_o)^{-1} | x_o$ a fixed choice of $x\}$. To see this let H''_σ be the group so generated. Consider $G''_\sigma = U_\sigma^- H''_\sigma \cup U_\sigma^- H''_\sigma n(x_o) U_\sigma^-$. This set is closed under multiplication by U_σ^-. It is also closed under right multiplication by $n(x_o)^{-1}$. This follows from $n(x_o)^{-1} = n(x_o^{-1})$ $= n(x_o^{-1})n(x_o)^{-1}n(x_o)$ and $n(x_o)U_\sigma^- n(x_o)^{-1} = U_\sigma \subseteq G''_\sigma$ since $x = u_1(n(x)n(x_o)^{-1})n(x_o)u_2$ for $x \in U_\sigma^- - \{1\}$. We see that $G''_\sigma = G'_\sigma$; whence $H''_\sigma = H'_\sigma$.

(2) If α and β are the simple roots of A_2, C_2, or G_2 labeled as in Lemma 63 (c), (d), or (e) respectively, then H_σ^- is isomorphic to k^* via the map φ: $t \to h_\alpha(t)h_\beta(t^\theta)$.

(3) Let λ be the weight such that $<\lambda,\alpha> = 1$, $<\lambda,\beta> = 0$, let R be a representation of $\mathcal{L}^k$ (obtained from one of $\mathcal{L}$ by shifting the coefficients to k) having λ as highest weight and let v^+ be a corresponding weight vector. Let μ be the lowest weight of R and let v^- be a corresponding weight vector. For $x \in U_\sigma^- - \{1\}$, write $xv^- = f(x)v^+ +$ terms for lower weights. Then $f(x) \neq 0$ and H'_σ is isomorphic under φ^{-1} in (2) to the subgroup m of k^* generated by all $f(x)f(x_o)^{-1}$. To prove (3), let $x \in U_\sigma^- - \{1\}$ and write $x = u_1 n(x) u_2$ as in (1). We see $xv^- = n(x)v^+ +$ terms for lower weights, so $n(x)v^- = f(x)v^+$ and $n(x)n(x_o)^{-1}v^+ = f(x)f(x_o)^{-1}v^+$. If $n(x)n(x_o)^{-1} = h_\alpha(t)h_\beta(t^\theta)$, then by the choice of λ, $f(x)f(x_o)^{-1} = t$ (see Lemma 19 (c)). (3)

then follows from (1).

(4) The case $G_\sigma \sim {}^2A_2$. Here $f(x) = -u^\theta$ and $m = k^*$. To see this, we note that the representation R of (3) in this case is $R: \mathcal{L}^k \to s\ell_3(k)$ and if $x = x_\alpha(t)x_\beta(t^\theta)x_{\alpha+\beta}(u)$

then $x \longrightarrow \begin{bmatrix} 1 & t & u+tt^\theta \\ 0 & 1 & t^\theta \\ 0 & 0 & 1 \end{bmatrix}$. Thus, $f(x) = u + tt^\theta = -u^\theta$

by Lemma 63 (c). Thus, m is the group generated by ratios of elements $(-u^\theta)$ of k^* whose traces are norms (tt^θ). Let $u \in k^*$. If $u^\theta \neq u$, set $u_1 = (u - u^\theta)^{-1}$, and if $u^\theta = u$, choose $u_1 \in k^*$ so that $u_1^\theta = -u_1$. Then uu_1 and u_1 are values of f (their traces are 0 or 1), so that $u \in m$ and $m = k^*$.

(5) The case $G_\sigma \sim {}^2C_2$. Here $f(x) = t^{2+2\theta} + u^{2\theta} + tu$ and $m = k^*$. To see this, first note that since the characteristic of k is 2, there is an ideal in $\mathcal{L}^k$ "supported" by short roots. The representation R can be taken as $\mathcal{L}^k$ acting on this ideal, and $v^+ = X_{\alpha+\beta}$ while $v^- = X_{-\alpha-\beta}$. Letting $x = x_\alpha(t)x_\beta(t^\theta)x_{\alpha+2\beta}(u)x_{\alpha+\beta}(u^\theta + t^{1+\theta})$ we can determine $f(x)$. By taking $t = 0$ in the expression for $f(x)$ and writing $v = (v^\theta)^{2\theta}$, we see that $m = k^*$.

(6) The case $G_\sigma \sim {}^2G_2$. Here $f(x) = t^{4+6\theta} - u^{1+3\theta} - v^2 + t^{3+3\theta}u + t^{1+3\theta}u^{3\theta} + tv^{3\theta} - tuv$. The group m is generated by all values of f for which $(t,u,v) \neq (0,0,0)$, and it contains

k^{*2} and -1 ; hence $m = k^*$, if k is finite. Here the representation R can be taken to be the adjoint representation on $\mathcal{L}^k$, $v^+ = X_{2\alpha+3\beta}$, and $v^- = X_{-2\alpha-3\beta}$. Letting x be as in Lemma 63 (e), and working modulo the ideal in $\mathcal{L}^k$ "supported" by the short roots, we can compute $f(x)$. Setting $t = u = 0$, we see that $-v^2 \in m$, hence $-1 \in m$ and $k^{*2} \subseteq m$. If k is finite $m = k^*$ follows from (*) $-1 \notin k^{*2}$. To show (*), suppose $t^2 = -1$ with $t \in k$. Then $t^{2\theta} = -1$, so $t^\theta = \pm t$ and $t^{\theta^2} = t$. Since $3\theta^2 = 1$, we see $t = (t^{\theta^2})^3 = t^3$. But $t^3 = t^2 t = -t$, so $t = 0$, a contradiction. This proves the lemma.

Corollary: If G is universal, then $G'_\sigma = G_\sigma$ and $H'_\sigma = H_\sigma$ except possibly for ${}^2G_2$ with k infinite in which case $G_\sigma/G'_\sigma = H_\sigma/H'_\sigma \cong k^*/m$ with m as in (6) above.

Remarks: (a) It is not known whether $m = k^*$ always if $G_\sigma \sim {}^2G_2$. One can make the changes in variables $v \to v + tu$ and then $u \to u - t^{1+3\theta}$ to convert the form f in (6) to $t^{4+6\theta} - u^{1+3\theta} - v^2 + t^2u^2 + tv^{3\theta}$. Both before and after this simplification the form satisfies the condition of homogenity:

$$f(t,u,v) = t^{4+6\theta} f(1, u/t^{1+3\theta}, v/t^{2+3\theta}) \quad \text{if} \quad t \neq 0 .$$

(b) A corollary of (3) above, is that the forms in (5) and (6) are definite, i.e., $f = 0$ implies $t = u\ (= v) = 0$. A direct proof in case f is as in (5) can be made as follows: Suppose $0 = f(t,u) = t^{2+2\theta} + u^{2\theta} + tu$ with one of t, u nonzero.

If $t = 0$, then $u = 0$, so we have $t \neq 0$. We see $f(t,u) = t^{2+2\theta} f(1,u/t^{2\theta+1})$ using $2\theta^2 = 1$. Hence we may assume $t = 1$. Thus, $1 + u^{2\theta} + u = 0$ or (by applying θ) $u^{\theta} = 1 + u$. Hence $u^{\theta^2} = 1 + u^{\theta} = u$ and $u = u^{2\theta^2} = u^2$. Thus, $u = 0$ or 1, a contradiction. A direct proof in case f is as (6) appears to be quite complicated.

(c) The form in (5) leads to a geometric interpretation of ${}^2C_2$. Form the graph $v = t^{2+2\theta} + u^{2\theta} + tu$ in k^3 of the form $f(x)$. Imbed k^3 in $P^3(k)$, projective 3-space over k, by adding the plane at ∞, and adjoin the point at ∞ in the direction $(0,0,1)$ to the graph to obtain a subset Q of $P^3(k)$. Q is then an ovoid in $P^3(k)$; i.e.

(1) No line meets Q in more than two points.

(2) The lines through any point of Q not meeting Q again always lie in a plane.

The group ${}^2C_2$ is then realized as the group of projective transformations of $P^3(k)$ fixing Q. For further details as well as a corresponding geometric interpretation of ${}^2G_2$ see J. Tits, Séminaire Bourbaki, 210 (1960). For an exhaustive treatment of ${}^2C_2$, especially in the finite case, see Lüneberg, Springer Lecture Notes 10 (1965).

Theorem 34: Let G and σ be as above with G universal. Excluding the cases: (a) ${}^2A_2(4)$, (b) ${}^2B_2(2)$, (c) ${}^2G_2(3)$, (d) ${}^2F_4(2)$, we have that G_σ° is simple over its center.

Sketch of proof: Using a calculus of double cosets re B_σ, which can be developed exactly as for the Chevalley groups with W_σ in place of W and Σ/R (or Σ_σ (see Theorem 32)) in place of Σ, and Theorem 33, the proof can be reduced exactly as for the Chevalley groups to the proof of: $G'_\sigma = \mathcal{D}G'_\sigma$. If k has "enough" elements, so does H'_σ by the Corollary to Lemma 64 and the action of H'_σ on $\mathcal{X}_{a,\sigma}$ can be used to show $\mathcal{X}_{a,\sigma} \subseteq \mathcal{D}G'_\sigma$. This takes care of nearly everything. If k has "few" elements then the commutator relations within the $\mathcal{X}_a$'s and among them can be used. This leads to a number of special calculations. The details are omitted.

Remark: The groups in (a) and (b) above are solvable. The group in (c) contains a normal subgroup of index 3 isomorphic to $A_1(8)$. The group in (d) contains a "new" simple normal subgroup of index 2. (See J. Tits, "Algebraic and abstract simple groups," Annals of Math. 1964.)

Exercise: Center of G'_σ = (Center of G)$_\sigma$.

We now are going to determine the orders of the finite Chevalley groups of twisted type. Let k be a finite field of characteristic p. Let a be minimal such that $\theta = p^a$ (i.e., such that $t^\theta = t^{p^a}$ for all $t \in k$). Then $|k| = p^{2a}$ for ${}^2A_n$, ${}^2D_n$, ${}^2E_6$; $|k| = p^{3a}$ for ${}^3D_4$; and $|k| = p^{2a+1}$ for ${}^2C_2$, ${}^2F_4$, ${}^2G_2$. We can write $\sigma x_\alpha(t) = x_{\rho\alpha}(\epsilon_\alpha t^{q(\alpha)})$

where $q(\alpha)$ is some power of p less than $|k|$. If q is the geometric average of $q(\alpha)$ over each ρ-orbit then $q = p^a$ except when G_σ is of type ${}^2C_2$, ${}^2F_4$, or ${}^2G_2$ in which case $q = p^{a+1/2}$.

Let V be the real Euclidean space generated by the roots and let σ_o be the automorphism of V permuting the rays through the roots as ρ permutes the roots. Since σ_o normalizes W, we see that σ_o acts on the space I of polynomials invariant under W. Since σ_o also acts on the subspace of I of homogeneous elements of a given positive degree, we may choose the basic invariants I_j, $j = 1, \ldots, \ell$, of Theorem 27 such that $\sigma_o I_j = \epsilon_j I_j$ for some $\epsilon_j \in \mathbb{C}$ (here we have extended the base field $\mathbb{R}$ to $\mathbb{C}$). As before, we let d_j be the degree of I_j, and these are uniquely determined. Since σ_o acts on V, we also have the set $\{\epsilon_{oj} | j = 1, \ldots, \ell\}$ of eigenvalues of σ_o on V. We recall also that N denotes the number of positive roots in Σ.

Theorem 35: Let σ, q, N, ϵ_j, and d_j be as above, and assume G is universal. We have

(a) $|G_\sigma| = q^N \prod_j (q^{d_j} - \epsilon_j)$.

(b) The order of the corresponding simple group is obtained by dividing $|G_\sigma|$ by $|C_\sigma|$ where C is the center of G.

Lemma 65: Let σ, H, U, etc. be as above.

(a) $|U_\sigma| = q^N$, $|U_{w,\sigma}| = q^{N(w)}$.

(b) $|H_\sigma| = \prod_j (q - \epsilon_{oj})$.

(c) $|G_\sigma| = q^N \prod_j (q - \epsilon_{oj}) \sum_{w \in W_\sigma} q^{N(w)}$.

where $N(w)$ is the number of positive roots in Σ made negative by w .

Proof: (a) It suffices to show that $|\mathfrak{X}_{a,\sigma}| = q^{|a|}$ for $a \in \Sigma/R$ by Lemma 62. This is so by Lemma 63. (b) Let π be a ρ-orbit of simple roots. Since $\sigma h_\alpha(t) = h_{\rho\alpha}(t^{q(\alpha)})$, the contribution to $|H_\sigma|$ made by elements of H_σ "supported" by π is $(\prod_{\alpha \in \pi} q(\alpha)) - 1 = q^m - 1$ if $m = |\pi|$. Since the ϵ_{oj}'s corresponding to π are the roots of the polynomial $X^m - 1$, (b) follows. (c) This follows from (a), (b), and Theorem 33.

Corollary: U_σ is a p-Sylow subgroup.

Lemma 66: We have the following formal identity in t:

$$\sum_{w \in W_\sigma} t^{N(w)} = \prod_j (1 - \epsilon_j t^{d_j})/(1 - \epsilon_{oj} t)$$

Proof: We modify the proof of Theorem 26 as follows:

(a) σ there is replaced by σ_o here.

(b) Σ there is replaced by Σ_o here, where Σ_o is the set of unit vectors in V which lie in the same directions of the roots.

(c) Only those subsets π of $\prod$ fixed by σ_o are considered.

(d) $(-1)^{\pi}$ is now defined to be $(-1)^k$ where k is the number of σ_o orbits in π.

(e) $W(t)$ is now defined to be $\sum_{w \in W_\sigma} t^{N(w)}$.

With these modifications the proof proceeds exactly as before through step (5). Steps (6)-(8) become:

(6') For $\pi \subseteq \prod$, $w \in W$, let N_π be the number of cells in K congruent to D_π under W and fixed by $w\sigma_o$. Then $\Sigma(-1)^{\pi} N_\pi = \det w$. (Hint: If $V' = V_{w\sigma_o}$ and K' is the complex on V' cut by K, then the cells of K' are the intersections with V' of the cells of K fixed by $w\sigma_o$.)

(7') Let χ be a character on $< W, \sigma_o >$ and χ_π the restriction of χ to $< W_\pi, \sigma_o >$ induced up to $< W, \sigma_o >$. Then $\Sigma(-1)^{\pi} \chi_\pi(w\sigma_o) = \chi(w\sigma_o)\det w$ $(w \in W)$.

(8') Let M be a $< W, \sigma_o >$ module, let $\hat{I}(M)$ be the space of skew invariants under W, and let $I_\pi(M)$ be the space of invariants under W_π. Then

$$\Sigma\ (-1)^{\pi}\ \mathrm{tr}\ (\sigma_o,\ I_\pi(M)) = \mathrm{tr}\ (\sigma_o, \hat{I}(M)) .$$

The remainder of the proof proceeds as before.

Lemma 67: The ϵ_j's form a permutation of the ϵ_{oj}'s.

Proof: Set $t = 1$ in Lemma 66. Then (*) 1 has the same multiplicity among the ϵ_j's as among the ϵ_{oj}'s. This is so since otherwise the right side of the expression would have either a root or a pole at $t = 1$. Assume $\sigma_o \neq 1$, then either $\sigma_o^2 = 1$ and all ϵ's not 1 are -1 or else $\sigma_o^3 = 1$ and all ϵ's not 1 are cube roots of 1, coming in conjugate complex pairs since σ_o is real. Thus in all cases (*) implies the lemma.

Proof of Theorem 35: (a) follows from Lemmas 65, 66, 67. Now let C' be the center G_σ. Clearly $C' \supseteq C_\sigma$. Using the corollary to Theorem 33 and an argument similar to that in the proof of Corollary 1(b) to Theorem 4', we see $C' \subseteq H_\sigma \subseteq H$. Since H acts "diagonally," we have $C' \subseteq C$, hence $C' = C_\sigma$, proving (b).

Corollary: The values of $|G_\sigma|$ and $|C_\sigma| = |\mathrm{Hom}\,(L_o/L_1, k^*)\sigma|$ are as follows:

G_σ	ϵ_j's $\neq 1$	$\lvert G_\sigma \rvert$	$\lvert C_\sigma \rvert$
Chevalley group ($\sigma = 1$)	None	(*) $q^N \prod (q^{d_j}-1)$	$\lvert \mathrm{Hom}(L_o/L_1, k^*) \rvert$
${}^2A_n (n \geq 2)$	-1 if d_j is odd	Replace $q^{d_j}-1$ by $q^{d_j}-(-1)^{d_j}$ in (*)	Same change; i.e $(n+1, q+1)$
${}^2E_6$	Same as ${}^2A_n$	Same change as ${}^2A_n$	$(3, q+1)$
${}^2D_n$	-1 for one $d_j = n$	Replace one q^n-1 by q^n+1 in (*)	$(4, q^n+1)$
${}^3D_4$	ω, ω^2 for $d_j = 4, 4$	$q^{12}(q^2-1)(q^6-1) \cdot (q^8+q^4+1)$	1

G_σ	ϵ_j's $\neq 1$	$\lvert G_\sigma \rvert$	$\lvert C_\sigma \rvert$
${}^2C_2$	-1 for $d_j = 4$	$q^4(q^2-1)(q^4+1)$	1
${}^2G_2$	-1 for $d_j = 6$	$q^6(q^2-1)(q^6+1)$	1
${}^2F_4$	-1 for $d_j = 6,12$	$q^{24}(q^2-1)(q^6+1)(q^8-1)$ $(q^{12}+1)$	1

Here ω denotes a primitive cube root of 1 .

Proof (except for $\lvert C_\sigma \rvert$): We consider the cases:

${}^2A_n$. We first note (*) $-1 \in W\sigma_o$. To prove (*) we use the standard coordinates $\{\omega_i \mid 1 \leq i \leq n+1\}$ for A_n . Then σ_o is given by $\omega_i \to -\omega_{n+2-i}$. Since W acts via all permutations of $\{\omega_i\}$, we see $-1 \in W\sigma_o$. Alternatively, since W is transitive on the simple systems (Appendix II.24), there exists $w_o \in W$ such that $w_o(-\Pi) = \Pi$. Hence, $-w_o(-1) = 1$ or σ_o ; i.e., $-1 \in W\sigma_o$. Since there are invariants of odd degree ($d_i = 2,3, \ldots$ or $-1 \in W\sigma_o$. Since there are invariants of even degree and $-1 \notin W$. By (*) σ_o fixes the invariants of even degree and changes the signs of those of odd degree.

${}^2E_6$, ${}^2D_{2n+1}$. The second argument to establish (*) in the case ${}^2A_n$ may be used here, and the same conclusion holds.

${}^2D_n$ (n even or odd). Relative to the standard coordinates $\{v_i \mid 1 \leq i \leq n\}$, the basic invariants are the first n-1 elementary

symmetric polynomials in $\{v_i^2\}$ together with $\prod v_i$, and W acts via all permutations and even number of sign changes. Here σ_o can be taken to be the map $v_i \to v_i$ $(1 \le i \le n-1)$, $v_n \to -v_n$. Hence, only the last invariant changes sign under σ_o.

$\underline{{}^3D_4}$. The degrees of the invariants are 2, 4, 6, and 4. By Lemma 67, the ϵ_j's are $1, 1, \omega, \omega^2$. Since σ_o is real, ω and ω^2 must occur in the same dimension. Thus, we replace $(q^4-1)^2$ in the usual formula by $(q^4-\omega)(q^4-\omega^2) = q^8 + q^4 + 1$.

$\underline{{}^2C_2}$, $\underline{{}^2G_2}$. In both cases the ϵ_j's are 1, -1 by Lemma 67. Since $< W, \sigma_o >$ is a finite group, it fixes some nonzero quadratic form, so that $\epsilon_j = 1$ for $d_j = 2$.

$\underline{{}^2F_4}$. The degrees of the invariants are 2, 6, 8, 12 and the ϵ_j's are 1, 1, -1, -1. As before there is a quadratic invariant fixed by σ_o. Consider $I = \sum_{\alpha \text{ long root}} \alpha^8 + \sum_{\beta \text{ short root}} (\sqrt{2}\,\beta)^8$. We claim that I is an invariant of degree 8 fixed by σ_o and there is a quadratic invariant fixed by σ_o which does not divide I. The first part is clear since W and σ_o preserve lengths and permute the rays through the roots. To see the second part, choose coordinates $\{v_i \mid i = 1, 2, 3, 4\}$ so that the long roots (respectively, the short roots) are the vectors obtained from $2v_1$, $v_1 + v_2 + v_3 + v_4$ (respectively, $v_1 + v_2$) by all permutations and sign changes. The quadratic invariant is $v_1^2 + v_2^2 + v_3^2 + v_4^2$.

To show that this does not divide I, consider the sum of those terms in I which involve only v_1 and v_2 and note that this is not divisible by $v_1^2 + v_2^2$. Hence, I can be taken as one of the basic invariants, and $\epsilon_j = 1$ if $d_j = 8$.

Remark: $|{}^2C_2|$ is not divisible by 3. Aside from cyclic groups of prime order, these are the only known finite simple groups with this property.

Now we consider the automorphisms of the twisted groups. As for the untwisted groups diagonal automorphisms and field automorphisms can be defined.

Theorem 36: Let G and σ be as in this section and G'_σ the subgroup of G (or G_σ) generated by U_σ and U^-_σ. Assume that σ is not the identity. Then every automorphism of G'_σ is a product of an inner, a diagonal, and a field automorphism.

Remark: Observe that graph automorphisms are missing. Thus the twisted groups cannot themselves be twisted, at least not in the simple way we have been considering.

Sketch of proof: As in step (1) of the proof of Theorem 30, the automorphism, call it φ, may be normalized by an inner automorphism so that it fixes U_σ and U^-_σ (in the finite case by Sylow's theorem, in the infinite case by arguments from the theory of algebraic groups). Then it also fixes H'_σ, and it permutes the $\mathcal{X}_a$'s (a a simple, $a \in \Sigma/R$; henceforth we write $\mathcal{X}_a$ for $\mathcal{X}_{a,\sigma}$) and also the $\mathcal{X}_{-a}$'s according to the same permutation,

in an angle preserving manner (see step (2)) in terms of the corresponding simple system Π_σ of V_σ. By checking cases one sees that the permutation is necessarily the identity: if k is finite, one need only compare the various $|\mathcal{X}_a|$'s with each other, while if k is arbitrary further argument is necessary (one can, for example, check which $\mathcal{X}_a$'s are Abelian and which are not, thus ruling out all possibilities except for ${}^2A_3$, ${}^2E_6$, and ${}^3D_4$, and then rule out these cases (the first two together) by considering the commutator relations among the $\mathcal{X}_a$'s). As in step (4) of the proof of Theorem 30, we need only complete the proof of our theorem when G'_σ is one of the groups $G_a = \langle \mathcal{X}_a, \mathcal{X}_{-a} \rangle$, in other words, when G'_σ is of one of the types A_1, ${}^2A_2$, ${}^2C_2$ or ${}^2G_2$ (with ${}^2C_2(2)$ and ${}^2G_2(3)$ excluded, but not $A_1(2)$, $A_1(3)$, or ${}^2A_2(4)$), which we henceforth assume. The case A_1 having been treated in §§ 10, we will treat only the other cases, in a sequence of steps. We write $x(t,u)$ or $x(t,u,v)$ for the general element of U_σ as given in Lemma 63 and $d(s) = h_\alpha(s)h_\beta(s^\theta)$.

(1) We have the equations

$$d(s)x(t,u)d(s)^{-1} = x(s^{2-\theta}t,\ s^{1+\theta}u) \quad \text{in } {}^2A_2$$

$$= x(s^{2-2\theta}t,\ s^{2\theta}u) \quad \text{in } {}^2C_2$$

$$d(s)x(t,u,v)d(s)^{-1} = x(s^{2-3\theta}t,\ s^{-1+3\theta}u,\ sv) \quad \text{in } {}^2G_2 .$$

This follows from the definitions and Lemma 20(c) .

(2) Let U_1, U_2 be the subgroups of U_σ obtained by setting $t = 0$, then also $u = 0$. Then $U_\sigma \supset U_1 \supset U_2 = 1$ is the lower central series $U_\sigma \supset (U_\sigma, U_\sigma) \supset (U_\sigma, (U_\sigma, U_\sigma)) \supset \ldots$ for U_σ if the type is ${}^2A_2$ or ${}^2C_2$, while $U_\sigma \supset U_1 \supset U_2 \supset 1$ is if the type is ${}^2G_2$.

Exercise: Prove this.

(3) If the case ${}^2A_2(4)$ is excluded, then

$$d(s)x(t,\ldots)d(s)^{-1} = x(g(s)t,\ldots) \text{ , with } g: k^* \to k^*$$

a homomorphism whose image generates k additively.

Proof: Consider ${}^2A_2$. By (1) we have $g(s) = s^{2-\theta}$, so that $g(s) = s$ for $s \in k_\theta$. Since $[k: k_\theta] = 2$, we need only show that g takes on a value outside of k_θ . Now if g doesn't, then $s^{2-\theta} = (s^{2-\theta})^\theta$ so that $s^3 \in k_\theta$, for all $s \in k^*$, whence we easily conclude (the reader is asked to supply the proof) that k has at most 4 elements, a contradiction. For ${}^2C_2$ and ${}^2G_2$ the proof is similar, but easier.

(4) The automorphism φ (of G_σ') can be normalized by a diagonal and a field automorphism to be the identity on U_σ/U_1 .

Proof: Since φ fixes U_σ , it also fixes U_1, hence acts on U_σ/U_1 . Thus there is an additive isomorphism $f: k \to k$ such that $\varphi\, x(t,\ldots) = x(f(t), \ldots)$.

By multiplying φ by a diagonal automorphism we may assume $f(1) = 1$. Since φ fixes H_σ°, there is an isomorphism $i : k^* \to k^*$ such that $\varphi d(s) = d(i(s))$. Combining these equations with the one in (3) we get

$$f(g(s)t) = g(i(s))f(t) \quad \text{for all } s \in k^*, \ t \in k.$$

Setting $t = 1$, we get (*) $f(g(s)) = g(i(s))$, so that $f(g(s)t) = f(g(s))f(t)$. If the case ${}^2A_2$ (4) is excluded, then f is multiplicative on k by (3), hence is an automorphism. The same conclusion, however, holds in that case also since f fixes 0 and 1 and permutes the two elements of k not in k_θ.

Our object now is to show that once the normalization in (4) has been attained φ is necessarily the identity.

(5) φ fixes each element of U_1/U_2 and U_2, and also some $w \in G_\sigma^\circ$ which represents the nontrivial element of the Weyl group.

Proof: The first part easily follows from (2) and (4), then the second follows as in the proof of Theorem 33(b).

(6) If the type is ${}^2C_2$ or ${}^2G_2$, then φ is the identity.

Proof: Consider the type ${}^2C_2$. From the equation (*) of (4) and the fact that $f = 1$, we get $g(s) = g(i(s))$, i.e., $s^{2-2\theta} = i(s)^{2-2\theta}$, and then taking the $1 + \theta$ th power, $s = i(s)$; in other words φ fixes every $d(s)$. By (4) and (5), $\varphi x(t,u) = x(t,u + j(t))$ with j an additive homomorphism.

Conjugating this equation by $d(s) = \varphi d(s)$, using (1), and comparing the new equation with the old, we get $j(s^{2-2\theta}t) = s^{2\theta}j(t)$, and on replacing s by $s^{1+\theta}$, $j(st) = s^{1+2\theta}j(t)$. Choosing $s \neq 0, 1$, which is possible because ${}^2C_2(2)$ has been excluded, and replacing s by $s+1$ and by 1 and combining the three equations, we get $(s + s^{2\theta})j(t) = 0$. Now $s + s^{2\theta} \neq 0$, since otherwise we would have $s + s^{2\theta} = (s + s^{2\theta})^{2\theta}$, then $s = s^2$, contrary to the choice of s. Thus $j(t) = 0$. In other words φ fixes every element of U_σ. If the type is ${}^2G_2$ instead, the argument is similar, requiring one extra step. Since G'_σ is generated by U_σ and the element w of (5), φ is the identity.

The preceding argument, slightly modified, barely fails for ${}^2A_2$, in fact fails just for the smallest case ${}^2A_2(4)$. The proof to follow, however, works in all cases.

(7) If the type is ${}^2A_2$, then φ is the identity.

Proof: Choose w as in (5) and, assuming $u \neq 0$, write $wx(t,u)w^{-1} = xnx'$ with $x, x' \in U_\sigma$, $n \in H'_\sigma - w$. A simple calculation in SL_3 shows that $x = x(at\bar{u}^{-1}, *)$ for some $a \in k^*$ depending on w but not on t or u. (Prove this.) If now we write $\varphi x(t,u) = x(t, u + j(t))$, apply φ to the above equation, and use (4) and (5), we get $t\bar{u}^{-1} = t(\overline{u + j(t)})^{-1}$, so that $j(t) = 0$ and we may complete the proof as before.

It is also possible to determine the isomorphisms among the various Chevalley groups, both twisted and untwisted. We state the results for the finite groups, omitting the proofs.

Theorem 37 : (a) Among the finite simple Chevalley groups, their twisted analogues, and the alternating groups $\mathcal{A}_n (n \geq 5)$, a complete list of isomorphisms is given as follows.

(1) Those independent of k.

$C_1 \sim B_1 \sim A_1$

$C_2 \sim B_2$

$D_2 \sim A_1 \times A_1$ $\qquad$ ${}^2D_2 \sim {}^2(A_1 \times A_1) \sim A_1$

$D_3 \sim A_3$ $\qquad$ ${}^2D_3 \sim {}^2A_3$

${}^2A_1(q^2) \sim A_1(q)$

(2) $B_n(q) \sim C_n(q)$ if q is even.

(3) Just six other cases, of the indicated orders.

$A_1(4) \sim A_1(5) \sim \mathcal{A}_5$	60
$A_1(7) \sim A_2(2)$	168
$A_1(9) \sim \mathcal{A}_6$	360
$A_3(2) \sim \mathcal{A}_8$	20160
${}^2A_3(4) \sim B_2(3)$	25920

(b) In addition there are the following cases in which the Chevalley group just fails to be simple.

The derived group of	$B_2(2) \sim \mathcal{A}_6$	360
	$G_2(2) \sim {}^2A_2(9)$	6048
	${}^2G_2(3) \sim A_1(8)$	504
	${}^2F_4(2)$	

The indices in the original group are 2, 3, 2, 2, respectively.

Remarks: (a) The existence of the isomorphisms in (1) and (2) is easy, and in (3) is proved, e.g., in Dieudonné (Can. J. Math. 1949). There also the first case of (b), considered in the form $B_2(2) \sim S_6$ (symmetric group) is proved.

(b) It is natural to include the simple groups $\mathcal{A}_n$ in the above comparison since they are the derived groups of the Weyl groups of type A_{n-1} and the Weyl groups in a sense form the skeletons of the corresponding Chevalley groups. We would like to point out that the Weyl groups $W(E_n)$ are also almost simple and are related to earlier groups as follows.

Proposition: We have the isomorphisms:

$\mathcal{D}\, W(E_6) \sim B_2(3) \sim {}^2A_3(4)$

$\mathcal{D}\, W(E_7) \sim C_3(2)$

$\mathcal{D}\, W(E_8)/C \sim D_4(2)$, with C the center, of order 2.

Proof: The proof is similar to the proof of $S_6 = W(A_5) \sim B_2(2)$ given near the beginning of § 10.

Aside from the cyclic groups of prime order and the groups considered above, only 11 or 12 other finite simple groups are at present (May,1968) known. We will discuss them briefly.

(a) The five Mathieu groups M_n $(n = 11, 12, 22, 23, 24)$. These were discovered by Mathieu about a hundred years ago and put on a firm footing by Witt (Hamburger Abh. 12 (1938)). They arise as highly transitive permutation groups on the indicated numbers of letters. Their orders are:

$|M_{11}| = 7920 = 8.9.10.11$

$|M_{12}| = 95040 = 8.9.10.11.12$

$|M_{22}| = 443520 = 48.20.21.22$

$|M_{23}| = 10200960 = 48.20.21.22.23$

$|M_{24}| = 244823040 = 48.20.21.22.23.24$.

(b) The first Janko group J_1 discovered by Janko (J. Algebra 3 (1966)) about five years ago. It is a subgroup of $G_2(11)$ and can be represented as a permutation group on 266 letters. Its order is

$$|J_1| = 175560 = 11(11 + 1)(11^3 - 1) = 19.20.21.22 = 55.56.57 .$$

The remaining groups were all uncovered last fall, more or less.

(c) The groups J_2 and $J_{2\ 1/2}$ of Janko. The existence of J_2 was put on a firm basis first by Hall and Wales using a machine, and then by Tits in terms of a "geometry." It has a subgroup of index 100 isomorphic to $\mathcal{U}G_2(2) \sim {}^2A_2(9)$, and is itself of index 416 in $G_2(4)$. The group $J_{2\ 1/2}$ has not yet been put on a firm basis, and it appears that it will take a great deal of work to do so (because it does not seem to have any "large" subgroups), but the evidence for its existence is overwhelming. The orders are:

$$|J_2| = 604800$$

$$|J_{2\ 1/2}| = 50232960 .$$

(d) The group H of D. Higman and Sims, and the group H' of G. Higman. The first group contains M_{22} as a subgroup of index 100 and was constructed in terms of the automorphism group of a graph with 100 vertices whose existence depends on properties of Steiner systems. Inspired by this construction, G. Higman then constructed his own group in terms of a very special geometry invented for the occasion. The two groups have the same order, and everyone seems to feel that they are isomorphic, but no one has yet proved this. The order is:

$$|H| = |H'| = 44352000 .$$

(e) The (latest) group S of Suzuki. This contains $G_2(4)$ as a subgroup of index 1782, and is contructed in terms of a graph whose existence depends on the imbedding $J_2 \subset G_2(4)$. It possesses

an involutory automorphism whose set of fixed points is exactly J_2. Its order is:

$|S| = 448345497600$.

(f) The group M of McLaughlin. This group is constructed in terms of a graph and contains ${}^2A_3(9)$ as a subgroup of index 275. Its order is:

$|M| = 898128000$.

Theorem 38: Among all the finite simple groups above (i.e., all that are currently known), the only coincidences in the orders which do not come from isomorphisms are:

(a) $B_n(q)$ and $C_n(q)$ for $n \geq 3$ and q odd.

(b) $A_2(4)$ and $A_3(2) \sim A_8$.

(c) H and H' if they aren't isomorphic.

That the groups in (a) have the same order and are not isomorphic has been proved earlier. The orders in (b) are both equal to 20160 by Theorem 25, and the groups are not isomorphic since relative to the normalizer B of a 2-Sylow subgroup the first group has six double cosets and the second has 24. The proof that (a), (b) and (c) represent the only possibilities depends on an exhaustive analysis of the group orders which can not be undertaken here.

§12. Representations. In this section we consider the irreducible representations of the infinite Chevalley groups. As we shall see, here the theory is quite complete. All representations are assumed to be finite-dimensional and the standard terminology is used. In particular 1 must act as the identity, and the trivial 0-dimensional (but not the trivial 1-dimensional) representation is excluded from the list of irreducible representations. We start with a general lemma.

Lemma 68: Let K be an algebraically closed field, B and C associative algebras with 1 over K, and $A = B \otimes C$.

(a) If (β,V) and (γ,W) are (finite-dimensional) irreducible modules for B and C, then $(\alpha,U) = (\beta \otimes \gamma, V \otimes W)$ is one for A.

(b) Conversely, every irreducible A-module (α,U) is realizable, uniquely, as a tensor product as in (a).

Proof: (a) By Burnside's Theorem (see, e.g., Jacobson, Lectures in Abstract Algebra, Vol. 2), $\beta B = \operatorname{End} V$ and $\gamma C = \operatorname{End} W$, whence $\alpha A = \operatorname{End} U$ and (α,U) is irreducible.

(b) Let V be an irreducible B-submodule of U. Such exist since U is finite-dimensional. Let L be the space of B-homomorphisms of V into U. This is nonzero and is a C-module under the rule $c\iota = \alpha(c) \circ \iota$. (Check this.) Let (γ,W) be an irreducible submodule. The map $\varphi: V \otimes W \longrightarrow U$ defined by $v \otimes f \longrightarrow f(v)$ is easily checked to be an A-homomorphism. $V \otimes W$ is irreducible by (a), and U is by assumption. Hence by Schur's