Steinberg, Robert, 1922-

LECTURES ON CHEVALLEY GROUPS

Robert Steinberg

Yale University

1967

Notes prepared by

John Faulkner and Robert Wilson

This work was partially supported by Contract ARO-D-336-8230-31-43033.

Acknowledgement

These notes are dedicated to my wife, Maria. They might also have been dedicated to the Yale Mathematics Department typing staff whose uniformly high standards will become apparent to anyone reading the notes. Needless to say, I am greatly indebted to John Faulkner and Robert Wilson for writing up a major part of the notes. Finally, it is a pleasure to acknowledge the great stimulus derived from my class and from many colleagues, too many to mention by name, during my stay at Yale.

Robert Steinberg

June, 1968

Guide to the Reader

These notes presuppose the theory of complex semisimple Lie algebras through the classification, as may be found, for example, in the books of E. B. Dynkin, N. Jacobson, or J.-P. Serre, or in the notes of Séminaire Sophus Lie. An appendix dealing with the most frequently needed results about finite reflection groups and root systems has been included. The reader is advised to read this part first. This he can do rather quickly.

TABLE OF CONTENTS

Lectures on Chevalley Groups

§1. A basis for $\mathcal{L}$

We start with some basic properties of semisimple Lie algebras over $\mathbb{C}$, and establish some notation to be used throughout. The assertions not proved here are proved in the standard books on Lie algebras, e.g., those of Dynkin, Jacobson or Sophus Lie (Séminaire).

Let $\mathcal{L}$ be a semisimple Lie algebra over $\mathbb{C}$, and $\mathcal{H}$ a Cartan subalgebra of $\mathcal{L}$. Then $\mathcal{H}$ is necessarily Abelian and $\mathcal{L} = \mathcal{H} \oplus \sum_{\alpha \neq 0} \mathcal{L}_\alpha$ where $\alpha \in \mathcal{H}^*$ and $\mathcal{L}_\alpha$ $= \{X \in \mathcal{L} \mid [H,X] = \alpha(H)X \text{ for all } H \in \mathcal{H}\}$. Note that $\mathcal{H} = \mathcal{L}_0$. The α's are linear functions on $\mathcal{H}$, called <u>roots</u>. We adopt the convention that $\mathcal{L}_\gamma = 0$ if γ is not a root. Then $[\mathcal{L}_\alpha, \mathcal{L}_\beta] \subseteq \mathcal{L}_{\alpha+\beta}$. The rank of $\mathcal{L} = \dim_{\mathbb{C}} \mathcal{H} = \ell$, say. The roots generate $\mathcal{H}^*$ as a vector space over $\mathbb{C}$.

Write V for $\mathcal{H}^*_{\mathbb{Q}}$, the vector space over $\mathbb{Q}$ generated by the roots. Then $\dim_{\mathbb{Q}} V = \ell$. Let $\gamma \in V$. Since the Killing form is nondegenerate there exists an $H'_\gamma \in \mathcal{H}$ such that $(H,H'_\gamma) = \gamma(H)$ for all $H \in \mathcal{H}$. Define $(\gamma,\delta) = (H'_\gamma, H'_\delta)$ for all $\gamma, \delta \in V$. This is a symmetric, nondegenerate, positive definite bilinear form on V.

Denote the collection of all roots by Σ. Then Σ is a subset of the nonzero elements of V satisfying:

(0) Σ generates V as a vector space over $\mathbb{Q}$.

(1) $\alpha \in \Sigma \Longrightarrow -\alpha \in \Sigma$ and $k\alpha \notin \Sigma$ for k an integer $\neq \pm 1$.

(2) $2(\alpha,\beta)/(\beta,\beta) \in \mathbb{Z}$ for all $\alpha, \beta \in \Sigma$. (Write $<\alpha,\beta> = 2(\alpha,\beta)/(\beta,\beta)$. These are called Cartan integers).

(3) Σ is invariant under all reflections $w_\alpha(\alpha \in \Sigma)$ (where w_α is the reflection in the hyperplane orthogonal to α , i.e., $w_\alpha v = v - 2(v,\alpha)/(\alpha,\alpha)\ \alpha)$.

Thus Σ is a root system in the sense of Appendix I. Conversely, if Σ is any root system satisfying condition (2), then Σ is the root system of some Lie algebra.

The group W generated by all w_α is a finite group (Appendix I.6) called the Weyl group. If $\{\alpha_1, \ldots, \alpha_\ell\}$ is a simple system of roots (Appendix I.8), then W is generated by the w_{α_i} $(i = 1, \ldots, n)$ (Appendix I.16) and every root is congruent under W to a simple root (Appendix I.15).

Lemma 1: For each root α , let $H'_\alpha \in \mathcal{H}$ be such that $(H,H'_\alpha) = \alpha(H)$ for all $H \in \mathcal{H}$. Define $H_\alpha = 2/(\alpha,\alpha)\ H'_\alpha$ and $H_i = H_{\alpha_i}$ $(i = 1, \ldots, \ell)$. Then each H_α is an integral linear combination of the H_i .

Proof: Write w_i for $w_{\alpha_i} \in W$. Define an action of W on $\mathcal{H}$ by $w_i H'_j = H'_j - <\alpha_j,\alpha_i> H'_i$.

Then

$$w_i H_j = \frac{2}{(\alpha_j,\alpha_j)} w_i H'_j$$

$$= \frac{2}{(\alpha_j,\alpha_j)} H'_j - \frac{2}{(\alpha_j,\alpha_j)} \cdot \frac{2(\alpha_i,\alpha_j)}{(\alpha_i,\alpha_i)} H'_i$$

$$= H_j - \frac{2}{(\alpha_i,\alpha_i)} \cdot \frac{2(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)} H'_i$$

$$= H_j - < \alpha_i,\alpha_j > H_i$$

$$= H_{w_i \alpha_j}$$

Then since the w_i generate W, wH_j is an integral linear combination of the H_i for all $w \in W$. Now if α is an arbitrary root then $\alpha = w\alpha_j$ for some $w \in W$ and some j. Then $H_\alpha = H_{w\alpha_j} = wH_{\alpha_j} = wH_j$ = an integral linear combination of the H_i.

For every root α choose $X_\alpha \in \mathcal{L}_\alpha$, $X_\alpha \neq 0$. If $\alpha + \beta \neq 0$ define $N_{\alpha,\beta}$ by $[X_\alpha, X_\beta] = N_{\alpha,\beta} X_{\alpha+\beta}$. Set $N_{\alpha,\beta} = 0$ if $\alpha + \beta$ is not a root.

If α and β are roots the <u>α-string of roots through β</u> is the sequence $\beta - r\alpha, \ldots, \beta, \ldots, \beta + q\alpha$ where $\beta + i\alpha$ is a root for $-r \leq i \leq q$ but $\beta - (r+1)\alpha$ and $\beta + (q+1)\alpha$ are not roots.

<u>Lemma 2:</u> The X_α can be chosen so that:

(a) $[X_\alpha, X_{-\alpha}] = H_\alpha$.

(b) If α and β are roots, $\beta \neq \pm \alpha$, and $\beta - r\alpha, \ldots, \beta, \ldots \beta + q\alpha$ is the α-string of roots through β then $N^2_{\alpha,\beta} = q(r+1)|\alpha+\beta|^2/|\beta|^2$.

Proof: See the first part of the proof of Theorem 10, p. 147 in Jacobson, Lie Algebras.

Lemma 3: If α, β and $\alpha + \beta$ are roots, then $q(r+1)|\alpha+\beta|^2/|\beta|^2 = (r+1)^2$.

Proof: We use two facts:

(*) $r - q = <\beta,\alpha>$.

(For w_α maps $\beta - r\alpha$ to $\beta + q\alpha$ so $\beta + q\alpha = w_\alpha(\beta - r\alpha) = \beta - r\alpha - 2(\beta - r\alpha,\alpha)/(\alpha,\alpha)\alpha = \beta - <\beta,\alpha>\alpha + r\alpha)$.

(**) In the α-string of roots through β at most two root lengths occur.

(For if V' is the vector space over Q generated by α and β and $\Sigma' = \Sigma \cap V$, then Σ' is a root system and every root in the α-string of roots through β belongs to Σ' . Now V' is two dimensional; so a system of simple roots for Σ' has at most two elements. Since every root in Σ' is conjugate under the Weyl group of Σ' to a simple root, Σ' and hence the α-string of roots through β has at most two root lengths).

We must show that $q|\alpha+\beta|^2/|\beta|^2 = r + 1$. Now by (*):

$$r + 1 - q|\alpha+\beta|^2/|\beta|^2 = q + <\beta,\alpha> + 1 - q\,(\alpha+\beta,\alpha+\beta)/(\beta,\beta)$$

$$= <\beta,\alpha> + 1 - q|\alpha|^2/|\beta|^2 - q<\alpha,\beta>$$

$$= (<\beta,\alpha> + 1)(1 - q|\alpha|^2/|\beta|^2) .$$

Set $A = <\beta,\alpha> + 1$ and $B = 1 - q|\alpha|^2/|\beta|^2$.
We must show $A = 0$ or $B = 0$.

If $|\alpha| \geq |\beta|$ then $|<\beta,\alpha>| = 2|(\beta,\alpha)|/|\alpha|^2 \leq 2|(\beta,\alpha)|/|\beta|^2 = |<\alpha,\beta>|$. By Schwarz's inequality $<\beta,\alpha><\alpha,\beta> = 4\,(\alpha,\beta)^2/|\alpha||\beta| \leq 4$ with equality if and only if $\alpha = k\beta$. Since α and β are roots and $\alpha \neq \pm\beta$ we have $\alpha \neq k\beta$ so $<\beta,\alpha><\alpha,\beta> < 4$. Then since $|<\beta,\alpha>| \leq |<\alpha,\beta>|$ we have $<\beta,\alpha> = -1$, 0, or 1 . If $<\beta,\alpha> = -1$ then $A = 0$. If $<\beta,\alpha> \geq 0$ then $|\beta + 2\alpha| > |\beta + \alpha| > |\beta|$. Since there are only two root lengths $\beta + 2\alpha$ is not a root and hence $q = 1$. Since $|\beta + \alpha| > |\alpha|$ and $|\beta + \alpha| > |\beta|$ and at most two root lengths occur $|\alpha| = |\beta|$. Hence $B = 0$.

If $|\alpha| < |\beta|$, then $|\alpha + \beta| \leq |\beta|$ (since otherwise three root lengths would occur). Hence $(\alpha,\beta) < 0$ so $<\alpha,\beta> < 0$. Then $|\beta - \alpha| > |\beta| > |\alpha|$ so $\beta - \alpha$ is not a root and hence $r = 0$. As above $<\alpha,\beta><\beta,\alpha> < 4$ and $|<\alpha,\beta>| < |<\beta,\alpha>|$ so $<\alpha,\beta> = -1$, 0, or 1 . Hence $<\alpha,\beta> = -1$. Then by (*) $q = -<\beta,\alpha> = <\beta,\alpha>/<\alpha,\beta> = |\beta|^2/|\alpha|^2$. Hence $B = 0$.

We collect these results in:

Theorem 1: The H_i $(i=1, 2, \ldots, \ell)$ chosen as in Lemma 1 together with the X_α chosen as in Lemma 2 form a basis for $\mathcal{L}$ relative to which the equations of structure are as follows (and, in particular, are integral):

(a) $[H_i, H_j] = 0$

(b) $[H_i, X_\alpha] = <\alpha, \alpha_i> X_\alpha$

(c) $[X_\alpha, X_{-\alpha}] = H_\alpha =$ an integral linear combination of the H_i.

(d) $[X_\alpha, X_\beta] = \pm (r+1) X_{\alpha+\beta}$ if $\alpha+\beta$ is a root.

(e) $[X_\alpha, X_\beta] = 0$ if $\alpha + \beta \neq 0$ and $\alpha+\beta$ is not a root.

Proof: (a) holds since $\mathcal{H}$ is abelian. (b) holds since $[H_\beta, X_\alpha] = \alpha(H_\beta) X_\alpha = <\alpha, \beta> X_\alpha$. (c) follows from the choice of the X_α and the H_i and from Lemma 1. (d) follows from Lemma 2(b) and Lemma 3. . (e) holds since $[\mathcal{L}_\alpha, \mathcal{L}_\beta] = 0$ if $\alpha+\beta$ is not a root.

Remarks: (a) Such a basis is called a Chevalley basis. It is unique up to sign changes and automorphisms of $\mathcal{L}$.

(b) X_α, $X_{-\alpha}$ and H_α span a 3-dimensional subalgebra isomorphic to $s\ell_2$ (2x2 matrices of trace 0).

$$X_\alpha \longleftrightarrow \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad X_{-\alpha} \longleftrightarrow \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad H_\alpha \longleftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(c) As an example let $\mathcal{L} = s\ell_{\ell+1}$.

Then $\mathcal{H}$ = {diagonal matrices} is a Cartan subalgebra. For $i,j = 1, \ldots, \ell+1$, $i \neq j$, define $\alpha = \alpha(i,j)$ by $\alpha(i,j)$: $\mathrm{diag}(a_1, \ldots, a_{\ell+1}) \longrightarrow a_i - a_j$. Then the $\alpha(i,j)$ are the roots. Let $E_{i,j}$ be the matrix unit with 1 in the (i,j) position and 0 elsewhere. Then $X_\alpha = E_{i,j}$, $X_{-\alpha} = E_{j,i}$, $H_{\alpha(i,j)} = E_{i,i} - E_{j,j}$ and $H_i = E_{i,i} - E_{i+1,i+1}$.

Exercise: If only one root length occurs then all coefficients in (d) of Theorem 1 are ± 1. Otherwise ± 2 and ± 3 can occur.

§2. A basis for $\mathcal{U}$

Let $\mathcal{L}$ be a Lie algebra over a field k and $\mathcal{U}$ an associative algebra over k. We say that $\varphi : \mathcal{L} \longrightarrow \mathcal{U}$ is a homomorphism if:

(1) φ is linear.

(2) $\varphi[X,Y] = \varphi(X)\varphi(Y) - \varphi(Y)\varphi(X)$ for all $X, Y \in \mathcal{L}$.

A universal enveloping algebra of a Lie algebra $\mathcal{L}$ is a couple $(\mathcal{U},\varphi)$ such that:

(1) $\mathcal{U}$ is an associative algebra with 1.

(2) φ is a homomorphism of $\mathcal{L}$ into $\mathcal{U}$.

(3) If $(\mathcal{A}, \psi)$ is any other such couple then there exists a unique homomorphism $\theta : \mathcal{U} \longrightarrow \mathcal{A}$ such that $\theta \circ \varphi = \psi$ and $\theta\, 1 = 1$.

For the existence and uniqueness of $(\mathcal{U}, \varphi)$ see, e.g., Jacobson, Lie Algebras.

Birkhoff-Witt Theorem: Let $\mathcal{L}$ be a Lie algebra over a field k and $(\mathcal{U}, \varphi)$ its universal enveloping algebra. Then:

(a) φ is injective.

(b) If $\mathcal{L}$ is identified with its image in $\mathcal{U}$ and if $X_1, X_2, \ldots, X_r$ is a linear basis for $\mathcal{L}$, the monomials $X_1^{k_1} X_2^{k_2} \ldots X_r^{k_r}$ form a basis for $\mathcal{U}$ (where the k_i are nonnegative integers).

The proof here too can be found in Jacobson.

Theorem 2: Assume the basis elements $\{H_i, X_\alpha\}$ of $\mathcal{L}$ are as in Theorem 1 and are arranged in some order. For each choice of numbers $n_i, m_\alpha \in \mathbb{Z}^+$ $(i = 1, 2, \ldots, \ell\ ;\ \alpha \in \Sigma)$ form the product, in $\mathcal{U}$, of all $\binom{H_i}{n_i}$ and $X_\alpha^{m_\alpha}/m_\alpha!$ according to the given order. The resulting collection is a basis for the $\mathbb{Z}$-algebra $\mathcal{U}_{\mathbb{Z}}$ generated by all $X_\alpha^m/m!$ $(m \in \mathbb{Z}^+\ ;\ \alpha \in \Sigma)$.

Remark: The collection is a $\mathbb{C}$-basis for $\mathcal{U}$ by the Birkhoff-Witt Theorem.

The proof of Theorem 2 will depend on a sequence of lemmas.

Lemma 4: Every polynomial over $\mathbb{C}$ in ℓ variables $H_1, \ldots H_\ell$ which takes on integral values at all integral values of the variables is an integral combination of the polynomials

$\prod_{i=1}^{\ell} \binom{H_i}{n_i}$ where $n_i \in \mathbb{Z}^+$ and $n_i \leq$ degree of the polynomial in H_i (and conversely, of course).

Proof: Let f be such a polynomial. We may write

$f = \sum_{j=0}^{r} f_j \binom{H_\ell}{j}$, each f_j being a polynomial in $H_1, \ldots, H_{\ell-1}$.

We replace H_ℓ by $H_\ell + 1$ and take the difference. If we do this r times we get f_r. Assuming the lemma true for polynomials in ℓ-1 variables (it clearly holds for polynomials in no variables), hence for f_r, we may subtract the term $f_r\binom{H_\ell}{r}$ from f and complete the proof by induction on r.

Lemma 5: If α is a root and we write X, Y, H for $X_\alpha, X_{-\alpha}, H_\alpha$, then

$$(X^m/m!)(Y^n/n!) = \sum_{j=0}^{\min(m,n)} (Y^{n-j}/(n-j)!)\binom{H-m-n+2j}{j}(X^{m-j}/(m-j)!)$$

Proof: The case $m = n = 1$, $XY = YX + H$, together with induction on n yield $X(Y^n/n!) = (Y^n/n!)X + (Y^{n-1}/(n-1)!)(H-n+1)$. This equation and induction on m yield the lemma.

Corollary: Each $\binom{H_\alpha}{n}$ is in $\mathcal{U}_{\mathbb{Z}}$.

Proof: Set $m=n$ in Lemma 5, write the right side as $\binom{H}{n} + \sum_{j=0}^{n-1} (Y^{n-j}/(n-j)!)\binom{H-2n+2j}{j}(X^{n-j}/(n-j)!)$, then use induction on n and Lemma 4.

Lemma 6: Let $\mathcal{L}_{\mathbb{Z}}$ be the $\mathbb{Z}$-span of the basis $\{H_i, X_\alpha\}$ of $\mathcal{L}$. Then under the adjoint representation, extended to $\mathcal{U}$, every $X_\alpha^m/m!$ preserves $\mathcal{L}_{\mathbb{Z}}$, and the same holds for $\mathcal{L}_{\mathbb{Z}} \otimes \mathcal{L}_{\mathbb{Z}} \otimes \dots$, any number of factors.

Proof: Making $X_\alpha^m/m!$ act on the basis of $\mathcal{L}_{\mathbb{Z}}$ we get

$(X_\alpha^m/m!)\cdot X_\beta = \pm (r+1)(r+2) \dots (r+m-1)/m! X_{\beta+m\alpha}$ if $\beta \neq -\alpha$ (see the definition of $r = r(\alpha,\beta)$ in Theorem 1),

$X_\alpha \cdot X_{-\alpha} = H_\alpha$, $(X_\alpha^2/2)\cdot X_{-\alpha} = -X_\alpha$, $X_\alpha \cdot H_i = -\langle \alpha, \alpha_i \rangle X_\alpha$,

and 0 in all other cases, which proves $\mathcal{L}_{\mathbb{Z}}$ is preserved. The second part follows by induction on the number of factors and:

Lemma 7: Let U and V be $\mathcal{L}$-modules and A and B additive subgroups thereof. If A and B are preserved by every $X_\alpha^m/m!$ then so is $A \otimes B$ (in $U \otimes V$).

Proof: Since X acts on $U \otimes V$ as $X \otimes 1 + 1 \otimes X$ it follows from the binomial expansion that $X^m/m!$ acts as $\Sigma\, X^j/j! \otimes X^{m-j}/(m-j)!$, whence the lemma.

Lemma 8: Let S be a set of roots such that (a) $\alpha \in S \Rightarrow -\alpha \notin S$ and (b) $\alpha, \beta \in S$, $\alpha + \beta \in \Sigma \Rightarrow \alpha + \beta \in S$ (e.g. the set of positive roots), arranged in some order. Then $\{ \prod_{\alpha \in S} X_\alpha^{m_\alpha}/m_\alpha! \mid m_\alpha \geq 0 \}$

is a basis for the $\mathbb{Z}$-algebra $\mathcal{A}$ generated by all $X_\alpha^m/m!$ ($\alpha \in S$; $m \geq 0$) .

Proof: By the Birkhoff-Witt Theorem applied to the Lie algebra for which $\{X_\alpha | \alpha \in S\}$ is a basis we see that every $A \in \mathcal{A}$ is a complex combination of the given elements. We must show all coefficients are integers. Write $A = c \prod X_\alpha^{m_\alpha}/m_\alpha! +$ terms of at most the same total degree. We make A act on $\mathcal{L} \otimes \mathcal{L} \otimes \cdots$ ($\Sigma\, m_\alpha$ copies) and look for the component of $A \cdot \bigotimes_\alpha \underbrace{X_{-\alpha} \otimes \cdots \otimes X_{-\alpha}}_{m_\alpha \text{ copies}}$ in $\mathcal{H} \otimes \mathcal{H} \otimes \cdots$. Any term of A other than the first leads to a zero component since there are either not enough factors (at least one is needed for each $X_{-\alpha}$) or barely enough but with the wrong distribution (since $X_\beta \cdot X_{-\alpha}$ is a nonzero element of $\mathcal{H}$ only if $\beta = \alpha$) , while the first leads to a non-zero component only if the X_α's and the $X_{-\alpha}$'s are matched up, in all possible permutations. It follows that the component sought is $cH_\alpha \otimes \cdots \otimes H_\alpha$. Now each H_α is a primitive element of $\mathcal{L}_\mathbb{Z}$ (to see this imbed α in a simple system of roots and then use Lemma 1). Since A preserves $\mathcal{L}_\mathbb{Z} \otimes \mathcal{L}_\mathbb{Z} \otimes \cdots$ by Lemma 6 it follows that $c \in \mathbb{Z}$, whence Lemma 8.

Any formal product of elements of $\mathcal{U}$ of the form $\binom{H_i - k}{n}$ or $X_\alpha^m/m!$ ($m, n \in \mathbb{Z}^+$; $k \in \mathbb{Z}$) will be called a monomial and the total degree in the X's its degree.

Lemma 9: If $\beta, \gamma \in \Sigma$ and $m, n \in \mathbb{Z}^+$, then $(X_\gamma^m/m!)(X_\beta^n/n!)$ is an integral combination of $(X_\beta^n/n!)(X_\gamma^m/m!)$ and monomials of lower degree.

Proof: This holds if $\beta = \gamma$ obviously and if $\beta = -\gamma$ by Lemma 5. Assume $\beta \neq \pm \gamma$. By Lemma 8 applied to the set S of roots of the form $i\gamma + j\beta$ $(i, j \in \mathbb{Z}^+)$, arranged in the order $\beta, \gamma, \beta + \gamma, \cdots$ we see that $(X_\gamma^m/m!)(X_\beta^n/n!)$ is an integral combination of terms of the form $(X_\beta^b/b!)(X_\gamma^c/c!)(X_{\beta+\gamma}^d/d!)\cdots$. The map $X_\alpha \longrightarrow \alpha$ $(\alpha \in S)$ leads to a grading of the algebra $\mathcal{A}$ with values in the additive group generated by S. The left side of the preceding equation has degree $n\beta + m\gamma$. Hence so does each term on the right, whence $b, c, \cdots$ are restricted by the condition $b\beta + c\gamma + d(\beta+\gamma) + \cdots = n\beta + m\gamma$, hence also by $b + c + 2d + \cdots = n + m$. Clearly $b + c + d + \cdots$, the ordinary degree of the above term, can be as large as $n + m$ only if $b + c = n + m$ and $d = \cdots = 0$ by the last condition, and then $b = n$ and $c = m$ by the first, which proves Lemma 9.

Lemma 10: If α and β are roots and f is any polynomial, then $X_\alpha^n f(H_\beta) = f(H_\beta - n\alpha(H_\beta))X_\alpha^n$.

Proof: By linearity this need only be proved when f is a power of H_β and then it easily follows by induction on the two exponents starting with the equation $X_\alpha H_\beta = (H_\beta - \alpha(H_\beta))X_\alpha$.

Observe that each $\alpha(H_\beta)$ is an integer.

Now we can prove Theorem 2. By the corollary to Lemma 5

each $\binom{H_i}{n}$ is in $\mathcal{U}_{\mathbb{Z}}$, hence so is each of the proposed basis elements. We must show that each element of $\mathcal{U}_{\mathbb{Z}}$ is an integral combination of the latter elements, and for this it suffices to show that each monomial is. Any monomial may, by induction on the degree, Lemma 9, and Lemma 10, be expressed as an integral combination of monomials such that for each α the X_α terms all come together and in the order of the roots prescribed by Theorem 2, then also such that each α is represented at most once, because $(X^m/m!)(X^n/n!) = \binom{m+n}{n} X^{m+n}/(m+n)!$. The H terms may now be brought to the front (see Lemma 10), the resulting polynomial expressed as an integral combination of $\prod \binom{H_i}{n_i}$'s by Lemma 4, each H_i term shifted to the position prescribed by Theorem 2, and Lemma 4 used for each H_i separately, to yield finally an integral combination of basis elements, as required.

Let $\mathcal{L}$ be a semisimple Lie algebra having Cartan subalgebra $\mathcal{H}$. Let V be a representation space for $\mathcal{L}$. We call a vector $v \in V$ a <u>weight vector</u> if there is a linear function λ on $\mathcal{H}$ such that $Hv = \lambda(H)v$ for all $H \in \mathcal{H}$. If such a $v \neq 0$ exists, we call the corresponding λ a <u>weight</u> of the representation.

<u>Lemma 11</u>: If v is a weight vector belonging to the weight λ, then for α a root we have $X_\alpha v$ is a weight vector belonging to the weight $\lambda + \alpha$, if $X_\alpha v \neq 0$.

<u>Proof</u>: If $H \in \mathcal{H}$, then $HX_\alpha v = X_\alpha(H + \alpha(H))v = (\lambda + \alpha)(H)X_\alpha v$.

Theorem 3: If $\mathcal{L}$ is a semisimple Lie algebra having Cartan subalgebra $\mathcal{H}$, then

(a) Every finite dimensional irreducible $\mathcal{L}$-module V contains a nonzero vector v^+ such that v^+ is a weight vector belonging to some weight λ and $X_\alpha v^+ = 0$ $(\alpha > 0)$.

(b) It then follows that if V_λ is the subspace of V consisting of weight vectors belonging to λ, then $\dim V_\lambda = 1$. Moreover, every weight μ has the form $\lambda - \Sigma\alpha$, where the α's are positive roots. Also, $V = \Sigma V_\mu$ (μ a weight).

(c) The weight λ and the line containing v^+ are uniquely determined.

(d) $\lambda(H_\alpha) \in \mathbb{Z}^+$ for $\alpha > 0$.

(e) Given any linear function λ satisfying (d), then there is a unique finite dimensional $\mathcal{L}$-module V in which λ is realized as in (a).

Proof: (a) There exists at least one weight on V since $\mathcal{H}$ acts as an Abelian set of endomorphisms. We introduce a partial order on the weights by $\mu < \nu$ if $\nu - \mu = \Sigma\alpha$ (α a positive root). Since the weights are finite in number, we have a maximal weight λ. Let v^+ be a nonzero weight vector belonging to λ. Since $\lambda + \alpha$ is not a weight for $\alpha > 0$, we have by Lemma 11 that $X_\alpha v^+ = 0$ $(\alpha > 0)$.

(b) and (c) Now let $W = \mathbb{C} v^+ + \sum_{\mu < \lambda} V_\mu$. Let $\mathcal{L}^-$ ($\mathcal{L}^+$) be the Lie subalgebra of $\mathcal{L}$ generated by X_α with $\alpha < 0$ ($\alpha > 0$). Let $\mathcal{U}^-$, $\mathcal{U}^\circ$, and $\mathcal{U}^+$ be the universal enveloping algebras of $\mathcal{L}^-$, $\mathcal{H}$, and $\mathcal{L}^+$ respectively. By the Birkhoff-Witt theorem, $\mathcal{U}^-$ has a basis $\{\prod_{\alpha<0} X_\alpha^{m(\alpha)}\}$, $\mathcal{U}^\circ$ has a basis $\{\prod_{i=1}^{\ell} H_i^{n_i}\}$, $\mathcal{U}^+$ has a basis $\{\prod_{\alpha>0} X_\alpha^{p(\alpha)}\}$, and $\mathcal{U}$, the universal enveloping algebra of $\mathcal{L}$, has a basis

$$\{\prod_{\alpha<0} X_\alpha^{m(\alpha)} \prod_{i=1}^{\ell} H_i^{n_i} X_\alpha^{p(\alpha)}\} \text{ where } m(\alpha),\ n_i,\ p(\alpha) \in \mathbb{Z}^+.$$

Hence, $\mathcal{U} = \mathcal{U}^- \mathcal{U}^\circ \mathcal{U}^+$. Now W is invariant under $\mathcal{U}^-$. Also, $V = \mathcal{U} v^+ = \mathcal{U}^- \mathcal{U}^\circ v^+ = \mathcal{U}^- v^+$ since V is irreducible, $\mathcal{U}^+ v^+ = 0$, and $\mathcal{U}^\circ v^+ = \mathbb{C} v^+$. Hence $V = W$ and (b) and (c) follow.

(d) H_α is in the 3-dimensional subalgebra generated by H_α, X_α, $X_{-\alpha}$. Hence, by the theory of representations of this subalgebra, $\lambda(H_\alpha) \in \mathbb{Z}^+$ (See Jacobson, Lie Algebras, pp. 83-85.)

(e) See Séminaire "Sophus LIE," Exposé n° 17.

Corollary: If μ is a weight and α a root, then $\mu(H_\alpha) \in \mathbb{Z}$.

Proof: This follows from (b) and (d) of Theorem 3 and $\beta(H_\alpha) = \langle \beta, \alpha \rangle \in \mathbb{Z}$ for $\alpha, \beta \in \Sigma$.

Remark: λ, v^+ are called the highest weight, a highest weight vector, respectively.

By Theorem 2, we know that the $\mathbb{Z}$-algebra $\mathcal{U}_\mathbb{Z}$ generated by $X_\alpha^m/m!$ ($\alpha \in \Sigma$, $m \in \mathbb{Z}^+$) has a $\mathbb{Z}$-basis

$$\left\{ \prod_{\alpha<0} \frac{X_\alpha^{m(\alpha)}}{m(\alpha)!} \prod_{i=1}^{\ell} \binom{H_i}{n_i} \prod_{\alpha>0} \frac{X_\alpha^{p(\alpha)}}{p(\alpha)!} \;\middle|\; m(\alpha)\ ,\ n_i\ ,\ p(\alpha) \in \mathbb{Z}^+ \right\}.$$

Now if $\mathcal{U}_{\mathbb{Z}}^-$, $\mathcal{U}_{\mathbb{Z}}^+$, and $\mathcal{U}_{\mathbb{Z}}^\circ$ denote the $\mathbb{Z}$-algebras generated by $X_\alpha^m/m!$ $(\alpha < 0)$, $X_\alpha^m/m!$ $(\alpha > 0)$, and $\binom{H_i}{n_i}$ respectively,

then $\mathcal{U}_{\mathbb{Z}} = \mathcal{U}_{\mathbb{Z}}^- \mathcal{U}_{\mathbb{Z}}^\circ \mathcal{U}_{\mathbb{Z}}^+$.

Lemma 12: If $u \in \mathcal{U}_{\mathbb{Z}}$ and v^+ is a highest weight vector, then the component of uv^+ in $\mathbb{C}v^+$ is nv^+ for some $n \in \mathbb{Z}$.

Proof: We know that $\mathcal{U}_{\mathbb{Z}}^+ v^+ = 0$ and $\mathcal{U}_{\mathbb{Z}}^- v^+ \subseteq \sum_{\mu < \lambda} V_\mu$.

Hence the component is nonzero only if $u \in \mathcal{U}_{\mathbb{Z}}^\circ$. Now $\binom{H_i}{n_i}$ acts as an integer on $\mathbb{C}v^+$ by Theorem 3 (d), so

$\mathcal{U}_{\mathbb{Z}}^\circ v^+ = \mathbb{Z}v^+$.

Lemma 13: Let P be a point of $\mathbb{Z}^\ell$ and S a finite subset of $\mathbb{Z}^\ell$ not containing P . Then there is a polynomial f in ℓ variables such that:

(a) $f(\mathbb{Z}^\ell) \subseteq \mathbb{Z}$.

(b) $f(P) = 1$.

(c) $f(S) = 0$.

Proof: Let $P = (p_1, p_2, \ldots, p_\ell)$ with $p_i \in \mathbb{Z}$, $i = 1, 2, \ldots, \ell$.

Set $f_k(H_1, H_2, \ldots, H_\ell) = \prod_{i=1}^{\ell} \binom{H_i - p_i + k}{k} \binom{-H_i + p_i + k}{k}$.

We see that $f_k(P) = 1$ and f_k takes the value zero at all other points of $\mathbb{Z}^i$ within a box with edges $2k$ and center P. For k sufficiently large, this box contains S.

If V is a vector space over $\mathbb{C}$ and M is a finitely generated (free Abelian) subgroup of V which has a $\mathbb{Z}$-basis which is a $\mathbb{C}$-basis for V, we say M is a lattice in V.

We can now state the following corollaries to Theorem 2.

Corollary 1:

(a) Every finite dimensional $\mathcal{L}$-module V contains a lattice M invariant under all $X_\alpha^m/m!$ ($\alpha \in \Sigma$, $m \in \mathbb{Z}^+$); i.e., M is invariant under $\mathcal{U}_\mathbb{Z}$.

(b) Every such lattice is the direct sum of its weight components; in fact, every such additive group is.

Proof: (a) By the theorem of complete reducibility of representations of semisimple Lie algebras over a field of characteristic 0 (See Jacobson, Lie Algebras, p. 79), we may assume that V is irreducible. Using Theorem 3, we find v^+ and set $M = \mathcal{U}^-_\mathbb{Z} v^+$. M is finitely generated over $\mathbb{Z}$ since only finitely many monomials in $\mathcal{U}^-_\mathbb{Z}$ fail to annihilate v^+. Since $\mathcal{U}^- v^+ = V$ and since $\mathcal{U}^-_\mathbb{Z}$ spans $\mathcal{U}^-$ over $\mathbb{C}$, we see that M spans V over $\mathbb{C}$. Before completing the proof of (a), we will first show that if $\Sigma c_i v_i = 0$ with $c_i \in \mathbb{C}$, $v_i \in M$ and $v_1 \neq 0$, then there exist $n_i \in \mathbb{Z}$, $n_1 \neq 0$, such that $\Sigma c_i n_i = 0$. To see this, let $u \in \mathcal{U}_\mathbb{Z}$ be such that the component of uv_1 in $\mathbb{C} v^+$ is nonzero.

Then $\Sigma c_i uv_i = 0$ implies $\Sigma c_i n_i = 0$ where $n_i v^+$ is the component of uv_i in $\mathbb{C}v^+$. We have $n_i \in \mathbb{Z}$ by Lemma 12 and $n_1 \neq 0$ by choice of u. Finally, suppose a basis for M is not a basis for V. Le ℓ be minimal such that there exist $v_1, \ldots, v_\ell \in M$ linearly independent over $\mathbb{Z}$ but linearly dependent over $\mathbb{C}$. Suppose $\sum_{i=1}^{\ell} c_i v_i = 0$. Then there exist $n_i \in \mathbb{Z}$, $n_1 \neq 0$ such that $\sum_{i=1}^{\ell} c_i n_i = 0$. We see that $0 = n_1 \sum_{i=1}^{\ell} c_i v_i = \sum_{i=2}^{\ell} c_i (n_1 v_i - n_i v_1)$. Since $n_1 v_i - n_i v_1$ $i = 2, 3, \ldots, \ell$ are linearly independent over $\mathbb{Z}$, we have a contradiction to the choice of $v_1, v_2, \ldots, v_\ell$. Hence, M is a lattice in V.

(b) Let M be any subgroup of the additive group of V invariant under $\mathcal{U}_{\mathbb{Z}}$. If μ is a weight, set $P_\mu = (\mu(H_1), \mu(H_2), \ldots, \mu(H_\ell)) \in \mathbb{Z}^\ell$. For a fixed μ let $S = \{P_\lambda | \lambda \text{ a weight}, \lambda \neq \mu\}$. Let f be as in Lemma 13 with $P = P_\mu$. If $u = f(H_1, \ldots, H_\ell)$ then $u \in \mathcal{U}_{\mathbb{Z}}$, and u acts on V like the projection of V onto V_μ. Thus, if $v \in M$, the projection of v to V_μ is in M, and M is the direct sum of its weight components.

<u>Corollary 2</u>: Let $\mathcal{L}$ be faithfully represented on a finite dimensional vector space V. Let M be a lattice in V invariant under $\mathcal{U}_{\mathbb{Z}}$. Let $\mathcal{L}_{\mathbb{Z}}$ be the part of $\mathcal{L}$ which preserves M. Then $\mathcal{L}_{\mathbb{Z}}$ is a lattice, and $\mathcal{L}_{\mathbb{Z}} = \sum_\alpha \mathbb{Z} X_\alpha + \mathcal{H}_{\mathbb{Z}}$ where $\mathcal{H}_{\mathbb{Z}} = \{H \in \mathcal{H} | \mu(H) \in \mathbb{Z}$ for all weights μ of the given representation$\}$. In particular,

$\mathcal{L}_{\mathbb{Z}}$ is independent of M. (But, of course, $\mathcal{L}_{\mathbb{Z}}$ is not independent of the representation.)

Proof: We recall that associated with the representation on V, there is a representation on the dual space V^* of V called the contragredient representation given by $< x, \ell y^* > = - < \ell x, y^* >$ where $x \in V$, $y \in V^*$, $\ell \in \mathcal{L}$ and where $< x, y^* >$ denotes the value of the linear function y^* at x. If M^* is the dual lattice in V^* of M; i.e., $< M, M^* > \subset \mathbb{Z}$; then clearly $\ell \in \mathcal{L}$ preserves M^* if and only if ℓ preserves M. We know that $V \otimes V^*$ is isomorphic with $\mathrm{End}(V)$ and that the tensor product of the two representations corresponds to the representation $\ell: A \to [\ell, A]$ ($\ell \in \mathcal{L}$, $A \in \mathrm{End}(V)$) of $\mathcal{L}$ in $\mathrm{End}(V)$ (See Jacobson, Lie Algebras, p. 22). Now $\mathrm{End}(M) \simeq M \otimes M^*$ is a lattice in $\mathrm{End}(V)$ since the tensor product of two lattices is a lattice. Also, $\mathcal{L}_{\mathbb{Z}}$ is a lattice in $\mathcal{L}$ since $\mathcal{L}_{\mathbb{Z}} \subseteq \mathrm{End}(M)$ and $\dim_{\mathbb{Z}} \mathcal{L}_{\mathbb{Z}} \geq \dim_{\mathbb{C}} \mathcal{L}$ because all H_i and X_α are in $\mathcal{L}_{\mathbb{Z}}$. Since $\mathcal{U}_{\mathbb{Z}}$ preserves M and M^*, $\mathcal{U}_{\mathbb{Z}}$ preserves $M \otimes M^*$ by Lemma 7, and hence $\mathcal{U}_{\mathbb{Z}}$ preserves the lattice $\mathcal{L}_{\mathbb{Z}}$ in $\mathcal{L}$ under the adjoint representation. By Corollary 1 (b), $\mathcal{L}_{\mathbb{Z}} = \sum_\alpha (\mathbb{C} X_\alpha \cap \mathcal{L}_{\mathbb{Z}}) + \mathcal{H}_{\mathbb{Z}}$.

Now $X_\alpha \in \mathcal{U}_{\mathbb{Z}}$ implies $X_\alpha \in \mathbb{C} X_\alpha \cap \mathcal{L}_{\mathbb{Z}}$. If X_α/n spans $\mathbb{C} X_\alpha \cap \mathcal{L}_{\mathbb{Z}}$ over $\mathbb{Z}$ for $n \in \mathbb{Z}$, $n \geq 1$, then $\mathrm{ad}(X_{-\alpha}^2/2!)(X_\alpha/n) = X_{-\alpha}/n \in \mathcal{L}_{\mathbb{Z}}$. Hence $-(\mathrm{ad}\, X_\alpha/n)^2 (X_{-\alpha}/n) = 2 X_\alpha/n^3 \in \mathcal{L}_{\mathbb{Z}}$. Thus, $2/n^3 \in (1/n)\mathbb{Z}$ which implies $2/n^2 \in \mathbb{Z}$ and $n = 1$. Hence, $\mathbb{C} X_\alpha \cap \mathcal{L}_{\mathbb{Z}} = \mathbb{Z} X_\alpha$.

Example: Let $\mathcal{L}$ be the 3 dimensional Lie algebra generated by X, Y, and H with $[X,Y] = H$, $[H,X] = 2X$, and $[H,Y] = -2Y$. Let $V = \mathcal{L}$ and let M be the lattice in $\mathcal{L}$ spanned by X, Y, and H. Then since the only weights of the adjoint representation are $\pm\alpha$, 0 with $\alpha(H) = 2$, $\mathcal{L}_{\mathbb{Z}} = \mathbb{Z}X + \mathbb{Z}Y + \mathbb{Z}(H/2)$. Now $\mathcal{L}$ is isomorphic with $\mathcal{L}' = s\ell_2$ on a 2 dimensional vector space V'. Here H corresponds to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and the weights are $\pm\mu$, with $\mu(H) = 1$. Hence $\mathcal{L}'_{\mathbb{Z}} = \mathbb{Z}X + \mathbb{Z}Y + \mathbb{Z}H$ and $\mathcal{L}_{\mathbb{Z}} \neq \mathcal{L}'_{\mathbb{Z}}$.

We are now in a position to transfer our attention to an arbitrary field k. We have already defined the lattices M, $\mathcal{L}_{\mathbb{Z}}$, $\mathcal{H}_{\mathbb{Z}}$, $M_\mu = V_\mu \cap M$, and $\mathbb{Z}X_\alpha$. Considering these lattices as $\mathbb{Z}$-modules and considering k as a $\mathbb{Z}$-module, we can form the tensor products, $V^k = M \otimes_{\mathbb{Z}} k$, $\mathcal{L}^k = \mathcal{L}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$, $\mathcal{H}^k = \mathcal{H}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$, $V^k_\mu = M_\mu \otimes_{\mathbb{Z}} k$, and $kX^k_\alpha = \mathbb{Z}X_\alpha \otimes_{\mathbb{Z}} k$. We then have:

Corollary 3:

(a) $V^k = \Sigma V^k_\mu$ (direct sum) and $\dim_k V^k_\mu = \dim_{\mathbb{C}} V_\mu$.

(b) $\mathcal{L}^k = \Sigma kX^k_\alpha + \mathcal{H}^k$ (direct sum), each $X^k_\alpha \neq 0$, $\dim_k \mathcal{H}^k = \dim_{\mathbb{C}} \mathcal{H}$, and $\dim_k \mathcal{L}^k = \dim_{\mathbb{C}} \mathcal{L}$.

Proof: This follows from Corollaries 1 and 2.

§ 3. The Chevalley groups. We wish to study automorphisms of V^k of the form $\exp tX_\alpha$ $(t \in k,\ \alpha \in \Sigma)$, where

$$\exp tX_\alpha = \sum_{n=0}^{\infty} t^n X_\alpha^n/n!$$

The right side of the above expression is interpreted as follows. Since $X_\alpha^n/n! \in \mathcal{U}_\mathbb{Z}$, we have an action of $X_\alpha^n/n!$ on M. Thus, we get an action of $\lambda^n X_\alpha^n/n!$ on $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda]$. Since X_α^n acts as zero for n sufficiently large, we see that $\sum_{n=0}^{\infty} \lambda^n X_\alpha^n/n!$ acts on $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda]$ and hence on $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda] \otimes_\mathbb{Z} k$. Following this last action by the homomorphism of $M \otimes_\mathbb{Z} \mathbb{Z}[\lambda] \otimes_\mathbb{Z} k$ into $V^k = M \otimes_\mathbb{Z} k$ given by $\lambda \to t$, we get an action of $\sum_{n=0}^{\infty} t^n X_\alpha^n/n!$ on V^k.

We will write $x_\alpha(t)$ for $\exp tX_\alpha$ and $\mathcal{X}_\alpha$ for the group $\{x_\alpha(t) \mid t \in k\}$ (clearly $x_\alpha(t)$ is additive in t). Our main object of study is the group G generated by all $\mathcal{X}_\alpha$ $(\alpha \in \Sigma)$. We will call it a Chevalley group.

Exercise: Interpret $\sum_{n=0}^{\infty} t^n \binom{H}{n}$ $(H \in \mathcal{H}_\mathbb{Z},\ t \in k,\ t \neq -1)$.

Lemma 14: Let $\mathcal{A}$ be an associative algebra, $A \in \mathcal{A}$, and let d_A be the derivation of $\mathcal{A}$, $d_A = \ell_A - r_A$ where $\ell_A B = AB$, $r_A B = BA$, $B \in \mathcal{A}$. Suppose $\exp d_A$, $\exp \ell_A$, $\exp r_A$, and $\exp A$ have meaning and that the usual rules of exponentiation apply. Then $\exp d_A = \ell_{\exp A}\, r_{\exp(-A)}$ (= conjugation by $\exp A$).

Proof: $\exp d_A = \exp \ell_A \exp(-r_A) = \ell_{\exp A}\, r_{\exp(-A)}$.

Lemma 15: Let α, β be roots with $\alpha + \beta \neq 0$. Then in the ring of formal power series in two variables t, u over $\mathcal{U}_{\mathbb{Z}}$, $\mathcal{U}_{\mathbb{Z}}[[t,u]]$, we have the identity

$$(\exp tX_\alpha, \exp uX_\beta) = \prod\prod \exp c_{ij} t^i u^j X_{i\alpha+j\beta}$$

where $(A,B) = ABA^{-1}B^{-1}$, where the product on the right is taken over all roots $i\alpha + j\beta$ $(i,j \in \mathbb{Z}^+)$ arranged in some fixed order, and where the c_{ij}'s are integers depending on α, β, and the chosen ordering, but not on t or u. Furthermore $C_{11} = N_{\alpha,\beta}$.

Proof: In $\mathcal{U}[[t,u]]$ set $f(t,u) =$

$$(\exp tX_\alpha, \exp uX_\beta) \prod\prod \exp(-c_{ij} t^i u^j X_{i\alpha+j\beta})$$

where $c_{ij} \in \mathbb{C}$. We shall show that we may choose the c_{ij}'s in $\mathbb{Z}$ such that $f(t,u) = 1$.

We note that $t \frac{d}{dt}(\exp tX_\alpha) = t X_\alpha \exp tX_\alpha$.

Thus, using the product rule we get

$$\begin{aligned} t\frac{d}{dt} f(t,u) &= t X_\alpha f(t,u) \\ &\quad + \exp(t X_\alpha)\exp(u X_\beta)\exp(-t X_\alpha)\exp(-u X_\beta) \\ &\quad \cdot \prod\prod \exp(-c_{ij} t^i u^j X_{i\alpha+j\beta} \\ &\quad + \Sigma\, (\exp tX_\alpha, \exp u X_\beta) \\ &\quad \cdot \prod_{\substack{i\alpha+j\beta \\ > k\alpha+\ell\beta}}\prod \exp(-c_{ij} t^i u^j X_{i\alpha+j\beta}) \cdot (-c_{k\ell} k t^k u^\ell X_{k\alpha+\ell\beta}) \\ &\quad \cdot \prod_{\substack{i\alpha+j\beta \\ \leq k\alpha+\ell\beta}}\prod \exp(-c_{ij} t^i u^j X_{i\alpha+j\beta}) . \end{aligned}$$

We bring the terms $-tX_\alpha$ and $(*)-c_{k\ell}kt^k u^\ell X_{k\alpha+\ell\beta}$ to the front using, e.g., the relations

$$(\exp u X_\beta)(-tX_\alpha) = (\exp \operatorname{ad} u X_\beta)(-t X_\alpha) \exp u X_\beta$$

(see Lemma 14) and

$$(\exp \operatorname{ad} u X_\beta)\cdot(-tX_\alpha) = - tX_\alpha - N_{\beta,\alpha} tu X_{\alpha+\beta} - \cdots .$$

We get an expression of the form $A\, f(t,u)$ with $A \in \mathcal{L}[[t,u]]$. Because $f(t,u)$ is homogeneous of degree 0 relative to the grading $t \to -\alpha$, $u \to -\beta$, $X_\gamma \to \gamma$, A is also, and from formulas such as those above we see that $c_{k\ell}$ is involved in the term $(*)$ above but otherwise only in terms of degree $> k + \ell$ in t and u. Thus $A = \sum_{k,\ell \geq 1} (-c_{k\ell} + p_{k\ell}) t^k u^\ell X_{k\alpha+\ell\beta}$ with $p_{k\ell}$ a polynomial in c_{ij}'s for which $i + j < k + \ell$.

Now we may inductively determine values of $c_{k\ell} \in \mathbb{C}$ using the lexicographic ordering of the c_{ij}'s such that $A = 0$. Then $t \frac{d}{dt} f(t,u) = 0$ implies $f(t,u) = f(0,u) = 1$.

To show that the c_{ij}'s are integers, we examine the coefficient of $t^i u^j$ in the definition of $f(t,u)$. This coefficient is $-c_{ij} X_{i\alpha+j\beta}$ + (terms coming from exponentials of multiples of $X_{k\alpha+\ell\beta}$ with $k + \ell < i + j$). Using induction, we see that $c_{ij} X_{i\alpha+j\beta} \in \mathcal{U}_{\mathbb{Z}}$. Hence, $c_{ij} \in \mathbb{Z}$, by Theorem 2. If $i = j = 1$, the coefficient is $- c_{11} X_{\alpha+\beta} + N_{\alpha,\beta} X_{\alpha+\beta}$, so that $c_{11} = N_{\alpha,\beta}$.

Examples: (a) If $\alpha + \beta$ is not a root, the right side of the formula in Lemma 15 is 1. (b) If $\alpha + \beta$ is the only root of the form $i\alpha + j\beta$, the right side is $\exp N_{\alpha,\beta} tu$, and $N_{\alpha,\beta} = \pm (r+1)$, with $r = r(\alpha,\beta)$ as in Theorem 1. (c) If all the roots have one length, the right side is 1 in case (a) and $\exp(\pm tu)$ in case (b).

Corollary: If $\exp tX_\alpha$, etc. in the formula in Lemma 15 are replaced by $\chi_\alpha(t)$, etc., then the resulting equation holds for all $t, u \in k$.

We call a set S of roots closed if $\alpha, \beta \in S$, $\alpha + \beta \in \Sigma$ implies $\alpha + \beta \in S$. The following are examples of closed sets of roots: (a) P = set of all positive roots. (b) $P - \{\alpha\}$, α a simple root. (c) $P_r = \{\alpha \mid \text{ht } \alpha \geq r, \ r \geq 1$.

We shall call a subset I of a closed set S an ideal if $\alpha \in I$, $\beta \in S$, $\alpha + \beta \in S$ implies $\alpha + \beta \in I$. We see that (a), (b) and (c) above are ideals in P.

Lemma 16: Let I be an ideal in the closed set S. Let $\mathcal{X}_S$ and $\mathcal{X}_I$ denote the groups generated by all χ_α ($\alpha \in S$ and $\alpha \in I$, respectively). If $\alpha \in S$ implies $-\alpha \notin S$, then $\mathcal{X}_I$ is a normal subgroup of $\mathcal{X}_S$.

Proof: This follows immediately from Lemma 15.

Lemma 17: Let S be a closed set of roots such that $\alpha \in S$ implies $-\alpha \notin S$, then every element of $\mathcal{X}_S$ can be written uniquely as $\prod_{\alpha \in S} \chi_\alpha(t_\alpha)$ where $t_\alpha \in k$ and the product is taken in any fixed order.

Proof: We shall first prove the lemma in the case in which the ordering is consistent with heights; i.e., ht $\alpha <$ ht β implies $\alpha < \beta$. If α_1 is the first element of S, then $S - \{\alpha_1\}$ is an ideal in S. Hence $\mathfrak{X}_S = \mathfrak{X}_{\alpha_1} \mathfrak{X}_{S-\{\alpha_1\}}$. Using induction on the size of S, we see $\mathfrak{X}_S = \prod \mathfrak{X}_\alpha$.

Now suppose $y \in \mathfrak{X}_S$, $y = \prod \chi_\alpha(t_\alpha)$. Since $X_{\alpha_1}^k \neq 0$, there is a weight vector $v \in M$ corresponding to a weight λ such that $X_{\alpha_1} v \neq 0$. Now $yv = v + t_{\alpha_1} X_{\alpha_1} v + z$ where $v \in V_\lambda$, $t_{\alpha_1} X_{\alpha_1} v \in V_{\lambda+\alpha_1}$, and z is a sum of terms from other weight spaces. Hence $t_{\alpha_1} \in k$ is uniquely determined by y. Since $\chi_{\alpha_1}(t_{\alpha_1})^{-1} y \in \mathfrak{X}_{S-\{\alpha_1\}}$, we may complete the proof of this case by induction.

The proof Lemma 17 for an arbitrary ordering follows immediately from:

Lemma 18: Let $\mathfrak{X}$ be a group with subgroups $\mathfrak{X}_1, \mathfrak{X}_2, \ldots, \mathfrak{X}_r$ such that:

(a) $\mathfrak{X} = \mathfrak{X}_1 \mathfrak{X}_2 \cdots \mathfrak{X}_r$, with uniqueness of expression.

(b) $\mathfrak{X}_i \mathfrak{X}_{i+1} \cdots \mathfrak{X}_r$ is a normal subgroup of $\mathfrak{X}$ for $i = 1, 2, \ldots, r$.

If p is any permutation of 1, 2, ..., r then $\mathfrak{X} = \mathfrak{X}_{p1} \mathfrak{X}_{p2} \cdots \mathfrak{X}_{pr}$ with uniqueness of expression.

Proof: (Exercise) Consider $\mathfrak{X}/\mathfrak{X}_r$ and use induction.

Corollary 1: The map $t \to \mathfrak{X}_\alpha(t)$ is an isomorphism of the additive group of k onto $\mathfrak{X}_\alpha$.

Corollary 2: Let P be the set of all positive roots and let $U = \mathfrak{X}_P$. Then $U = \prod \mathfrak{X}_\alpha$ with uniqueness of expression, where the product is taken over all $\alpha \in P$ arranged in any fixed order.

Corollary 3: U is unipotent and is superdiagonal relative to an appropriate choice of a basis for V^k. Similarly, $U^- = \mathfrak{X}_{-P}$ is unipotent and is subdiagonal relative to the same choice of basis.

Proof: Choose a basis of weight vectors and order them in a manner consistent with the following partial ordering of the weights: μ precedes ν if $\mu - \nu$ is a sum of positive roots.

Corollary 4: If $i \geq 1$ let U_i be the group generated by all $\mathfrak{X}_\alpha$ with $\text{ht}\ \alpha \geq i$. We have then:

(a) U_i is normal in U.

(b) $(U, U_i) \subseteq U_{i+1}$, in particular, $(U, U) \subseteq U_2$.

(c) U is nilpotent.

Corollary 5: If $P = Q \cup R$ with Q and R closed sets such that $Q \cap R = \emptyset$, then $U = \mathfrak{X}_Q \mathfrak{X}_R$ and $\mathfrak{X}_Q \cap \mathfrak{X}_R = 1$. (e.g., if α is a simple root, one can take $Q = \{\alpha\}$ and $R = P - \{\alpha\}$.

Example: If $\mathcal{L} = s\ell_{\ell+1}$, we have seen that the roots correspond to pairs (i,j) $i \neq j$, the positive roots to pairs (i,j) $i < j$, and that we may take $X_{ij} = E_{ij}$, the usual matrix unit. Thus, $\chi_{ij}(t) = 1 + tE_{ij}$. We see that U = {all unipotent, superdiagonal matrices}, U^- = {all unipotent, subdiagonal matrices}, and that G is $SL_{\ell+1}$, the group of $\ell + 1$ square matrices of determinant 1. The nontrivial commutator relations are: $(\chi_{ij}(t), \chi_{jk}(u)) = \chi_{ik}(tu)$ if i,j,k are distinct.

Lemma 19: For any root α and any $t \in k^*$ define

$w_\alpha(t) = \chi_\alpha(t)\chi_{-\alpha}(-t^{-1})\chi_\alpha(t)$ and $h_\alpha(t) = w_\alpha(t)w_\alpha(1)^{-1}$.

Then:

(a) $w_\alpha(t)X_\beta\, w_\alpha(t)^{-1} = ct^{-\langle\beta,\alpha\rangle}X_{w_\alpha\beta}$ where

$c = c(\alpha,\beta) = \pm 1$ is independent of

t,k and the representation chosen, and

$c(\alpha,\beta) = c(\alpha, -\beta)$.

(b) If $v \in V^k_\mu$ there exists $v' \in V^k_{w_\alpha\mu}$

independent of t such that

$w_\alpha(t)v = t^{-\langle\mu,\alpha\rangle}v'$.

(c) $h_\alpha(t)$ acts "diagonally" on V^k_μ as multiplication

by $t^{\langle\mu,\alpha\rangle}$.

(Note that w_α is being used to denote both the defined automorphism and the reflection in the hyperplane orthogonal to α).

Proof: We prove this assuming $k = \mathbb{C}$. The transfer of coefficients to an arbitrary field is almost immediate.

We show first that $w_\alpha(t)Hw_\alpha(t)^{-1} = w_\alpha H$ for all $H \in \mathcal{H}$. By linearity it suffices to prove this for H_α, for if $\alpha(H) = 0$ then X_α commutes with H so that both sides equal H. If $H = H_\alpha$, the left side, because of Lemma 2 and the definitions of $x_\alpha(t)$ and $w_\alpha(t)$, is an element of the three dimensional algebra $< X_\alpha, Y_\alpha, H_\alpha >$ whose value depends on calculations within this algebra, not on the representation chosen. Taking the usual representation in sl_2, we get

$$H_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad w_\alpha(t) = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -t^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$$

so that the desired equation follows.

We next prove (b). From the definitions of $x_\alpha(t)$ and $w_\alpha(t)$ it follows that if

$$v'' = w_\alpha(t)v, \quad \text{then} \quad v'' = \sum_{i=-\infty}^{\infty} t^i v_i \quad \text{where} \quad v_i \in V_{\mu+i\alpha}$$

(the sum is actually finite since there are only finitely many weights). Then for $H \in \mathcal{H}$, $Hv'' = Hw_\alpha(t)v = w_\alpha(t)w_\alpha(t)^{-1} Hw_\alpha(t)v = w_\alpha(t)\,(w_\alpha H)v = \mu(w_\alpha H)v'' = (w_\alpha\mu)(H)v''$. Hence v'' corresponds to the weight $w_\alpha\mu = \mu - < \mu, \alpha > \alpha$. Thus the only nonzero term in the sum occurs for $i = - < \mu, \alpha >$.

By (b) applied to the adjoint representation $w_\alpha(t)\, X_\beta w_\alpha(t)^{-1} = ct^{-\langle\beta,\alpha\rangle} X_{w_\alpha\beta}$ where $c \in \mathbb{C}$ and is independent of t and of the representation chosen. Now $w_\alpha(1)$ is an automorphism of $\mathcal{L}_{\mathbb{Z}}$ and X_γ is a primitive element of $\mathcal{L}_{\mathbb{Z}}$ for all γ so $c = \pm 1$. Finally $H_{w_\alpha\beta} = w_\alpha(1)H_\beta w_\alpha(1)^{-1} = [w_\alpha(1)\, X_\beta w_\alpha(1)^{-1}\,,\ w_\alpha(1)\, X_{-\beta} w_\alpha(1)^{-1}] = c(\alpha,\beta)c(\alpha,-\beta)\, H_{w_\alpha\beta}$ so $c(\alpha,\beta) = c(\alpha,-\beta)$, which proves (a).

Note that $w_\alpha(t)^{-1} = w_\alpha(-t)$ so that $h_\alpha(t) = w_\alpha(-t)^{-1}w_\alpha(-1)$. By (b) $w_\alpha(-t)v = (-t)^{-\langle\mu,\alpha\rangle} v'$ and $w_\alpha(-1)v = (-1)^{-\langle\mu,\alpha\rangle}v'$. Hence $w_\alpha(-t)^{-1}\, w_\alpha(-1)v = t^{\langle\mu,\alpha\rangle}v$, proving (c).

Lemma 20: Write ω_α for $w_\alpha(1)$. Then:

(a) $\omega_\alpha h_\beta(t)\omega_\alpha^{-1} = h_{w_\alpha\beta}(t) =$ an expression as a product of h's, independent of the representation space.

(b) $\omega_\alpha x_\beta(t)\omega_\alpha^{-1} = x_{w_\alpha\beta}(ct)$ with c as in Lemma 19(a).

(c) $h_\alpha(t)\, x_\beta(u) h_\alpha(t)^{-1} = x_\beta\,(t^{\langle\beta,\alpha\rangle}\, u)$.

Proof: To prove (a) we apply both sides to $v \in V_\mu^k$.

$\omega_\alpha h_\beta(t)\omega_\alpha^{-1} v = \omega_\alpha t^{\langle w_\alpha\mu,\beta\rangle}\omega_\alpha^{-1} v$ (by Lemma 19 (c) applied

to $\omega_\alpha^{-1} v \in V^k_{w_\alpha \mu}) = t^{\langle w_\alpha \mu, \beta \rangle} v = t^{\langle \mu, w_\alpha \beta \rangle} v = h_{w_\alpha \beta}(t)\, v$. By Lemma 19(a) $\omega_\alpha X_\beta \omega_\alpha^{-1} = cX_{w_\alpha \beta}$. Exponentiating this gives (b). By Lemma 19(c) applied to the adjoint representation $h_\alpha(t) X_\beta h_\alpha(t)^{-1} = t^{\langle \beta, \alpha \rangle} X_\beta$. Exponentiating this gives (c).

Denote by (R) the following set of relations:

(R1) $$\chi_\alpha(t)\chi_\alpha(u) = \chi_\alpha(t + u) .$$

(R2) $$(\chi_\alpha(t), \chi_\beta(u)) = \prod \chi_{i\alpha+j\beta}\ (c_{ij} t^i u^j)\ (\alpha + \beta \neq 0)$$

with the c_{ij} as in Lemma 15.

(R3) $$w_\alpha(t) = \chi_\alpha(t)\chi_{-\alpha}(-t^{-1})\chi_\alpha(t) .$$

(R4) $$h_\alpha(t) = w_\alpha(t) w_\alpha(1)^{-1} .$$

(R5) $$\omega_\alpha = w_\alpha(1) .$$

(R6) $\omega_\alpha h_\beta(t) \omega_\alpha^{-1} =$ some expression as a product of h's (independent of the representation space).

(R7) $\omega_\alpha \chi_\beta(t) \omega_\alpha^{-1} = \chi_{w_\alpha \beta}(ct)$ c as in Lemma 19(a).

(R8) $$h_\alpha(t)\chi_\beta(u)h_\alpha(t)^{-1} = \chi_\beta(t^{\langle \beta, \alpha \rangle} u) .$$

Since all the relations in (R) are independent of the representation space chosen, results proved using only the relations (R) will be independent of the representation space

chosen. Such results will be labeled (E) (usually for existence). Results proved using other information will be labeled (U) (usually for uniqueness).

Lemma 21: Let U be the group generated by all x_α $(\alpha > 0)$, H the group generated by all $h_\alpha(t)$ and B the group generated by U and H. Then:

(a) U is normal in B and $B = UH$. (E)

(b) $U \cap H = 1$. (U)

Proof: Since conjugation by $h_\alpha(t)$ preserves x_β (by (R8)) U is normal in B and (a) holds. Relative to an appropriate basis of V any element of $U \cap H$ is both diagonal and unipotent, hence $= 1$.

Example: In SL_n $H = \{\text{diagonal matrices}\}$, $U = \{\text{unipotent superdiagonal matrices}\}$, $B = \{\text{superdiagonal matrices}\}$.

Lemma 22: Let N be the group generated by all $w_\alpha(t)$, H be the subgroup generated by all $h_\alpha(t)$, and W the Weyl group. Then:

(a) H is normal in N. (E)

(b) There exists a homomorphism φ of W onto N/H such that $\varphi(w_\alpha) = Hw_\alpha(t)$ for all roots α. (E)

(c) φ is an isomorphism. (U)

Proof: Since by (R6) conjugation by ω_α preserves H and by (R4) and (R5) $w_\alpha(t) = h_\alpha(t)\omega_\alpha$, (a) holds. Since $Hw_\alpha(t) = Hw_\alpha(t)\, w_\alpha(1)^{-1}\, w_\alpha(1) = Hw_\alpha(1)$, $Hw_\alpha(t)$ is independent of t. Write $\hat{w}_\alpha = Hw_\alpha(t)$. Then since $w_\alpha(1) \in \hat{w}_\alpha$ and $w_\alpha(-1) \in \hat{w}_\alpha$, $1 = w_\alpha(1)w_\alpha(-1) \in \hat{w}_\alpha^2$. Hence (*) $\hat{w}_\alpha^2 = 1$. Also $\omega_\beta = w_\beta(1) \in \hat{w}_\beta$ so $\omega_\alpha \omega_\beta \omega_\alpha^{-1} \in \hat{w}_\alpha \hat{w}_\beta \hat{w}_\alpha^{-1}$.

But $\omega_\alpha \omega_\beta \omega_\alpha^{-1} = \omega_\alpha x_\beta(1)x_{-\beta}(-1)x_\beta(1)\omega_\alpha^{-1}$ (by (R3))

$= x_{w_\alpha\beta}(c)x_{-w_\alpha\beta}(-c)x_{w_\alpha\beta}(c)$ (by (R7)) $= \omega_{w_\alpha\beta}^{c} \in \hat{w}_{w_\alpha\beta}$.

Thus (*) $\hat{w}_\alpha \hat{w}_\beta \hat{w}_\alpha^{-1} = \hat{w}_{w_\alpha\beta}$. By Appendix IV. 40 the relations (*) form a defining set for W. Thus there exists a homomorphism $\varphi : W \to N/H$ such that $\varphi w_\alpha = \hat{w}_\alpha = Hw_\alpha(t)$. φ is clearly onto.

Suppose $w \in \ker \varphi$. If $w = w_{\alpha_1} w_{\alpha_2} \ldots$, a product of reflections, then $w_{\alpha_1}(1)w_{\alpha_2}(1) \ldots = h \in H$. Conjugating $\mathcal{X}_\alpha$ by $w_{\alpha_1}(1)w_{\alpha_2}(1) \ldots$ we get $\mathcal{X}_{w\alpha}$ and conjugating by h we get $\mathcal{X}_\alpha$. Hence $\mathcal{X}_{w\alpha} = \mathcal{X}_\alpha$ for all roots α. Since $w\alpha = \alpha$ for all α implies $w = 1$ the proof is completed by:

Lemma 23: If α and β are distinct roots then $\mathcal{X}_\alpha \neq \mathcal{X}_\beta$.

Proof: We know that $\mathcal{X}_\alpha$ is nontrivial. If α and β have the same sign, the result follows from Lemma 17. If they have opposite signs, then one is superdiagonal unipotent, the other subdiagonal (relative to an appropriate basis), and the result

again follows.

Convention: If $n \in N$ represents $w \in W$ (under $\varphi : W \longrightarrow N/H$) we will write wB (Bw) in place of nB (Bn).

Lemma 24: If α is a simple root then

$B \cup Bw_\alpha B$ is a group. (E)

Proof: Let $S = B \cup Bw_\alpha B$. Since B is a group and $\varphi(w_\alpha) = \varphi(w_\alpha)^{-1}$, S is closed under inversion, and since $S^2 \subseteq BB \cup BBw_\alpha B \cup Bw_\alpha BB \cup Bw_\alpha Bw_\alpha B \subseteq S \cup Bw_\alpha Bw_\alpha B$ it suffices to show $w_\alpha Bw_\alpha \subseteq S$. We first show that $\mathfrak{X}_{-\alpha} \subseteq S$. If $1 \neq y \in \mathfrak{X}_{-\alpha}$ then there exists $t \in k^*$ such that $y = x_{-\alpha}(t)$ $= x_\alpha(t^{-1})w_\alpha(-t^{-1})x_\alpha(t^{-1}) \in Bw_\alpha B$. Hence $\mathfrak{X}_{-\alpha} \subseteq S$. Now let P be the collection of all positive roots. Then $w_\alpha Bw_\alpha = w_\alpha Bw_\alpha^{-1}$ $= w_\alpha \mathfrak{X}_\alpha \mathfrak{X}_{P-\{\alpha\}} Hw_\alpha^{-1} = w_\alpha \mathfrak{X}_\alpha w_\alpha^{-1} w_\alpha \mathfrak{X}_{P-\{\alpha\}} w_\alpha^{-1} w_\alpha Hw_\alpha^{-1} = \mathfrak{X}_{-\alpha} \mathfrak{X}_{P-\{\alpha\}} H$ (since w_α preserves $P-\{\alpha\}$ by Appendix I.11) $\subseteq SB = S$.

Lemma 25: If $w \in W$ and α is a simple root, then:

(a) If $w\alpha > 0$ (i.e. if $N(ww_\alpha) = N(w) + 1$ (see Appendix II.17)) then $BwB \cdot Bw_\alpha B \subseteq Bww_\alpha B$. (E)

(b) In any case $BwB \cdot Bw_\alpha B \subseteq Bww_\alpha B \cup BwB$. (E)

Proof: (a) $BwB \cdot Bw_\alpha B = Bw\, \mathfrak{X}_\alpha\, \mathfrak{X}_{P-\{\alpha\}} Hw_\alpha B =$

$Bw\, \mathfrak{X}_\alpha w^{-1} ww_\alpha w_\alpha^{-1}\, \mathfrak{X}_{P-\{\alpha\}} w_\alpha w_\alpha^{-1} Hw_\alpha B = Bww_\alpha B$

(for $w\, \mathfrak{X}_\alpha w^{-1} \subseteq B$, $w_\alpha^{-1}\, \mathfrak{X}_{P-\{\alpha\}} w_\alpha \subseteq B$ and $w_\alpha^{-1} Hw_\alpha \subseteq B$) .

(b) If $w\alpha > 0$ (a) gives the result. If $w\alpha < 0$ set $w' = ww_\alpha$. Then $w'\alpha > 0$ and $w = w'w_\alpha$. By (a) $BwB \cdot Bw_\alpha B = Bw'w_\alpha B \cdot Bw_\alpha B = Bw'B \cdot Bw_\alpha B \cdot Bw_\alpha B = Bw'B\ (B \cup Bw_\alpha B)$ (by Lemma 24) $= Bw'B \cup Bw'w_\alpha B = BwB \cup Bww_\alpha B$.

Corollary: If $w \in W$ and $w = w_\alpha w_\beta \cdots$ is an expression of minimal length of w as a product of simple reflections then $BwB = Bw_\alpha BBw_\beta B \cdots$.

Lemma 26: Let G be the Chevalley group $(G = \langle \mathfrak{X}_\alpha | \text{all } \alpha \rangle)$. Then G is generated by all $\mathfrak{X}_\alpha$, ω_α for α a simple root. (E)

Proof: We have $\omega_\alpha\, \mathfrak{X}_\beta\, \omega_\alpha^{-1} = \mathfrak{X}_{w_\alpha \beta}$. Since the simple reflections generate W and every root is conjugate under W to a simple root the result follows.

Theorem 4: (Bruhat, Chevalley)

(a) $\bigcup_{w \in W} BwB = G$. (E)

(b) $BwB = Bw'B \Rightarrow w = w'$. (U)

Thus any system of representatives for N/H is also a system of representatives for $B \backslash G / B$.

Proof: (a) By Lemma 26 $\bigcup_{w \in W} BwB$ contains a set of generators for G. Since $\bigcup_{w \in W} BwB$ is closed under multiplication by these generators (by Lemma 25) and reciprocation it is equal to G.

(b) Suppose $BwB = Bw'B$ with $w, w' \in W$.

We will show by induction on $N(w)$ that $w = w'$. (Here $N(w)$ is as in the Appendix II.) If $N(w) = 0$ then $w = 1$ so $w' \in B$. Then $w'Bw'^{-1} = B$ so $w'P = P$ and $w' = 1$ (see Appendix II.23). Assume $N(w) > 0$ and choose α simple so that $N(ww_\alpha) < N(w)$. Then $ww_\alpha \in Bw'BBw_\alpha B \subseteq Bw'B \cup Bw'w_\alpha B = BwB \cup Bw'w_\alpha B$. Hence by induction $ww_\alpha = w$ or $ww_\alpha = w'w_\alpha$. But $ww_\alpha = w$ implies $w_\alpha = 1$ which is impossible. Hence $ww_\alpha = w'w_\alpha$ so $w = w'$.

Remark: The groups B, N form a $B - N$ pair in the sense of J. Tits (Annals of Math. 1964). We shall not axiomatize this concept but adapt certain arguments, such as the last one, to the present context.

Theorem 4': For a fixed $w \in W$ choose ω_w representing w in N. Set $Q = P \cap w^{-1}(-P)$, $R = P \cap w^{-1}P$ (as before P denotes the set of positive roots). Write U_w for $\mathfrak{X}_Q$. Then:

(a) $BwB = B\,\omega_w\,U_w$. (E)

(b) Every element of BwB has a unique expression in this form. (U)

Proof: (a) $BwB = Bw\mathfrak{X}_R\mathfrak{X}_Q H$ (by Lemma 17 and Lemma 21)
$= Bw\mathfrak{X}_R w^{-1} w\mathfrak{X}_Q H = Bw\mathfrak{X}_Q H$ (since $w\mathfrak{X}_R w^{-1} \subseteq B$) $= B\omega_w\mathfrak{X}_Q$.

(b) If $b\omega_w x = b'\omega_w x'$ then
$b^{-1}b' = \omega_w x x'^{-1}\omega_w^{-1}$. Relative to an appropriate basis this is both superdiagonal and subdiagonal unipotent and hence $= 1$.
Thus $b = b'$, $x = x'$.

Exercise: (a) Prove B is the normalizer in G of U and also of B. (b) Prove N is the normalizer in G of H if k has more than 3 elements.

Examples: Let $\mathfrak{L} = \mathfrak{sl}_n$ so that $G = SL_n$, and B, H, N are respectively the superdiagonal, diagonal, monomial subgroups, and W may be identified with the group of permutations of the coordinates. Going to $G = GL_n$ for convenience, we get from Theorem 4: (*) the permutation matrices S_n form a system of representatives for $B\backslash G/B$. We shall give a simple direct proof of this. Here k can be any division ring. Assume given $x \in G$. Choose $b \in B$ to maximize the total number of zeros at the beginnings of all of the rows of bx. These beginnings must all be of different lengths since otherwise we could subtract a multiple of some row from an earlier one, i.e., modify b, and increase the total number of zeros. It follows that for some $w \in S_n$, wbx is superdiagonal, whence $x \in Bw^{-1}B$. Now assume $BwB = Bw'B$

with $w, w' \in S_n$. Then $w^{-1}bw'$ is superdiagonal for some $b \in B$. Since w, w' are permutation matrices and the matric positions where the identity is nonzero are included among those of b, we conclude that $w^{-1}w'$ is superdiagonal, whence $w = w'$, which proves (*). Next we will give a geometric interpretation of the result just proved. Let V be the underlying vector space. A flag in V is an increasing sequence of subspaces $V_1 \subset V_2 \subset \cdots \subset V_n$, where $\dim V_i = i$. Associated with the chosen basis $\{v_1, \ldots, v_n\}$ of V there is a flag $F_1 \subset \cdots \subset F_n$ defined by $F_i = \langle v_1, \ldots, v_i \rangle$ called the <u>standard flag</u>. Now G acts on V and hence on flags. B is the stabilizer of the standard flag, so $B \backslash G / B$ is in one-to-one correspondence with the set of G-orbits of pairs of flags. Define a <u>simplex</u> to be a set of points $\{p_1, \ldots, p_n\}$ of V such that $\dim \langle p_1, \ldots, p_n \rangle = n$. A flag $V_1 \subset \cdots \subset V_n$ is said to be <u>incident</u> with this simplex if $V_i = \langle p_{\pi 1}, \ldots, p_{\pi i} \rangle$ for some $\pi \in S_n$. Hence there are $n!$ flags incident with a given simplex.

It can be shown, by induction on n (see Steinberg, T.A.M.S. 1951), that (*) given any two flags there is a simplex incident with both. Thus associated to each pair of flags there is an element of S_n, the permutation which transforms one to the other. Hence $B \backslash G / B$ corresponds to S_n. Thus (*) is the geometric interpretation of the Bruhat decomposition.

(b) Consider $\mathcal{L} = \{X \in s\ell_m \mid XA + AX^t = 0\}$

where A is fixed and nonsingular (i.e., consider the invariants of the automorphism $X \to A(-X^t)A^{-1}$). If $m = 2n$ and A is skew this gives an algebra of type C_n, if $m = 2n$ and A is symmetric this gives an algebra of type D_n, and if $m = 2n+1$ and A is symmetric this gives an algebra of type B_n. If we take $A = \begin{bmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{bmatrix}$ in the first case

and $A = \begin{bmatrix} & & 1 \\ & \cdot & \\ 1 & & \end{bmatrix}$ in the second and third cases an element

$y \in \mathcal{L}$ is superdiagonal if and only if $\operatorname{ad} y$ preserves $\sum_{\alpha>0} \mathcal{L}_\alpha$

(with the usual ordering of roots). Exponentiating we get the invariants of $X \xrightarrow{\sigma} AX^{-1t}A^{-1}$ (that is $XAX^t = A$). In the first case we get $G \subset Sp_m$, in the second and third cases $G \subset SO_m$

(relative to a form of maximal index). (For the proof that equality holds see Ree, T.A.M.S. 1957.) The automorphism σ above preserves the basic ingredients B, H, N of the Bruhat decomposition of SL_m. From this a Bruhat decomposition for Sp_m and SO_m can be inferred. By a slight modification of the procedure, we can at the same time take care of unitary groups.

(c) If $\mathcal{L}$ is of type G_2 it is the derivation algebra of a split Cayley algebra. The corresponding group G is the group of automorphisms of this algebra.

Since the results labelled (E) depend only on the relations (R) (which are independent of the representation chosen) we may extract from the discussion so far the following result.

Proposition: Let G' be a group generated by elements labelled $x'_\alpha(t)$ $(\alpha \in \Sigma,\ t \in k)$ such that the relations (R) hold and let U', H', ... be defined as in G.

(1) Every element of U' can be written in the form $\prod_{\alpha>0} x'_\alpha(t_\alpha)$.

(2) For each $w \in W$, write $w = w_\alpha w_\beta \ldots$ a product of reflections. Define $\omega'_w = \omega'_\alpha \omega'_\beta \ldots$ (where $\omega'_\alpha = w'_\alpha(1)$). Then every element of G' can be written $u'h'\omega'_w v'$ (where $u' \in U'$, $h' \in H'$, $v' \in U'_w$).

Corollary 1: Suppose G' is as above and φ is a homomorphism of G' onto G such that $\varphi(x'_\alpha(t)) = x_\alpha(t)$ for all α and t. Then:

(a) Uniqueness of expression holds in (1) and (2) above.

(b) $\ker \varphi \subseteq$ center of $G' \subseteq H'$.

Proof: (a) Suppose $\prod x'_\alpha(t_\alpha) = \prod x'_\alpha(\tilde{t}_\alpha)$. Applying φ we get $\prod x_\alpha(t_\alpha) = \prod x_\alpha(\tilde{t}_\alpha)$ and by Lemma 17 $t_\alpha = \tilde{t}_\alpha$ for all α. Hence $\varphi|U'$ is an isomorphism. Now if $u'h'\omega_w v' = \tilde{u}'\tilde{h}'\omega_w\tilde{v}'$ by applying φ we get $\varphi(u')\varphi(h')\omega_w\varphi(v') = \varphi(\tilde{u}')\varphi(\tilde{h}')\omega_w\varphi(\tilde{v}')$. By Theorem 4' and Lemma 21 $\varphi(u') = \varphi(\tilde{u}')$ and $\varphi(v') = \varphi(\tilde{v}')$. Hence $u' = \tilde{u}'$ and $v' = \tilde{v}'$ so $h'\omega_w' = \tilde{h}'\omega_w'$ so $h' = \tilde{h}'$.

(b) Let $x' = u'h'\omega_w v' \in \ker\varphi$. Then

$1 = \varphi(u')\varphi(h')\omega_w\varphi(v') \in UH\omega_w U_w$; so $w = 1$, $\omega_w' = 1$, $\varphi(u') = 1$, $\varphi(v') = 1$. Hence $u' = v' = 1$ so $x' = h' = \prod h'_\alpha(t_\alpha)$. Then $x'x'_\beta(u)x'^{-1} = x'_\beta(\prod_\alpha t_\alpha^{<\beta,\alpha>} u)$ by (R8). Applying φ we see that $\prod_\alpha t_\alpha^{<\beta,\alpha>} = 1$. Hence x' commutes with $x'_\beta(u)$ for all β and u, so is in center of G'. To complete the proof it is enough to show that center of $G \subset H$ (for we have shown $\ker\varphi \subset H'$). If $x = uh\omega_w v \in$ center of G and $w \neq 1$ then there exists $\alpha > 0$ such that $w\alpha < 0$. Then $xx_\alpha(1) = x_\alpha(1)x$ which contradicts Theorem 4'. Hence $w = 1$ so $x = uh$. Let w_o be the element of W making all positive roots negative. Then $x = \omega_{w_o} x \omega_{w_o}^{-1}$ is both superdiagonal and subdiagonal. Since h is diagonal, u is diagonal, and also unipotent.

Hence $u = 1$ and $x = h \in H$.

Corollary 2: Center $G \subseteq H$.

Corollary 3: The relations (R) and those in H on the $h_\alpha(t)$ form a defining set of relations for G.

Proof: If the relations in H are imposed on H' then φ in Corollary 1 becomes an isomorphism by (b).

Corollary 4: If G' is constructed as G from $\mathcal{L}$, k, ... but using a perhaps different representation space V' in place of V, then there exists a homomorphism φ of G' onto G such that $\varphi(x'_\alpha(t)) = x_\alpha(t)$ if and only if there exists a homomorphism $\theta : H' \to H$ such that $\theta\, h'_\alpha(t) = h_\alpha(t)$ for all α and t.

Proof: Clearly if φ exists then θ exists. Conversely assume θ exists. Matching up the generators of H' and H, we see that the relations in H' form a subset of those in H. By Corollary 3 and the fact that the relations (R) are the same for G' and G, the relations on $x'_\alpha(t)$, ... in G' form a subset of those on $x_\alpha(t)$, ... in G. Thus φ exists.

So far the structure of H has played a minor role in the proceedings. To make the preceding results more precise we will now determine it.

We recall that H is the group generated by all $h_\alpha(t)$ ($\alpha \in \Sigma$, $t \in k$) and (*) $h_\alpha(t)$ acts on the weight space V_μ as multiplication by $t^{<\mu,\alpha>}$. Also, we recall that by Theorem 3(e), a linear function μ on $\mathfrak{H}$ is the highest weight of some irreducible representation provided $<\mu, \alpha> = \mu(H_\alpha) \in \mathbb{Z}^+$ for all $\alpha > 0$. Clearly, it suffices that $<\mu, \alpha_i> \in \mathbb{Z}^+$ for all simple roots α_i. Define λ_i, $i = 1, 2, \ldots, \ell$ by $<\lambda_i, \alpha_j> = \delta_{ij}$. We see that λ_i occurs as the highest weight of some irreducible representation, and we call λ_i a <u>fundamental weight</u>.

<u>Lemma 27:</u>

(a) The additive group generated by all the weights of all representations forms a lattice L_1 having $\{\lambda_i\}$ as a basis.

(b) The additive group generated by all roots is a sub-lattice L_0 of L_1. Moreover, $(<\alpha_i, \alpha_j>)$ $i, j = 1, 2, \ldots, \ell$ is a relation matrix for L_1/L_0, which is thus finite.

(c) The additive group generated by all weights of a faithful representation on V forms a lattice L_V between L_0 and L_1.

Proof: Part (a) is immediate from the definition of the fundamental weights. (b) If α_i is a simple root and $\alpha_i = \Sigma\, c_{ij}\, \lambda_j (c_{ij} \in \mathbb{C})$ then $< \alpha_i, \alpha_k > = c_{ik}$ and $\alpha_i = \Sigma < \alpha_i, \alpha_j > \lambda_j$. (c) If α is a root, then since $X_\alpha \neq 0$ there exists $0 \neq v \in V_\mu$ for some weight μ with $0 \neq X_\alpha v \in V_{\mu+\alpha}$. Hence $\alpha = (\mu + \alpha) - \mu \in L_V$ and $L_0 \subseteq L_V \subseteq L_1$.

Remark: All lattices between L_0 and L_1 can be realized as in Lemma 27 (c) by an appropriate choice of V. In particular, $L_V = L_0$ if V corresponds to the adjoint representation, and $L_V = L_1$ if V corresponds to the sum of the representations having the fundamental weights as highest weights.

Lemma 28 (Structure of H):

(a) For each α, $h_\alpha(t)$ is multiplicative as a function of t.

(b) H is an Abelian group generated by the $h_i(t)$'s (with $h_i(t) = h_{\alpha_i}(t)$).

(c) $\prod_{i=1}^{\ell} h_i(t_i) = 1$ if and only if

$$\prod_{i=1}^{\ell} t_i^{< \mu, \alpha_i >} = 1 \quad \text{for all } \mu \in L_V .$$

(d) The center of $G = \{ \prod_{i=1}^{\ell} h_i(t_i) \mid \prod_{i=1}^{\ell} t_i^{< \beta, \alpha_i >} = 1$ for all $\beta \in L_0 \}$, hence is finite.

Proof: (a), (b), and (c) follow from (*) above. (a) and (c) are immediate and (b) results from $t^{< \mu, \alpha >} = t^{\mu(H_\alpha)} = t^{\mu(\Sigma n_i H_i)} = t^{\Sigma n_i < \mu, \alpha_i >}$ if $H_\alpha = \Sigma n_i H_i$. For (d), we note

that $\prod_{i=1}^{\ell} h_i(t_i)$ commutes with $x_\beta(u)$ if and only if $\prod_{i=1}^{\ell} t_i^{<\beta,\alpha_i>} = 1$ by Lemma 19(c).

Corollary:

(a) If $L_V = L_1$, then every $h \in H$ can be written uniquely as $h = \prod_{i=1}^{\ell} h_i(t_i)$, $t_i \in k^*$.

(b) If $L_V = L_Q$, then G has center 1.

Corollary 5 (To Theorem 4'): Let G be a Chevalley group as usual and let G' be another Chevalley group constructed from the same $\mathcal{L}$ and k as G but using V' in place of V. If $L_{V'} \supseteq L_V$, then there exists a homomorphism $\varphi: G' \to G$ such that $\varphi(x'_\alpha(t)) = x_\alpha(t)$ for all α, t and $\ker \varphi \subseteq$ Center of G' where $x'_\alpha(t)$ corresponds to $x_\alpha(t)$ in G'. If $L_V = L_{V'}$, then φ is an isomorphism.

Proof: There exists a homomorphism $\theta : H' \to H$ such that $\theta h'_i(t) = h_i(t)$ by Lemma 28(c). If α is any root and $H_\alpha = \Sigma n_i H_i$, $n_i \in \mathbb{Z}$, then $h_\alpha(t) = \prod h_i(t)^{n_i}$ and similarly for $h'_\alpha(t)$. Hence $\theta h'_\alpha(t) = h_\alpha(t)$. By Corollary 4 to Theorem 4' φ exists. By Corollary 1, $\ker \varphi \subseteq$ Center of G'. If $L_V = L_{V'}$ we have a homomorphism $\psi : G \to G'$ such that $\psi(x_\alpha(t)) = x'_\alpha(t)$ Hence, $\psi\circ\varphi = id_{G'}$: $\varphi\circ\psi = id_G$, and φ is an isomorphism.

We call the Chevalley groups G_0 and G_1 corresponding to the lattices L_0 and L_1 the <u>adjoint group</u> and the <u>universal group</u> respectively. If $G = G_V$ is a Chevalley group corresponding to the lattice L_V, then by Corollary 5, we have central homomorphisms α and β such that $\alpha : G_1 \to G_V$ and $\beta : G_V \to G_0$. We call $\ker \alpha$ the <u>fundamental group of</u> G, and we see $\ker \beta =$ center of G.

<u>Exercise</u>: The center of the universal group, i.e., the fundamental group of the adjoint group is isomorphic to $\mathrm{Hom}(L_1/L_0, k^*)$. E.g., if $k = \mathbb{C}$, the last group is isomorphic with L_1/L_0. Also in this case the Center of $G_V \cong L_V/L_0$, and the fundamental group of $G_V \cong L_1/L_V$.

In the following table, we list some information known about the lattices and Chevalley groups of the various Lie algebras $\mathcal{L}$:

<u>Type of $\mathcal{L}$</u>	<u>L_1/L_0</u>	<u>G_0</u>	<u>G_V</u>	<u>G_1</u>
A_ℓ	$\mathbb{Z}_{\ell+1}$	$PSL_{\ell+1}$		$SL_{\ell+1}$
B_ℓ	$\mathbb{Z}_2$	$PSO_{2\ell+1} = SO_{2\ell+1}$		$Spin_{2\ell+1}$
C_ℓ	$\mathbb{Z}_2$	$PSp_{2\ell}$		$Sp_{2\ell}$
D_{2n+1}	$\mathbb{Z}_4$	PSO_{4n+2}	SO_{4n+2}	$Spin_{4n+2}$
D_{2n}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	PSO_{4n}	SO_{4n}	$Spin_{4n}$
E_6	$\mathbb{Z}_3$			
E_7	$\mathbb{Z}_2$			
E_8	$\mathbb{Z}_1$	G_0	=	G_1
F_4	$\mathbb{Z}_1$	G_0	=	G_1
G_2	$\mathbb{Z}_1$	G_0	=	G_1

Here G_V is a Chevalley group other than G_0 and G_1, $\mathbb{Z}_n$ is the cyclic group or order n, SO_n is the special orthogonal group, $Spin_n$ is the spin group, Sp_n is the simplectic group, and PG denotes the projective group of G.

To obtain the column headed by L_1/L_0 one reduces the relation matrix $(<\alpha_i, \alpha_j>)$ to diagonal form. To show, for example, that SL_n is the universal group of $\mathcal{L} = s\ell_n$ of type A_{n-1}, we let ω_i be the weight $\omega_i : \mathrm{diag}(a_1, \ldots, a_n) \to a_1 \cdots a_i$. Then if $\lambda_i = \omega_1 + \omega_2 + \ldots + \omega_i$, $1 \leq i \leq n-1$, we have $\lambda_i(H_j) = \lambda_i (E_{jj} - E_{j+1,j+1}) = \delta_{ij}$. Hence the fundamental weights are in the lattice associated with this representation. Since the center of SL_n is generically cyclic of order n, it follows that L_1/L_0 is isomorphic to $\mathbb{Z}_n$ in this case.

Exercise: If G is a Chevalley group, $G_1, G_2, \ldots, G_r$ subgroups of G corresponding to indecomposable components of Σ, then:

(a) Each G_i is normal in G and $G = G_1 G_2 \cdots G_r$.

(b) G is universal (respectively adjoint) if and only if each G_i is.

(c) In each case in (b), the product in (a) is direct.

Corollary 6: If α is a root, then there exists a homomorphism $\varphi_\alpha : SL_2 \to \langle \mathcal{X}_\alpha, \mathcal{X}_{-\alpha} \rangle$ such that $\varphi_\alpha \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} = x_\alpha(t)$, $\varphi_\alpha \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$

$= x_{-\alpha}(t)$, $\varphi_\alpha \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \omega_\alpha$, and $\varphi_\alpha \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} = h_\alpha(t)$. Moreover, $\ker \varphi_\alpha = \{1\}$ or $\{\pm 1\}$ so that $\langle \mathcal{X}_\alpha, \mathcal{X}_{-\alpha} \rangle$ is isomorphic to either SL_2 or PSL_2 .

Proof: Let $\mathcal{L}_1$ be of rank 1 spanned by X, Y and H with $[X, Y] = H$, $[H, X] = 2X$ and $[H, Y] = -2Y$. Now $\mathcal{L}_1$ has a representation $X \to \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $Y \to \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ $H \to \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ as sl_2 on a vector space V' and a representation $X \to X_\alpha$, $Y \to X_{-\alpha}$, $H \to H_\alpha$ on the same vector space V as the original representation of $\mathcal{L}$. Since SL_2 is universal, the required homomorphism φ exists and has $\ker \varphi \subseteq \{\pm 1\}$ by Corollary 5.

Exercise: If G is universal, each φ_α is an isomorphism.

§4 Simplicity of G . The main purpose of this section is to prove the following theorem:

Theorem 5 (Chevalley, Dickson): Let G be an adjoint group and assume $\mathcal{L}$ is simple (Σ indecomposable). If $|k| = 2$, assume $\mathcal{L}$ is not of type A_1, B_2, or G_2 . If $|k| = 3$, assume $\mathcal{L}$ is not of type A_1 . Then G is simple.

Remark: The cases excluded in Theorem 5 must be excluded. If $|k| = 2$, then G has $\mathcal{A}_3$, $\mathcal{A}_6$, $SU_3(3)$ as a normal subgroup

of index 2 if $\mathcal{L}$ is of type A_1, B_2, G_2 respectively. If $|k| = 3$ and $\mathcal{L}$ is of type A_1, then $\mathcal{A}_4$ is a normal subgroup of G of index 2. Here $\mathcal{A}$ denotes the alternating group.

A proof of Theorem 5 essentially due to Iwasawa and Tits will be given here in a sequence of lemmas.

Lemma 29: Let G be a Chevalley group. If $w \in W$, $w = w_\alpha w_\beta \cdots$ is a minimal expression as a product of simple reflections, then w_α, w_β, $\cdots \in G_1$, the group generated by B and wBw^{-1}.

Proof: We know $w^{-1}\alpha < 0$ by the minimality of the expression (see Appendix II.19 and II.22). Hence if $\beta = -w^{-1}\alpha > 0$, then $G_1 \supseteq w\mathfrak{X}_\beta w^{-1} = \mathfrak{X}_{w\beta} = \mathfrak{X}_{-\alpha}$. Thus, $w_\alpha \in G_1$. Since $w_\alpha wBw^{-1}w_\alpha^{-1} \subseteq G_1$ and since length $w_\alpha w <$ length w, we may complete the proof by induction.

Lemma 30: If G again is any Chevalley group, if π is a subset of the set of simple roots, if W_π is the group generated by all w_α, $\alpha \in \pi$, and if $G_\pi = \bigcup_{w \in W_\pi} BwB$, then

(a) G_π is a group.

(b) The 2^l groups so obtained are all distinct.

(c) Every subgroup of G containing B is equal to one of them.

Proof: Part (a) follows from $BwB \cdot Bw_\alpha B \subseteq B\, ww_\alpha B \cup BwB$.

(b) Suppose π, π' are distinct subsets of the set of simple

roots, say $\alpha \in \pi'$ $\alpha \notin \pi$. Now $w_\alpha \alpha = -\alpha$ and $w\alpha = \alpha + \sum_{\beta \in \pi} C_\beta \beta$ if $w \in W_\pi$. Thus $w_\alpha \alpha \neq w\alpha$, since simple roots are linearly independent. Hence, $w_\alpha \notin W_\pi$, $W_{\pi'} \neq W_\pi$, and $G_{\pi'} \neq G_\pi$ since distinct elements of the Weyl group correspond to distinct double cosets. (c) Let A be any subgroup containing B . Set $\pi = \{\alpha | \alpha \text{ simple}, w_\alpha \in A\}$. We shall show $A = G_\pi$. Clearly, $A \supseteq G_\pi$. Since $G = \bigcup_{w \in W} BwB$ and $A \supseteq B$, we need only show $w \in A$ implies $w \in G_\pi$ to get $A \subseteq G_\pi$. Let $w \in A$, $w = w_\alpha w_\beta \ldots$, a minimal expression of w as a product of simple reflections. By Lemma 29, $w_\alpha, w_\beta, \ldots \in A$. Hence, $\alpha, \beta, \ldots \in \pi$, $w \in W_\pi$, and $w \in G_\pi$.

A group conjugate to some G_π is called a <u>parabolic subgroup</u> of G . We state without proof some further properties of parabolic subgroups which follow from Lemma 29.

(1) No two G_π's are conjugate.

(2) Each parabolic subgroup is its own normalizer.

(3) $G_\pi \cap G_{\pi'} = G_{\pi \cap \pi'}$.

(4) $B \cup BwB$ $(w \in W)$ is a group if and only if $w = 1$ or w is a simple reflection.

<u>Example:</u> If $G = SL_n$, then π corresponds to a partition of the n x n matrices into blocks with the diagonal blocks being square matrices. Clearly, there are 2^{n-1} possibilities for such

partitions. G_π is then the subset of SL_n of matrices whose subdiagonal blocks are zero.

Lemma 31: Let $\mathcal{L}$ be simple and let G be the adjoint Chevalley group. If $N \neq 1$ is a normal subgroup of G, then $NB = G$.

Proof: We first show $N \not\subseteq B$. Suppose $N \subseteq B$ and $1 \neq x \in N$, $x = uh$, $u \in U$, $h \in H$. If $u \neq 1$, then for some $w \in W$, $wxw^{-1} \notin B$, a contradiction. If $u = 1$, then $h \neq 1$. Since G is adjoint, it has center 1, and $h\,x_\alpha(t)h^{-1} = x_\alpha(t')$ with $t' \neq t$ for some $t, t' \in k$, $\alpha \in \Sigma$. Hence $(h, x_\alpha(t)) = x_\alpha(t'-t) \in N$, $x_\alpha(t'-t) \neq 1$, and we are back in the first case.

We now prove the lemma. By Lemma 30(c), $NB = G_\pi$ for some π. We must show π contains all simple roots. Suppose it does not. Since $N \not\subseteq B$, we see $\pi \neq \emptyset$. Also since Σ is indecomposable, we can find simple roots α, β with $\alpha \in \pi$, $\beta \notin \pi$ and α not orthogonal to β. Let $b_1 w_\alpha b_2 \in N$, $b_i \in B$, then $bw_\alpha \in N$ with $b = b_2 b_1 \in B$. Then $w_\beta\, bw_\alpha w_\beta^{-1} \in N \cap (Bw_\alpha w_\beta B \cup Bw_\beta w_\alpha w_\beta B)$ by Lemma 25(b). Hence either $w_\alpha w_\beta \in W_\pi$ or $w_\beta w_\alpha w_\beta \in W_\pi$. Now $w_\beta w_\alpha w_\beta = w_\gamma$, where $\gamma = w_\beta \alpha = \alpha - \langle \alpha, \beta \rangle \beta$. Since $\langle \alpha, \beta \rangle \neq 0$, γ is not a simple root and $N(w_\beta w_\alpha w_\beta) \neq 1$, so that $N(w_\beta w_\alpha w_\beta) \geq 3$ by Appendix II.20. Hence $w_\alpha w_\beta$ and $w_\alpha w_\beta w_\alpha$ are both expressions of minimal length. By Lemma 29,

$w_\beta \in W_\pi$, a contradiction. Thus, π is the set of all simple roots and $NB = G_\pi = G$.

Lemma 32: If $\mathcal{L}$ and G are as in Theorem 5, then $G = G'$, the derived group of G.

Before proving Lemma 32, we first show that Theorem 5 follows from Lemmas 31 and 32. Let $N \neq 1$ be a a normal subgroup of G. By Lemma 31, $NB = G$ so $G/N \simeq B/B \cap N$. Now G/N equals its derived group and $B/B \cap N$ is solvable. Hence $G/N = 1$ and $N = G$.

Instead of proving Lemma 32 directly, we prove the following stronger statement:

Lemma 32': If $\mathcal{L}$ is as in Theorem 5 then $G' = G$ holds in any group G in which the relations (R) hold, in fact in which the relations:

$$(A) \quad (x_\beta(t), x_\gamma(u)) = \prod x_{i\beta+j\gamma}(c_{ij}t^i u^j)$$

$$(B) \quad h_\alpha(t)\, x_\alpha(u) h_\alpha(t)^{-1} = x_\alpha(t^2 u)$$

hold.

Proof: Since G is generated by the $\mathcal{X}_\alpha$'s we must show that every $\mathcal{X}_\alpha \subseteq G'$. We will do this in several steps, excluding as we proceed the cases already treated. The first step takes us almost all the way.

(a) Assume $|k| \geq 4$. We may choose $t \in k^*$, $t^2 \neq 1$.

Then $(h_\alpha(t)\ ,\ x_\alpha(u)) = x_\alpha((t^2-1)u)$. Since α and u are arbitrary, every $\mathcal{X}_\alpha \subseteq G'$.

By (a) we may henceforth assume that the rank ℓ is at least 2 and that $|k| = 2$ or 3 . By the corollary to Lemma 15, we may write the right side of (A) as $x_{\beta+\gamma}(N_{\beta,\gamma}tu) \cdot \Pi'$ the factor with $i = j = 1$ having been isolated. We will use the fact (*) that $N_{\beta,\gamma} = \pm (r + 1)$ with $r = r(\beta,\gamma)$ as in Theorem 1, the maximum number of times one can subtract γ from β and still have a root.

(b) Assume that α is a root which can be written $\beta + \gamma$ so that no other positive integral combination of β and γ is a root and $N_{\beta,\gamma} \neq 0$. Then $\mathcal{X}_\alpha \subseteq G'$, as follows at once from (A) with $\Pi' = 1$. This covers the following cases:

(1) If all roots have the same length:
types A_ℓ, D_ℓ, E_ℓ .

(2) $B_\ell (\ell \geq 3)$, α long ; B_2, α long, $|k| = 3$.

(3) C_ℓ $(\ell \geq 3)$, α short; or α long and $|k| = 3$.

(4) F_4 .

(5) G_2 , α long.

To see this we use the fact that all roots of the same length are congruent under the Weyl group, imbed α in an appropriate root system based on a pair of simple roots, and use (*). In all cases but the second cases in (2) and (3)

this system can be chosen of type A_2 with β and γ roots of the same length as α, while in those cases it can be chosen of type B_2 with β and γ short roots.

Because of the exclusions in the theorem, this leaves the following cases:

(6) $B_\ell (\ell \geq 2)$, α short.

(7) G_2, α short, $|k| = 3$.

(8) C_ℓ $(\ell \geq 3)$, α long, $|k| = 2$.

(c) If (6) or (7) holds, then $\mathfrak{X}_\alpha \subseteq G'$. In both of these cases we can find roots β, γ so that $\alpha = \beta + \gamma$, all other roots $i\beta + j\gamma$ (i,j positive integers) are long, and $N_{\beta\gamma} \neq 0$: in (6) we can choose β long and γ short, in (7) both short. Then $\prod'$ belongs to G' by cases already treated, hence so does $\mathfrak{X}_\alpha$, by (A).

(d) If (8) holds, then $\mathfrak{X}_\alpha \subseteq G'$. Choose roots β, γ with β long, γ short, and $\alpha = \beta + 2\gamma$. Since $\mathfrak{X}_{\beta+\gamma} \subseteq G'$ because $\beta + \gamma$ is short, our assertion will follow from $C_{12} \neq 0$ in (A), hence from the next lemma.

Lemma 33: If β and γ form a simple system of type B_2 with β long and γ short, then $(x_\beta(t), x_\gamma(u)) = x_{\beta+\gamma}(\pm tu)\, x_{\beta+2\gamma}(\pm tu^2)$

Proof: By Lemma 14, we have

$$x_\gamma(u)X_\beta\ x_\gamma(u)^{-1} = \exp\ (\mathrm{ad}\ uX_\gamma)\ X_\beta$$

$$= X_\beta + uN_{\gamma,\beta}\ X_{\beta+\gamma} + u^2\ N_{\gamma,\beta}N_{\gamma,\beta+\gamma}\ /2\ X_{\beta+2\gamma}\ .$$

Here $N_{\gamma,\beta} = \pm 1$ and $N_{\gamma,\beta+\gamma} = \pm 2$ since $\beta - \gamma$ is not a root. If we multiply this equation by $-t$, exponentiate, observe that the three factors on the right side commute, and then shift the first of them to the left, we get Lemma 33.

The proof of Theorem 5 is now complete.

In the course of this discussion, we have established the following result.

Corollary: If Σ is indecomposable and of rank > 1 and if α is any root, then there exist roots β and γ and a positive integer n such that $\alpha = \beta + n\gamma$ and $c_{1n} \neq 0$ in the relations (A) of Lemma 32' .

Corollary (To Theorem 5): If $|k| \geq 4$ and G is a Chevalley group based on k, then every solvable normal subgroup of G is central and hence finite.

Proof: Since the center of a Chevalley group is always finite by Lemma 28(d), we need only prove the first statement. Also we may assume $G = G_0$, the adjoint group, since by Corollary 5 to Theorem 4', there is a homomorphism φ of G onto G_0 with

ker $\varphi \subseteq$ center of G and G_0 has center 1. Now we may write $G = G_1 \cdot G_2 \cdot \cdot \cdot G_r$ where G_i $i = 1, 2, \ldots, r$ is the adjoint group corresponding to an indecomposable subsystem of Σ. By Theorem 5, each G_i is simple. Thus any normal subgroup of G is a product of some of the G_i's. If it also is solvable, the product is empty and the subgroup is 1.

§5. Chevalley groups and algebraic groups.

The significance of the results so far to the theory of semi-simple algebraic groups will now be indicated.

Let k be an algebraically closed field. A subset $V \subseteq k^n$ is said to be algebraic if there exists a subset $\mathcal{P} \subseteq k[x_1,\ldots,x_n]$ such that $V = \{v = (v_1,\ldots,v_n) \in k^n \mid p(v_1,\ldots,v_n) = 0 \text{ for all } p \in \mathcal{P}\}$. The algebraic subsets of k^n are the closed sets of the Zariski topology on k^n. For $V \subseteq k^n$ set $I_k(V) = \{p \in k[x_1,\ldots,x_n] \mid p(v_1,\ldots,v_n) = 0 \text{ for all } (v_1,\ldots,v_n) \in V\}$.

Let $r = n^2 + 1$. Define $D(x) \in k[x_o; x_{ij}]_{1 \le i,\, j \le n}$ by $D(x) = 1 - x_o \det(x_{ij})$. Then $GL_n(k) = \{v \in k^r \mid D(v) = 0\}$ is an algebraic subset of k^r. G is a matric algebraic group if G is a subgroup of $GL_n(k)$ for some n and some algebraically closed field k, and G is an algebraic subset of k^{n^2+1}.

If k_o is a subfield of k, G is defined over k_o if $I_k(G)$ has a basis of polynomials with coefficients in k_o.

Examples: (a) $SL_n(k)$, (b) Superdiagonal subgroup, (c) Diagonal subgroup, (d) $\left\{\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}\right\} = G_a$ = additive group, (e) $\left\{\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}\right\} = G_m$ = multiplicative group, (f) Sp_{2n}, (g) SO_n, (h) any finite subgroup.

The groups in (a) - (e) are defined over the prime field. Whether Sp_{2n}, SO_n are or not depends on the coefficients of the defining forms. The groups in (h) are not connected in the Zariski topology, the others are.

A map of algebraic groups $\varphi: G \longrightarrow H$ is a homomorphism if it is a group homomorphism and each of the matric coefficients $\varphi(g)_{ij}$ is a rational function of the g_{ij}. A homomorphism $\varphi: G \longrightarrow H$ is an isomorphism if there exists a homomorphism $\psi: H \longrightarrow G$ such that $\varphi\psi = id_H$ and $\psi\varphi = id_G$. A homomorphism $\varphi: G \longrightarrow H$ is defined over k_o if each of the rational functions above has its coefficients in k_o.

Except for the last assertion, the following results are proved in Séminaire Chevalley (1956-8), Exposé 3.

(i) Let G be a matric algebraic group. Then the following are equivalent:

  (a) G is connected (in the Zariski topology).

  (b) G is irreducible (as an algebraic variety).

  (c) $I_k(G)$ is a prime ideal.

(ii) The image of an algebraic group under a rational homomorphism is algebraic.

(iii) A group generated by connected algebraic subgroups is algebraic and connected (e.g. (a) - (g) are connected). It is defined over the perfect field k_o if each of the subgroups is.

If G is an algebraic group, the radical of G (rad G) is the maximal connected solvable normal subgroup. G is semisimple if (1) rad $G = \{1\}$ and (2) G is connected.

Example: $\left\{ \begin{bmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{bmatrix} \;\middle|\; A \in SL_{n-1} \right\}$ has radical $\left\{ \begin{bmatrix} 1 & * & \cdots & * \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} \right\}$

For the remainder of this section we assume that k is algebraically closed, k_o is the prime field, G is a Chevalley group based on k and M the lattice. (Since a change of basis in M is given by polynomials with integral coefficients we may speak of a basis over M.)

Theorem 6: With the preceding notations:

(a) G is a semisimple algebraic group relative to M.

(b) B is a maximal connected solvable subgroup (Borel subgroup).

(c) H is a maximal connected diagonalizable subgroup (maximal torus).

(d) N is the normalizer of H and $N/H \cong W$.

(e) G, B, H, and N are all defined over k_o relative to M.

Remark: B and H are determined by the abstract group G:

(a) B is maximal solvable and has no subgroups of finite index.

(b) H is maximal nilpotent and every subgroup of finite index is of finite index in its normalizer.

Proof of Theorem 6: (a) Map $G_a \longrightarrow \mathcal{X}_\alpha$ by x_α: $t \longrightarrow x_\alpha(t)$. This is a rational homomorphism. So since G_a is a connected

algebraic group so is $\mathfrak{X}_\alpha$. Hence G is algebraic and connected. Let R = rad G. Since R is solvable and normal it is finite by the Corollary to Theorem 5. Since R is also connected R = 1, and hence G is semisimple.

(b and c) H is the image of G_m^ℓ under $(t_1,\ldots,t_\ell) \longrightarrow \prod_{i=1}^{\ell} h_i(t_i)$ and hence is algebraic and connected; so B = UH is connected, algebraic, and solvable. Let $G_1 \supsetneq B$. Then $G_1 \supseteq B\, w_\alpha\, B$ (some simple root α), so $G_1 \supseteq \langle \mathfrak{X}_\alpha, \mathfrak{X}_{-\alpha} \rangle$, and hence by Corollary 6 of Theorem 4' G_1 is not solvable and hence (b) holds. H is a maximal connected diagonalizable subgroup of B (for any larger subgroup must intersect U nontrivially). Hence H is a maximal connected diagonalizable subgroup of G (by a theorem in Chevalley's Séminaire); so (c) holds.

(d) is clear. To prove (e) it suffices by (iii) to prove:

Lemma 34: Let $\mathfrak{X}_\alpha = \{x_\alpha(t) \mid t \in k\}$ and $\mathfrak{h}_\alpha = \{h_\alpha(t) \mid t \in k^*\}$. Then: (a) $\mathfrak{X}_\alpha$ is defined over k_o and x_α: $G_a \longrightarrow \mathfrak{X}_\alpha$ is an isomorphism over k_o.

(b) $\mathfrak{h}_\alpha$ is defined over k_o and h_α: $G_m \longrightarrow \mathfrak{h}_\alpha$ is a homomorphism over k_o.

Proof: Let $\{v_i\}$ be a basis of M formed of weight vectors. Choose v_i so that $X_\alpha v_i \neq 0$, then write $X_\alpha v_i = \Sigma\, c_{ij} v_j$, and choose v_j so that $c_{ij} \neq 0$. If v_i is of weight μ, then v_j is of weight $\mu + \alpha$. Since $x_\alpha(t) = 1 + tX_\alpha + t^2X_\alpha^2/2 + \cdots$ it follows that if a_{ij} is the (i,j) matric coordinate ($i \neq j$)

function then $a_{ij}(x_\alpha(t)) = c_{ij}t$. All other coefficients of $x_\alpha(t)$ are polynomials over k_o in t , hence also in a_{ij} . This set of polynomial relations defines $\mathcal{X}_\alpha$ as a group over k_o . Now $\frac{1}{c_{ij}}a_{ij}$: $x_\alpha(t) \longrightarrow t$ is an inverse of x_α , so the map x_α is an isomorphism over k_o . The proof of (b) is left as an excercise.

We can recover the lattices L_o and L from the group G as follows. Let $\mu \in L$. Define $\hat{\mu}$: $H \longrightarrow G_m$ by $\hat{\mu}(\prod h_i(t_i)) = \prod t_i^{\mu(H_i)}$. This is a character defined over k_o . $\{\hat{\mu}\}$ generates a lattice $\hat{L}$, the character group of H . The $\mathcal{X}_\alpha$'s are determined by H as the unique minimal unipotent subgroups normalized by H . If $h = \prod h_i(t_i)$ then $h\, x_\alpha(t) h^{-1} = x_\alpha(\hat{\alpha}(h)t)$ where $\hat{\alpha}(h) = \prod t_i^{\alpha(H_i)}$. $\hat{\alpha}$ is called a <u>global root</u>. Define $\hat{L}_o$ = the lattice generated by all $\hat{\alpha}$. Then $\hat{L}_o \subset \hat{L}$.

<u>Exercise</u>: There exists a W-isomorphism: $L \longrightarrow \hat{L}$ such that $L_o \longrightarrow \hat{L}_o$, $\mu \longrightarrow \hat{\mu}$, and $\alpha \longrightarrow \hat{\alpha}$. (The action of W on $\hat{L}$ is given by the action of N/H on the character group).

We summarize our results in:

<u>Existence Theorem</u>: Given a root system Σ , a lattice L with $L_o \subset L \subset L_1$ (where L_o and L_1 are the root and weight lattices, respectively), and an algebraically closed field k , then there exists a semisimple algebraic group G defined over k such that L_o and L are realized as the lattices of global roots and characters, respectively, relative to a maximal torus. Furthermore

G, X_α, ... can be taken over the prime field.

The classification theorem, that up to k-isomorphism every semisimple algebraic group over k has been obtained above, is much more difficult. (See Séminair Chevalley, 1956-8).

We recall that $\mathcal{H}_{\mathbb{Z}} = \mathcal{H} \cap \mathcal{L}_{\mathbb{Z}}$
$= \{H \in \mathcal{H} \mid \mu(H) \in \mathbb{Z} \text{ for all } \mu \in L\}$.

Lemma 35: Let k be algebraically closed, G a Chevalley group over k, $H_1', \ldots, H_\ell'$ a basis for $\mathcal{H}_{\mathbb{Z}}$. Define h_i' by $h_i'(v) = t^{\mu(H_i')} v$ for $v \in V_\mu$. Then the map $\varphi: G_m^\ell \longrightarrow H$ given by $(t_1', \ldots, t_\ell') \longrightarrow \prod_{j=1}^{\ell} h_j'(t_j')$ is an isomorphism over k_o of algebraic groups.

Proof: Write $H_i = \Sigma\, n_{ij} H_j'$, $n_{ij} \in \mathbb{Z}$. Given $\{t_j'\}$ we can find $\{t_i\}$ such that $t_j' = \prod_i t_i^{n_{ij}}$ (for $\det(n_{ij}) \neq 0$ and k^* is divisible). Then $\prod_j h_j'(t_j')$ acts on V_μ as multiplication by $\prod_j t_j'^{\mu(H_j')} = \prod_i t_i^{\mu(H_i)}$, i.e. as $\prod h_i(t_i)$. This shows that φ maps G_m^ℓ onto H. Clearly φ is a rational mapping defined over k_o. Let $\{\mu_i\}$ be the basis of L dual to $\{H_j'\}$ (i.e. $\mu_i(H_j') = \delta_{ij}$). Write $\mu_i = \sum_{\mu \in L} n_\mu \mu$. Then $\prod_\mu (\prod_j t_j'^{\mu(H_j')})^{n_\mu}$ $= t_i'$, so φ^{-1} exists and is defined over k_o.

Theorem 7: Let k be an algebraically closed field and k_o the prime subfield. Let G be a Chevalley group parametrized by k and viewed as an algebraic group defined over k_o as above. Then:

(a) U^-HU is an open subvariety of G defined over k_o.

(b) If n is the number of positive roots, then the map $\varphi: k^n \times k^{*\ell} \times k^n \longrightarrow U^-HU$ defined by $\varphi((t_\alpha)_{\alpha<0}, (t_i)_{1\le i\le \ell}, (t_\alpha)_{\alpha>0}) = \prod_{\alpha<0} x_\alpha(t_\alpha) \prod h_i'(t_i) \prod_{\alpha>0} x_\alpha(t_\alpha)$ is an isomorphism of of varieties over k_o.

Proof: (a) We consider the natural action of G on $\wedge^n \mathcal{L}$ relative to a basis $\{Y_1, Y_2, \ldots, Y_r\}$ over k_o made up of products of H_i's and X_α's such that $Y_1 = \wedge X_\alpha (\alpha > 0)$. For $x \in G$ we set $xY_i = \Sigma\, a_{ij}(x) Y_j$ and then $d = a_{11}$, a function on G over k_o. We claim that $x \in U^-HU = U^-B$ if and only if $d(x) \neq 0$. Assume $x \in U^-B$. Since B fixes Y_1 up to a nonzero multiple and if $u \in U^-$ then $uX_\alpha \in X_\alpha + \mathcal{H} + \sum_{ht(\beta) < ht(\alpha)} kX_\beta$, it follows that $d(x) \neq 0$. If $x \in U^- w B$ with $w \in W$, $w \neq 1$, the same considerations show that $d(x) = 0$. If $w_o \in W$ makes all positive roots negative then by the equation $w_o U^{--} w B = B\, w_o w B$ and Theorem 4' the two cases above are exclusive and exhaustive, whence (a).

(b) The map φ is composed of the two maps $\Psi = (\Psi_1, \Psi_2, \Psi_3): (t_\alpha)_{\alpha>0} \times (t_i) \times (t_\alpha)_{\alpha>0} \longrightarrow U^- \times H \times U$, and $\theta: U^- \times H \times U \longrightarrow U^-HU$. We will show that these are isomorphisms over k_o. For Ψ_2 this follows from Lemma 35. Consider Ψ_3. Let $\{v_i\}$ be a basis for V, the underlying vector space, made up of weight vectors in the lattice M, and f_{ij} the

corresponding coordinate functions on End V . For each root α choose $i = i(\alpha)$, $j = j(\alpha)$, $n_{ij} = n(\alpha)$ as in the proof of Lemma 34. Set $x = \prod_{\beta > 0} x_\beta(t_\beta)$. Choosing an ordering of the positive roots consistent with addition, we see at once that $f_{i(\alpha),j(\alpha)}(x) = n(\alpha)t_\alpha +$ an integral polynomial in the earlier t's and that $f_{ij}(x)$ is an integral polynomial in the t's for all i,j . Thus Ψ_3 is an isomorphism over k_o , and similarly for Ψ_1 . To prove θ is an isomorphism we order the v_i so that U^-,H,U consist respectively of subdiagonal unipotent, diagonal, superdiagonal unipotent matrices (see Lemma 18, Cor. 3), and then we may assume that they consist of all of the invertible matrices of these types. Let $x = u^-hu$ be in U^-HU and let the subdiagonal entries of u^- , the diagonal entries of h , the superdiagonal entries of u be labelled t_{ij} with $i > j$, $i = j$, $i < j$ respectively. We order the indices so that ij precedes $k\ell$ in case $i \leq k$, $j \leq \ell$ and $ij \neq k\ell$. Then in the three cases above $f_{ij}(x) = t_{ij}t_{jj}$, resp. t_{ij}, resp. $t_{ii}t_{ij}$, increased by an integral polynomial in t's preceeding t_{ij} . We may now inductively solve for the t's as rational forms over $\mathbb{Z}$ in the f's , the division by the forms representing the t_{jj}'s being justified by the fact that they are nonzero on U^-HU . Thus θ is an isomorphism over k_o and (b) follows.

Example: In SL_n U^-HU consists of all (a_{ij}) such that the minors $[a_{11}]$, $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, ... are nonsingular.

Remark : It easily follows that the Lie algebra of G is $\mathcal{L}^k$.

We can now easily prove the following important fact (but will refer the reader to Séminaire Bourbaki, Exp. 219 instead). Let G be a Chevalley group over $\mathbb{C}$, viewed as above as an algebraic matric group over $\mathbb{Q}$, the prime field, and I the corresponding ideal over $\mathbb{Z}$ (consisting of all polynomials over $\mathbb{Z}$ which vanish on G) . Then the set of zeros of I in any algebraically closed field k is just the Chevalley group over k of the same type (same root system and same weight lattice) as G . Thus we have a functorial definition in terms of equations of all of the semisimple algebraic groups of any given type.

Corollary 1: Let k, k_o, G, V be as above. Let G' be a Chevalley group constructed using V' instead of V but with the same $\mathcal{L}$. Assume that $L_V \supseteq L_{V'}$. Then the homomorphism φ: $G \longrightarrow G'$ taking $x_\alpha(t) \longrightarrow x'_\alpha(t)$ for all α and t is a homomorphism of algebraic groups over k_o .

Proof: Consider first $\varphi | U^- HU$. By Theorem 7 we need only show that $\varphi | H$ is rational over k_o . The nonzero coordinates of $\prod h'_i(t_i)$ are $\prod t_i^{\mu'(H_i)}$ ($\mu' \in L_{V'}$) . The nonzero coordinates of $\prod h_i(t_i)$ are $\prod t_i^{\mu(H_i)}$ ($\mu \in L_V$) . Each of the former is a monomial in the latter (because $L_{V'} \subseteq L_V$) , and hence is rational over k_o . Now for $w \in W, \omega_w$ (resp. ω'_w) can be chosen with coefficients in k_o (for $w_\alpha(1) = x_\alpha(1)\, x_{-\alpha}(-1)\, x_\alpha(1)$) , so that $\varphi | \omega_w^{-1} U^- B$ is rational over k_o . Since $B\omega_w B \subseteq \omega_w^{-1} U^- B$, we conclude that φ is rational over k_o .

Corollary 2: The homomorphism φ_α: $SL_2 \longrightarrow \langle \mathcal{X}_\alpha, \mathcal{X}_{-\alpha} \rangle$ (of Corollary 6 to Theorem 4') is a homomorphism of algebraic groups over k_o.

Proof: This is a special case of Corollary 1.

Corollary 3: Assume $\mathcal{L}$, V, and M are fixed, that V is universal, $k \subset K$ are fields and G_k and G_K are the corresponding Chevalley groups. Then $G_k = G_K \cap GL_{M,k}$.

Proof: Clearly $G_k \subseteq G_K \cap GL_{M,k}$. Suppose $x \in G_K \cap GL_{M,k}$. Then $x = uh\omega_w v$ (see Theorem 4') with ω_w defined over the prime field. We must show that $x\omega_w^{-1} \in G_k$, i.e. $uhu^- \in G_k$ where $u^- = \omega_w v \omega_w^{-1}$. Write $uhu^- = \prod_{\alpha > 0} x_\alpha(t) \prod h_i(t_i) \prod_{\alpha < 0} x_\alpha(t)$ with t_α, $t_i \in K$. Applying φ^{-1} of Theorem 7, we get $(t_\alpha)_{\alpha > 0}\ x\ (t_i)\ x\ (t_\alpha)_{\alpha < 0}$. Since uhu^- is defined over k and φ^{-1} is defined over k_o, all t_α, $t_i \in k$. Hence $uhu^- \in G_k$.

Remark: Suppose $k = \mathbb{C}$ and G is a Chevalley group over k. Then G has the structure of a complex Lie group, and all the preceding statements have obvious modifications in the language of Lie groups, all of which are true. For example, all complex semisimple Lie groups are included in the construction, and φ in Theorem 7 is an isomorphism of complex analytic manifolds.

§6. Generators and relations

In this section we give a presentation of the universal Chevalley group in terms of generators and relations. If Σ is a root system and k a field we consider the group generated by the collection of symbols $\{x_\alpha(t) | \alpha \in \Sigma, t \in k\}$ subject to the following relations, taken from the corresponding Chevalley groups:

(A) $x_\alpha(t)$ is additive in t.

(B) If α and β are roots and $\alpha + \beta \neq 0$, then $(x_\alpha(t), x_\beta(u)) = \prod x_{i\alpha+j\beta}(c_{ij} t^i u^j)$, where i and j are positive integers and the c_{ij} are as in Lemma 15.

(B') $w_\alpha(t) x_\alpha(u) w_\alpha(-t) = x_{-\alpha}(-t^{-2}u)$ for $t \in k^*$; where $w_\alpha(t) = x_\alpha(t) x_{-\alpha}(-t^{-1}) x_\alpha(t)$ for $t \in k^*$.

(C) $h_\alpha(t)$ is multiplicative in t, where $h_\alpha(t) = w_\alpha(t) w_\alpha(-1)$ for $t \in k^*$.

The reader is referred to the lecturer's paper in Colloque sur la théorie des groupes algébriques, Bruxelles, 1962.

Theorem 8: Assume that Σ is orthogonally indecomposable. Then:

(a) The relations (R) (see §3) are consequences of (A) and (B) if rank $\Sigma \geq 2$ and of (A) and (B') if rank $\Sigma = 1$.

(b) In either case if we add the relation (C) we obtain a complete set of relations for the universal Chevalley group constructed from Σ and k.

The proof depends on a sequence of lemmas.

Throughout we let G' be the group generated by $\{x'_\alpha(t) \mid \alpha \in \Sigma, t \in k\}$ subject to relations (A) and (B) if rank $\Sigma \geq 2$ or (A) and (B') if rank $\Sigma = 1$, G be the universal Chevalley group constructed from Σ and k, and $\pi: G' \longrightarrow G$ be the homomorphism defined by $\pi(x'_\alpha(t)) = x_\alpha(t)$ for all $\alpha \in \Sigma$, $t \in k$.

Lemma 36: Let S be a set of roots such that:

(a) $\alpha \in S$ implies $-\alpha \notin S$.

(b) $\alpha, \beta \in S$ and $\alpha + \beta \in \Sigma$ implies $\alpha + \beta \in S$.

Let X'_S be the subgroup of G' generated by $\{x'_\alpha(t) \mid \alpha \in S, t \in k\}$. Then π maps X'_S isomorphically onto the corresponding group in G.

Proof: Using (A) and (B) we can reduce every element of X'_S to the form $\prod_{\alpha \in S} x'_\alpha(t_\alpha)$ $(t_\alpha \in k)$, and we know by Lemma 17 that every element of X_S can be written uniquely in this form.

Lemma 37: The following are consequences of (A) and (B) if rank $\Sigma \geq 2$ and of (A) and (B') if rank $\Sigma = 1$:

(a) $w'_\alpha(t)x'_\beta(u)w'_\alpha(-t) = x'_\gamma(ct^{-\langle\beta,\alpha\rangle}u)$.

(b) $w'_\alpha(t)w'_\beta(u)w'_\alpha(-t) = w'_\alpha(ct^{-\langle\beta,\alpha\rangle}u)$.

(c) $w'_\alpha(t)h'_\beta(u)w'_\alpha(-t) = h'_\gamma(ct^{-\langle\beta,\alpha\rangle}u)h'_\gamma(ct^{-\langle\beta,\alpha\rangle})^{-1}$, where $\gamma = w_\alpha\beta$, $c = c(\alpha,\beta) = \pm 1$ is independent of t and u, and $c(\alpha,\beta) = c(\alpha,-\beta)$.

(d) $h'_\alpha(t)x'_\beta(u)h'_\alpha(t)^{-1} = x'_\beta(t^{\langle\beta,\alpha\rangle}u)$.

(e) $h'_\alpha(t)w'_\beta(u)h'_\alpha(t)^{-1} = w'_\beta(t^{\langle\beta,\alpha\rangle}u)$.

(f) $h'_\alpha(t)h'_\beta(u)h'_\alpha(t)^{-1} = h'_\beta(t^{\langle\beta,\alpha\rangle}u)h'_\beta(t^{\langle\beta,\alpha\rangle})^{-1}$.

Proof: (a) Assume $\alpha \neq \pm\beta$. Let S be the set of roots of the form $i\alpha + j\beta$ where i and j are integers and $j > 0$. By (B) $\mathcal{X}'_S$ is normalized by $\mathcal{X}'_\alpha$ and $\mathcal{X}'_{-\alpha}$ and hence by $w'_\alpha(t)$. Thus $w'_\alpha(t)x'_\beta(u)w'_\alpha(-t) \in \mathcal{X}'_S$. By Lemma 36 we need only prove that relation (a) holds in G . But in G (a) follows from the relations (R) . Now assume $\alpha = \beta$ and rank $\Sigma \geq 2$. In this case we use the fact (see the Corollary to Lemma 33)

(*) There exist roots δ and γ and a positive integer j such that $\alpha = \delta + j\gamma$ and

$$(x'_\delta(t),x'_\gamma(u)) = \prod_{m,n>0} x'_{m\delta+n\gamma}(c_{m,n}t^m u^n) \quad \text{and} \quad c_{1j} \neq 0 .$$

Set $T = \{mw_\alpha\delta + nw_\alpha\gamma \mid m,n \text{ positive integers}\}$. Transforming both sides of the above equation by $w'_\alpha(t)$ and applying the case of (a) already proved we see that the transform of every term except $x'_{\delta+j\gamma}(c_{1j}t\,u^j) \in \mathcal{X}'_T$. Hence $w'_\alpha(t)x'_{\delta+j\gamma}(c_{1j}t\,u^j)w'_\alpha(-t) \in \mathcal{X}'_T$, so by the earlier argument, with T in place of S , (a) holds. If $\alpha = \beta$ and rank $\Sigma = 1$ then (a) holds by (B'). Since $w'_\alpha(t)^{-1} = w'_\alpha(-t)$, the case $\alpha = -\beta$ follows from the case $\alpha = \beta$.

(b) -(f) follow from (a) and the definitions of $w'_\alpha(t)$ and $h'_\alpha(t)$.

Part (a) of Theorem 8 follows from parts (a) - (d) of Lemma 37.

Lemma 38: Let $\mathfrak{h}'_\alpha$ be the group generated by all $h'_\alpha(t)$, $\mathfrak{h}'_i = \mathfrak{h}'_{\alpha_i}$, and H' the group generated by all $\mathfrak{h}'_\alpha$. Then:

(a) Each $\mathfrak{h}'_\alpha$ is normal in H'.

(b) $H' = \prod_{i=1}^{\ell} \mathfrak{h}'_i$.

Proof: (a) follows from Lemma 37 (f).

(b) Let β be any root, and write $\beta = w\alpha_i$ with α_i simple and $w \in W$. Let $w = w_\alpha \ldots$ be a minimal expression for w as a product of simple reflections. Set $\gamma = w_\alpha \beta$. Then $h'_\beta(t) = w'_\alpha(1) h'_\gamma(c(-1)^{-\langle\beta,\alpha\rangle} t) h'_\gamma(c(-1)^{-\langle\beta,\alpha\rangle})^{-1} w'_\alpha(-1)$ by Lemma 37 (c), and hence by Lemma 37 (e)
$h'_\beta(t) = h'_\gamma(c(-1)^{-\langle\beta,\alpha\rangle} t) h'_\gamma(c(-1)^{-\langle\beta,\alpha\rangle})^{-1} w'_\alpha(t^{-\langle\beta,\alpha\rangle}) w'_\alpha(-1)$
$\in \mathfrak{h}'_\gamma \cdot \mathfrak{h}'_\alpha$. By induction on the length of w, (b) follows.

Proof of Theorem 8 (b): Let G'' be the group generated by $\{x''_\alpha(t) \mid \alpha \in \Sigma, t \in k\}$ subject to the relations (A), (B) if rank $\Sigma > 1$ or (B') if rank $\Sigma = 1$, and (C). Let $w''_\alpha(t)$, $h''_\alpha(t), \ldots$ be defined as usual in terms of the $x''_\alpha(t)$. We wish to prove that $\pi'' : G'' \longrightarrow G$ is an isomorphism. Let $x \in \ker \pi''$. By Corollary 1 of the proposition in §3, $x \in H''$. By Lemma 38 and (C) $x = \prod h''_i(t_i)$ $(t_i \in k^*)$. Applying π'' we obtain $1 = \prod h_i(t_i)$. Since G is universal each $t_i = 1$, so $x = 1$.

Remarks: (a) In (A) and (B) it is sufficient to use as generators $x_\alpha(t)$ where α is a linear combination of 2 simple roots and the relations (A) and (B) which can be written in

terms of such elements.

(b) It is sufficient to assume (C) for one root in each orbit under W.

Exercise: If Σ is indecomposable, prove that it is sufficient to assume (C) for any long root α.

We will now show that if k is an algebraic extension of a finite field then (A) and (B) imply (C).

Lemma 39: Let α be a root and G' as above. In G' set $f(t,u) = h_\alpha(t)h_\alpha(u)h_\alpha(tu)^{-1}$. Then:

(a) $f(t,u^2v) = f(t,u^2)f(t,v)$.

(b) If t,u generate a cyclic subgroup of k^* then $f(t,u) = f(u,t)$.

(c) If $f(t,u) = f(u,t)$, then $f(t,u^2) = 1$.

(d) If $t,u \neq 0$ and $t + u = 1$, then $f(t,u) = 1$.

Proof: Since $f(t,u) \in \ker \pi$, $f(t,u) \in$ center of G'. Set $h_\alpha(t) = h(t)$.

(a) $f(t,v) = h(u)f(t,v)h(u)^{-1}$

$= h(u)h(t)h(v)h(tv)^{-1}h(u)^{-1}$

$= h(tu^2)h(u^2)^{-1}h(vu^2)h(u^2)^{-1}h(u^2)h(tu^2v)^{-1}$ (by Lemma 37(f))

$= h(tu^2)h(u^2)^{-1}h(vu^2)h(tu^2v)^{-1}$

$= f(t,u^2)^{-1}f(t,u^2v)$.

(b) Let $t = v^m$, $u = v^n$ with $m,n \in \mathbb{Z}$. Then $h(t) = h(v)^m c$, $h(u) = h(v)^n d$ with $c, d \in$ center G', since

G' is a central extension of G. Thus $h(t)$, $h(u)$ commute and $f(t,u) = f(u,t)$.

(c) $h(t) = h(u)h(t)h(u)^{-1} = h(tu^2)h(u^2)^{-1}$ (by Lemma 37 (f)), so that $f(t,u^2) = 1$.

(d) Abbreviate x_α, $x_{-\alpha}$, w_α, h_α to x, y, w, h, respectively. We have:

(1) $w(t)x(u)w(-t) = y(-t^2u)$

(2) $w(t)y(u)w(-t) = x(-t^2u)$ (by (1))

(3) $w(t) = x(t)y(-t^{-1})x(t)$

(3') $w(t) = y(-t^{-1})x(t)y(-t^{-1})$ (by (1), (2), (3)).

Then $h(tu)h(u)^{-1} = w(tu)w(-u)$ by definition of h

$= x(t)x(-t)w(tu)w(-u) = x(t)w(tu)y(t^{-1}u^{-2})w(-u)$ (by (1))

$= x(t)y(-t^{-1}u^{-1})x(tu)y(-t^{-1}u^{-1})y(t^{-1}u^{-2})w(-u)$ (by (3'))

$= x(t)y(-t^{-1}u^{-1})x(tu)y(u^{-2})w)-u)$(by (A)

for $y(-t^{-1}u^{-1})y(t^{-1}u^{-2}) = y(t^{-1}u^{-2}(1-u)) = y(u^{-2})$)

$= x(t)y(-t^{-1}u^{-1})w(-u)y(-tu^{-1})x(-1)$ (by (1) and (2))

$= x(t)y(-t^{-1}u^{-1})y(u^{-1})x(-u)y(u^{-1})y(-tu^{-1})x(-1)$ (by (3'))

$= x(t)y(-t^{-1}u^{-1}(1-t))x(t-1)y(u^{-1}(1-t))x(-1)$

$= x(t)y(-t^{-1})x(t)x(-1)y(1)x(-1) = w(t)w(-1) = h(t)$, proving (d).

Lemma 40: In a field k of finite odd order there exist elements t,u such that t and u are not squares and $t + u = 1$.

Proof: If $|k| = q$ there are $(q+1)/2$ squares. Since $((q+1)/2)+q$ the squares do not form an additive group, so we can find a,b,c so that $a + b = c$ where a and b are squares

and c is not. Then take $t = a/c$, $u = b/c$.

Theorem 9: Assume that Σ is indecomposable and that k is an algebraic extension of a finite field. Then the relations (A) and (B) (or (B') if rank $\Sigma = 1$) suffice to define the corresponding universal Chevalley group, i.e. they imply the relations (C) .

Proof: Let $t, u \in k^*$. We must show $f(t,u) = 1$ where f is as in Lemma 39. By Lemma 39(b and c) if either t or u is a square $f(t,u) = 1$. Assume that both are not squares. By Lemma 40 (applied to the finite field generated by t and u) $t = r^2 t_1$, $u = s^2 u_1$ with $r, s \in k^*$, $t_1 + u_1 = 1$, t_1 and u_1 not squares. Then $f(t,u) = f(t,s^2u_1) = f(t,u_1) = f(r^2t_1,u_1) = f(t_1,u_1) = 1$ by Lemma 39(a and d).

Example: If $n \geq 3$ and k is a finite field, the symbols $x_{ij}(t)$ $(1 \leq i, j \leq n, i \neq j, t \in k)$ subject to the relations:

(A) $x_{ij}(t)x_{ij}(u) = x_{ij}(t+u)$

(B) $(x_{ij}(t),x_{jk}(u)) = x_{ik}(tu)$ if i,j,k are distinct,

$(x_{ij}(t),x_{k\ell}(u)) = 1$ if $j \neq k$, $i \neq \ell$,

define the group $SL_n(k)$.

§7. Central extensions.

Our object is to prove that if π, G', and G are as in §6, then (π, G') is a universal central extension of G in a sense to be defined. The reader is referred to the lecturer's paper in Colloque sur la théorie des groupes algébriques, Bruxelles, 1962 and for generalities to Schur's papers in J. Reine Angew. Math. 1904, 1907, 1911.

Definition: A central extension of a group G is a couple (π, G') where G' is a group, π is a homomorphism of G' onto G, and $\ker \pi \subset$ center of G'.

Examples:

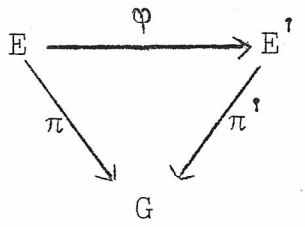
(a) π, G', G as in §6.

(b) $\pi : G' \longrightarrow G$ the natural homomorphism of one Chevalley group onto another constructed from a smaller weight lattice. E.g., $\pi : SL_n \longrightarrow PSL_n$, $\pi : Sp_n \longrightarrow PSp_n$, and $\pi : Spin_n \longrightarrow SO_n$.

(c) $\pi : G' \longrightarrow G$ a topological covering of a connected topological group; i.e., π is a local isomorphism, carrying a neighborhood of 1 isomorphically onto one of G. We note that π is central since a discrete normal subgroup of a connected group is necessarily central. To see this, let N be a discrete normal subgroup of a connected group G and let $n \in N$. Since the map $G \longrightarrow N$ given by $g \longrightarrow gng^{-1}$, $g \in G$, has a

discrete and connected image, $gng^{-1} = n$ for all $g \in G$.

Definition: A central extension (π, E) of a group G is universal if for any central extension (π', E') of G there exists a unique homomorphism $\varphi : E \longrightarrow E'$ such that $\pi'\varphi = \pi$, i.e., the following diagram is commutative:



We abbreviate univeral central extension by u.c.e. We develop this property in a sequence of statements.

(i) If a u.c.e. exists, it is unique up to isomorphism.

Proof: If (π, E) and (π', E') are u.c.e. of G, let $\varphi : E \longrightarrow E'$ and $\varphi' : E' \longrightarrow E$ be such that $\pi'\varphi = \pi$ and $\pi\varphi' = \pi'$. Now $\varphi'\varphi : E \longrightarrow E$ and $\pi(\varphi'\varphi) = \pi$. Hence $\varphi'\varphi$ is the identity on E by the uniqueness of φ in the definition of a u.c.e. Similarly $\varphi\varphi'$ is the identity on E'.

(ii) If (π, E) is a u.c.e. of G then $E = \mathcal{D}E$ and hence $G = \mathcal{D}G$, where $\mathcal{D}H$ is the derived group of H.

Proof: Consider the central extension (π', E') where $E' = E \times E/\mathcal{D}E$ and $\pi'(a,b) = \pi(a)$, $a \in E$, $b \in E/\mathcal{D}E$. Now if $\varphi_1(a) = (a,1)$ and $\varphi_2(a) = (a, a+\mathcal{D}E)$, then $\pi'\varphi_i = \pi$, $i = 1,2$, and hence $\varphi_1 = \varphi_2$. Thus, $E/\mathcal{D}E = 1$ and $E = \mathcal{D}E$.

(iii) If $G = \mathcal{D}G$ and (π,E) is a central extension of G, then $E = C.\mathcal{D}E$ where C is a central subgroup of E on which π is trivial. Moreover, $\mathcal{D}E = \mathcal{D}^2E$.

Proof: We have $\pi\mathcal{D}E = \mathcal{D}(\pi E) = \mathcal{D}G = G$. Hence, $E = C\mathcal{D}E$ where $C = \ker\pi$. Also, $\mathcal{D}E = \mathcal{D}(C\mathcal{D}E) = \mathcal{D}^2E$.

(iv) If $G = \mathcal{D}G$, then G possesses a u.c.e.

Proof: For each $x \in G$ we introduce a symbol $e(x)$. Let F be the group generated by $\{e(x), x \in G\}$ subject to the condition that $e(x)e(y)e(xy)^{-1}$ commutes with $e(z)$ for all $x,y,z \in G$. If $\pi : e(x) \longrightarrow x$, then by using induction on the length of an expression in F, we see that π extends to a central homomorphism of F onto G.

(a) (π,F) covers all central extensions of G. To see this, let (E', π') be any central extension of G. Choose $e'(x) \in E'$ such that $\pi'e'(x) = x$. Since π' is central, the $e'(x)$'s satisfy the condition on the $e(x)$'s. Hence, there is a homomorphism $\varphi : F \longrightarrow E'$ such that $\varphi e(x) = e'(x)$, and thus $\pi'\varphi = \pi$.

(b) If $E = \mathcal{D}F$ and π also denotes the restriction of π to E, then (π,E) covers all central extensions uniquely. By (iii), we have that (π,E) covers all central extensions. If (π,E') is a central extension of G and if $\pi'\varphi = \pi = \pi'\varphi'$, then $\varphi(x)\varphi'(x)^{-1} \in$ center of E. Thus, $\psi : x \to \varphi(x)\varphi'(x)^{-1}$ is a homomorphism of E into an Abelian group. Since $E = \mathcal{D}E$, ψ is trivial and $\varphi = \varphi'$.

Remark: Part (a) shows that if G is any group then there is a central extension covering all others.

(iv') If (π,E) is a central extension of G which covers all others and if $E = \mathcal{D}E$, then (π,E) is a u. c. e.

(v) If $\pi : E \longrightarrow F$ and $\Psi : F \longrightarrow G$ are central extensions, then so is $\Psi\pi : E \longrightarrow G$, provided $E = \mathcal{D}E$.

Proof: If $a \in \ker \Psi\pi$, let φ be the map $\varphi : x \longrightarrow (a,x) = axa^{-1}x^{-1}$, $x \in E$. Now $\varphi(x) \in$ center of E, since $\pi(a,x) = (\pi a, \pi x) = 1$ because $\pi a \in$ center of F. Now φ is a homomorphism, so φ is trivial, and $a \in$ center of E.

(vi) Exercise: In (v), (π,E) is a u. c. e of F if and only if $(\Psi\pi,E)$ is a u.c. e. of G.

Definition: A group G is said to be centrally closed if (id,G) is a u. c. e. of G.

(vii) Corollary: If (π,E) is a u.c. e. of G, then E is centrally closed.

(viii) If E is centrally closed, then every central extension $\Psi : F \longrightarrow E$ of E splits; i.e, there exists a homomorphism $\varphi : E \longrightarrow F$ such that $\Psi\varphi = id$.

(ix) (π,E) is a u.c. e. of G if and only if every diagram of the form

$$\begin{array}{ccc} E & \dashrightarrow & E' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ G & \xrightarrow[\rho]{} & G' \end{array}$$

can be uniquely completed, where (π', E') is a central extension of G' and ρ is a homomorphism.

Proof: One direction is immediate by taking $G' = G$ and $\rho = id$. Conversely, suppose the diagram is given and (ψ, E) is a u.c.e. Let H be the subgroup of $G \times E'$, $H = \{(x,e') \mid \rho x = \pi' e'\}$. If $\psi: H \to G$ is given by $\psi(x,e') = x$, then ψ is central. Since (π,E) is a u.c.e. of G, there is a unique homomorphism $\theta : E \to H$ such that $\psi\theta = \pi$. Now the homomorphism $\varphi : E \to E'$, $\varphi = \psi'\theta$, where $\psi' : H \to E'$ is given by $\psi'(x,e') = e'$, satisfies $\rho\pi = \rho\psi\theta = \pi'\psi'\theta = \pi'\varphi$. If $\rho\pi = \pi'\varphi'$, then let $\theta' : E \to H$ be given by $\theta'(e) = (\pi(e), \varphi'(e))$. Since $\psi\theta' = \pi$, we have $\theta' = \theta$ and $\varphi' = \psi'\theta' = \psi'\theta = \varphi$, proving the uniqueness of φ.

Definition: A linear (respectively projective) representation of a group G is a homomorphism of G into some $GL(V)$ (respectively $PGL(V)$).

Since $GL(V)$ is a central extension of $PGL(V)$ we have the following result:

(x) Corollary: If (π,E) is a u.c.e. of G, then every projective representation of G can be lifted uniquely to a linear representation of E.

(xi) Topological situation: If G is a topological group one can replace the condition $G = \mathcal{D}G$ by G is connected, the condition (π,E) is a u.c.e. by (π,E) is a universal covering group in the topological sense, and the condition G is centrally closed

by G is simply connected in the above discussion and obtain similar results.

Definition: If (π,E) is a u.c.e of the group G, then we call $\ker \pi$ the Schur multiplier of G.

If we write $\ker \pi = M(G)$ to indicate the dependence on G, then a homomorphism, $\varphi : G \longrightarrow G'$ leads to a corresponding one $M(\varphi): M(G) \longrightarrow M(G')$ by (ix). Thus M is a functor from the category of groups G such that $G = \mathcal{D} G$ to the category of Abelian groups with the following property: if φ is onto, then so is $M(\varphi)$.

Remark: Schur used different definitions (and terminology) since he considered only finite groups but did not require that $G = \mathcal{D} G$. If $G = \mathcal{D} G$ our definitions are equivalent to his. One of Schur's results, which we shall not use, is that if G is finite then so is M(G).

Theorem 10: Let Σ be an indecomposable root system and k a field such that $|k| > 4$ and, if rank $\Sigma = 1$, then $|k| \neq 9$. If G is the corresponding universal Chevalley group (abstractly defined by the relations (A),(B),(B'),(C) of §6), if G' is the group defined by the relations (A),(B),(B') (we use (B') only if rank $\Sigma = 1$), and if π is the natural homomorphism from G' to G, then (π,G') is a u.c.e. of G.

Remark: There are exceptions to the conclusion. E.g. $SL_2(4)$ and $SL_2(9)$ are such. Indeed $SL_2(4) \cong PSL_2(5)$ and $SL_2(5)$ is a central

extension of $PSL_2(5)$. For $SL_2(9)$ see Schur. It can be shown that the number of couples (Σ,k) for which the conclusion fails is finite.

Proof: Since $|k| > 4$, $G = \mathcal{D}G$, $G' = \mathcal{D}G'$, and u.c.e. exist for both G and G'. The conclusion becomes G' is centrally closed, by the above remarks. We need only show that every central extension (Ψ, E) of G' splits, i.e., there exists $\theta : G' \longrightarrow E$ so that $\Psi\theta = id_{G'}$; i.e., the relations defining G' can be lifted to E.

We may assume $E = \mathcal{D}E$; but then $(\pi\Psi, E)$ is a central extension of G by (v). We need only show

(1) If (Ψ, E) is a central extension of G, then the relations (A), (B), (B') can be lifted to E.

Let $C = \ker \Psi$, a central subgroup of E. We have:

(2) A commutator (x,y) with $x,y \in E$ depends only on the classes mod C to which x and y belong.

Choose $a \in k^*$ so that $c = a^2 - 1 \neq 0$. Then in G $(h_\alpha(a), x_\alpha(t)) = x_\alpha(ct)$ for all $\alpha \in \Sigma$, $t \in k$. We define $\varphi x_\alpha(t) \in E$ $(\alpha \in \Sigma, t \in k)$ so that $\Psi \varphi x_\alpha(t) = x_\alpha(t)$ and so that

(3) $(\varphi h_\alpha(a), \varphi x_\alpha(t)) = \varphi x_\alpha(ct)$ and then φh's (and later φw's) in terms of the φx's by the same formulas which define the h's and the w's in terms of the x's. Note that this choice is not circular because of (2). We shall show that the relations (A), (B), (B') hold with φx's in place of x's.

(4) $\varphi h \varphi x_\alpha(t)(\varphi h)^{-1} = \varphi(h x_\alpha(t) h^{-1})$ for all $h \in H$, $\alpha \in \Sigma$, $t \in k$.

Set $h x_\alpha(t)h^{-1} = x_\alpha(dt)$ with $d \in k^*$. Conjugating (3) by φh, we get $(\varphi h_\alpha(a), \varphi x_\alpha(dt)) = \varphi h \varphi x_\alpha(ct)\varphi(h)^{-1}$, and the left side equals $\varphi x_\alpha(cdt) = \varphi(h x_\alpha(ct)h^{-1})$ by (3). Similarly we have

(4') $\varphi n \varphi x_\alpha(t)(\varphi n)^{-1} = \varphi(n x_\alpha(t)n^{-1})$ for all $n \in N$, $\alpha \in \Sigma$, $t \in k$.

(5) If α and β are roots, $\alpha + \beta \neq 0$, and $\alpha + \beta$ is not a root, then $\varphi x_\alpha(t)$ and $\varphi x_\beta(u)$ commute for all $t,u \in k$. Set $\varphi x_\alpha(t) \varphi x_\beta(u) \varphi x_\alpha(t)^{-1} = f(t,u) \varphi x_\beta(u)$, $t,u \in k$, $f(t,u) \in C$. We must show $f(t,u) = 1$. Clearly, from the definitions we have

(6) f is additive in both positions.

(5a) Assume $\alpha \neq \beta$. If $(\alpha,\beta) = 0$, then $f(t,u) = f(tv^2,u)(v \neq 0)$ by Lemma 20(c) and by (4) with $h = h_\alpha(v)$. If $(\alpha,\beta) > 0$, then $f(t,u) = f(tv^d,u)$ where $d = 4 - \langle\alpha,\beta\rangle\langle\beta,\alpha\rangle$ by Lemma 20(c) and by (4) with $h = h_\alpha(v^2)\, h_\beta\left(v^{-\langle\beta,\alpha\rangle}\right)$. In both cass, $f(t(1-v^d),u) = 1$ by (6) for some $d = 1,2,$ or 3. Choose v so $v^d - 1 \neq 0$. Then we get $f \equiv 1$.

(5b) Assume $\alpha = \beta$ and rank $\Sigma > 1$. If there is a root γ so that $\langle\alpha,\gamma\rangle = 1$, set $h = h_\gamma(v)$ in the preceding argument and obtain (*) $f(t,u) = f(tv,uv)$. Choose v so that $v - v^2 \neq 0$ and $1 - v + v^2 \neq 0$. By (*) and (6), $f(t(v-v^2),u) = f\left(t,u/(v-v^2)\right) = f(t,u/v)f\left(t,u/(1-v)\right) = f(vt,u)f((1-v)t,u)$ $= f(t,u)$, whence $f(t(1-v+v^2),u) = 1$ and $f \equiv 1$. If there is no

such γ, then Σ is of type C_n and α is a long root. In this case, however, $\alpha = \beta + 2\gamma$ with β and γ roots. Thus, $(\varphi x_\beta(t), \varphi x_\gamma(u)) = g\varphi x_{\beta+\gamma}(\pm tu)\varphi x_{\beta+2\gamma}(\pm tu^2)$ with $g \in C$, by Lemma 33. Since $\varphi x_\alpha(v)$ commutes with all factors but the last by (5a), it also commutes with the last.

(5c) Assume $\alpha = \beta$ and rank $\Sigma = 1$. At least we have $f(t,u) = f(tv^2, uv^2)$, $t,u \in k$, $v \in k^*$, using $h = h_\alpha(v)$ in the argument above. We may also assume that $|k|$ is not a prime. If it were, then $x_\alpha(t)$ and $x_\alpha(u)$ would be powers of $x_\alpha(1)$ and (5) would be immediate. Referring to the proof of (5b), we see it will suffice to be able to choose v so that v, $1-v$ are squares and $v - v^2 \neq 0$, $1 - v + v^2 \neq 0$. If k is finite of characteristic 2, this is possible since all elements of k are squares. Otherwise, set $v = \left(2w/(1+w^2)\right)^2$. Then $1 - v = \left((1-w^2)/(1+w^2)\right)^2$, and we need only choose w so that $1 + w^2 \neq 0$, $v - v^2 \neq 0$, and $1 - v + v^2 \neq 0$. Since at most 13 values of w are to be avoided and $|k| \geq 25$ in the present case, this too is possible. This completes the proof of (5).

(7) φ preserves the relations (A). The element $x = \varphi x_\alpha(tc^{-1})\varphi x_\alpha(uc^{-1})\left(\varphi x_\alpha((t+u)c^{-1})\right)^{-1}$ is in C, and hence the transform of x by $h_\alpha(a)$ is x itself. However, by (3), (4), (5) this transform is also $x\varphi x_\alpha(t)\varphi x_\alpha(u)\left(\varphi x_\alpha(t+u)\right)^{-1}$.

(8) φ preserves the relations (B). We have $\varphi x_\alpha(t)\varphi x_\beta(u)\varphi x_\alpha(t)^{-1} = f(t,u)\prod \varphi x_{i\alpha+j\beta}(c_{ij}t^i u^j)\varphi x_\beta(u)$, where $f(t,u) \in C$. One proves $f = 1$ by induction on n, the

number of roots of the form $i\alpha + j\beta$ i, $j \in \mathbb{Z}^+$. If $n = 0$, this is just (5). If $n > 0$, the inductive hypothesis and (7) imply f satisfies (6), and then the argument in (5a) may be used.

(9) φ preserves the relations (B'). This follows from $(4')$.

This completes the proof of the theorem.

Exercise: Assume $\mathcal{L}$ is the original Lie algebra with coefficients transferred by means of a Chevalley basis to a field k whose characteristic does not divide any $N_{\alpha,\beta} \neq 0$. Also assume Σ is indecomposable of rank > 1. Prove:

(a) The relations $[X_\alpha, X_\beta] = N_{\alpha,\beta} X_{\alpha+\beta}$, $\alpha + \beta \neq 0$, form a defining set for $\mathcal{L}$. Hint: define $H_\alpha = [X_\alpha, X_{-\alpha}]$ and show that the relations of Theorem 1 hold.

(b) $\mathcal{L} = \mathcal{D}\mathcal{L}$, the derived algebra of $\mathcal{L}$.

(c) Every central extension of $\mathcal{L}$ splits.
Hint: parallel the proof of Theorem 10.

Corollary 1: The relations $(A), (B), (B')$ can be lifted to any central extension of G.

Corollary 2:

(a) G' is centrally closed. Each of its central extensions splits. Its Schur multiplier is trivial. It yields the u. c. e. of all the Chevalley groups of the given type, and covers linearly all of the projective representations of these groups.

(b) If k is finite or more generally an algebraic extension of a finite field, then (a) holds with G' replaced by G.

Proof: This follows from various of the generalities at the beginning of this section.

E.g., if k is finite, $|k| > 4$ and $SL_2(9)$ is excluded, then $SL_n(k)$, $Sp_n(k)$, and $Spin_n(k)$ all have trivial Schur multipliers, and the natural central extensions $SL_n \longrightarrow PSL_n$, $Sp_n \longrightarrow PSp_n$, $Spin_n \longrightarrow SO_n$ are all universal.

Corollary 3: Assume G, G', and π are as above. If k^* is infinite and divisible ($u \in k^*$, $n \in \mathbb{Z}$ implies there exists $v \in k^*$ with $v^n = u$), then the Schur multiplier of G; i.e., $C = \ker \pi$, is also divisible.

Proof: Elements of the form $f(t,u) = h_\alpha(t)h_\alpha(u)h_\alpha(tu)^{-1}$ in G' $\alpha \in \Sigma$ generate C. We have $f(t,vw^2) = f(t,v)f(t,w^2)$ by Lemma 39(a). By induction, we get $f(t,w^{2n}) = f(t,w^2)^n$ for arbitrary n. Since for $u \in k^*$ we can find $w \in k^*$ such that $u = w^{2n}$, the proof is complete.

Corollary 3a: If k^* is infinite and divisible by a set of primes including 2, then C is also divisible by these primes.

Corollary 3b: If k^* is infinite and divisible, then any central extension of G by a kernel which is a reduced group (no divisible subgroups other than 1) is trivial; i.e., it splits.

Proof: Let (Ψ, E) be a central extension of G with $\ker \Psi$ reduced. Since (π, G') is a u.c.e. we have $\varphi : G' \longrightarrow E$ so that $\Psi\varphi = \pi$. Since $C = \ker \pi$ is divisible, so is $\varphi C \subseteq \ker \Psi$. Hence $\varphi C = 1$ and $\ker \varphi \supseteq \ker \pi$. Thus, there is a homomorphism $\Theta : G \longrightarrow E$ so that $\Theta\pi = \varphi$. Therefore,

$\psi\theta\pi = \pi$ on G' and $\psi\theta = 1$ on $\mathfrak{C}$.

Corollary 3c: If k^* is infinite and divisible, then any finite dimensional projective representation of G can be lifted uniquely to a linear representation.

Proof: Assume $\sigma : G \to PGL(V)$. Since $G = \mathfrak{O}G$, we have $\sigma : G \to PSL(V)$. Let $\rho : SL(V) \to PSL(V)$ be the natural projection. Since $\dim V$ is finite, we have $\ker \rho$ is finite and thus $\ker \rho$ is reduced. Consider the central extension (ψ, E) of G where $E = \{(x,y) \mid \sigma x = \rho y, x \in G, y \in SL(V)\} \subseteq G \times SL(V)$ and $\psi(x,y) = x$, $(x,y) \in E$. Now $\ker \psi = 1 \times \ker \rho$ is reduced, so by Corollary 3b, we have $\theta : G \to E$ with $\psi\theta = 1$ on G. If $\psi'(x,y) = y, (x,y) \in E$, then $\sigma' = \psi'\theta : G \to SL(V) \subset GL(V)$ with $\rho\sigma' = \rho\psi'\theta = \sigma\psi\theta = \sigma$.

Example: Corollary 3c says, for example, that every finite dimensional representation of $SL_n(\mathbb{C})$ can be lifted to a linear one. (The novelty is that the representation is not assumed to be continuous.)

Theorem 11: If Σ is an indecomposable root system, if $\operatorname{char} k = p \neq 0$, and if $G = \mathfrak{O}G$ (i.e. we exclude $|k| = 2$, Σ of type A_1, B_2, or G_2 and $|k| = 3$, Σ of type A_1), then (π, G') uniquely covers all central extensions of G for which the kernel has no p-torsion.

Proof: By Theorem 10, we could assume $|k| \leq 4$ or $|k| = 9$. However, the proof does not use this assumption or Theorem 10. If (ψ, E) is a central extension of G such that $C = \ker \psi$

has no p-torsion, then we wish to show (A),(B), and (B') can be lifted to E.

(1) Assume C is divisible by p. Choose $\varphi x_\alpha(t) \in E$ so that $\psi \varphi x_\alpha(t) = x_\alpha(t)$ and $(\varphi x_\alpha(t))^p = 1, \alpha \in \Sigma, t \in k$. We claim relations (A),(B) and (B') hold on the φx's.

(1a) If α,β are roots, $\alpha+\beta$ not a root, and $\alpha+\beta \neq 0$, then $\varphi x_\alpha(t)$ and $\varphi x_\beta(u)$ commute, $t,u \in k$. We have $\varphi x_\alpha(t)\varphi x_\beta(u)\varphi x_\alpha(t)^{-1} = f\varphi x_\alpha(u)$ with $f \in C$. Taking p-th powers, we get $1 = f^p$ which implies $f = 1$ since C has no p-torsion.

(1b) The relations (A) hold. Taking p-th powers of $\varphi x_\alpha(t)\varphi x_\alpha(u) = f\varphi_\alpha(t+u)$, $f \in C$, we get $f = 1$ as before.

(1c) Exercise: Relations (B) and (B') also hold.

(2) General case.

(2a) C can be embedded in a group C' which is divisible by p and has no p-torsion. We have a homomorphism θ of a free Abelian group F onto C. Now $F \otimes_{\mathbb{Z}} Q$ is a divisible group, and we can identify F with $F \otimes_{\mathbb{Z}} \mathbb{Z} \subset F \otimes_{\mathbb{Z}} Q$. Hence $C = F/\ker\theta \subset F \otimes_{\mathbb{Z}} Q/\ker\theta = D$, say, and D is a divisible group. Moreover, since C has no p-torsion, $C \cap D_p = 1$ where D_p is the p-component of D. Thus, C projects faithfully into $D/D_p = C'$ which is divisible and has no p-torsion.

(2b) Conclusion of proof. Form $E' = EC'$, the direct product of E and C' with C amalgamated, and define $\psi' : E' \longrightarrow G$ by $\psi'(e\,c') = \psi(e)$, $e \in E$, $c' \in C'$.

Now (ψ', E') satisfies the assumptions of (1) so the relations (A),(B),(B') can be lifted to E'. However, by Lemma 32', the lifted group is its own derived group and hence contained in E.

Corollary 1: Every projective representation of G' in a field of characteristic p can be lifted to a linear one.

Corollary 2: The Schur multiplier of G' is a p-group.

Proofs: These are easy exercises.

Since the kernel of the map $\pi : G' \longrightarrow G$ above turns out to be the Schur multiplier of G, its structure for k arbitrary is of some interest. The result is:

Theorem 12: (Moore, Matsumoto) Assume Σ is an indecomposable root system and k a field with $|k| > 4$. If G is the universal Chevalley group based on Σ and k, if G' is the group defined by (A),(B),(B'), and if π is the natural map from G' to G with $C = \ker \pi$, the Schur multiplier of G, then C is isomorphic to the abstract group A generated by the symbols $f(t,u)$ $(t,u \in k^*)$ subject to the relations:

(a) $f(t,u)f(tu,v) = f(t,uv)f(u,v)$, $f(1,u) = f(u,1) = 1$

(b) $f(t,u)f(t,-u^{-1}) = f(t,-1)$

(c) $f(t,u) = f(u^{-1},t)$

(d) $f(t,u) = f(t,-tu)$

(e) $f(t,u) = f(t,(1-t)u)$

and in the case Σ is not of type C_n $(n \geq 1)(C_1 = A_1)$ the

additional relation:

(ab') f is bimultiplicative.

In this case relations (a) - (e) may be replaced by (ab') and

(c') f is skew

(d') $f(t,-t) = 1$

(e') $f(t,1-t) = 1$.

The isomorphism is given by $\varphi: f(t,u) \longrightarrow h_\alpha(t)h_\alpha(u)h_\alpha(tu)^{-1}$, α a fixed long root.

Remark: These relations are satisfied by the norm residue symbol in class field theory, which is a significant aspect of Moore's work.

Partial Proof:

(1) If $\mathfrak{h}_\alpha$ is the group generated (in G') by all $h_\alpha(t)$, α a fixed long root, then $C \subseteq \mathfrak{h}_\alpha$. We know that $h_\alpha(t)h_\alpha(u)h_\alpha(tu)^{-1}$, $\alpha \in \Sigma$, $t \in k^*$, form a generating set for C. Using the Weyl group we can narrow the situation to at most two roots α,β with α long, β short, and $(\alpha,\beta) > 0$. Hence, $\langle\beta,\alpha\rangle = 1$ and $\left(h_\alpha(t),h_\beta(u)\right) = h_\beta(tu)h_\beta(t)^{-1}h_\beta(u)^{-1}$ $= h_\alpha(t)h_\alpha(u^{\langle\alpha,\beta\rangle})h_\alpha(tu^{\langle\alpha,\beta\rangle})^{-1}$ by Lemma 37(f). This shows α will suffice.

(2) φ is a mapping onto C. This follows from (1).

(3) φ is a homomorphism. We must show that the relations hold if $f(t,u)$ is replaced by $h_\alpha(t)h_\alpha(u)h_\alpha(tu)^{-1}$. The relations (a) are obvious. A special case ($u = 1$) of (e) has been shown

in Lemma 39(d). The other relations (b),(c),(d) follow from the commutator relations connecting the h's and the w's.

(3') Assume Σ is not of type C_n. In this case there is a root γ so that $\langle \alpha, \gamma \rangle = 1$. Thus $f(t,v) = h_\gamma(u) f(t,v) h_\gamma(u)^{-1} = h_\alpha(tu) h_\alpha(u)^{-1} h_\alpha(uv) h_\alpha(tuv)^{-1} = f(t,u)^{-1} f(t,uv)$ or $f(t,uv) = f(t,u) f(t,v)$. By relation (c), $f(uv,t) = f(u,t) f(v,t)$.

(4) φ is an isomorphism. This is done by constructing an explicit model for G'.

Now let G be a connected topological group. A <u>covering</u> of G is a couple (π, E) such that E is a connected topological group and π is a homomorphism of E onto G which maps a neighborhood of 1 in E homeomorphically onto a neighborhood of 1 in G; i.e., which is a local isomorphism. A covering is <u>universal</u> if it covers all other covering groups. If (id,G) is a universal covering, we say that G is <u>simply connected</u>.

<u>Remarks</u>:

(a) A covering (π, E) of a connected group is necessarily central as was noted at the beginning of this section.

(b) If a universal covering exists, then it is unique and each of its coverings of other covering groups is unique. This follows from the fact that a connected group is generated by any neighborhood of 1.

(c) If G is a Lie group, then a universal covering for G exists and simple connectedness is equivalent to the property that every continuous loop can be shrunk to a point (See Chevalley, Lie Groups or Cohn, Lie Groups.)

Theorem 13: If G is a universal Chevalley group over $\mathbb{C}$ viewed as a Lie group, then G is simply connected.

Before proving Theorem 13, we shall first state a lemma whose proof we leave as an exercise.

Lemma 41: If $t_1, t_2, \ldots, t_n$ are complex numbers such that $|t_i| < \epsilon, i = 1,2,\ldots,n$ and $\sum_{i=1}^{n} t_i = 0$, there exist t_i and t_j such that $|t_i + t_j| < \epsilon$.

Proof of Theorem 13: Let (π, E) be a covering of G. Locally π is invertible so we may set $\varphi = \pi^{-1}$ on some neighborhood of 1 in G. We shall show that φ can be extended to a homomorphism of G onto E; i.e., (id, G) covers (π, E). It suffices to show that φ can be extended to all of G so that the relations (A), (B), (B'), (C) hold on the φx's.

Consider the relations

(A) $\varphi x_\alpha(t)\, \varphi x_\alpha(u) = \varphi x_\alpha(t+u) \qquad \alpha \in \Sigma$.

Since φ is locally an isomorphism, there is $\epsilon > 0$ such that (A) holds for $|t| < \epsilon$, $|u| < \epsilon$. If $t \in k$, $t = \Sigma t_i$, $|t_i| < \epsilon$, then set $\varphi x_\alpha(t) = \prod \varphi x_\alpha(t_i)$. Using induction and Lemma 41, we see that $\varphi x_\alpha(t)$ is well defined. Clearly, (A) then holds for all $t, u \in k$. Alternatively, we could note that $\mathcal{X}_\alpha$ is topologically equivalent to $\mathbb{C}$ and hence simply connected. Thus, φ

extends to a homomorphism of $\mathcal{X}_\alpha$ into E and (A) holds. Clearly the extension of φ to $\mathcal{X}_\alpha$ is unique.

To obtain the relations (B), let α, β be roots $\alpha \neq \pm \beta$, let S be the set of roots of the form $i\alpha + j\beta$ $(i,j \in \mathbb{Z}^+)$, and let $\mathcal{X}_S$ be the corresponding unipotent subgroup of G. Topologically, $\mathcal{X}_S$ is equivalent to $\mathbb{C}^n$ for some n, and is hence simply connected. As before φ can be extended to a homomorphism of $\mathcal{X}_S$ into E, and the relations (B) hold. This extension is consistent with those above, by the uniqueness of the latter.

We now consider $h_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$. $w_\alpha(-1) = x_\alpha(t-1)x_{-\alpha}(1-t^{-1})^{x_\alpha(-1)} x_\alpha(t-1)^{w_\alpha(-1)}$ where $x^y = y^{-1}xy$. Hence, if t is near 1 in $\mathbb{C}$, then $\varphi h_\alpha(t)$ is near 1 in E. Thus, $\varphi h_\alpha(t)$ is multiplicative near 1 and hence Abelian everywhere (recall that $\mathcal{Y}$ is central). We then have $\varphi h_\alpha(u) = \varphi h_\alpha(t)\varphi h_\alpha(u)\varphi h_\alpha(t)^{-1} = \varphi h_\alpha(t^2u)\varphi h_\alpha(t^2)^{-1}$ by Lemma 37(f). Since $\mathbb{C}$ has square roots, we have φh_α is multiplicative, i.e., (C) holds.

Examples: $SL_n(\mathbb{C})$, $Sp_n(\mathbb{C})$, and $Spin_n(\mathbb{C})$ are simply connected. These cases can also be proved by induction on n. (See Chevalley, Lie Groups, Chapter II.)

Remarks:

(a) If $\mathbb{C}$ is replaced by $\mathbb{R}$ in the preceding discussion, then relations (A),(B) can be lifted exactly as before. Also φh_α is still multiplicative if one of the two arguments is

positive. Further $\ker \pi$ is generated by $\varphi h_\alpha(-1)^2$, α a fixed long root, and, if type C_n $(n \geq 1)$ is excluded, then $h_\alpha(-1)^4 = 1$ or $w_\alpha(-1)^8 = 1$. Prove all of this.

(b) Moore has constructed a universal covering of G and has determined the fundamental group in case k is a p-adic field, using appropriate modifications of the definitions (here G is totally disconnected.)

(c) Let G be a Chevalley group over k, G' the corresponding universal group, and $\pi : G' \longrightarrow G$ the natural homomorphism. If k is algebraically closed and if only appropriate coverings are allowed, then (π, G') is a universal covering of G in the sense of algebraic groups.

We close this section with a result in which the coefficients may come from any ring (associative with 1). The development is based in part on a letter from J. Milnor. Let R be the ring, and let $GL(R)$ be the group of infinite matrices which are equal to the identity everywhere except for a finite invertible block in the upper left hand corner. Thus, $GL_n(R) \subset GL(R)$, $n = 1,2,\ldots$. Let $E(R)$ be the subgroup of $GL(R)$ generated by the elementary matrices $1 + tE_{ij}$ $(t \in R, i \neq j, i, j = 1,2,\ldots)$, where E_{ij} is the usual matrix unit. For example, if R is a field, then $E(R) = SL(R)$, a simple group whose double coset decomposition involves the infinite symmetric group. Indeed, if R is a Euclidean domain, then $E(R) = SL(R)$.

Lemma 42:

(a) $E(R) = \mathcal{D} GL(R)$

(b) $E(R) = \mathcal{D} E(R)$

Proof: The relation $(1+tE_{ik}, 1+E_{kj}) = 1+tE_{ij}$ shows (b) and hence also $E(R) \subseteq \mathcal{D} GL(R)$. If $x,y \in GL_n(R)$, then $xyx^{-1}y^{-1} \in E(R)$ because in $GL_{2n}(R)$ we have

$$(1)\quad \begin{bmatrix} xyx^{-1}y^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix} \begin{bmatrix} (yx)^{-1} & 0 \\ 0 & yx \end{bmatrix}$$

$$(2)\quad \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-x^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-x & 1 \end{bmatrix}$$

$$(3)\quad \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \prod_{i=1}^{n} \prod_{j=n+1}^{2n} (1 + x_{ij}E_{ij}), \quad \text{if } x = (x_{ij}).$$

We call $K_1(R) = GL(R)/E(R)$ the Whitehead group of R. This concept is used in topology. The case in which $R = \mathbb{Z}[G]$ is of particular interest.

Example: If R is a Euclidean domain, then $K_1(R) = R^*$, the group of units. (See Milnor, Whitehead Torsion.)

By Lemma 42 and (iv), $E(R)$ has a u.c.e. $(\pi, U(R))$. Set $K_2(R) = \ker \pi$. This notation is partly motived by the following exact sequence.

$$1 \longrightarrow K_2(R) \longrightarrow U(R) \longrightarrow GL(R) \longrightarrow K_1(R) \longrightarrow 1.$$

K_2 is a functor from rings to Abelian groups with the following property: if $R \longrightarrow R'$ is onto, then so is the associated map $K_2(R) \longrightarrow K_2(R')$.

Remark: K_2 is known to the lecturer in the following cases:

(a) If R is a finite field (or an algebraic extension of a finite field), then $K_2 = 1$.

(b) If R is any field, see Theorem 12.

(c) If $R = \mathbb{Z}$, then $|K_2| = 2$.

Here (a) follows from Theorem 9 and the next theorem, and a proof of (c) will be sketched after the remarks following the corollaries to the next theorem.

Theorem 14: Let $U(R)$ be the abstract group generated by the symbols $x_{ij}(t)$ $(t \in R,\ i \neq j,\ i,j = 1,2,\ldots)$ subject to the relations

(A) $x_{ij}(t)$ is additive in t.

(B) $(x_{ik}(t), x_{\ell j}(u)) = \begin{cases} x_{ij}(tu) & \text{if } k = \ell\ ,\ i \neq j\ . \\ 1 & \text{if } k \neq \ell\ ,\ i \neq j\ . \end{cases}$

If $\pi : U(R) \longrightarrow E(R)$ is the homomorphism given by $x_{ij}(t) \longrightarrow 1 + tE_{ij}$, then $(\pi, U(R))$ is a u.c.e. for $E(R)$.

Proof: (a) π is central. If $x \in \ker \pi$, choose n large enough so that x is a product of x_{ij}'s with $i,j < n$. Let P_n be the subgroup of $U(R)$ generated by the x_{kn}'s $(k \neq n,\ k = 1,2,\ldots)$. Now by (A) and (B), any element of P_n can be expressed as

$\prod_k x_{kn}(t_k)$. Since in $E(R)$ this form is unique, $\pi|P_n$ is an isomorphism. Also by (A) and (B), $x_{ij}(t)\, P_n\, x_{ij}(t)^{-1} \subseteq P_n$ if $i,j < n$. Thus, $x\, P_n\, x^{-1} \in P_n$. If $y \in P_n$, then $\pi(x,y) = 1$, and since $\pi|P_n$ is an isomorphism we have $(x,y) = 1$. In particular, x commutes with all $x_{kn}(t)$. Similarly, x commutes with all $x_{nk}(t)$ and hence with all $x_{ij}(t) = (x_{in}(t), x_{nj}(1))$. Thus, x is in the center of $U(R)$.

(b) π is universal. From (B), it follows that $U(R) = \mathfrak{D}U(R)$. Hence it suffices to show it covers all central extensions. Let (Ψ, A) be a central extension of $E(R)$ and let C be the center of A. We must show that we can lift the relations (A) and (B) to A. Fix i,j $i \neq j$ and choose $p \neq i,j$. Choose $y_{ij}(t) \in \Psi^{-1} x_{ij}(t)$ so that (*) $(y_{ip}(t), y_{pj}(1)) = y_{ij}(t)$. We will prove that the y's satisfy the equations (A) and (B).

(b1) If $i \neq j$, $k \neq \ell$, then $y_{ik}(t)$ and $y_{\ell j}(u)$ commute. Choose $q \neq i,j,k,\ell$ and write $y_{\ell j}(u) = c(y_{\ell q}(u), y_{qj}(1))$, $c \in C$. Since $y_{ik}(t)$ commutes up to an element of C with $y_{\ell q}(u)$ and $y_{qj}(1)$, it commutes with $y_{\ell j}(u)$. Hence

(b2) $\{y_{ij}(t)\}$, i,j fixed, is Abelian.

(b3) The relations (A) hold. The proof is exactly the same as that of statement (7) in the proof of Theorem 10.

(b4) $y_{ij}(t)$ in (*) is independent of the choice of p. If $q \neq p,i,j$, set $w = y_{qp}(1)\, y_{pq}(-1)\, y_{qp}(1)$. Transforming (*) by w and using (b1) we get (*) with q in place of p.

(b5) The relations (B) hold. We will use:

(**) If, a,b,c are elements of a group such that a

commutes with c and such that (b,c) commutes with (a,b) and c, then $(a,(b,c)) = ((a,b),c)$. Since a commutes with c, $(a,(b,c))$ $=((a,b),(b,c)c)$. The other conditions insure $((a,b),(b,c)c) = ((a,b),c)$. Now assume i,j,k are distinct. Choose $q \neq i,j,k$, so that $(y_{ik}(t),y_{kj}(u)) = (y_{ik}(t),(y_{kq}(u),y_{qj}(1))) = ((y_{ik}(t),y_{kq}(u)),y_{qj}(1))$ $= (y_{iq}(tu),y_{qj}(1)) = y_{ij}(tu)$ by (*), (**), and (b4).

This completes the proof of the theorem.

Let $U_n(R)$ denote the subgroup of $U(R)$ generated by $y_{ij}(t)$ with $i,j \leq n$.

Corollary 1: If $n \geq 5$, then $U_n(R)$ is centrally closed.

Corollary 2: If R is a finite field and $n \geq 5$ then $SL_n(R)$ is centrally closed.

Proof: This follows from Corollary 1 and the equations $E_n(R) = SL_n(R) = U_n(R)$.

Remarks: (a) It follows that if R is a finite field and if $SL_n(R)$ is not centrally closed, then either $|R| = 9$, $n = 2$ or $|R| \leq 4$ and $n \leq 4$. The exact set of exceptions is : $SL_2(4)$, $SL_2(9)$, $SL_3(2)$, $SL_3(4)$, $SL_4(2)$.

* Exercise: Prove this.

(b) The argument above can be phrased in terms of roots, etc. As such, it carries over very easily to the case in which all roots have one length. The only other exception is $D_4(2)$.

(c) By a more complicated extension of the argument, it can also be shown that the universal Chevalley group of type B_n or C_n

over a finite field (or an algebraic extension of a finite field) is centrally closed if n is large enough. Hence, only a finite number of universal Chevalley groups with Σ indecomposable and k finite fail to be centrally closed.

Now we sketch a proof that $K_2(\mathbb{Z})$ is a group of order 2. The notation $U, U_n, \ldots$ above will be used. The proof depends on the following result:

(1) For $n \geq 3$, $SL_n(\mathbb{Z})$ is generated by symbols $x_{ij}(i,j = 1,2,\ldots,n;\ i \neq j)$ subject to the relations

$$(B)\quad (x_{ik}, x_{\ell j}) = \begin{cases} x_{ij} & \text{if } k = \ell,\ i \neq j, \\ 1 & \text{if } k \neq \ell,\ i \neq j. \end{cases}$$

(C) If $w_{ij} = x_{ij}\, x_{ij}^{-1} x_{ij}$, $h_{ij} = w_{ij}^2$, then $h_{ij}^2 = 1$.

Identifying x_{ij} with the usual $x_{ij}(1)$ and using $x_{ij}(t) = x_{ij}(1)^t$, we see that the relations (B) here imply those of Theorem 14. Since the last relation may be written $h_{ij}(-1)^2 = h_{ij}(1)$ and ± 1 are the only units of $\mathbb{Z}$, we have $SL_n(\mathbb{Z})$ defined by the usual relations (A),(B),(C) of §6. Perhaps there are other rings, e.g., the p-adic integers, for which this result holds. For the proof of (1) see W. Magnus, Acta Math. 64 (1934), which gives the reference to Nielsen, who proved the key case $n = 3$ (it takes some work to cast Nielsen's result into the above form). The case $n = 2$, with (B) replaced by (B') $w_{12}\, x_{12}\, w_{12}^{-1} = x_{21}^{-1}$, is simpler and is proved in an appendix

to Kurosh, Theory of Groups.

Now let x_{ij}, w_{ij}, h_{ij} refer to elements of $U_n(\mathbb{Z})$.

(2) If C_n is the kernel of $\pi_n : U_n(\mathbb{Z}) \longrightarrow SL_n(\mathbb{Z})$ and $n \geq 3$, then C_n is generated by h_{12}^2, and $(h_{12}^2)^2 = 1$.

As usual, we only require (C) when $i,j = 1,2$, and $h_{12}^2 \in C_n$ Setting $h_{12}^2 = 1$ amounts to dividing by $\langle h_{12}^2 \rangle$, which thus equals C_n. The relation $h_{23}h_{12}h_{23}^{-1} = h_{12}^{-1}$, which may be deduced from (B) as in the proof of Lemma 37, then yields $h_{12}^2 = h_{12}^{-2}$.

(3) $h_{12}^2 \neq 1$ if $n \geq 3$.

Assume not. There is a natural map $U_n(\mathbb{Z}) \longrightarrow U_n(\mathbb{R})$, $x_{ij} \longrightarrow x_{ij}(1)$. This maps h_{12}^2 onto $h_{12}(-1)^2$, which (see Remark (a) after the proof of Theorem 13) generates the kernel of $U_n(\mathbb{R}) \longrightarrow SL_n(\mathbb{R})$. Thus $SL_n(\mathbb{R})$ is centrally closed, hence simply connected. Since $SL_n(\mathbb{R})$ can be contracted to SO_n (by the polar decomposition, which will be proved in the next section) which is not simply connected since $Spin_n \longrightarrow SO_n$ is a nontrivial covering, we have a contradiction.

It now follows from (2), (3) and Theorem 14 that $|K_2(\mathbb{Z})| = 2$.

By Corollary 1 above the same conclusion holds with $SL(\mathbb{Z})$ replaced by any $SL_n(\mathbb{Z})$ with $n \geq 5$.

Exercise: Let SA_n be SL_n x translations of the underlying space, k^n with k again a field. I.e., SA_n is the group of all

$(n+1)\times(n+1)$ matrices of the form $\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$ where $x \in SL_n, y \in k^n$.

SA_n is generated by $x_{ij}(t)$, $t \in k$, $i \neq j$, $i = 1,2,\ldots,n$, $j = 1,2,\ldots,n+1$. Prove:

(1) If the relation

(C) $h_{ij}(t)$ is multiplicative.

is added to the relations (A) and (B) of Theorem 14, a complete set of relations for SA_n is obtained.

(2) If k is finite, (C) may be omitted.

(3) If n is large enough, the group defined by (A) and (B) is a u.c.e. for SA_n.

(4) Other analogues of results for SL_n.

We remark that $SA_2(\mathbb{C})$ is the universal covering group of the inhomogeneous Lorentz group, hence is of interest in quantum mechanics.

§ 8. Variants of the Bruhat lemma. Let G be a Chevalley group, k, B ... as usual. We recall (Theorems 4 and 4'):

(a) $G = \bigcup_{w \in W} BwB$, a disjoint union.

(b) For each $w \in W$, $BwB = BwU_w$, with uniqueness of expression on the right. Our purpose is to present some analogues of (b) with applications.

For each simple root α we set $G_\alpha = \langle \mathfrak{X}_\alpha , \mathfrak{X}_{-\alpha} \rangle$, a group of rank 1, $B_\alpha = B \cap G_\alpha$, and assume that the representative of w_α in N/H , also denoted w_α , is chosen in G_α .

Theorem 15: For each simple root α let Y_α be a system of representatives for $B_\alpha \backslash (G_\alpha - B_\alpha)$, or more generally for $B \backslash Bw_\alpha B$. For each $w \in W$ choose a minimal expression $w = w_\alpha w_\beta \ldots w_\delta$ as a product of reflections relative to simple roots $\alpha, \beta \ldots$. Then $B w B = BY_\alpha Y_\beta \ldots Y_\delta$ with uniqueness of expression on the right.

Proof: Since $G_\alpha - B_\alpha = B_\alpha w_\alpha B_\alpha$, the second case above really is more general than the first. We have

$$\begin{aligned} BwB &= Bw_\alpha Bw_\alpha wB && \text{(by Lemma 25)} \\ &= Bw_\alpha BY_\beta \ldots Y_\delta && \text{(by induction)} \\ &= BY_\alpha Y_\beta \ldots Y_\delta && \text{(by the choice of } Y_\alpha\text{)} . \end{aligned}$$

Now assume $by_\alpha y_\beta \dots y_\gamma y_\delta = b' y'_\alpha y'_\beta \dots y'_\gamma y'_\delta$ with $b, b' \in B$, etc. Then $by_\alpha \dots y_\gamma = b' y'_\alpha \dots y'_\gamma y'_\delta y_\delta^{-1}$. We have $y'_\delta y_\delta^{-1} \in B$ or $Bw_\delta B$. The second case can not occur since then the left side would be in $Bww_\delta B$ and the right side in BwB (by Lemma 25). From the definition of Y_δ it follows that $y_\delta = y'_\delta$, and then by induction that $y_\gamma = y'_\gamma$, ..., whence the uniqueness in Theorem 15.

Lemma 43: Let $\varphi_\alpha : SL_2 \to G_\alpha$ be the canonical homomorphism (see Theorem 4', Cor. 6). Then Y_α satisfies the conditions of Theorem 15 in each of the following cases.

(a) $Y_\alpha = w_\alpha \mathfrak{X}_\alpha$.

(b) $k = \mathbb{C}$ (resp. $\mathbb{R}$) and Y_α is the image under φ_α of the elements of SU_2 (resp. SO_2) (standard compact forms) of the form $\begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$ with $b > 0$.

(c) If $\mathfrak{o}$ is a principal ideal domain (commutative with 1), $\mathfrak{o}^*$ is the group of units, k is the quotient field, and Y_α is the image under φ_α of the elements of $SL_2(\mathfrak{o})$ of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with c running through a set of representatives for $(\mathfrak{o}-0)/\mathfrak{o}^*$, and for each c, a running over a set of representatives for the residue classes of $\mathfrak{o}$ mod c.

Proof: We have (a) by Theorem 4' applied to G_α. To verify (b) and (c) we may assume that G_α is SL_2 and B_α the

superdiagonal subgroup B_2 since $\ker \varphi_\alpha \subseteq B_2$. Any element of $SL_2(\mathbb{C})$ can be converted to one of SU_2 by adding a multiple of the second row to the first and normalizing the lengths of the rows. Thus $SL_2(\mathbb{C}) = B_2(\mathbb{C}) \cdot SU_2$. Then $B_2(\mathbb{C}) \backslash SL_2(\mathbb{C}) \sim (B_2(\mathbb{C}) \cap SU_2) \backslash SU_2$, whence (b). Now assume $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(k)$ with k as in (c). We choose a, c in $\mathfrak{o}$ relatively prime and such that $pa + qc = 0$ (using unique factorization), and then b, d in $\mathfrak{o}$ so that $ad - bc = 1$. Multiplying the preceding matrix on the right by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ we get an element of $B_2(k)$. Thus $SL_2(k) = B_2(k)SL_2(\mathfrak{o})$, and (c) follows.

Remarks: (a) The case (a) above is essentially Theorem 4' since $wU_w = w_\alpha \mathfrak{X}_\alpha \cdot w_\beta \mathfrak{X}_\beta \cdots w_\delta \mathfrak{X}_\delta$ in the notation of Theorem 15, by Appendix II 25, or else by induction on the length of the expression.

(b) In (c) above the choice can be made precise in the following cases:

(1) $\mathfrak{o} = \mathbb{Z}$; choose a, c so that $0 \leq a < c$.

(2) $\mathfrak{o} = F[X]$ (F a field); choose so that c is monic and $\deg a < \deg c$.

(3) $\mathfrak{o} = \mathbb{Z}_p$ (p-adic integers); choose c a power of p and a an integer such that $0 \leq a < c$.

In what follows we will give separate but parallel developments of the consequences of (b) and (c) above. In (b) we will treat the case $k = \mathbb{C}$ for definiteness, the case $k = \mathbb{R}$ being similar.

Lemma 44: Let $\mathcal{L}$ and $\{X_\alpha, H_\alpha\}$ be as in Theorem 1.

(a) There exists an involutory semiautomorphism σ_0 of $\mathcal{L}$ (relative to complex conjugation of $\mathbb{C}$) such that $\sigma_0 X_\alpha = -X_{-\alpha}$ and $\sigma_0 H_\alpha = - H_\alpha$ for every root α.

(b) On $\mathcal{L}$ the form $\{X, Y\}$ defined by $(X, \sigma_0 Y)$ in terms of the Killing form is negative definite.

Proof: This basic result is proved, e.g., in Jacobson, Lie algebras, p. 147.

Theorem 16: Let G be a Chevalley group over $\mathbb{C}$ viewed as a Lie group over $\mathbb{R}$.

(a) There exists an analytic automorphism σ of G such that $\sigma x_\alpha(t) = x_{-\alpha}(-\bar{t})$ and $\sigma h_\alpha(t) = h_\alpha(\bar{t}^{-1})$ for all α and t.

(b) The group $K = G_\sigma$ of fixed points of σ is a maximal compact subgroup of G and the decomposition $G = BK$ holds (Iwasawa decomposition).

Proof: Let σ_1 be σ_0 in Lemma 44 composed with complex conjugation, and ρ the representation of $\mathcal{L}$ used to define G.

Applying Theorem 4', Cor. 5 to the Chevalley groups (both equal to G) constructed from the representations ρ and $\rho_0 \sigma_1$ of $\mathcal{L}$, we get an automorphism of G which aside from complex conjugation satisfies the equations of (a), hence composed with conjugation satisfies these equations. From Theorem 7 adapted to the present situation (see the remark at the end of §§ 5) it follows that σ is analytic, whence (a). We observe that if G is defined by the ajoint representation of $\mathcal{L}$, then σ is effected by conjugation by the semiautomorphism σ_0 of Lemma 44.

Lemma 45: Let $K = G_\sigma$, $K_\alpha = K \cap G_\alpha$ for each simple root α.

(a) $K_\alpha = \varphi_\alpha SU_2$ (see Lemma 43(b)), hence $Y_\alpha \subset K_\alpha$.

(b) $B_\sigma = H_\sigma = \{h \in H \mid |\hat{\mu}(h)| = 1$ for all $\hat{\mu} \in \hat{L}$ (global weights)$\}$

$= \{\prod h_i(t_i)$ (see Lemma 28) $\mid |t_i| = 1\}$

= maximal torus in K.

Proof: The kernel of $\varphi_\alpha : SL_2 \to G_\alpha$ is contained in $\{\pm 1\}$, and σ pulls back to the inverse transpose conjugate, say σ_2, on SL_2. Since the equation $\sigma_2 x = -x$ has no solutions we get (a).

Since $\sigma h_\alpha(t) = h_\alpha(\bar{t}^{-1})$, $\qquad \hat{\mu}(h_\alpha(t)) = t^{\mu(H_\alpha)}$

(here μ and $\hat{\mu}$ are corresponding weights on $\mathcal{H}$ and H),

and the $h_\alpha(t)$ generate H, we have $\hat{\mu}(\sigma h) = \overline{\hat{\mu}(h)}^{-1}$ for all $h \in H$, so that $\sigma h = h$ if and only if $|\hat{\mu}(h)| = 1$ for all weights $\hat{\mu}$. If $h = \prod h_i(t_i)$, then $\hat{\mu}(h) = \prod t_i^{\mu(H_i)}$. Since there are ℓ linearly independent weights μ, we see that if $|\hat{\mu}(h)| = 1$ for all $\hat{\mu}$, then $|t_i|^n = 1$ for some $n > 0$, whence $|t_i| = 1$, for all i. If G is universal, then B_σ is the product of the ℓ circles $\{h_i(\cdot)\}$, hence is a torus; if not, we have to take the quotient by a finite group, thus still have a torus. Now if $h \in H_\sigma$ is general enough, so that the numbers $\hat{\alpha}(h)$ $(\alpha \in \Sigma)$ are distinct and different from 1, then G_h, the centralizer of h in G, is H, by the uniqueness in Theorem 4', so that H_σ is in fact a maximal Abelian subgroup of G_σ, which proves the lemma.

Exercise: Check out the existence of h and the property $G_h = H$ above.

Now we consider part (b) of Theorem 16. By Theorem 15 and Lemmas 43(b) and 45(a) we have $G = BK$. By the same results $(BwB)_\sigma \subseteq B_\sigma K_\alpha \ldots K_\delta$, a compact set since each factor is (the compactness of tori and SU_2 is being used). Thus $K = G_\sigma$ is compact. (This also follows easily from Lemma 44(b)). Let K_1 be a compact subgroup of G, $K_1 \supseteq K$. Assume $x \in K_1$. Write $x = by$ with $b \in B$, $y \in K$, and then $b = uh$ with $u \in U$, $h \in H$. Since K_1 is compact, all eigenvalues $\hat{\mu}(h^n)$ $(n = 0, \pm 1, \pm 2, \ldots)$ are bounded, whence $h \in K$ by Lemma 45(b). Then all coefficients of all u^n are bounded so that $u = 1$.

Thus $x \in K$, so that K is maximal compact

Remark: It can be shown also that K is semisimple and that a complete set of semisimple compact Lie groups is got from the above construction.

Corollary 1: Let G' be of the same type as G with a weight lattice containing that of G, $K' = G'_\sigma$, and $\pi: G' \longrightarrow G$ the natural projection. Then $\pi K' = K$.

Proof: This follows from the fact proved in Lemma 45 that K is generated by the groups $\varphi_\alpha SU_2$.

Examples: (a) If $G = SL_n(\mathbb{C})$, then $K = SU_n$.

(b) If $G = SO_n(\mathbb{C})$, then K fixes simultaneously the forms $\Sigma x_i x_{n+1-i}$ and $\Sigma x_i \overline{x_i}$, hence equals $SO_n(\mathbb{R})$ (compact form) after a change of coordinates. Prove this.

(c) If $G = Sp_{2n}(\mathbb{C})$, then K fixes the forms $\sum_1^n (x_i y_{2n+1-i} - x_{2n+1-i} y_i)$ and $\Sigma x_i \overline{x_i}$, and is isomorphic to $SU_n(\mathbb{H})$ (compact form, $\mathbb{H}$ = quaternions). For this see Chevalley, Lie groups, p. 22.

(d) We have isomorphisms and central extensions,

$$\mathbb{H}^* = SU_1(\mathbb{H}) \cong SU_2(\mathbb{C}) \longrightarrow SO_3(\mathbb{R}),$$

$$SU_2(\mathbb{H}) \longrightarrow SO_5(\mathbb{R}), \quad SU_2(\mathbb{C})^2 \longrightarrow SO_4(\mathbb{R}),$$

$$SU_4(\mathbb{C}) \longrightarrow SO_6(\mathbb{R}) \quad \text{(compact forms)}.$$

This follows from (a), (b), (c), Corollary 1 and the equivalences $C_1 = A_1 = B_1$, $C_2 = B_2$, $A_1^2 = D_2$, $A_3 = D_3$.

Corollary 2: The group K is connected.

Proof: As already remarked, K is generated by the groups $\varphi_\alpha SU_2$. Since SU_2 is connected, so is K.

Corollary 3: If T denotes the maximal torus H_σ, then $T\backslash K$ is homeomorphic to $B\backslash G$ under the natural map.

Proof: The map $K \longrightarrow B\backslash G$, $k \longrightarrow Bk$, is continuous and constant on the fibres of $T\backslash K$, hence leads to a continuous map of $T\backslash K$ into $B\backslash G$ which is $1-1$ and onto since $T = B \cap K$ and $G = BK$. Since $T\backslash K$ is compact, the map is a homeomorphism.

Corollary 4: (a) G is contractible to K.

(b) If G is universal, then K is simply connected.

Proof: Let $A = \{h \in H | \hat{\mu}(h) > 0 \text{ for all } \hat{\mu} \in \hat{L}\}$. Then we have $H = AT$, so that $G = BK = UAK$. On the right there is uniqueness of expression. Since K is compact it easily follows that the natural map $UA \times K \longrightarrow G$ is a homeomorphism. Since UA is contractible to a point, G is contractible to K. If also G is universal, then G is simply connected by Theorem 13; hence so is K.

Corollary 5: For $w \in W$ set $(BwB)_\sigma = BwB \cap K = K_w$, and let $\alpha, \beta, \ldots, \delta$ be as in Theorem 15. Then $K = \bigcup_w K_w$ and $K_w = TY_\alpha \ldots Y_\delta$, with uniqueness of expression on the right.

Proof: This follows from Theorem 15 and Lemma 43(b).

Remark: Observe that K_w is essentially a cell since each Y_α is homeomorphic to $\mathbb{C}$ (consider the values of a in Lemma 43(b)). A true cellular decomposition is obtained by writing T as a union of cells. Perhaps this decomposition can be used to give an elementary treatment of the cohomology of K.

Corollary 6: $B\backslash G$ and $T\backslash K$ have as their Poincaré polynomials $\sum_{w\in W} t^{2N(w)}$. They have no torsion.

Proof: We have $B\backslash BwB$ homeomorphic to wU_w, a cell of real dimension $2N(w)$. Since each dimension is even, it follows that the cells represent independent elements of the homology group and that there is no torsion (essentially because the boundary operator lowers dimensions by exactly 1), whence Cor. 6. Alternately one may use the fact that each Y_α is homeomorphic to $\mathbb{C}$.

Remark: The above series will be summed in the next section, where it arises in connection with the orders of the finite Chevalley groups.

Corollary 7: For $w \in W$ let $w = w_\alpha \dots w_\delta$ be a minimal expression as before and let S denote the set of elements of W each of which is a product of some subsequence of the expression for w. Then $\overline{K}_w$ (topological closure) $= \bigcup_{w' \in S} K_{w'}$.

Proof: If $T_\alpha = T \cap K_\alpha$, we have $K_\alpha = T_\alpha Y_\alpha \cup T_\alpha$ by Lemma 45(a) and $\overline{T_\alpha Y_\alpha} = K_\alpha$ by the corresponding result in SU_2. Now $BwB = B \cdot T_\alpha Y_\alpha \dots T_\delta Y_\delta$ by Lemma 43(b). Hence $K_w = T \cdot T_\alpha Y_\alpha \dots T_\delta Y_\delta$, so that $\overline{K}_w \supseteq TK_\alpha \dots K_\delta$, and we have equality since each factor

on the right is compact, so that the right side is compact, hence closed. Since $K_w \cap K_\alpha \subseteq K_w \cup K_{w w_\alpha}$ if $w' \in W$ and α is simple, by Lemma 25, Cor. 7 follows.

Corollary 8: (a) $T = K_1$ is in the closure of every K_w.

(b) K_w is closed if and only if $w = 1$.

Corollary 9: The set S of Cor. 7 depends only on w, not on the minimal expression chosen, hence may be written $S(w)$.

Proof: Because $\overline{K}_w$ doesn't depend on the expression.

Lemma 46: Let w_o be the element of W which makes all positive roots negative. Then $S(w_o) = W$.

Proof: Assume $w \in W$, and let $w = w_1 \ldots w_m$ be a minimal expression as a product of simple reflections and similarly for $w^{-1} w_o = w_{m+1} \ldots w_n$. Then $w_o = w_1 \ldots w_m \ldots w_n$ is one for w_o since if N is the number of positive roots then $m = N(w)$, $n = N - N(w)$, and $m + n = N = N(w_o)$. Looking at the initial segment of w_o we see that $w \in S(w_o)$.

Corollary 10: If w_o is as above and $w_o = w_\alpha w_\beta \ldots w_\delta$ is a minimal expression, then

(a) $K = \overline{K}_{w_o}$.

(b) $K = K_\alpha K_\beta \ldots K_\delta$.

Proof: (a) By Cor. 7 and Lemma 46.

(b) By (a) $K = T K_\alpha K_\beta \ldots K_\delta$. We may write $T = \prod T_\gamma$ (γ simple), then absorb the T_γ's in appropriate K_γ's to get (b).

Exercise: If G is any Chevalley group and $w_o, \alpha, \beta, \ldots$ are as above, show that $G = BG_\alpha G_\beta \ldots G_\delta$.

Remarks: (a) If $\mathbb{C}$ and SU_2 are replaced by $\mathbb{R}$ and SO_2 in accordance with Lemma 43(b), then everything above goes through except for Cor. 4, Cor. 6 and the fact that T is no longer a torus. In this case each K_α is a circle since SO_2 is. The corresponding angles in Cor. 10(b), which we have to restrict suitably to get uniqueness, may be called the Euler angles in analogy with the classical case:

$G = SL_3(\mathbb{R})$, $K = SO_3(\mathbb{R})$,

K_α, K_β = {rotations around the z-axis, x-axis} ,

$K = K_\alpha K_\beta K_\alpha$.

(b) If K_w is replaced by $BwB = BK_w$ in Cor. 7, the formula for $\overline{BwB}$ is obtained. (Prove this.) If $\mathbb{C}$ (or $\mathbb{R}$) is replaced by any algebraically closed field and the Zariski topology is used, the same formula holds. So as not to interrupt the present development, we give the proof later, at the end of this section.

Theorem 17: (Cartan). Again let G be a Chevalley group over $\mathbb{C}$ or $\mathbb{R}$, $K = G_\sigma$ as above, and $A = \{h \in H \mid \hat{\mu}(h) > 0$ for all $\hat{\mu} \in \hat{L}\}$.

(a) $G = KAK$ (Cartan decomposition).

(b) In (a) the A-component is determined uniquely up to conjugacy under the Weyl group.

Proof: (a) Assume $x \in G$. By the decompositions $H = AT$ and $G = BK$ (Theorem 16), there exist elements in $KxK \cap UA$. Given such an element $y = ua$, we write $a = \exp H$ ($H \in \mathcal{H}_{\mathbb{R}}$, uniquely determined by a), then set $|a| = |H|$, the Killing norm in $\mathcal{L}_{\mathbb{R}}$. This norm is invariant under W. We now choose y to maximize $|a|$ (recall that K is compact). We must show that $u = 1$. This follows from: (*) if $u \neq 1$, then $|a|$ can be increased. We will reduce (*) to the rank 1 case. Write $u = \prod_{\beta>0} u_\beta$ ($u_\beta \in \mathcal{X}_\beta$). We may assume $u_\alpha \neq 1$ for some simple α: choose α of minimum height, say n, such that $u_\alpha \neq 1$, then if $n > 1$, choose β simple so that $(\alpha,\beta) > 0$ and $\mathrm{ht}\, w_\beta\alpha < n$, then replace y by $w_\beta(1)yw_\beta(1)^{-1}$ and proceed by induction on n. We write $u = u'u_\alpha$ with $u' \in \mathcal{X}_{P-\{\alpha\}}$ (here P is the set of positive roots). Then we write $a = \exp H$, choose c so that $H' = H - cH_\alpha$ is orthogonal to H_α, set $a_\alpha = \exp cH_\alpha \in A \cap G_\alpha$, $a' = \exp H' \in A$, $a = a_\alpha a'$. Then a' commutes with G_α elementwise and is orthogonal to a_α relative to the bilinear form corresponding to the norm introduced above. By (*) for groups of rank 1, there exist $y, z \in K_\alpha$ such that $yu_\alpha a_\alpha z = a_\alpha' \in A \cap G_\alpha$ and $|a_\alpha'| > |a_\alpha|$. Then $yuaz = yu'u_\alpha a_\alpha a'z$ $= yu'y^{-1}a_\alpha' a'$. Since G_α normalizes $\mathcal{X}_{P-\{\alpha\}}$ (since $\mathcal{X}_\alpha$ and $\mathcal{X}_{-\alpha}$ do), $yu'y^{-1} \in U$. Since $|a_\alpha' a'|^2 = |a_\alpha'|^2 + |a'|^2$ $> |a_\alpha|^2 + |a'|^2 = |a_\alpha a'|^2 = |a|^2$, we have (*), modulo the rank 1 case. This case, essentially $G = SL_2$, will be left as an exercise.

(b) Assume $x \in G$, $x = k_1 a k_2$ as in (a). Then $\sigma x = k_1 a^{-1} k_2$, so that $x \sigma x^{-1} = k_1 a^2 k_1^{-1}$. Here $\sigma a = a^{-1}$ since $\hat{\mu}(\sigma a) = \overline{\hat{\mu}(a)}^{-1} = \hat{\mu}(a^{-1})$ for all $\hat{\mu} \in \hat{L}$.

Lemma 47: If elements of H are conjugate in G (any Chevalley group), they are conjugate under the Weyl group.

This easily follows from the uniqueness in Theorem 4'.

By the lemma x above uniquely determines a^2 up to conjugacy under the Weyl group, hence also a since square-roots in A are unique.

Remark: We can get uniqueness in (b) by replacing A by $A^+ = \{a \in A \mid \hat{\alpha}(a) \geq 1 \text{ for all } \hat{\alpha} > 0\}$. This follows from Appendix III 33.

Corollary: Let P consist of the elements of G which satisfy $\sigma x = x^{-1}$ and have all eigenvalues positive.

(a) $A \subset P$.

(b) Every $p \in P$ is conjugate under K to some $a \in A$, uniquely determined up to conjugacy under W (spectral theorem).

(c) $G = KP$, with uniqueness on the right (polar decomposition).

Proof: (a) This has been noted in (b) above.

(b) We can assume $p = ka \in KA$, by the theorem. Apply σ^{-1}: $p = ak^{-1}$. Thus k commutes with a^2, hence also with a. (Since a is diagonal (relative to a basis of weight vectors) and positive, the matrices commuting with a have a certain

block structure which does not change when it is replaced by a^2.)
Then $k^2 = 1$ and $k = a^{-\frac{1}{2}} p a^{-\frac{1}{2}} \in P$, so that k is unipotent by the definition of P. Since K is compact, $k = 1$. Thus $p = a$. The uniqueness in (b) follows as before.

(c) If $x \in G$, then $x = k_1 a k_2$ as in the theorem, so that $x = k_1 k_2 \cdot k_2^{-1} a k_2 \in KP$. Thus $G = KP$. Assume $k_1 p_1 = k_2 p_2$ with $k_i \in K$ and $p_i \in P$. By (b) we can assume that $p_2 \in A$. Then $p_1 = k_1^{-1} k_2 p_2$. As in (b) we conclude that $k_1^{-1} k_2 = 1$, whence the uniqueness in (c).

Example: If $G = SL_n(\mathbb{C})$, so that $K = SU_n(\mathbb{C})$,
$A = \{$positive diagonal matrices$\}$,
$P = \{$positive-definite Hermitean matrices$\}$,
then (b) and (c) reduce to classical results.

We now consider the case (c) of Lemma 43. The development is strikingly parallel to that for case (b) just completed although the results are basically arithmetic in one case, geometric in the other. Throughout we assume that o, o^*, k, Y_α are as in Lemma 43(c) and that the Chevalley group G under discussion is based on k. We write G_o for the subgroup of elements of G whose coordinates, relative to the original lattice M, all lie in o.

Lemma 48: If φ_α is as in Theorem 4', Cor. 6, then $\varphi_\alpha SL_2(o) \subseteq G_o$.

Proof: If o is a Euclidean domain then $SL_2(o)$ is generated by its unipotent superdiagonal and subdiagonal elements, so that the lemma follows from the fact that $x_\alpha(t)$ acts on M as an integral polynomial in t. In the general case it follows that if p is a prime in o and o_p is the localization of o at p (all $a/b \in k$ such that $a,b \in o$ with b prime to p) then $\varphi_\alpha SL_2(o) \subseteq G_{o_p}$. Since $\bigcap_p o_p = o$, e.g. by unique factorization, we have our result.

Remark: A version of Lemma 48 is true if o is any commutative ring since $\varphi_\alpha \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is generically expressible as a polynomial in a,b,c,d with integral coefficients (proof omitted). The proof just given works if o is any integral domain for which $o = \bigcap o_p$ (p = maximal ideal), which includes most of the interesting cases.

Lemma 49: Write $K = G_\theta$, $K_\alpha = G_\alpha \cap K$.

(a) $B \cap K = (U \cap K)(H \cap K)$.

(b) $U \cap K = \{\prod_{\alpha>0} x_\alpha(t_\alpha) \mid t_\alpha \in \theta\}$.

(c) $H \cap K = \{h \in H \mid \hat{\mu}(h) \in \theta^* \text{ for all } \hat{\mu} \in \hat{L}\}$

$= \{\prod h_i(t_i) \mid \text{all } t_i \in \theta^*\}$.

(d) $\varphi_\alpha SL_2(\theta) = K_\alpha$. Hence $Y_\alpha \subset K_\alpha$.

Proof: (a) If $b = uh \in B \cap K$, then its diagonal h , relative to a basis of M made up of weight vectors (see Lemma 18, Cor. 3), must be in K , hence u must also.

(b) If $u = \prod x_\alpha(t_\alpha) \in U \cap K$, then by induction on heights, the equation $x_\alpha(t) = 1 + tX_\alpha + \ldots$ and the primitivity of X_α in End (M) (Theorem 2, Cor. 2) we get all $t_\alpha \in \theta$.

(c) If $h \in H \cap K$, in diagonal form as above, then $\hat{\mu}(h)$ must be in θ for each weight $\hat{\mu}$ of the representation defining G , in fact in θ^* since the sum of these weights is 0 (the sum is invariant under W) . If we write $h = \prod h_i(t_i)$ and use what has just been proved, we get $t_i^n \in \theta^*$ for some $n > 0$, whence $t_i \in \theta^*$ by unique factorization.

(d) Set $S_\alpha = \varphi_\alpha SL_2(\theta)$. By Lemma 48, $S_\alpha \subseteq K_\alpha$. Since $G_\alpha = B_\alpha \cup B_\alpha Y_\alpha$ by Lemma 43(c) and $Y_\alpha \subset S_\alpha$, the reverse inclusion follows from: $B_\alpha \cap K \subset S_\alpha$. Now if $x = x_\alpha(t)h_\alpha(t^*) \in B_\alpha \cap K$, then $t \in \theta$ and $t^* \in \theta^*$ by (a), (b), (c) applied to G_α , so that $x \in \langle x_\alpha(\theta), x_{-\alpha}(\theta)\rangle = S_\alpha$, whence (d) .

Theorem 18: Let θ, k, G and $K = G_\theta$ be as above. Then $G = BK$ (Iwasawa decomposition).

Proof: By Lemmas 43(c) and 49(d), $BwB = BY_\alpha \ldots Y_\delta \subseteq BK$ for every $w \in W$, so that $G = BK$.

Corollary 1: Write $K_w = BwB \cap K$.

(a) $K = \bigcup_{w \in W} K_w$.

(b) $K_w = (B \cap K)Y_\alpha \ldots Y_\delta$, with $B \cap K$ given by Lemma 49, and on the right there is uniqueness of expression.

Remark: This normal form in $K = G_\Theta$ has all components in G_Θ whereas the usual one obtained by imbedding G_Θ in G doesn't.

Corollary 2: K is generated by the groups K_α.

Proof: By Lemma 49 and Cor. 1.

Corollary 3: If Θ is a Euclidean domain, then K is generated by $\{x_\alpha(t) \mid \alpha \in \Sigma, t \in \Theta\}$.

Proof: Since the corresponding result holds for $SL_2(\Theta)$, this follows from Lemma 49(d) and Cor. 2.

Example: Assume $\Theta = \mathbb{Z}$, $k = \mathbb{Q}$. We get that $G_{\mathbb{Z}}$ is generated by $\{x_\alpha(1)\}$. The normal form in Cor. 1 can be used to extend Nielsen's theorem (see (1) on p. 96) from $SL_3(\mathbb{Z})$ to $G_{\mathbb{Z}}$ whenever Σ has rank ≥ 2, is indecomposable, and has all roots of equal length (W. Wardlaw, Thesis, U. C. L. A. 1966). It would be nice if the form could be used to handle $SL_3(\mathbb{Z})$ itself since Nielsen's proof is quite involved. The case of unequal root lengths is at present in poor shape. In analogy with the fact that in the earlier development K is a simple compact group if Σ is indecomposable, we have here: Every normal subgroup of $G_{\mathbb{Z}}$ is

finite or of finite index if Σ is indecomposable and has rank ≥ 2 . The proof isn't easy.

Exercise: Prove that $G_{\mathbb{Z}}/\mathcal{D}G_{\mathbb{Z}}$ is finite, and is trivial if Σ is indecomposable and not of type A_1, B_2 or G_2 .

Returning to the general set up, if p is a prime in o , we write $|\ |_p$ for the p-adic norm defined by $|0|_p = 0$ and $|x|_p = 2^{-r}$ if $x = p^r a/b$ with a and b prime to p .

Theorem 19: (Approximation theorem): Let o and k be as above, a principal ideal domain and its quotient field, S a finite set of inequivalent primes in o , and for each $p \in S$, $t_p \in k$. Then for any $\varepsilon > 0$ there exists $t \in k$ such that $|t - t_p|_p < \varepsilon$ for all $p \in S$ and $|t|_q \leq 1$ for all primes $q \notin S$.

Proof: We may assume every $t_p \in o$. To see this write $t_p = p^r a/b$ as above. By choosing $s \geq -r$ and c and d so that $a = cp^s + db$ and replacing a/b by d , we may assume $b = 1$. If we then multiply by a sufficiently high power of the product of the elements of S , we achieve $r \geq 0$, for all $p \in S$. If we now choose n so that $2^{-n} < \varepsilon$, $e = \prod_{p \in S} p^n$, $e_p = e/p^n$, then f_p, g_p so that $f_p p^n + g_p e_p = 1$, and finally $t = \Sigma\, g_p e_p t_p$, we achieve the requirements of the theorem.

Now given a matrix $x = (a_{ij})$ over k , we define $|x|_p = \max |a_{ij}|_p$. The following properties are easily verified.

(1) $|x + y|_p \leq \max |x|_p, |y|_p$.

(2) $|xy|_p \leq |x|_p|y|_p$.

(3) If $|x_i|_p = |y_i|_p$ for $i = 1,2,\ldots,n$, then
$|\prod x_i - \prod y_i|_p \leq \max_i |y_1|_p \cdots \widehat{|y_i|_p} \cdots |y_n|_p |x_i - y_i|_p$.

Theorem 20: (Approximation theorem for split groups): Let $\Theta, k, S, \varepsilon$ be as in Theorem 19, G a Chevalley group over k , and $x_p \in G$ for each $p \in S$. Then there exists $x \in G$ so that $|x - x_p|_p < \varepsilon$ for all $p \in S$ and $|x|_q \leq 1$ for all $q \notin S$.

Proof: Assume first that all x_p are contained in some $\mathcal{X}_\alpha$, $x_p = x_\alpha(t_p)$ with $t_p \in k$. If $x = x_\alpha(t)$, $t \in k$, then $|x|_q \leq \max |t|_q, 1$ because $x_\alpha(t)$ is an integral polynomial in t and similarly $|xx_p^{-1} - 1|_p \leq |t - t_p|_p$, so that $|x - x_p|_p \leq |x_p|_p |t - t_p|_p$ by (1) and (2) above. Thus our result follows from Theorem 19 in this case. In the general case we choose a sequence of roots $\alpha_1, \alpha_2, \ldots$ so that $x_p = x_{p1}x_{p2}\cdots$ with $x_{pi} \in \mathcal{X}_{\alpha_i}$ for all $p \in S$. By the first case there exists $x_i \in \mathcal{X}_{\alpha_i}$ so that

$$|x_i - x_{pi}|_p < |x_{pi}|_p \quad \text{and} \quad \varepsilon |x_{pi}|_p / |x_{p1}|_p |x_{p2}|_p \cdots$$

if $p \in S$ and $|x_i|_q \leq 1$ if $q \notin S$. We set $x = x_1 x_2 \cdots$. Then the conclusion of the theorem holds by (3) above.

With Theorem 20 available we can now prove:

Theorem 21: (Elementary divisor theorem): Assume Θ, k, G, $K = G_\Theta$ are as before. Let A^+ be the subset of H defined by: $\hat{\alpha}(h) \in \Theta$ for all positive roots $\hat{\alpha}$.

(a) $G = KA^+K$ (Cartan decomposition).

(b) The A^+ component in (a) is uniquely determined mod $H \cap K$, i.e. mod units (see Lemma 49); in other words, the set of numbers $\{\hat{\mu}(h) | \hat{\mu}$ weight of the representation defining $G\}$ is.

Example: The classical case occurs when $G = SL_n(k)$, $K = SL_n(\mathfrak{o})$, and A^+ consists of the diagonal elements $\mathrm{diag}(a_1, a_2, \ldots, a_n)$ such that a_i is a multiple of a_{i+1} for $i = 1, 2, \ldots$.

Proof of theorem: First we reduce the theorem to the local case, in which $\mathfrak{o}$ has a single prime, modulo units. Assume the result ture in this case. Assume $x \in G$. Let S be the finite set of primes at which x fails to be integral. For $p \in S$, we write $\mathfrak{o}_p$ for the local ring at p in $\mathfrak{o}$, and define K_p and A_p^+ in terms of $\mathfrak{o}_p$ as K and A^+ are defined for $\mathfrak{o}$. By the local case of the theorem we may write $x = c_p a_p c_p'$ with $c_p, c_p' \in K_p$ and $a \in A_p^+$, for all $p \in S$. Since we may choose a_p so that $\hat{\mu}(a_p)$ is always a power of p and then replace all a_p by their product, adjusting the c's accordingly, we may assume that a_p is independent of p, is in A^+, and is integral outside of S. We have $c_p a c_p' x^{-1} = 1$ with $a = a_p$ for $p \in S$. By Theorem 20 there exist $c, c' \in G$ so that $|c - c_p|_p < |c_p|_p$ for $p \in S$ and $|c|_q \leq 1$ for $q \notin S$, the same equations hold for c' and c_p', and $|cac'x^{-1} - 1|_p \leq 1$ for all $p \in S$. By properties (1), (2), (3) of $|\ |_p$, it is now easily verified that $|c|_p \leq 1$, $|c_p'| \leq 1$ and $|cac'x^{-1} - 1|_p \leq 1$,

whether p is in S or not. Thus $c \in K$, $c' \in K$ and $cac'x^{-1} \in K$, so that $x \in KA^+K$ as required. The uniqueness in Theorem 21 clearly also follows from that in the local case.

We now consider the local case, p being the unique prime in $\mathfrak{o}$. The proof to follow is quite close to that of Theorem 17. Let A be the subgroup of all $h \in H$ such that all $\hat{\mu}(h)$ are powers of p, and redefine A^+, casting out units, so that in addition all $\hat{\alpha}(h)$ $(\hat{\alpha} > 0)$ are nonnegative powers of p.

Lemma 50: For each $a \in A$ there exists a unique $H \in \mathcal{H}_{\mathbb{Z}}$, the $\mathbb{Z}$-module generated by the elements H_α of the Lie algebra $\mathcal{L}$, such that $\hat{\mu}(a) = p^{\mu(H)}$ for all weights μ.

Proof: Write $a = \prod h_\alpha(c_\alpha p^{n_\alpha})$ with $c_\alpha \in \mathfrak{o}^*$, $n_\alpha \in \mathbb{Z}$. Then $\hat{\mu}(a) = \prod (c_\alpha p^{n_\alpha})^{\mu(H_\alpha)}$. Since $\hat{\mu}(a)$ is a power of p the c_α, being units, may be omitted, so that $\hat{\mu}(a) = p^{\mu(H)}$ with $H = \Sigma\, n_\alpha H_\alpha$. If H' is a second possibility for H, then $\mu(H') = \mu(H)$ for all μ, so that $H' = H$.

If a and H are as above, we write $H = \log_p a$, $a = p^H$, and introduce a norm: $|a| = |H|$, the Killing norm. This norm is invariant under the Weyl group. Now assume $x \in G$. We want to show $x \in KA^+K$. From the definitions if $T = H \cap K$ then $H = AT$. Thus by Theorem 18 there exists $y = ua \in KxK$ with $u \in U$, $a \in A$. There is only a finite number of possibilities for a: if $a = p^H$, then $\{\mu(H) \mid \mu$ a weight in the given representation$\}$ is bounded below (by $-n$ if n is chosen so that the matrix of $p^n x$ is integral, because $\{p^{\mu(H)}\}$ are the

diagonal entries of y), and also above since the sum of the weights is 0, so that H is confined to a bounded region of the lattice $\mathcal{H}_{\mathbb{Z}}$. We choose $y = ua$ above so as to maximize $|a|$. If $u = \prod u_\alpha$ ($u_\alpha \in \mathcal{X}_\alpha$), we set $\operatorname{supp} u = \{\alpha | u_\alpha \neq 1\}$ and then minimize $\operatorname{supp} u$ subject to a lexicographic ordering of the supports based on an ordering of the roots consistent with addition (thus $\operatorname{supp} u < \operatorname{supp} u'$ means that the first α in one but not in the other lies in the second). We claim $u = 1$. Suppose not. We claim (*) $u_\alpha \notin K$ and $a^{-1}u_\alpha a \notin K$ for $\alpha \in \operatorname{supp} u$. If u_α were not in K, we could move it to the extreme left in the expression for y and then remove it. The new terms introduced by this shift would, by the relations (B), correspond to roots higher than α, so that $\operatorname{supp} u$ would be diminished, a contradiction. Similarly a shift to the right yields the second part of (*). Now as in the proof of Theorem 17 we may conjugate y by a product of $w_\beta(1)$'s (all in K) to get $u_\alpha \neq 1$ for some simple α, as well as (*). We write $a = p^H$, choose c so that $H' = H - cH_\alpha$ is orthogonal to H_α, set $a_\alpha = p^{cH_\alpha}$, $a' = p^{H'}$, $a = a_\alpha a'$. We only know that $2c = \langle H, H_\alpha \rangle \in \mathbb{Z}$, so that this may involve an adjunction of $p^{1/2}$ which must eventually be removed. If we bear this in mind, then after reducing (*) to the rank 1 case, exactly as in the proof of Theorem 17, what remains to be proved is this:

Lemma 51: Assume $y = ua = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p^c & \\ & p^{-c} \end{bmatrix}$ with $2c \in \mathbb{Z}$, $t \in k$,

$t \notin e$ and $tp^{-2c} \notin e$. Then c can be increased by an integer by multiplications by elements of K.

Proof: Let $t = ep^{-n}$ with $e \in e^*$. Then $n \in \mathbb{Z}$, $n > 0$ and $n + 2c > 0$ by the assumptions, so that $c + n > c$, $c + n > -c$ and $|c + n| > |c|$. If we multiply y on the left by $\begin{bmatrix} p^n & e \\ -e^{-1} & 0 \end{bmatrix}$, on the right by $\begin{bmatrix} 1 & 0 \\ -e^{-1}p^{n+2c} & 1 \end{bmatrix}$, both in K, we get $\begin{bmatrix} p^{c+n} & 0 \\ 0 & p^{-c-n} \end{bmatrix}$, which proves the lemma, hence that $u = 1$. Thus $y = a \in A$, so that $x \in KAK$. Thus $G = KAK$. Finally every element of A is conjugate to an element of A^+ under the Weyl group, which is fully represented in K (every $w_\alpha(1) \in K$). Thus $G = KA^+K$. It remains to prove the uniqueness of the A^+ component. If G' is the universal group of the same type as G and π is the natural homomorphism, it follows from Lemma 49(d) and Theorem 18, Cor. 2 that $\pi K' = K$ and from Lemma 49 that π maps A'^+ isomorphically onto A^+. Thus we may assume that G is universal. Then G is a direct product of its indecomposable factors so that we may also assume that G is indecomposable. Let λ_i be the i^{th} fundamental weight, V_i an $\mathcal{L}$-module with λ_i as highest weight, G_i the corresponding Chevalley group, $\pi_i: G \longrightarrow G_i$ the corresponding homomorphism, and μ_i the corresponding lowest weight. Assume now that $x = cac' \in G$, with $c, c' \in K$ and $a \in A^+$. Set $\hat{\mu}_i(a) = p^{-n_i}$. Each weight on V_i is μ_i increased by a sum of positive roots, Thus n_i is the smallest integer such that $p^{n_i}\pi_i a$ is integral, i.e. such

that $p^{n_i}\pi_i x$ is since $\pi_i c$ and $\pi_i c'$ are integral, thus is uniquely determined by x. Since $\{\mu_i\}$ is a basis of the lattice of weights $(\mu_i = w_o\lambda_i)$, this yields the uniqueness in the local case and completes the proof of Theorem 21.

Corollary 1: If o is not a field, the group K is maximal in its commensurability class.

Proof: Assume K' is a subgroup of G containing K properly. By the theorem there exists $a \in A^+ \cap K'$, $a \notin K$. Some entry of the diagonal matrix a is nonintegral so that by unique factorization $|K'/K|$ is infinite.

Remark: The case $o = \mathbb{Z}$ is of some importance here.

Corollary 2: If $o = \mathbb{Z}_p$ and $k = \mathbb{Q}_p$ (p-adic integers and numbers) and the p-adic topology is used, then K is a maximal compact subgroup of G.

Proof: We will use the fact that $\mathbb{Z}_p$ is compact. (The proof is a good exercise.) We may assume that G is universal. Let $\bar{k}$ be the algebraic closure of k and $\bar{G}$ the corresponding Chevalley group. Then $G = \bar{G} \cap SL(V,k)$ (Theorem 7, Cor. 3), so that $K = \bar{G} \cap SL(V,o)$. Since o is compact, so is $End(V,o)$, hence also is K, the set of solutions of a system of polynomial equations since $\bar{G}$ is an algebraic group, by Theorem 6. If K' is a subgroup of G containing K properly, there exists $a \in A^+ \cap K'$, $a \notin K$, by the theorem. Then $\{|a^n|_p \mid n \in \mathbb{Z}\}$ is not bounded so that K' is not compact.

Remark: We observe that in this case the decompositions $G = BK$ and $G = KA^+K$ are relative to a maximal compact subgroup just as in Theorems 16 and 17. Also in this case the closure formula of Theorem 16, Cor. 7 holds.

Exercise (optional): Assume that G is a Chevalley group over $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$ and that K is the corresponding maximal compact subgroup discussed above. Prove the commutativity under convolution of the algebra of functions on G which are complex-valued, continuous, with compact support, and invariant under left and right multiplications by elements of K. (Such functions are sometimes called zonal functions and are of importance in the harmonic analysis of G.) Hint: prove that there exists an antiautomorphism φ of G such that $\varphi x_\alpha(t) = x_{-\alpha}(t)$ for all α and t, that φ preserves every double coset relative to K, and that φ preserves Haar measure. A much harder exercise is to determine the exact structure of the algebra.

Next we consider a double coset decomposition of $K = G_\Theta$ itself in the local case. We will use the following result, the first step in the proof of Theorem 7.

Lemma 52: Let $\mathcal{L}$ be the Lie algebra of G (the original Lie algebra of $S\ell_1$ with its coefficients transferred to k), N the number of positive roots, and $\{Y_1, Y_2, \ldots, Y_r\}$ a basis of $\bigwedge^N \mathcal{L}$ made up of products of X_α's and H_i's with $Y_1 = \bigwedge_{\alpha>0} X_\alpha$. For $x \in G$ write $xY_1 = \sum c_j(x) Y_j$. Then $x \in U^- HU$ if and only if $c_1(x) \neq 0$.

Theorem 22: Assume that o is a local principal ideal domain, that p is its unique prime, and that k and G are as before.

(a) $B_I = U_p^- H_o U_o$ is a subgroup of G_o.

(b) $G_o = \underset{w\varepsilon W}{U} B_I w B_I$ (disjoint), if the representatives for W in G are chosen in G_o.

(c) $B_I w B_I = B_I w U_{w,o}$ with the last component of the right uniquely determined mod $U_{w,p}$.

Proof: Let $\bar{o}$ denote the residue class field o/po, $G_{\bar{o}}$ the Chevalley group of the same type as G over $\bar{o}$, and $B_{\bar{o}}, H_{\bar{o}}, \ldots$ the usual subgroups. By Theorem 18, Cor. 3 reduction mod p yields a homomorphism π of G_o onto $G_{\bar{o}}$.

(1) $\pi^{-1}(U_{\bar{o}}^- H_{\bar{o}} U_{\bar{o}}) \subseteq U^- HU$. We consider G acting on $\Lambda^N \mathfrak{L}$ as in Lemma 52. As is easily seen G_o acts integrally relative to the basis of Y's. Now assume $\pi x \varepsilon U_{\bar{o}}^- H_{\bar{o}} U_{\bar{o}}$. Then $c_1(\pi x) \neq 0$ by the lemma applied to $G_{\bar{o}}$, whence $c_1(x) \neq 0$ and $x \varepsilon U^- HU$ again by the lemma.

(2) Corollary: $\ker \pi \subseteq U^- HU$.

(3) $B_I = \pi^{-1} B_{\bar{o}}$. Assume $x \varepsilon \pi^{-1} B_{\bar{o}}$. Then $x \varepsilon U^- BU$ by (1). From this and $x \varepsilon G_o$ it follows as in the proof of Theorem 7(b) that $x \varepsilon U_o^- H_o U_o$, and then that $x \varepsilon B_I$.

(4) Completion of proof: By (3) we have (a). To get (b) we simply apply π^{-1} to the decomposition in $G_{\bar{o}}$ relative to $B_{\bar{o}}$. We need only remark that a choice as indicated is always possible since each $w_\alpha(1) \varepsilon G_o$. From (b) the equation in (c) easily

follows. (Check this.) Assume $b_1 w u_1 = b_2 w u_2$ with $b_i \in B_I$, $u_i \in U_{w,\theta}$. Then $b_1^{-1} b_2 = w u_1 u_2^{-1} w^{-1} \in B_I \cap U_\theta^- = U_p^-$, whence $u_1 u_2^{-1} \in U_{w,p}$ and (c) follows.

Remark: The subgroup B_I above is called an Iwahori subgroup. It was introduced in an interesting paper by Iwahori and Matsumoto (Publ. Math. I.H.E.S. No. 25 (1965)). There a decomposition which combines those of Theorems 21(a) and 22(b) can be found. The present development is completely different from theirs.

There is an interesting connection between the decomposition $G_\theta = \bigcup B_I w B_I$ above and the one, $G_o = \bigcup (BwB)_\theta$, that G_θ inherits as a subgroup of G, namely:

Corollary: Assume $w \in W$, that $S(w)$ is as in Theorem 16, Cor. 9, and that $\pi: G_\theta \longrightarrow G_{\bar{\theta}}$ is, as above, the natural projection. Then $\pi(B_I w B_I) = B_{\bar{\theta}} w B_{\bar{\theta}}$, and $\pi(BwB)_\theta = \bigcup_{w' \in S(w)} B_{\bar{\theta}} w' B_{\bar{\theta}}$. Hence if $\bar{\theta}$ is a topological field, e.g. $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$, then $\pi(BwB)_\theta$ is the topological closure of $\pi(B_I w B_I)$.

Proof: The first equation follows from $\pi^{-1} B_{\bar{\theta}} = B_I$, proved above. Write $w = w_\alpha w_\beta \ldots$ as in Lemma 25, Cor. Then (*) $(BwB)_\theta = (Bw_\alpha B)_\theta (Bw_\beta B)_\theta \ldots$ by Theorem 18, Cor. 1. Now $(Bw_\alpha B)_\theta \supseteq x_{-\alpha}(p)$ and $w_\alpha(1)$ and is a union of B_θ double cosets. Thus $\pi(Bw_\alpha B)_\theta \supseteq B_{\bar{\theta}} \cup B_{\bar{\theta}} w_\alpha B_{\bar{\theta}} = B_\theta G_{\alpha,\bar{\theta}}$. The reverse inequality also holds since $(Bw_\alpha B)_\theta \subseteq B_\theta G_{\alpha,\theta}$ by Theorem 18, Cor. 1. From this, (*), the definition of $S(w)$, and Lemma 25, the required expression for $\pi(BwB)_\theta$ now follows.

Appendix. Our purpose is to prove Theorem 23 below which gives the closure of BwB under very general conditions. We will write $w' \leq w$ if $w' \in S(w)$ with $S(w)$ as in Theorem 16, Cor. 9, i.e. if w' is a subexpression (i.e. the product of a subsequence) of some minimal expression of w as a product of simple reflections.

Lemma 53: The following are true.

(a) If w' is a subexpression of some minimal expression for w, it is a subexpression of all of them.

(b) In (a) the subexpressions for w' can all be taken to be minimal.

(c) The relation $\leq$ is transitive.

(d) If $w \in W$ and α is a simple root such that $w\alpha > 0$ (resp. $w^{-1}\alpha > 0$), then $ww_\alpha > w$ (resp. $w_\alpha w > w$).

(e) $w_o \geq w$ for all $w \in W$.

Proof: (a) This was proved in Theorem 16, Cor. 7 and 9 in a rather roundabout way. It is a direct consequence of the following fact, which will be proved in a later section: the equality of two minimal expressions for w (as a product of simple reflections) is a consequence of the relations $w_1w_2\ldots = w_2w_1\ldots$ (w_1, w_2 distinct simple reflections, n terms on each side, n = order w_1w_2).

(b) If $w' = w_1w_2\ldots w_r$ is an expression as in (b) and it is not minimal, then two of the terms on the right can be cancelled by Appendix II 21.

(c) By (a) and (b).

(d) If $w\alpha > 0$ and $w_1 w_2 \ldots w_s$ is a minimal expression for w, then $w_1 \ldots w_s w_\alpha$ is one for ww_α by Appendix II 19, so that $ww_\alpha > w$, and similarly for the other case.

(e) This is proved in Lemma 46.

Now we come to our main result.

Theorem 23: Let G be a Chevalley group. Assume that k is a nondiscrete topological field and that the topology inherited by G as a matric group over k is used. Then the following conditions on w, w' are equivalent.

(a) $Bw'B \subseteq \overline{BwB}$.

(b) $w' \leq w$.

Proof: Let Y_1 be as in Lemma 52 and more generally $Y_w = \bigwedge_{\alpha>0} X_{w\alpha}$ for $w \in W$. For $x \in G$ let $c_w(x)$ denote the coefficient of Y_w in xY_1. We will show that (a) and (b) are equivalent to:

(c) $c_{w'}$ is not identically 0 on BwB.

(a) $\Longrightarrow$ (c). We have $x_\beta(t)X_\alpha = X_\alpha + \Sigma\, t^j X_j$ with X_j of weight (0 or a root) $\alpha + j\beta$, and $n_w X_\alpha = cX_{w\alpha}$ $(c \neq 0)$ if n_w represents w in W in N/H. Thus (*) $BwBY_1 \subseteq k^* Y_w +$ higher terms in the ordering given by sums of positive roots. Thus $c_{w'}$ is not identically 0 on $Bw'B$, hence also not on BwB, by (a).

(c) $\Longrightarrow$ (b). We use downward induction on $N(w')$. If this is maximal then $w' = w_o$, the element of W making all positive

roots negative, and then $w = w_o$ by (c) and (*) above. Assume $w' \neq w_o$. Choose α simple so that $w'^{-1}\alpha > 0$, hence $N(w_\alpha w') > N(w')$. Since $c_{w'}(BwB) \neq 0$ and $Bw_\alpha bwB \subseteq BwB \cup Bw_\alpha wB$, we see that $c_{w_\alpha w'}(BwB) \neq 0$ or $c_{w_\alpha w'}(Bw_\alpha wB) \neq 0$, so that $w_\alpha w' \leq w$ or $w_\alpha w' \leq w_\alpha w$. In the first case $w' < w$ by Lemma 53(c) and (d). In the second case if $w^{-1}\alpha < 0$ then $w_\alpha w < w$ by Lemma 53(d) which puts us back in the first case, while if not we may choose a minimal expression for w starting with w_α and conclude that $w' \leq w$.

(b) ⟹ (a). By the definitions and the usual calculus of double cosets, this is equivalent to: if α is simple, then $\overline{Bw_\alpha B} = B \cup Bw_\alpha B$. The left side is contained in the right, an algebraic group, hence a closed subset of G. Since $Bw_\alpha B$ contains $\mathfrak{x}_\alpha - 1$ and the topology on k is not discrete, its closure contains 1, hence also B, proving the reverse inequality and completing the proof of the theorem.

Remark: In case k above is $\mathbb{C}, \mathbb{R}$ or $\mathbb{Q}_p$, the theorem reduces to results obtained earlier. In case k is infinite and the Zariski topology on k and G are used it becomes a result of Chevalley (unpublished). Our proof is quite different from his.

Exercise: (a) If $w \in W$ and α is a positive root such that $w\alpha > 0$, prove that $ww_\alpha > w$ (compare this with Lemma 53(d)), and conversely if $w' \leq w$ then (*) there exists a sequence of positive roots $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that if $w_i = w_{\alpha_i}$ then

$w' w_1 \ldots w_{i-1} \alpha_i > 0$ for all i and $w' w_1 \ldots w_r = w$. Thus $w' \leq w$ and (*) are equivalent.

(b) It seems to us likely that $w' \leq w$ is also equivalent to: there exists a permutation π of the positive roots such that $w' \pi\alpha - w\alpha$ is a sum of positive roots for every $\alpha > 0$; or even to: $\sum_{\alpha>0} (w'\alpha - w\alpha)$ is a sum of positive roots.

§9. The orders of the finite Chevalley groups. Presently we will prove:

Theorem 24: Let W be a finite reflection group on a real space V of finite dimension ℓ, S the algebra of polynomials on V, $I(S)$ the subalgebra of invariants under W. Then:

(a) $I(S)$ is generated by ℓ homogeneous algebraically independent elements $I_1,\dots,I_\ell$.

(b) The degrees of the I_j's, say $d_1,\dots,d_\ell$, are uniquely determined and satisfy $\sum_j (d_j - 1) = N$, the number of positive roots.

(c) For the irreducible Weyl groups the d_i's are as follows:

W	d_i's
A_ℓ	$2, 3,\dots,\ell + 1$
B_ℓ, C_ℓ	$2, 4,\dots,2\ell$
D_ℓ	$2, 4,\dots,2\ell - 2, \ell$
E_6	2, 5, 6, 8, 9, 12
E_7	2, 6, 8, 10, 12, 14, 18
E_8	2, 8, 12, 14, 18, 20, 24, 30
F_4	2, 6, 8, 12
G_2	2, 6

Our main goal is:

Theorem 25: (a) Let G be a universal Chevalley group over a field k of q elements and the d_i's as in Theorem 24. Then

$|G| = q^N \prod_i (q^{d_i} - 1)$ with $N = \Sigma(d_i - 1)$ = the number of positive roots.

(b) If G is simple instead, then we have to divide by $c = |\mathrm{Hom}(L_1/L_0, k^*)|$, given as follows:

G	A_ℓ	B_ℓ, C_ℓ	D_ℓ	E_6	E_7	E_8	F_4	G_2
c	$(\ell+1, q-1)$	$(2, q-1)$	$(4, q^\ell - 1)$	$(3, q-1)$	$(2, q-1)$	1	1	1

Remark: We see that the groups of type B_ℓ and C_ℓ have the same order. If $\ell = 2$ the root systems are isomorphic so the groups are isomorphic. We will show later that if $\ell \geq 3$ the groups are isomorphic if and only if q is even.

The proof of Theorem 25 depends on the following identity.

Theorem 26: Let W and the d_i's be as in Theorem 24 and t an indeterminate. Then $\sum_{w \in W} t^{N(w)} = \prod_i (1 - t^{d_i})/(1 - t)$.

We show first that Theorem 25 is a consequence of Theorems 24 and 26.

Lemma 54: If G is as in Theorem 25(a) then $|G| = q^N (q - 1)^\ell \sum_{w \in W} q^{N(w)}$.

Proof: Recall that, by Theorems 4 and 4', $G = \bigcup_{w \in W} BwB$ (disjoint) and $BwB = UHwU_w$ with uniqueness of expression. Hence $|G| = |U||H| \cdot \sum_{w \in W} |U_w|$. Now by Corollary 1 to the proposition of §3, $|U| = q^N$ and $|U_w| = q^{N(w)}$. By Lemma 28, $|H| = (q - 1)^\ell$.

Corollary: U is a p-Sylow subgroup of G, if p denotes the characteristic of k.

Proof: $p \mid q^{N(w)}$ unless $N(w) = 0$. Since $N(w) = 0$ if and only if $w = 1$, $p \nmid \Sigma\, q^{N(w)}$.

Proof of Theorem 25: (a) follows from Lemma 54 and Theorem 26. (b) follows from the fact that the center of the universal group is isomorphic to $\mathrm{Hom}(L_1/L_0, k^*)$ and the values of L_1/L_0 found in S_3.

Before giving general proofs of Theorems 24 and 26 we give independent (case by case) verifications of Theorems 24 and 26 for the classical groups.

Theorem 24: Type A_ℓ: Here $W \cong S_{\ell+1}$ permuting $\ell + 1$ linear functions $\omega_1, \ldots, \omega_{\ell+1}$ such that $\sigma_1 = \Sigma\, \omega_i = 0$. In this case the elementary symmetric polynomials $\sigma_2, \ldots, \sigma_{\ell+1}$ are invariant and generate all other polynomials invariant under W.

Types B_ℓ, C_ℓ: Here W acts relative to a suitable basis $\omega_1, \ldots, \omega_\ell$ by all permutations and sign changes. Here the elementary symmetric polynomials in $\omega_1^2, \ldots, \omega_\ell^2$ are invariant and generate all other polynomials invariant under W.

Type D_ℓ: Here only an even number of sign changes can occur. Thus we can replace the last of the invariants for B_ℓ, $\omega_1^2 \ldots \omega_\ell^2$ by $\omega_1 \ldots \omega_\ell$.

Theorem 26: Type A_ℓ: Here $W \cong S_{\ell+1}$ and $N(w)$ is the number

of inversions in the sequence $(w(1),\ldots,w(\ell+1))$. If we write $P_\ell(t) = \sum_{w\in W=S_{\ell+1}} t^{N(w)}$ then $P_{\ell+1}(t) = P_\ell(t)(1 + t + t^2 +\ldots+ t^{\ell+1})$, as we see by considering separately the $\ell + 2$ values that $w(\ell + 2)$ can take on. Hence the formula $P_\ell(t) = \prod_{j=2}^{\ell+1}(1 - t^j)/(1 - t)$ follows by induction.

Exercise: Prove the corresponding formulas for types B_ℓ, C_ℓ and D_ℓ. Here the proof is similar, the induction step being a bit more complicated.

Part (a) of Theorem 24 follows from:

Theorem 27: Let G be a finite group of automorphisms of a real vector space V of finite dimension ℓ and I the algebra of polynomials on V invariant under G. Then:

(a) If G is generated by reflections, then I is generated by ℓ algebraically independent homogeneous elements (and 1).

(b) Conversely, if I is generated by ℓ algebraically independent homogeneous elements (and 1) then G is generated by reflections.

Example: Let $\ell = 2$ and V have coordinates x,y. If $G = \{\pm \text{id.}\}$, then G is not a reflection group. I is generated by x^2, xy, and y^2 and no smaller number of elements suffices.

Notation: Throughout the proof we let S be the algebra of all polynomials on V, S_o the ideal in S generated by the homogeneous elements of I of positive degree, and Av stand for

average over G (i.e. $\mathrm{Av}P = |G|^{-1} \sum_{g \in G} gP$) .

Proof of (a): (Chevalley, Am. J. of Math. 1955.)

(1) Assume $I_1, I_2, \ldots$ are elements of I such that I_1 is not in the ideal in I generated by the others and that $P_1, P_2, \ldots$ are homogeneous elements of S such that $\Sigma P_i I_i = 0$. Then $P_1 \in S_o$.

Proof: Suppose $I_1 \in$ ideal in S generated by $I_2, \ldots$. Then $I_1 = \sum_{i \geq 2} R_i I_i$ for some $R_2, \ldots \in S$ so that $I_1 = \mathrm{Av}I_1 = \sum_{i \geq 2} (\mathrm{Av}R_i) I_i$ belongs to the ideal in I generated by $I_2, \ldots$, a contradiction. Hence I_1 does not belong to the ideal in S generated by $I_2, \ldots$.

We now prove (1) by induction on $d = \deg P_1$. If $d = 0$, $P_1 = 0 \in S_o$. Assume $d > 0$ and let $g \in G$ be a reflection in a hyperplane $L = 0$. Then for each i, $L \mid (P_i - gP_i)$. Hence $\Sigma((P_i - gP_i)/L) I_i = 0$, so by the induction assumption $P_1 - gP_1 \in S_o$, i.e. $P_1 \equiv gP_1 \pmod{S_o}$. Since G is generated by reflections this holds for all $g \in G$ and hence $P_1 \equiv \mathrm{Av}P_1 \pmod{S_o}$. But $\mathrm{Av}P_1 \in S_o$ so $P_1 \in S_o$.

We choose a minimal finite basis $I_1, \ldots, I_n$ for S_o formed of homogeneous elements of I . Such a basis exists by Hilbert's Theorem.

(2) The I_i's are algebraically independent.

Proof: If the I_i are not algebraically independent, let $H(I_1, \ldots, I_n) = 0$ be a nontrivial relation with all monomials in

the I_i's of the same minimal degree in the underlying coordinates $x_1,\ldots,x_\ell$. Let $H_i = \partial H(I_1,\ldots,I_n)/\partial I_i$. By the choice of H not all H_i are 0. Choose the notation so that $\{H_1,\ldots,H_m\}$ $(m \leq n)$ but no subset of it generates the ideal in I generated by all the H_i. Let $H_j = \sum_{i=1}^{m} V_{j,i} H_i$ for $j = m+1,\ldots,n$ where $V_{j,i} \in I$ and all terms in the equation are homogeneous of the same degree. Then for $k = 1, 2,\ldots,\ell$ we have $0 = \partial H/\partial x_k = \sum_{i=1}^{n} H_i \partial I_i/\partial x_k$
$= \sum_{i=1}^{m} H_i(\partial I_i/\partial x_k + \sum_{j=m+1}^{n} V_{j,i} \partial I_j/\partial x_k)$. By (1) $\partial I_1/\partial x_k$
$+ \sum_{j=m+1}^{n} V_{j,1} \partial I_j/\partial x_k \in S_o$. Multiplying by x_k, summing over k, using Euler's formula, and writing $d_j = \deg I_j$ we get $d_1 I_1 + \sum_{j=m+1}^{n} V_{j,1} d_j I_j = \sum_{i=1}^{n} A_i I_i$ where A_i belongs to the ideal in S generated by the x_k. By homogeneity $A_1 = 0$. Thus I_1 is in the ideal generated by $I_2,\ldots,I_n$, a contradiction.

(3) The I_i's generate I as an algebra.

Proof: Assume $P \in I$ is homogeneous of positive degree. Then $P = \Sigma P_i I_i$, $P_i \in S$. By averaging we can assume that each $P_i \in I$. Each P_i is of degree less than the degree of P, so by induction on its degree P is a polynomial in the I_i's.

(4) $n = \ell$.

Proof: By (2) $n \leq \ell$. By Galois theory $\mathbb{R}(I)$ is of finite index in $\mathbb{R}(x_1, x_2,\ldots,x_n)$, hence has transcendence degree ℓ over $\mathbb{R}$, whence $n \geq \ell$.

By (2), (3) and (4) (a) holds.

Proof of (b): (Todd, Shephard Can. J. Math. 1954.)

Let $I_1,\dots,I_\ell$ be algebraically independent generators of I of degrees $d_1,\dots,d_\ell$, respectively.

(5) $\prod_{i=1}^{\ell}(1-t^{d_i})^{-1} = \operatorname{Av}_{g\in G} \det(1-gt)^{-1}$, as a formal identity in t.

Proof: Let $\varepsilon_1,\dots,\varepsilon_\ell$ be the eigenvalues of g and $x_1,\dots,x_\ell$ the corresponding eigenfunctions. Then $\det(1-gt)^{-1}$ $= \prod_i (1+\varepsilon_i t+\varepsilon_i^2 t^2+\dots)$. The coefficient of t^n is $\sum_{p_1+p_2+\dots=n} \varepsilon_1^{p_1}\varepsilon_2^{p_2}\dots$, i.e. the trace of g acting on the space of homogeneous polynomials in $x_1,\dots,x_\ell$ of degree n, since the monomials $x_1^{p_1}x_2^{p_2}\dots$ form a basis for this space. By averaging we get the dimension of the space of invariant homogeneous polynomials of degree n. This dimension is the number of monomials $I_1^{p_1}I_2^{p_2}\dots$ of degree n, i.e., the number of solutions of $p_1d_1+p_2d_2+\dots=n$, i.e. the coefficient of t^n in $\prod_{i=1}^{\ell}(1-t^{d_i})^{-1}$.

(6) $\prod d_i = |G|$ and $\Sigma(d_i-1) = N$ = number of reflections in G.

Proof: We have $\det(1-gt) =$
$\begin{cases} (1-t)^\ell & \text{if } g=1, \\ (1-t)^{\ell-1}(1+t) & \text{if } g \text{ is a reflection,} \\ \text{a polynomial not divisible by } (1-t)^{\ell-1} & \text{otherwise.} \end{cases}$

Substituting this in (5) and multiplying by $(1-t)^{\ell}$, we have $\prod (1 + t + \ldots + t^{d_i-1})^{-1} = |G|^{-1}(1 + N(1-t)/(1+t) + (1-t)^2P(t))$ where $P(t)$ is regular at $t = 1$. Setting $t = 1$ we get $\prod d_i^{-1} = |G|^{-1}$. Differentiating and setting $t = 1$ we get $(\prod d_i^{-1})\Sigma(-(d_i-1)/2) = |G|^{-1}(-N/2)$, so $\Sigma(d_i-1) = N$.

(7) Let G' be the subgroup of G generated by its reflections. Then $G' = G$ and hence G is a reflection group.

Proof: Let I_i', d_i', and N' refer to G'. The I_i' can be expressed as polynomials in the I_i with the determinant of the corresponding Jacobian not 0. Hence after a rearrangement of the I_i, $\partial I_i/\partial I_i' \neq 0$ for all i. Hence $d_i \geq d_i'$. But $\Sigma(d_i - 1) = N = N' = \Sigma(d_i' - 1)$ by (6). Hence $d_i = d_i'$ for all i, so, again by (6), $|G| = \prod d_i = \prod d_i' = |G'|$, so $G = G'$.

Corollary: The degrees $d_1, d_2, \ldots$ above are uniquely determined and satisfy the equations (6).

Thus Theorem 24(b) holds.

Exercise: For each reflection in G choose a root α. Then $\det \dfrac{\partial(I_1, I_2, \ldots)}{\partial(x_1, x_2, \ldots)} = \prod \alpha$ up to multiplication by a nonzero number.

Remark: The theorem remains true if $\mathbb{R}$ is replaced by any field of characteristic 0 and "reflection" is replaced by "automorphism of V with fixed point set a hyperplane".

For the proof of Theorem 24(c) (determination of the d_i) we use:

Proposition: Let G and the d_i be as in Theorem 27 and $w = w_1 \ldots w_\ell$, the product of the simple reflections (relative to an ordering of V (see Appendix I.8)) in any fixed order. Let h be the order of w. Then:

(a) $N = \ell h/2$.

(b) w contains $\omega = \exp 2\pi i/h$ as an eigenvalue, but not 1.

(c) If the eigenvalues of w are $\{\omega^{m_i} | 1 \leq m_i \leq h - 1\}$ then $\{m_i + 1\} = \{d_i\}$.

Proof: This was first proved by Coxeter (Duke Math. J. 1951), case by case, using the classification theory. For a proof not using the classification theory see Steinberg, T.A.M.S. 1959, for (a) and (b) and Coleman, Can. J. Math. 1958, for (c) using (a) and (b).

This can be used to determine the d_i for all the Chevalley groups. As an example we determine the d_i for E_8. Here $\ell = 8$, $N = 120$, so by (a) $h = 30$. Since w acts rationally $\{\omega^n | (n, 30) = 1\}$ are all eigenvalues. Since $\varphi(30) = 8 = \ell$ these are all the eigenvalues. Hence the d_i are $1, 7, 11, 13, 17, 19, 23, 29$ all increased by 1, as listed previously. The proofs for G_2 and F_4 are exactly the same. E_6 and E_7 require further argument.

Exercise: Argue further.

Remark: The d_i's also enter into the following results, related to Theorem 24:

(a) Let $\mathcal{L}$ be the original Lie algebra, k a field of characteristic 0, G the corresponding adjoint Chevalley group. The algebra of polynomials on $\mathcal{L}$ invariant under G is generated by ℓ algebraically independent elements of degree $d_1,\ldots,d_\ell$, the d_i's as above.

This is proved by showing that under restriction from $\mathcal{L}$ to $\mathcal{H}$ the G-invariant polynomials on $\mathcal{L}$ are mapped isomorphically onto the W-invariant polynomials on $\mathcal{H}$. The corresponding result for the universal enveloping algebra of $\mathcal{L}$ then follows easily.

(b) If G acts on the exterior algebra on $\mathcal{L}$, the algebra of invariants is an exterior algebra generated by ℓ independent homogeneous elements of degrees $\{2d_i - 1\}$.

This is more difficult. It implies that the Poincaré polynomial (whose coefficients are the Betti numbers) of the corresponding compact semisimple Lie group (the group K constructed from $\mathbb{C}$ in $\overset{S}{S}8$) is $\prod (1 + t^{2d_i-1})$.

Proof of Theorem 26: (Solomon, Journal of Algebra, 1966.)

Let $\prod$ be the set of simple roots. If $\pi \subseteq \prod$ let W_π be the subgroup generated by all w_α, $\alpha \in \pi$.

(1) If $w \in W_\pi$ then w permutes the positive roots with support not in π.

Proof: If β is a positive root and supp $\beta \not\subset \pi$ then $\beta = \sum_{\alpha\in\prod} e_\alpha \alpha$ with some $e_\alpha > 0$, $\alpha \notin \pi$. Now $w\beta$ is β plus a

vector with support in π, hence its coefficient of α is positive, so $w\beta > 0$.

(2) Corollary: If $w \in W_\pi$ then $N(w)$ is unambiguous (i.e. it is the same whether we consider $w \in W$ or $w \in W_\pi$).

(3) For $\pi \subseteq \Pi$ define $W_\pi' = \{w \in W \mid w\pi > 0\}$. Then:

(a) Every $w \in W$ can be written uniquely $w = w'w''$ with $w' \in W_\pi'$ and $w'' \in W_\pi$.

(b) In (a) $N(w) = N(w') + N(w'')$.

Proof: (a) For any $w \in W$ let $w' \in W_\pi w$ be such that $N(w')$ is minimal. Then $w'\alpha > 0$ for all $\alpha \in \pi$ by Appendix II.19(a'). Hence $w' \in W_\pi'$ so that $w \in W_\pi' W_\pi$. Suppose now $w = w'w'' = u'u''$ with $w', u' \in W_\pi'$ and $w'', u'' \in W_\pi$. Then $w'w''u''^{-1} = u'$. Hence $w'w''u''^{-1}\pi > 0$. Now $w'(-\pi) < 0$ so $w''u''^{-1}\pi$ has support in π. Hence $w''u''^{-1}\pi \subseteq \pi$ so by Appendix II.23 (applied to W_π) $w''u''^{-1} = 1$. Hence $w' = u'$, $w'' = u''$.

(b) follows from (a) and (1).

(4) Let $W(t) = \sum_{w \in W} t^{N(w)}$, $W_\pi(t) = \sum_{w \in W_\pi} t^{N(w)}$. Then $\sum_{\pi \subseteq \Pi} (-1)^\pi W(t)/W_\pi(t) = t^N$, where N is the number of positive roots and $(-1)^\pi = (-1)^{|\pi|}$.

Proof: We have, by (3), $W(t)/W_\pi(t) = \sum_{w \in W_\pi'} t^{N(w)}$. Therefore the contribution of the term for w to the sum in (4) is $c_w t^{N(w)}$ where $c_w = \sum_{\substack{\pi \subseteq \Pi \\ w\pi > 0}} (-1)^\pi$. If w keeps positive exactly k elements

of $\prod$ then $c_w = \begin{cases} (1-1)^k = 0 & \text{if } k \neq 0 \\ 1 & \text{if } k = 0 . \end{cases}$

Therefore the only contribution is made by w_o, the element of w which makes all positive roots negative, so the sum in (4) is equal to t^N as required.

Corollary: $\Sigma(-1)^{\pi}|W|/|W_\pi| = 1$.

Exercise: Deduce from (4) that if α and β are complementary subsets of $\prod$ then $\sum_{\pi \supseteq \alpha} (-1)^{\pi-\alpha}/W_\pi(t) = \sum_{\pi \supseteq \beta} (-1)^{\pi-\beta}/W_\pi(t^{-1})$.

Set $D = \{v \in V | (v, \alpha) \geq 0 \text{ for all } \alpha \in \prod\}$, and for each $\pi \subseteq \prod$ set $D_\pi = \{v \in V | (v, \alpha) = 0 \text{ for all } \alpha \in \pi, (v, \beta) > 0 \text{ for all } \beta \in \prod - \pi\}$. D_π is an open face of D.

(5) The following subgroups of W are equal:

(a) W_π .

(b) The stabilizer of D_π .

(c) The point stabilizer of D_π .

(d) The stabilizer of any point of D_π .

Proof: (a) $\subseteq$ (b) because π is orthogonal to D_π. (b) $\subseteq$ (c) because D is a fundamental domain for W by Appendix III.33. Clearly (c) $\subseteq$ (d). (d) $\subseteq$ (a) by Appendix III.32.

(6) In the complex cut on real k-space by a finite number of hyperplanes let n_i be the number of i-cells. Then $\Sigma(-1)^i n_i = (-1)^k$.

Proof: This follows from Euler's formula, but may be proved

directly by induction. In fact, if an extra hyperplane H is added to the configuration, each original i-cell cut in two by H has corresponding to it in H an $(i-1)$-cell separating the two parts from each other, so that $\Sigma(-1)^i n_i$ remains unchanged.

(7) In the complex K cut from V by the reflecting hyperplanes let $n_\pi(w)$ $(\pi \subseteq \Pi,\ w \in W)$ denote the number of cells W-congruent to D_π and w-fixed. Then $\sum_{\pi \subseteq \Pi} (-1)^\pi n_\pi(w) = \det w$.

Proof: Each cell of K is W-congruent to exactly one D_π. By (5) every cell fixed by w lies in V_w $(V_w = \{v \in V \mid wv = v\})$. Applying (6) to V_w and using $\dim D_\pi = \ell - |\pi|$ we get $\sum_{\pi \subseteq \Pi} (-1)^\pi n_\pi(w) = (-1)^{\ell - k}$, where $k = \dim V_w$. But w is orthogonal, so that its possible eigenvalues in V are $+1$, -1 and pairs of conjugate complex numbers. Hence $(-1)^{\ell-k} = \det w$.

If χ is a character on W_1, a subgroup of W, then χ^W denotes the induced character defined by (*) $\chi^W(w) = |W_1|^{-1} \sum_{\substack{x \in W \\ xwx^{-1} \in W_1}} \chi(xwx^{-1})$. (See, e.g., W. Feit, Characters of finite groups.)

(8) Let χ be a character on W and $\chi_\pi = (\chi | W_\pi)^W$ $(\pi \subseteq \Pi)$. Then $\sum_{\pi \subseteq \Pi} (-1)^\pi \chi_\pi(w) = \chi(w) \det w$ for all $w \in W$.

Proof: Assume first that $\chi \equiv 1$. Now $xwx^{-1} \in W_\pi$ if and only if xwx^{-1} fixes D_π (by (5)) which happens if and only if w fixes $x^{-1}D_\pi$. Therefore $1_\pi(w) = n_\pi(w)$ by (*). By (7) this gives the result for $\chi \equiv 1$. If χ is any character then

$\chi_\pi = \chi \cdot 1_\pi$ so (8) holds.

(9) Let M be a finite dimensional real W-module, $I_\pi(M)$ be the subspace of W_π-invariants, and $\hat{I}(M)$ be the space of W-skew-invariants (i.e. $\hat{I}(M) = \{m \in M \mid wm = (\det w)m$ for all $w \in W$ Then $\sum_{\pi \subseteq \prod} (-1)^\pi \dim I_\pi(M) = \dim \hat{I}(M)$.

Proof: In (8) take χ to be the character of M , average over $w \in W$, and use (*).

(10) If $p = \prod \alpha$, the product of the positive roots, then p is skew and p divides every skew polynomial on V .

Proof: We have $w_\alpha p = -p = (\det w_\alpha)p$ if α is a simple root by Appendix I.11. Since W is generated by simple reflections p is skew. If f is skew and α a root then $w_\alpha f = (\det w_\alpha)f = -f$ so $\alpha \mid f$. By unique factorization $p \mid f$.

(11) Let $P(t) = \prod (1 - t^{d_i})/(1 - t)$ and for $\pi \subseteq \prod$ let $\{d_{\pi i}\}$ and P_π be defined for W_π as $\{d_i\}$ and P are for W . Then $\sum_{\pi \subseteq \prod} (-1)^\pi P(t)/P_\pi(t) = t^N$.

Proof: We must show (*) $\sum_{\pi \subseteq \prod} (-1)^\pi \prod_i (1 - t^{d_{\pi i}})^{-1}$ $= t^N \prod_i (1 - t^{d_i})^{-1}$. Let $S = \sum_{k=0}^{\infty} S_k$ be the algebra of polynomials on V , graded as usual. As in (5) of the proof of Theorem 27 the coefficient of t^k on the left hand side of (*) is $\sum_{\pi \subseteq \prod} (-1)^\pi \dim I_\pi(S_k)$. Similarly, using (10), the coefficient of t^k on the right hand side of (*) is $\dim \hat{I}(S_k)$. These are equal by (9).

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

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 $\Sigma^* = \{\alpha^* = 2\alpha/(\alpha,\alpha) \mid \alpha \in \Sigma\}$ 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.

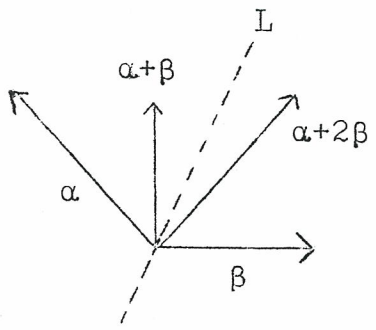
The root system Σ^* obtained in this way from Σ is called the root system dual to Σ.

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 $p \mid n_i$ 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 α, β, $\alpha + \beta$, $\alpha + 2\beta$ be the positive roots for Σ of type B_2. Then those for Σ^* are α^*, β^*, $(\alpha + \beta)^* = 2\alpha^* + \beta^*$, 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 $<(\alpha,\beta))$ 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:

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

(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 $w = w_\alpha w_\beta \ldots$).

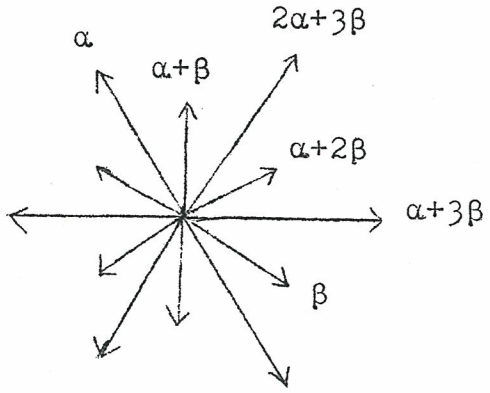
Proof: We may assume G is universal. For simplicity of notation we assume $n = 3$. Consider $x = w_\alpha(1)w_\beta(1)w_\alpha(1)w_\beta(-1)w_\alpha(-1)w_\beta(-1)$. Let $G_\alpha = \langle X_\alpha, X_{-\alpha} \rangle$. Then the product of the first five factors of x is in $w_\alpha(1)w_\beta(1)G_\alpha w_\beta(-1)w_\alpha(-1) = G_{w_\alpha w_\beta \alpha} = G_\beta$ 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 .

<u>Proof:</u> 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 $\mathcal{X}_\alpha$ 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 $\varphi = \mathrm{id}.$ 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 $d\varphi$ such that

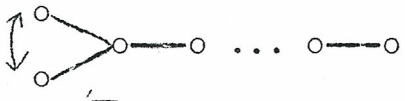
$$d\varphi : X_\alpha \longrightarrow \begin{cases} -X_{r\alpha} & \text{if } \alpha \text{ is long} \\ 3X_{r\alpha} = 0 & \text{if } \alpha \text{ is short.} \end{cases}$$

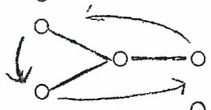
Thus $\mathcal{L} \xrightarrow{d\varphi} \mathcal{L}_{\text{short}} \xrightarrow{d\varphi} 0$ is exact, where $\mathcal{L}_{\text{short}}$ is the 7-dimensional ideal spanned by all X_γ and H_γ for γ short. This leads to an alternate proof of the existence of φ .

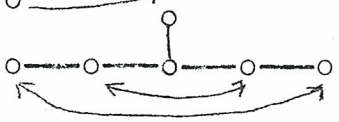
<u>Corollary:</u> (a) Let Σ be an indecomposable root system, σ an angle preserving permutation of the simple roots, $\sigma \neq 1$. If all roots are equal in length then σ extends to an automorphism of Σ . If not, and if p is defined as above, then σ must interchange long and short roots and σ extends 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:

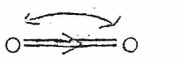
$A_n (n \geq 2)$:  $\sigma^2 = 1$

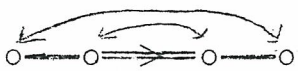
$D_n (n \geq 4)$:  $\sigma^2 = 1$

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 $\sigma \mathfrak{X}_\alpha = \mathfrak{X}_{\rho\alpha}$ and $\sigma \mathfrak{X}_{-\alpha} = \mathfrak{X}_{-\rho\alpha}$ 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 $(B \cup Bw_\alpha B) \cap U^- = \mathfrak{X}_{-\alpha}$. Since for $B \cup Bw_\alpha B$ $= Bw_\alpha^{-1} \cup Bw_\alpha Bw_\alpha^{-1} = Bw_\alpha^{-1} \cup B\mathfrak{X}_{-\alpha}$, and

$B \cap U^- = 1$, $B\mathcal{X}_{-\alpha} \cap U^- = \mathcal{X}_{-\alpha}$, 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 $\mathcal{X}_{-\alpha}$'s, α simple, are permuted by σ and similarly for the $\mathcal{X}_\alpha$'s. The permutation in both cases is the same since $\mathcal{X}_\alpha$ and $\mathcal{X}_{-\beta}$ 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 $\mathcal{Y}_{\alpha+\beta}$. 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 $\mathcal{Y}_{\alpha+\beta}$ 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) $\bar{B}\backslash\bar{G}$ where $\bar{G}$ is a connected linear algebraic group and $\bar{B}$ 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

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

(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 $\bar{G}$ 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 $xAx^{-1} \subseteq \bar{U}$. 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_o .

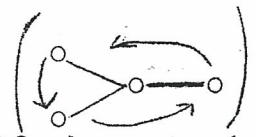
(b) If k is finite, $D \cong C$, the center of the corresponding universal group.

(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 $a = \begin{bmatrix} & & \epsilon_1 \\ & \epsilon_2 & \\ \cdot & & \end{bmatrix}$, $\epsilon_i = \pm 1$). 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 $\sigma x = a_1 a x^{t-1} a^{-1} a_1^{-1}$ $\left(a = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}, \; a_1 = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & 0 & 1 \\ & & 1 & 0 & \\ & & & & \ddots \\ & & & & & 1 \end{bmatrix} \right)$. 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_o consists of all $w\bar{\alpha}$ such that $w \in W_o$ 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.

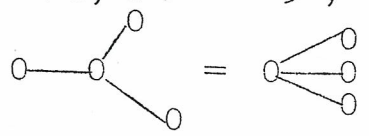
Remark: To achieve condition (1) for a root system, we can stick to the set of shortest projections in the various directions.

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.

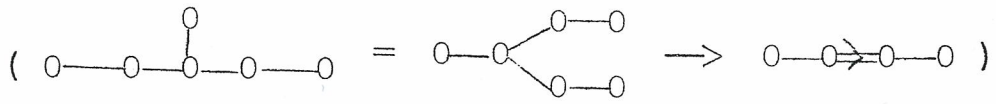
(b) For σ of order 2, W of type D_n, we get W_σ of type B_{n-1}.

(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:



)

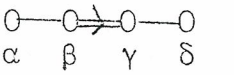
(d) For σ of order 2, W of type E_6, we get W_σ of type F_4.



(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 $\sigma x_\alpha(t)$

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

$\epsilon_\alpha = \pm 1$ 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 $\varphi: t \to h_\alpha(t)h_\beta(t^\theta)$.

(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 $\lambda, f(x)f(x_o)^{-1} = t$ (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.

<u>Theorem 35:</u> 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 $|\mathcal{X}_{a,\sigma}| = q^{|a|}$ 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., $-1 \in W$ or $-1 \in W\sigma_o$. Since there are invariants of odd degree ($d_i = 2,3, \ldots$), $-1 \notin W$. 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 $v_i \to v_i$ $(1 \leq i \leq n-1)$, $v_n \to -v_n$. 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 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 $\Pi_{\sigma'}$ of $V_{\sigma'}$. By checking cases one sees that the permutation is necessarily the identity: if k is finite, one need only compare the various $|\mathfrak{X}_a|$'s with each other, while if k is arbitrary further argument is necessary (one can, for example, check which $\mathfrak{X}_a$'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 $\mathfrak{X}_a$'s). As in step (4) of the proof of Theorem 30, we need only complete the proof of our theorem when $G'_{\sigma'}$ is one of the groups $G_a = \langle \mathfrak{X}_a, \mathfrak{X}_{-a} \rangle$, in other words, when $G'_{\sigma'}$ 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 <u>not</u> $A_1(2)$, $A_1(3)$, 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 $U_{\sigma'}$ as given in Lemma 63 and $d(s)$ for $h_\alpha(s)h_\beta(s^\theta)$.

(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

$d(s)x(t,\ldots)d(s)^{-1} = x(g(s)t,\ldots)$, 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

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

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 $w \in G^{\circ}_{\sigma}$ 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), $\beta B = \text{End } V$ and $\gamma C = \text{End } W$, whence $\alpha A = \text{End } U$ 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 $c\ell = \alpha(c) \circ \ell$. (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

Lemma (see loc. cit.) φ is an isomorphism. If $\alpha = \beta' \otimes \gamma'$ is a second decomposition of the required form, then restriction to B yields $\beta \otimes 1 \cong \beta' \otimes 1$, i.e. multiples of β and β' are isomorphic, so that by the Jordan-Holder or Krull-Schmidt theorems β and β' are also. Similarly γ and γ' are isomorphic, which proves the uniqueness in (b).

Corollary: (a) If K is an algebraically closed field and $G = \prod G_i$ is a direct product of a finite number of groups, then the tensor product V of irreducible KG_i-modules V_i is an irreducible KG-module, and every irreducible KG-module is uniquely realizable in this way.

(b) Similarly for a direct sum $\mathfrak{L} = \Sigma \mathfrak{L}_i$ of Lie algebras over K.

Proof: We apply Lemma 68, extended to several factors, in (a) to group algebras, in (b) to enveloping algebras.

Exercise: If the direct product above is one of algebraic groups over K (of topological groups, of Lie groups,...), then V is rational (continuous, analytic,...) if and only if each V_i is.

Remark: If we are interested in the irreducible representations of a Chevalley group G, we may as well assume it is universal. The corollary then implies that we may as well also assume that G (i.e. that Σ) is indecomposable. This we will do whenever it is convenient.

Now we take up the study of rational representations for

Chevalley groups over algebraically closed fields viewed as algebraic groups. In such representations the coordinates of the representative matrix are required to be rational functions of the original coordinates. Whether this requirement is to be taken locally (e.g. as in the proof of Theorem 7, Cor. 1) or globally is immaterial, in view of the following result.

Lemma 69: Let G be a Chevalley group viewed as an algebraic group as above, and $f: G \longrightarrow k$ a function. Then the following conditions are equivalent.

(a) f is expressible as a rational function locally.

(b) f is expressible as a rational function globally.

(c) f is expressible as a polynomial.

Proof: It will be enough to show that (a) implies (c). Let A be the algebra of polynomial functions on G. By assumption there exists an open covering $\{U_i\}$ of G, which may be taken finite by the maximal condition on the open subsets of G (which holds by Hilbert's basis theorem in A), and elements g_i, h_i in A such that $f = g_i/h_i$ and $h_i \neq 0$ on U_i for all i. Since the h_i don't all vanish together, by Hilbert's Nullstellensatz there exist elements a_i in A such that $1 = \Sigma\, a_i h_i$ on G. Let $U_o = \cap U_i$; it is nonempty, in fact dense, since G is irreducible. On U_o we have $f = \Sigma\, a_i f h_i = \Sigma\, a_i g_i$, a polynomial, hence by density also on each U_i and on G, as required.

Presently we will need the following result.

Lemma 70: The algebra A of polynomial functions on G is integrally closed (in its quotient field).

Proof: We observe first that A is an integral domain (since G is irreducible as an algebraic set, the polynomial ideal defining it is prime), so that it really has a quotient field. Assume $f = p_1/p_2$ ($p_i \in A$) is integral over A: $f^n + a_1 f^{n-1} + \ldots + a_n = 0$ for some $a_i \in A$. On restriction to the open set U^-HU of G the p_i and a_i become, by Theorem 7(b), polynomials in the coordinates $\{t_\alpha, t_i, t_i^{-1}\}$. Since such polynomials form a unique factorization domain, we see by the above equation that f itself is such a polynomial, on U^-HU. The same being true on each of the translates of U^-HU by elements of G, we conclude that f is a polynomial on G, i.e. f is in A, by Lemma 69.

Two more lemmas and then the main theorem.

Lemma 71: The rational characters of H (homomorphisms into k^*) are just the elements of the lattice L generated by the global weights of the representation defining G.

Proof: Let λ be a character. Then it is a polynomial in the diagonal elements of H (written as a group of diagonal matrices), i.e. a linear combination of elements of L. Being multiplicative, it equals some element of L. (Prove this.) Conversely, if $\lambda \in L$, then λ is a power product of weights in the representation defining G, and all exponents may be taken positive since the product of the latter weights (as functions) is 1, so that λ is a polynomial on H.

Now for any rational G-module V we may define the weights λ and the corresponding weight spaces V_λ, relative to H, in the obvious way.

Lemma 72: Let V be a rational G-module, λ a weight, v an element of V_λ, and α a root. Then there exist vectors $v_i \in V_{\lambda+i\alpha} (i = 1,2,\ldots)$ so that $x_\alpha(t)v = v + \Sigma\, t^i v_i$ for all $t \in k$.

Proof: Since V is rational and $t \longrightarrow x_\alpha(t)$ is an isomorphism, $x_\alpha(t)$ is a polynomial in t: $x_\alpha(t)v = \Sigma\, t^i v_i$. If we apply h to this equation and compare the result with the equation got by replacing $x_\alpha(t)$ by $hx_\alpha(t)h^{-1} = x_\alpha(\alpha(h)t)$, we get $v_i \in V_{\lambda+i\alpha}$. Setting $t = 0$, we get $v = v_0$, whence the lemma.

Theorem 39 (Compare with Theorem 3): Let G be a Chevalley group over an algebraically closed field k (i.e. a semisimple algebraic group over k), and assume the notations as above.

(a) Every nonzero rational G-module V contains a nonzero element v^+ which belongs to some weight $\lambda \in L$ and is fixed by all $x \in U$.

(b) Assume $V = kGv^+$ with v^+ as in (a). Then $V = kU^-v^+$. Further $\dim V_\lambda = 1$, every weight μ on V has the form $\lambda - \Sigma\, \alpha$ (α positive root), and $V = \Sigma\, V_\mu$.

(c) In (a) $\langle \lambda, \alpha \rangle \in \mathbb{Z}^+$ for every positive root α.

(d) If V is irreducible, then the weight λ (the "highest weight") and the line kv^+ of (a) are uniquely determined.

(e) Given any character λ on H satisfying (c), there exists a unique irreducible rational G-module V in which λ is realized as in (a).

Proof: (a) The proof is the same as that of Theorem 3(a) with Lemma 72 in place of Lemma 11.

(b) Since U^-B is dense in G (Theorem 7) and V is rational, any linear function on V which vanishes on U^-Bv^+ also vanishes on Gv^+. Thus $V = kU^-Bv^+ = kU^-v^+$. The other assertions of (b) follow from this equation and Lemma 72.

(c) $w_\alpha\lambda$ is a weight on V (with $w_\alpha v^+$ a corresponding weight vector). Since $w_\alpha\lambda = \lambda - \langle\lambda,\alpha\rangle\alpha$, it follows from (b) that $\langle\lambda,\alpha\rangle \in \mathbb{Z}^+$.

(d) This follows from the second and third parts of (b).

(e) We will use the correspondence between local weights (on $\mathcal{L}$) and global weights (on G) (see p. 60). Let λ be as in (e). By Lemma 71, $\lambda \in L$. Let λ also denote the corresponding weight on $\mathcal{L}$, so that $\lambda(H_\alpha) = \langle\lambda,\alpha\rangle \in \mathbb{Z}^+$ for all $\alpha > 0$. Let (ρ,V') be an irreducible $\mathcal{L}$-module with λ as its highest weight, v^+ a corresponding weight vector, and G' a corresponding Chevalley group over k (constructed from $\rho\mathcal{L}$ and some choice of the lattice M in V'). Since λ is in the lattice generated by the weights of the representation of $\mathcal{L}$ used to construct G, it follows (Theorem 7, Cor. 1) that there exists a rational homomorphism $\varphi: G \longrightarrow G'$ such that $x_\alpha(t) \longrightarrow x'_\alpha(t)$ or 1 for all α and t, in the usual notation. The resulting

representation of G on V' need not be irreducible (and its representation class may vary with the choice of M), but at least it contains the vector v^+ which is of weight λ and is fixed by every $x \in U$. Let V'' be the submodule of V' generated by v^+, and V''' a maximal submodule of V''. (V''' is in fact unique as follows from the equation $V'' = kU^-v^+$ of (b). Check this.) The G-module $V = V''/V'''$ meets the existence requirements of (e). For the uniqueness, let $V_i, v_i^+ (i = 1,2)$ satisfy the conditions on V, v^+ in (e). Let $v^+ = v_1^+ + v_2^+ \in V_1 \dotplus V_2$, and $V = kGv^+$. Then $V_\lambda = kv^+$ by (b), so that $v_2^+ \notin V$. Consider the G-homomorphism $p_1 : V \longrightarrow V_1$, projection on the first factor. Since v_1^+ generates V_1, p_1 is onto. Since also $\ker p_1 \subseteq V_2 \cap V$, which is 0 because V_2 is irreducible and $v_2^+ \notin V$, it follows that p_1 is an isomorphism. Thus V is isomorphic to V_1, and similarly to V_2, so that V_1 and V_2 are isomorphic, as required.

A complement: If $\operatorname{char} k = 0$, then in the existence proof above V' is itself irreducible, i.e. $V' = V''$ and $V''' = 0$. In other words, if the Chevalley group G is constructed from an irreducible $\mathcal{L}$-module V and a field k of characteristic 0, then as a linear group it is irreducible.

Proof: Recall that V was originally an $\mathcal{L}_{\mathbb{C}}$-module (irreducible by assumption), and that a lattice M as in Theorem 2, Cor. 1 was then used to shift the coefficients to k. Clearly $V_{\mathbb{Q}}$ is irreducible relative to $\mathcal{L}_{\mathbb{Q}}$. It follows that V_k is irreducible

relative to $\mathcal{L}_k$: otherwise there would be a proper invariant subspace V_1, excluding kv^+ since $kv^+ \cap V_{\mathbb{Q}} \neq 0$, then some nonzero $v \in V_1$ such that $X_\alpha v = 0$ for all $\alpha > 0$, so that writing $v = \Sigma\, t_i m_i$ ($m_i \in M$, $t_i \in k$ and linearly independent over $\mathbb{Q}$) and choosing α so that $X_\alpha m_i \neq 0$ for some i, we would arrive at the contradiction $\Sigma\, t_i X_\alpha m_i = 0$. Since we can recover each X_α from G by using $x_\alpha(t) = 1 + tX_\alpha + \ldots$ for several values of t and the X_α's generate $\mathcal{L}$, we conclude that V_k is irreducible for G.

In contrast to the case just considered, if char $k \neq 0$, then $V' \neq V''$ and $V''' \neq 0$ in general and the exact situation is not at all understood, except in a few scattered cases (types A_1, A_2, B_2 or when char k is large "compared" to λ). However, the following is true.

<u>Exercise:</u> (a) For the lattice M of Theorem 2, Cor. 1 (with V there assumed to be irreducible) assume that $\mathbb{C}v^+ \cap M$ is prescribed. Prove that there is a unique minimal choice for M (contained in all others) and a unique maximal choice.

Assume now as in the complement, except that char $k \neq 0$.

(b) If M is maximal, then $V''' = 0$, i.e. V'' is irreducible.

(c) If M is minimal, then $V' = V''$.

<u>Example:</u> If $\mathcal{L}$ is of type A_1, char $k = 2$, and the adjoint representation is used, then (b) holds for $M_{max} = \langle X, H/2, Y\rangle$ and (c) holds for $M_{min} = \langle X, H, Y\rangle$, but not vice versa.

The proof given above for the existence in Theorem 39(e) brings out the connection between the representations of G and those of $\mathcal{L}$ and shows that every irreducible rational representation of a Chevalley group in characteristic $p \neq 0$ can be constructed by the reduction mod p of a corresponding representation of a group in characteristic 0. It depends, however, on the existence of representations of $\mathcal{L}$, which we have not proved here, thus in its entirety is very long. We shall now develop an alternate, more intrinsic, proof.

We start with the connection between a G-module V and its dual V^*, on which G acts by the rule $(xf)(v) = f(x^{-1}v)$ for all $x \in G$, $f \in V^*$, and $v \in V$. We recall that w_o is the element of the Weyl group which makes all positive roots negative.

Lemma 73: Let V be an irreducible rational G-module, λ its highest weight, v^+ a corresponding weight vector, $\lambda^* = -w_o\lambda$, and f^+ the element of V^* defined thus: if we write $v^- = w_o v^+$ and $v \in V$ as $v = cv^-$ + terms of other (hence higher) weights, then $f^+(v) = c$. Then λ^* and f^+ are highest weight and highest weight vector for V^*.

Proof: In the definition of f^+ we have used the fact that $\dim V_{w_o\lambda} = \dim V_\lambda = 1$. Here, and also in similar situations later, we extend λ to B by the rule $\lambda(b) = \lambda(h)$ if $b = uh$ $(u \in U, h \in H)$, and similarly for λ^*. If we write $v \in V$ as in the lemma and use Lemma 72, we see that $bv = c(w_o\lambda)(h)v^-$ + higher terms. Since $c = f^+(v)$ and

$(w_o\lambda)(h) = \lambda^*(b^{-1})$, we have $f^+(bv) = \lambda^*(b^{-1})f^+(v)$. On replacing b by b^{-1} we get $bf^+ = \lambda^*(b)f^+$, as required.

Theorem 40: For $\lambda \in L$ let A_λ be the space of polynomial functions a on G such that $a(yb) = a(y)\lambda(b)$ for all $y \in G$, $b \in B$, made into a G-module in the obvious way.

(a) If V, λ, v^+ are as in Lemma 73, then the map $\varphi: V^* \longrightarrow A_\lambda$ defined by $(\varphi f)(x) = f(xv^+)$ for $f \in V^*$ and $x \in G$ is a G-isomorphism into.

(b) Conversely, if λ is such that $A_\lambda \neq 0$, then A_λ contains a unique irreducible G-submodule. The latter is finite-dimensional and rational and its highest wieght is λ^* .

Proof: (a) The points to be checked here will be left as an exercise.

(b) We observe first that as a G-module A_λ is locally finite-dimensional (in fact, it is finite-dimensional, but we shall not prove this), since the set of polynomials of a given degree is. Thus there exist irreducible submodules and all of them are finite-dimensional and rational. Let μ be the highest weight of any one of them and a^+ a corresponding nonzero weight vector. We have (*) $a^+(bxb') = \mu(b^{-1})a^+(x)\lambda(b')$ for all $x \in G$, b, $b' \in B$. Since Bw_oB is dense in G, $a^+(w_o) \neq 0$. Since also $a^+(bw_o) = a^+(w_o.w_o^{-1}bw_o)$, we get from the above equation that $\mu(b^{-1}) = \lambda(w_o^{-1}bw_o)$, so that $\mu = \lambda^*$. Since μ is uniquely determined by λ , the function a^+ is determined by its value at w_o by

(*) with $x = w_o$ and the density of Bw_oB in G, proving the uniqueness in (b).

Remarks: (a) In characteristic 0 it easily follows from the theorem of complete reducibility that A_λ itself is irreducible.

(b) The representation of G on A_λ is, in the context of polynomial representations, the one induced by the character λ on B. The fact that it contains a representation of highest weight λ^*, is, in view of Theorem 39(a), a form of Frobenius reciprocity.

Lemma 74: Let f^+ be as in Lemma 73 and $a^+ = \varphi f^+$ with φ as in Theorem 40(a) so that $xv^+ = a^+(x)w_ov^+ +$ higher terms. Let W_λ be the stabilizer of λ in W, and for $w \in W_\lambda$ assume that the corresponding representative $w \in G$ has been chosen so that $wv^+ = v^+$. Then if $x \in G$ is written uhw_owu_1 (see Theorem 4') we have $a^+(x) = \lambda^*(h^{-1})$ if $w \in W_\lambda$,

$= 0$ otherwise.

Proof: A choice for $w \in G$ as above is always possible: if $\lambda = 0$, then V is trivial since $G = \mathcal{D}G$, while if $\lambda \neq 0$, then wv^+ has weight $w\lambda = \lambda$, hence is a multiple of v^+, so that by modifying it by a suitable element of H we can achieve $wv^+ = v^+$. From the definitions and Lemma 72 we have $a^+(x)w_ov^+ = hw_owv^+$. If $w \in W_\lambda$, then $a^+(x) = \lambda^*(h^{-1})$ by the choice of w, while if $a^+(x) \neq 0$, then w fixes kv^+ by the equation so that $w \in W_\lambda$.

This brings us to the

Second proof of the existential part of Theorem 39(e):

Proof: Let λ be as in Theorem 39(c). It will be enough to prove that the function defined by the last equations of Lemma 74 is rational on G. The existence will then follow from Theorem 40(b) with λ^* in place of λ. By Lemma 70 any power of this function will do, so that by Lemma 74 it will be enough to construct an irreducible representation whose highest weight is some positive power (positive multiple if we write characters on H additively) of λ. This we will do, using the following interesting result.

Lemma 75 (Chevalley): Let G be a linear algebraic group and P a closed subgroup. Then there exists a rational G-module V and a line L in V whose stabilizer in G is P.

Proof: Let A be the algebra of polynomials in the matric entries and I the ideal defining P. By Hilbert's basis theorem I is generated by a finite number of its elements, so that there exists a finite-dimensional G-invariant subspace B of A such that $B \cap I$, say C, generates I. For $x \in G$ we have the following equivalent conditions: $x \in P$; $f(x^{-1}y) = 0$ for all $f \in I$, $y \in P$; $xI \subseteq I$; $xC \subseteq C$. If now $c = \dim C$, $V = \bigwedge^c B$, v is the product in V of a basis for C, and $L = kv$, it follows that the stabilizer of L is exactly P.

We resume the proof of existence. Let $\prod = \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$ be the set of simple roots. For $i = 1,2,\ldots,\ell$ let P_i be the parabolic subgroup of G corresponding to $\prod - \{\alpha_i\}$ (see Lemma

30), $L_i = kv_i$ the corresponding line of Lemma 75, μ_i the corresponding rational character on P_i, hence also on B and H, and $V_i = kGv_i$. If $j \neq i$, then w_j is represented in P_i, so that $w_j\mu_i = \mu_i$ and $\langle \mu_i, \alpha_j \rangle = 0$. Since w_i does not fix L_i, by choice, it follows from parts (b) and (c) of Theorem 39 applied to V_i that $\langle \mu_i, \alpha_i \rangle$ is a positive integer, say d_i. If now λ is as before so that $\langle \lambda, \alpha_i \rangle = c_i \in \mathbb{Z}^+$, it follows that $d\lambda = \Sigma\, e_i\mu_i$ with $d = \prod d_i$ and $e_i = c_i d/d_i$. If we form the tensor product $\prod V_i^{e_i}$, then $\prod v_i^{e_i}$ is a vector of weight $d\lambda$ for B, so that we may extract an irreducible component whose highest weight is $d\lambda$, and thus complete our second existence proof.

Remark: We are indebted to G. D. Mostow for the proof just given.

The extra problems that arise when char $k \neq 0$ are compensated for by the fact that only a finite number of representations has to considered in this case, as we shall now see.

Lemma 76: Assume char $k = p \neq 0$. Let Fr (for Frobenius) denote the operation of replacing the matric entries of the elements of G by their p^{th} powers. If ρ is an irreducible rational representation of G, then so is $\rho \circ \mathrm{Fr}$. If the highest weight of ρ is λ, that of $\rho \circ \mathrm{Fr}$ is $p\lambda$.

Proof: Exercise.

Theorem 41: Assume that G above is universal (i.e. G is a simply connected algebraic group), and that char $k = p \neq 0$. Let

$\mathcal{R}$ be the set of p^t irreducible rational representations of G for which the highest weight λ satisfies $0 \leq \langle \lambda, \alpha_i \rangle \leq p - 1$ (α_i simple). Then every irreducible rational representation of G can be written uniquely $\bigotimes_{j=0}^{\infty} \rho_j \circ \mathrm{Fr}^j$ ($\rho_j \in \mathcal{R}$).

Sketch of proof: We observe first that since G is universal $L = L_1$, so that all λ's with all $\langle \lambda, \alpha_i \rangle \in \mathbb{Z}^+$ occur as highest weights, in particular those used to define $\mathcal{R}$. Consider $\rho = \bigotimes \rho_j \circ \mathrm{Fr}^j$. Let λ_j be the highest weight of ρ_j. The product of the corresponding weight vectors yields for ρ a highest weight vector of weight $\lambda = \Sigma\, p^j \lambda_j$, by Lemma 76. If we vary the ρ_j's in $\mathcal{R}$, we obtain, in view of the uniqueness of the expansion of a number in the scale of p, each possible highest weight λ exactly once. Thus to prove the theorem we need only show that each ρ above is irreducible. The proof of this fact depends eventually on the linear independence of the distinct automorphisms $\mathrm{Fr}^j (j = 0,1,\ldots)$ of k. We omit the details, referring the reader to R. Steinberg, Nagoya Math. J. 22 (1963), or to P. Cartier, Sém. Bourbaki 255 (1963).

Corollary: Assume that one of the special situations of Theorem 28 holds. Let $\mathcal{R}_\ell$ (resp. $\mathcal{R}_s$) be the subsets of $\mathcal{R}$ defined by $\langle \lambda, \alpha_i \rangle = 0$ for all i such that α_i is long (resp. short). Then every element of $\mathcal{R}$ can be written uniquely $\rho_\ell \otimes \rho_s$ with $\rho_\ell \in \mathcal{R}_\ell$ and $\rho_s \in \mathcal{R}_s$.

Proof: Given $\rho \in \mathcal{R}$, write the corresponding highest weight λ

as $\lambda_\ell + \lambda_s$ so that the corresponding irreducible representations ρ_ℓ and ρ_s are in $\mathcal{R}_\ell$ and $\mathcal{R}_s$. We have to show that $\rho_\ell \otimes \rho_s$ is irreducible. If we define φ as in Theorem 28 but with G and G^* interchanged, and set $\rho_\ell^* = \varphi \circ \rho_\ell$, $\rho_s^* = \varphi \circ \rho_s$, we have to show that the representation $\rho_\ell^* \otimes \rho_s^*$ of G^* is irreducible. Since the corresponding highest weights satisfy

$$\langle \lambda_\ell^*, \alpha^* \rangle = \langle \lambda_\ell, \alpha \rangle \quad \text{if } \alpha \text{ is short}$$
$$= 0 \quad \text{if not}$$
$$\langle \lambda_s^*, \alpha^* \rangle = p\langle \lambda_s, \alpha \rangle \quad \text{if } \alpha \text{ is long}$$
$$= 0 \quad \text{if not,}$$

we see that λ_ℓ^* and λ_s^*/p correspond to elements of $\mathcal{R}^*$, so that the corollary follows from Theorem 41 applied to G^*.

Examples: (a) SL_2. Here there are p representations ρ_i $(i = 0,1,\ldots,p-1)$ in $\mathcal{R}$, the i^{th} being realized on the space of polynomials homogeneous of degree i over k^2.

(b) Sp_4, $p = 2$. Here there are 4 representations in $\mathcal{R}$. If φ is the graph automorphism of Theorem 28 then $\mathcal{R}_\ell \circ \varphi = \mathcal{R}_s$ so that by the above corollary, these 4 are, in terms of the defining representation ρ, just 1 (trivial), ρ, $\rho \circ \varphi$, and $\rho \otimes (\rho \circ \varphi)$.

The results we have obtained can easily be extended to the case that k is infinite (but perhaps not algebraically closed). We consider representations on vector spaces over K, some algebraically closed field containing k, and call them rational if

the coordinates of the image are polynomial functions over K in the coordinates of the source. The preceding theory is then applicable almost word for word because of the following two facts both coming from the denseness of G in G_K (this is G with k extended to K) .

(a) Every irreducible polynomial representation of G extends uniquely to one of G_K .

(b) On restriction to G every irreducible rational representation of G_K remains irreducible.

Exercise: Prove (a) and (b).

The structure of arbitrary irreducible representations is given in terms of the polynomial ones by the following general theorem. Given an isomorphism φ of k into K , we shall also write φ for the natural isomorphism of G onto the group φG obtained from G by replacing k by φk .

Theorem 42 (Borel, Tits): Let G be an indecomposable universal Chevalley group over an infinite field k , and let σ be an arbitrary (not necessarily rational) irreducible representation of G on a finite-dimensional vector space V over an algebraically closed field K . Assume that σ is nontrivial. Then there exist finitely-many isomorphisms φ_i of k into K and corresponding irreducible rational representations ρ_i of $\varphi_i G$ over K such that $\sigma = \bigotimes_i \rho_i \circ \varphi_i$.

Remarks: (a) As a corollary we see that k is necessarily

imbeddable as a subfield of K. In other words, if k and K are such that no such imbedding exists, e.g. if char $k \neq$ char K, then every irreducible representation of G on a finite-dimensional vector space over K is necessarily trivial. (Deduce that the same is true even if the representation is not irreducible.) If k is finite, these statements are, of course, false.

(b) The theorem can be completed by statements concerning the uniqueness of the decomposition and the condition for irreducibility if the factors are prescribed. Since these statements are a bit complicated we shall omit them.

(c) The theorem was conjectured by us in Nagoya Math. J. 22 (1963). The proof to follow is based on an as yet unpublished paper by A. Borel and J. Tits in which results of a more general character are considered.

Lemma 77: Let G, G' be indecomposable Chevalley groups over fields k, k' with k infinite and k' algebraically closed, and $\sigma: G \longrightarrow G'$ a homomorphism such that σG is dense in G'.

(a) There exists an isomorphism φ of k into k' and a rational homomorphism ρ of φG into G' such that $\sigma = \rho \circ \varphi$.

(b) If G is universal, then ρ can be lifted, uniquely, to the universal covering group of G'.

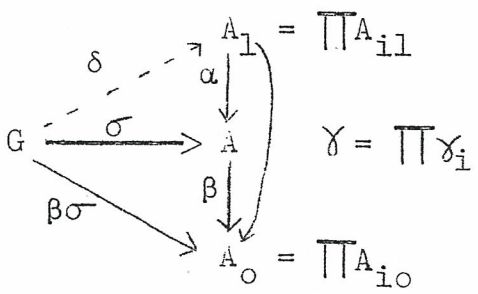
Proof: (a) If the reader will examine the proof of Theorem 31 he will observe that what is shown there is that σ can be normalized so that $\sigma x_\alpha(t) = x_{\alpha'}(\varepsilon_\alpha \varphi(t)^{q(\alpha)})$ with $\alpha \longrightarrow \alpha'$ an

angle-preserving map of Σ on Σ', $\varepsilon_\alpha = \pm 1$, φ an isomorphism of k onto k', and $q(\alpha) = 1$ on p. Since we are assuming only that σG is dense in G', not that $\sigma G = G'$, the proof of the corresponding result in the present case is somewhat harder. However, the main ideas are quite similar. We omit the proof. From the above equations and the corresponding ones on H, it follows from Theorem 7 that σ has the form of (a).

(b) From these equations we see also, e.g. by considering the relations (A), (B), (C) of Theorem 8, that ρ can be lifted to any covering of G', uniquely since $G = \mathcal{D}G$.

Proof of Theorem 42: Let $A = \overline{\sigma G}$, the smallest algebraic subgroup of $GL(V)$ containing σG. We claim A is a connected semisimple group, hence a Chevalley group. As in the proof of Theorem 30, step (12), $\overline{\sigma U}$ is connected, and similarly for $\overline{\sigma \bar{U}}$, so that A, being generated by these groups, is also. Let R be a connected solvable normal subgroup of A. By the Lie-Kolchin theorem R has weights on V, finite in number. A permutes the corresponding weight spaces, and, being connected, fixes them all. Since V is irreducible, there is only one such space and it is all of V, so that R consists of scalars, of determinant 1 since $A = \mathcal{D}A$, so that R is finite. Since R is connected, $R = 1$, so that A is semisimple, as claimed. Let $A_1 = \prod A_{i1}$ be the universal covering group of A written as a product of its indecomposable components, $A_o = \prod A_{io}$ the corresponding factorization of the adjoint group, and $\alpha, \beta, \gamma = \prod \gamma_i$ the

corresponding natural maps as shown:



By Lemma 77 we can lift $\beta\sigma$ componentwise to get a homomorphism $\delta: G \longrightarrow A_1$ of the form $\delta(x) = \prod \varepsilon_i \varphi_i(x)$ with each φ_i an isomorphism of k into K and ε_i a rational homomorphism of $\varphi_i G$ into A_{il}. We have $\alpha\delta = \sigma$ since otherwise we would have a homomorphism of G into the center of A. By Lemma 68, Cor. (a), α, interpreted as an irreducible rational representation of A_1, may be factored $\bigotimes_i \alpha_i$ with α_i an irreducible rational representation of A_{il}. On setting $\rho_i = \alpha_i \varepsilon_i$, we see that $\sigma = \alpha\delta = \bigotimes \alpha_i \varepsilon_i \varphi_i = \bigotimes_i \rho_i \varphi_i$, as required.

Corollary: (a) Every absolutely irreducible real representation of a real Chevalley group G is rational.

(b) Every holomorphic irreducible representation of a semisimple complex Lie group is rational.

(c) Every continuous irreducible representation of a simply connected semisimple complex Lie group is the tensor product of a holomorphic one and an antiholomorphic one.

Proof: (a) If G is universal, this follows from the theorem and the fact that the only isomorphism of $\mathbb{R}$ into $\mathbb{R}$ is id. The

transition to the nonuniversal case is an easy exercise.

(b) The proof is similar to that of (a).

(c) The only continuous isomorphisms of $\mathbb{C}$ into $\mathbb{C}$ are the identity and complex conjugation.

Exercise: Prove that the word "absolutely" in (a) and the words "simply connected" in (c) may not be removed.

Now we shall touch briefly on some additional results.

Characters. As is customary in representation theory, the characters (i.e. the traces of the representative matrices) play a vital role. We state the principal results in the form of an exercise.

Exercise: (a) Prove that two irreducible rational G-modules are isomorphic if and only if their characters are equal. (Consider the characters on H.)

(b) Assume that char $k = 0$ and that the theorem of complete reducibility has been proved in this case. Prove (a) for representations which need not be irreducible.

(c) Assume char $k = 0$. Prove Weyl's formulas: Let V, λ be as in Theorem 39(e), χ the corresponding character, and δ one-half the sum of the positive roots, a character on H. Set $S_\lambda = \sum_{w \in W} \det w.w(\lambda + \delta)$; a sum of functions on H. Then

(1) $\chi(h) = S_\lambda(h)/S_o(h)$ at all $h \in H$ where $S_o(h) \neq 0$.

(2) $\dim V = \prod_{\alpha > 0} \langle \lambda + \delta, \alpha \rangle / \langle \delta, \alpha \rangle$.

(Hint: use the corresponding formulas for Lie algebras (see, e.g., Jacobson, Lie Algebras) and the complement to Theorem 39).

Remark: The formula (1) determines χ uniquely since it turns out that the elements of G which are conjugate to those elements of H for which $S_o \neq 0$ form a dense open set in G.

The unitarian trick. The basic results about the irreducible complex representations of a compact semisimple Lie group K, i.e. a maximal compact subgroup of a complex Chevalley group G as in §8, can be deduced from those of G because of the following important fact: (*) K is Zariski-dense in G. Because of Lemmas 43(b) and 45 (K is generated by the groups $\varphi_2 SU_2$) this comes down to the fact that SU_2 is Zariski-dense in $SL_2(\mathbb{C})$, whose proof is an easy exercise. By (*) the rational irreducible representations of G remain distinct and irreducible on restriction to K. That a complete set of continuous representations of K is so obtained then follows from the fact that the corresponding characters form a complete set of continuous class functions on K. The proof of this uses the formula for Haar measure on K and the orthogonality and completeness properties of complex exponentials, and yields as a by-product Weyl's character formula itself. This is how Weyl proved his formula in Math. Zeit. 24 (1926) and it is still the best way. The theorem of complete reducibility can be proved as follows. Given any rational representation space V for G and an invariant subspace V', we can, by averaging over K, relative to Haar measure, any projection of V onto V' and taking the kernel of the result, get a complementary subspace invariant under K, thus also invariant under

G because of (*). It is then not difficult to replace the complex field by any field of characteristic 0 .

Invariant bilinear forms. G denotes an indecomposable infinite Chevalley group, V an irreducible rational G-module, and λ its highest weight.

Lemma 78: The following conditions are equivalent.

(a) There exists on V a (nonzero) invariant bilinear form.

(b) V and its dual V^* are isomorphic.

(c) $-w_o\lambda = \lambda$.

Proof: Exercise (see Lemma 73).

Exercise: Prove that $-w_o$ is the identity for all simple types except $A_n (n \geq 2)$, D_{2n+1}, E_6, and for these types it comes from involutory automorphism of the Dynkin diagram. (Hint: for all of the unlisted cases except for D_{2n} the Dynkin diagram has no symmetry.)

Exercise: If there exists an invariant bilinear form on V , then it is unique up to multiplication by a scalar and is either symmetric or skew-symmetric. (Hint: use Schur's Lemma.)

Lemma 79: Let $h = \prod h_\alpha(-1)$, the product over the positive roots.

(a) h is in the center of G and $h^2 = 1$.

(b) If V possesses an invariant bilinear form then it is symmetric if $\lambda(h) = 1$,
skew-symmetric if $\lambda(h) = -1$.

Proof: (a) Since $h_\alpha(-1) = h_{-\alpha}(-1)$ (check this), h is fixed by all elements of W. This implies that h is in the center, as easily follows from Theorem 4'. Since $h_\alpha(-1)^2 = h_\alpha(1) = 1$, we have $h^2 = 1$.

(b) We have an isomorphism $\varphi: V \longrightarrow V^*$, $v^+ \longrightarrow f^+$ with v^+ and f^+ as in Lemma 73; the corresponding bilinear form on V is given by $(v,v') = (\varphi v)(v')$. It follows that $(xv^+, yv^+) = f^+(x^{-1}yv^+)$ for all $x, y \in G$. Thus $(v^+, w_o v^+) = f^+(w_o v^+) \neq 0$ by the definition of f^+, and $(w_o v^+, v^+) = f(w_o^{-1} v^+)$. If $w_o = w_\alpha w_\beta w_\gamma \ldots$ is a minimal product of simple reflections in W, then for definiteness we pick $w_o = w_\alpha(1) w_\beta(1) \ldots$ in G, so that $w_o^{-1} = \ldots w_\gamma(-1) w_\beta(-1) w_\alpha(-1)$. We have $w_\alpha(-1) = w_\alpha(1) h_\alpha(1)$, and similarly for $\beta, \gamma, \ldots$. Substituting into the expression for w_o^{-1} and bringing all the h's to the right, by repeated conjugation by w's, we get to the right h by Appendix II (25) and to the left $\ldots w_\gamma(1) w_\beta(1) w_\alpha(1)$ which is just w_o by a lemma to be proved in the last section. Thus $w_o^{-1} = w_o h$, and $(w_o v^+, v^+)$ becomes $\lambda(h) f^+(w_o v^+) = \lambda(h)(v^+, w_o v^+)$, as required.

Observation: h as in Lemma 79 is 1 in each of the following cases, since the center is of odd order.

(a) G is adjoint.

(b) Char $k = 2$.

(c) G is of type A_{2n}, E_6, E_8, F_4, G_2.

Exercise: In the remaining cases find h, as a product $\prod h_\alpha(-1)^{n_\alpha}$ over the simple roots.

Example: SL_2 . For every V there is an invariant bilinear form. Assume char $k = 0$, so that for each $i = 1,2,3,\ldots$ there is exactly one V of dimension i , viz. the space of polynomials homogeneous of degree $i - 1$. Then the invariant form is symmetric if i is odd, skew-symmetric if i is even.

Invariant Hermitean forms. Assume now that G is complex, σ is the automorphism of Theorem 16, $K = G_\sigma$ is the corresponding maximal compact subgroup, V and v^+ are as before, and $f: G \longrightarrow \mathbb{C}$ is defined by $xv^+ = f(x)v^+ +$ terms of other weights.

(a) Prove that $f(\sigma x^{-1}) = \overline{f(x)}$. (First prove it on U^-HU , then use the density of U^-HU in G .)

(b) Prove that there exists a unique form $(\ ,\ )$ from $V \times V$ to $\mathbb{C}$ which is linear in the second position, conjugate linear in the first, and satisfies $(xv^+, yv^+) = f(\sigma x^{-1}y)$, and that this form is Hermitean.

(c) Prove that $(\ ,\ )$ is positive definite and invariant under K .

Dimensions. Assume now that G is a Chevalley group over an infinite field k , that V and λ are as before, and that $\mathcal{U}_\mathbb{Z}$ is the universal algebra of Theorem 2, written in the form $\mathcal{U}_\mathbb{Z}^- \mathcal{U}_\mathbb{Z}^0 \mathcal{U}_\mathbb{Z}^+$ of page 16.

(a) Prove that there exists an antiautomorphism σ of $\mathcal{U}_\mathbb{Z}$ such that $\sigma X_\alpha = X_{-\alpha}$ and $\sigma H_\alpha = H_\alpha$ for all α .

(b) Define a bilinear form (u,u') from $\mathcal{U}_\mathbb{Z}$ to $\mathcal{U}_\mathbb{Z}^0$ thus:

write $\sigma u.u^{\dagger}$ in the above form and then set every $X_\alpha = 0$. Prove that this form is symmetric.

(c) Now define a bilinear form from $\mathcal{U}_{\mathbb{Z}}$ to $\mathbb{Z}$ thus: $(\ , \ )_\lambda = \lambda \circ (\ , \ )$ (interpreting λ as a linear form on $\mathcal{H}$ such that $\lambda(H_\alpha) \in \mathbb{Z}^+$ for all $\alpha > 0$). Assuming now that this form is reduced modulo the characteristic of k, prove that its rank is just the dimension of V.

§ 13. Representations continued. In this section the irreducible representations of characteristic p (the characteristic of the base field k) of the finite Chevalley groups and their twisted analogues will be considered. The main result is as follows.

Theorem 43: Let G be a finite universal Chevalley group or one of its twisted analogues constructed as in §11 as the set of fixed points of an automorphism of the form $x_\alpha(t) \to x_{\rho\alpha}(\pm t^{q(\alpha)})$. Then the $\prod_{\alpha \text{ simple}} q(\alpha)$ irreducible polynomial representations of the including algebraic group (got by extending the base field k to its algebraic closure) for which the highest weights λ satisfy $0 \leq \langle \lambda, \alpha \rangle \leq q(\alpha) - 1$ for all simple α remain irreducible and distinct on restriction to G and form a complete set.

By Theorem 41 we also have a tensor product theorem with the product $\prod_0^\infty$ suitably truncated, for example to $\prod_0^{n-1}$ if G is a Chevalley group over a field of p^n elements.

Exercise: Deduce from Theorem 43 the nature of the truncations for the various twisted groups.

Instead of proving the above results (see Nagoya Math. J 22 (1963)), which would take too long, we shall give an a priori development, similar to the one of the last section.

We start with a group of twisted rank 1 (i.e. of type A_1, ${}^2A_2$, ${}^2C_2$, or ${}^2G_2$, the degenerate cases $A_1(2)$, $A_1(3)$, ... not being excluded). The subscript σ on G_σ, W_σ, ... will

henceforth be omitted. We write X, Y, w, K for $\mathcal{X}_a (a > o)$, $\mathcal{X}_{-a}$, the nontrivial element of the Weyl group realized in G, and an algebraically closed field of characteristic p. We observe that $U = X$ and $U^- = Y$ in the present case. In addition, $\overline{X}$ will denote the sum of the elements of X in KG.

Definition: An element v in a KG-module V is said to be a highest weight vector if it is nonzero and satisfies

(a) $xv = v$ for all $x \in U$.

(b) $hv = \lambda(h)v$ for all $h \in H$ and some character λ on H.

(c) $\overline{X}wv = \mu v$ for some $\mu \in K$.

The couple (λ, μ) is called the corresponding weight.

Remark: The refinement (c) of the usual definition is due to C. W. Curtis (Ill. J. Math. 7(1963) and J. für Math. 219 (1965)). That such a refinement is needed is already seen in the simplest case $G = SL_2(p)$. Here there are p representations realized on the spaces of homogeneous polynomials of degrees $i = 0, 1, \ldots, p - 1$, with the highest weight in the usual sense being $i\lambda_1$. Since the group H is cyclic of order $p - 1$, the weights 0 and $(p - 1)\lambda_1$ are identical on H, hence do not distinguish the corresponding representations from each other.

Theorem 44: Let G (of rank 1) and the notations be as above.

(a) Every nonzero KG-module V contains a highest weight vector v. For such a v we have $KGv = KYv = KU^-v$.

(b) If V is irreducible, then it determines Kv as the unique line of V fixed by U, hence it also determines the corresponding highest weight.

(c) Two irreducible KG-modules are isomorphic if and only if their highest weights are equal.

The proof depends on the following two lemmas.

Lemma 80: Let Y and K be as above, or, more generally, let Y be any finite p-group and K any field of characteristic p.

(a) Every nonzero KY-module V contains nonzero vectors invariant under Y.

(b) Every irreducible KY-module is trivial.

(c) $\mathrm{Rad}\, KY = \{\Sigma c(y)y \mid \Sigma c(y) = 0\}$ is the unique maximal (one-sided or two-sided) ideal of KY. It is nilpotent.

(d) $K\overline{Y}$ is the unique minimal ideal of KY.

Proof: (a) By induction on $|Y|$. Assume $|Y| > 1$. Since Y is a p-group, it has a normal subgroup Y_1 of index p, and the subspace V_1 of invariants of Y_1 on V is nonzero by the inductive assumption. Choose $y \in Y$ to generate Y/Y_1, and v in V_1 and nonzero. Then $(1 - y)^p v = 0$. Now choose r maximal so that $(1 - y)^r v \neq 0$. The resulting vector is fixed by Y, whence (a).

(b) By (a).

(c) By inspection Rad KY is an ideal, maximal because its codimension in KY is 1 . Bring the kernel of the trivial representation, which is the only irreducible one by (b), it is the unique maximal left ideal; and similarly for right ideals. On each factor of a composition series for the left regular representation of KY on itself Y acts trivially by (b), hence Rad KY acts as 0 , so that Rad KY is nilpotent.

(d) By (b).

Lemma 81: For $x \in X - 1$, write $wxw = f(x)h(x)wg(x)$ with $f(x), g(x) \in X$ and $h(x) \in H$.

(a) f and g are permutations of $X - 1$.

(b) $(\overline{X}w)^2 = \overline{X}w^2 + \sum_{x \in X-1} h(x)\overline{X}wg(x)$.

Proof: (a) If $f(x) = 1$, we get the contradiction $xw \in B$, while if $f(x') = f(x)$, we see that $w^{-1}x^{-1}x'w \in B$, so that $x' = x$. Similarly for g .

(b) $(\overline{X}w)^2 = \overline{X}w^2 + \sum_{x \in X-1} \overline{X}f(x)h(x)wg(x)$.

Here $f(x)$ gets absorbed in $\overline{X}$ and $h(x)$ normzlizes $\overline{X}$, whence (b).

Proof of Theorem 44: (a) By Lemma 80(b) the space of fixed points of $U = X$ on V is nonzero. Since H normalizes U and is Abelian, that space contains a nonzero vector v such that (a) and (b) of the definition of highest weight vector hold. Let

$\overline{X}wv = v_1$. If $v_1 = 0$, then (c) holds with $\mu = 0$. If not, we replace v by v_1 . Then (a) and (b) of the definition still hold with $w\lambda$ in place of λ , and by Lemma 81(b) so does (c) with $\mu = \Sigma\lambda(h(x))$. Now to prove that $KGv = KYv$ it is enough, because of the decomposition $G = YB \cup wB$, to prove that $wv \in KYv$. By the two parts of Lemma 81 we may write $\overline{X}wv = \mu v$, after some simplification, in the form

$$(*) \qquad wv + \sum_{x \in X^{-1}} \lambda(wh^{-1}w)y(x)v = \mu v \ ,$$

with $y(x) = wxw^{-1} \in Y$, whence our assertion.

(b) Let $V' = Kv$ and $V'' = \text{Rad } KY \cdot v$. It follows from Lemma 80(c) that the sum $V = V' + V''$ is direct. Now assume there exists some $v_1 \in V$, $v_1 \notin V'$, fixed by X . We may assume that $v_1 \in V''$ and also that v_1 is an eigenvector for H since H is Abelian. We have $\overline{X}wv_1 = w\overline{Y}v_1 = 0$; since $\overline{Y}(1-y) = 0$ for any $y \in Y$. Thus v_1 is a highest weight vector. By (a), $V = KYv_1 \subseteq KYV'' = V''$, a contradiction, whence (b) .

(c) By (b) an irreducible KG-module determines its highest weight (λ,μ) uniquely. Conversely, assume that V_1 and V_2 are irreducible KG-modules with highest weight vectors v_1 and v_2 of the same weight (λ,μ) . Set $v = v_1 + v_2 \in V_1 \dotplus V_2$ and then $V = KGv = KYv$. Now $v_2 \notin V$, since otherwise we could write $v_2 = cv + v''$ with $c \in K$ and $v'' \in \text{Rad } KY.v$ and then projecting on V_1 and V_2 get that $c = 0$ and $c = 1$, a contradiction. Thus we

may complete the proof as in the proof of Theorem 39(e).

Theorem 45: Let (λ,μ) be the highest weight of an irreducible KG-module V.

(a) If $\lambda \neq 1$, then $\mu = 0$. If $\lambda = 1$, then $\mu = 0$ or -1.

(b) Every weight as in (a) can be realized. Thus the number of possibilities is $|H| + 1$.

Proof: (1) Proof of (b). In KG let $H_\lambda = \sum_{h\in H} \lambda(h^{-1})h$, then $u = \bar{X}H_\lambda w\bar{X}$ and $v = \bar{X}H_\lambda$. As in the proof of Theorem 44(a), a simple calculation yields $\bar{X}w(u+cv) = \sum_{x\in X-1} \lambda(h(x))u + c\bar{X}wH_\lambda\bar{X}$. Here H acts, from the left, according to the characters $w\lambda,\lambda,w\lambda$ on the respective terms. Thus if $w\lambda \neq \lambda$, we may realize the weight $(\lambda,0)$ by taking $c = 0$. If $w\lambda = \lambda$, we take $c = -\Sigma\lambda(h(x))$ instead. Finally if $\lambda = 1$, then $\Sigma\lambda(h(x)) = -1$ and we get $\mu = -1$ by taking $c = 0$. To achieve (λ,μ) in an irreducible module we simply take $KG(u+cv)$ modulo a maximal submodule.

(2) If $\dim V = 1$, then V is trivial and $(\lambda,\mu) = (1,0)$. Since X and Y are p-groups, they act trivially by Lemma 80(b), whence (2).

(3) If $\dim V \neq 1$, then λ determines μ. Write $V = V' + V''$ as in the proof of Theorem 44(b). We have $V'' \neq 0$. Since Y fixes V'' it fixes some line in it, uniquely determined in V, by Theorem 44(b) with Y in place of X. Since Y clearly fixes wv, we conclude that $wv \in V''$. Projecting (*) of the proof

of Theorem 44(a) onto V', we get

(**) $\Sigma\, \lambda(wh^{-1}w) = \mu$,

whence (3).

(4) Proof of (a). Combine (1),(2) and (3).

Corollaries to Theorems 44 and 45:

(a) If $\lambda \neq 1$, then $\sum_{x \in X-1} \lambda(h(x)) = 0$. The number of solutions $n(h)$ of $h(x) = h$ with h given is, modulo p, independent of h, in particular for each h is at least 1 (cf. Lemma 64, Step (1)).

(b) The irreducible representation of weight (λ,μ) can be realized in the left ideal generated by $\bar{X}H_\lambda w\bar{X} + c\bar{X}H_\lambda$ with

$c = 1$ for the trivial representation $(1,0)$

$= 0$ otherwise.

(c) If $L \subset K$ is a splitting field for H, it is one for G.

(d) Dim $V = |X|$ if $(\lambda,\mu) = (1,-1)$

$< |X|$ if not.

(e) The number of p-regular conjugacy classes of G is $|H| + 1$.

Proof: (a) If $\lambda \neq 1$, then $\mu = 0$ by Theorem 45(a), so that $\Sigma\lambda(h(x)) = 0$ by (**) above applied with λ replaced by $w\lambda$. Then $\Sigma n(h)\lambda(h) = 0$ for every $\lambda \neq 1$. By the orthogonality relations for the characters on H (which are valid since $p \nmid |h|$), we conclude that $n(h)$, as an element of K, is independent of h. If $n(h)$ were 0 for some h, we would get $|H| = \Sigma\, n(h) = 0 \pmod p$, a contradiction.

(b) Let V be an irreducible module whose dual V^* has the highest weight (λ,μ). We consider, as in Theorem 40 the isomorphism φ of V^* into the induced representation space of functions $a : G \longrightarrow K$ such that $a(yb) = a(y)\lambda^*(b)$ for all $y \in G$, $b \in B$ defined by $(\varphi f)(x) = f(xv^+)$ with v^+ a highest weight vector for V. Using the decomposition $V = Kwv^+ + \text{Rad } KX \cdot wv^+$, we may define f^+ as in Lemma 73, prove that it is a highest weight vector, and that $a^+ = \varphi f^+$ is given by the equations of Lemma 74, with λ^* in place of λ. Coverting functions on G to elements of KG in the usual way, $a \sim \Sigma\, a(x)x$, we see that a^+ becomes the element of (b), whence (b). At the same time we see that V may be realized in the induced module $B_{\lambda^*} \longrightarrow G$, as the unique irreducible submodule in case $\lambda \neq 1$, as one of two in case $\lambda = 1$.

(c) By (b).

(d) If $\mu = 0$, then $\overline{X}wv = 0$, whence $\overline{Y}v = 0$ and $\dim V < |X|$ by Theorem 44(a). Conversely if $\dim V < |X|$, then the annihilator of v in KY contains $\overline{Y}$ by Lemma 80(d), so that $\mu = 0$.

(e) By a classical theorem of Brauer and Nesbitt (University of Toronto Studies, 1937) the number in question equals the number of irreducible KG-modules, hence equals $|H| + 1$ by Theorem 45(b).

Example: $G = SL_2(q)$. Here $|H| = q - 1$, so that $|H| + 1 = q$.

Remarks. (a) We see that the extra condition $\overline{X}v = \mu v$ serves two purposes. First it distinguishes the smallest module $\sim (1,0)$

from the largest $(1,-1)$. Secondly, in the proof of the key relation $KGv = KU\bar{}v$ it takes the place of the density argument ($U\bar{}B$ dense in G) used in the infinite case.

(b) The preceding development applies to a wide class of doubly transitive permutation groups (with B the stabilizer of a point, H of two points), since it depends only on the facts that H is Abelian and has in B a normal complement U which is a p-Sylow subgroup of G.

Now we consider groups of arbitrary rank. W ($= W_\sigma$) will be given the structure of reflection group as in Theorem 32 with Σ/R (see p. 177), projected into V_σ and scaled down to a set of unit vectors, the corresponding root system. For each simple root a, we write Y_a for X_{-a} and choose $\bar{w}_a$ in $\langle X_a, Y_a \rangle$ to represent w_a in W. If $w \in W$ is arbitrary, we choose a minimal expression $w = w_a w_b \cdots$ as a product of simple reflections, and set $\bar{w} = \bar{w}_a \bar{w}_b \cdots$. Then $\bar{w}$ is independent of the minimal expression chosen. We postpone the proof of this fact, which could (and probably should) have been given much earlier, to the end of the section so as not to interrupt the present development. As a consequance we have:

Lemma 82: If $w = w_a w_b \cdots$ is any minimal expression, then $\bar{X}_w = \bar{X}_a \bar{w}_a \cdot \bar{X}_b \bar{w}_b \cdots$.

Proof: Since $\bar{w} = \bar{w}_a \bar{w}_b \cdots$ this easily follows by induction on $N(w)$ or by Appendix II.25.

We extend the earlier definition of highest weight vector

by the new requirement:

(c) $\overline{X}_a \overline{w}_a v = \mu_a v$ $(\mu_a \in K)$ for every simple root a.

Theorem 46: Let G be a (perhaps twisted) finite Chevalley group (of arbitrary rank).

(a),(b),(c) Same as (a),(b),(c) of Theorem 44.

(d) Let $H_a = H \cap \langle X_a, Y_a \rangle$. If (λ, μ_a) is the highest weight of some irreducible module then $\mu_a = 0$ if $\lambda|H_a \neq 1$, and $\mu_a = 0$ or -1 if $\lambda|H_a = 1$.

(e) Every weight as in (a) can be realized on some irreducible KG-module.

Proof: We shall prove this theorem in several steps.

(a1) There exists in V a nonzero eigenvector v for B. This is proved as in Theorem 44(a).

(a2) If v is as in (a1), then so is $v_1 = \overline{X}_a \overline{w}_a v$ (a simple), unless it is 0.

Proof: Let x be any element of U. Write $x = x_a' x_a$ with $x_a \in X_a$ and $x_a' \in X_a'$, the subgroup of elements of U whose X_a components are 1. We recall that X_a and $\overline{w}_a$ normalize X_a' (see Appendix I.11). Thus $xv_1 = x_a' \overline{X}_a \overline{w}_a v = v_1$, since $Uv = v$. Since H normalizes X_a and is normalized by $\overline{w}_a$, we see that v_1 is also an eigenvector for H.

(a3) Choose v as in (a1), then $w \in W$ so that $N(w)$ is maximal subject to $v_1 = \overline{X}_w \overline{w} v \neq 0$. Then v_1 is a highest weight vector.

Proof: By Lemma 82 and (a2), v_1 is an eigenvector for B. Let a be any simple root. If $w^{-1}a > 0$, then $N(w_a w) = N(w) + 1$ by Appendix II.19, so that $\bar{X}_{w_a w}\bar{w_a w} = \bar{X}_a\bar{w}_a\bar{X}_w\bar{w}$ by Lemma 82, and $\bar{X}_a\bar{w}_a v_1 = 0$ by the choice of w. If $w^{-1}a < 0$, then we may choose a minimal expression $w = w_a w_b \ldots$ starting with w_a. Then

$$\bar{X}_a\bar{w}_a v_1 = (\bar{X}_a\bar{w}_a)^2\bar{X}_b\bar{w}_b \ldots v \quad \text{by Lemma 82}$$

$$= \mu\,\bar{X}_a\bar{w}_a\bar{X}_b\bar{w}_b \ldots v, \quad \text{with } \mu \in K \text{ by Lemma 81(b)}$$

$$= \mu v_1 .$$

By (a1) and (a3) we have the first statement in (a).

(a4) $KGv = KU^-v$.

Proof: We have $G = \bar{w}_o G \subseteq \bigcup_w \bar{w}\,U^-B$ by Theorem 4. Thus it is enough to show each $\bar{w}$ fixes KU^-v, and for this we may assume $w = w_a$ with a simple. Assume $y \in U^-$. Write $y = y_a y_a'$ as above, but using negative roots instead. Then y_a and $\bar{w}_a$ normalize Y_a', so that $\bar{w}_a yv = \bar{w}_a y_a y_a' v \in U^-\bar{w}_a y_a v \subseteq KU^-v$ by Theorem 44(a) applied to $\langle X_a, Y_a\rangle$.

(b1) If $V = V' + V''$ with $V' = Kv$ and $V'' = \text{Rad } KU^-v$ as before, then V'' is fixed by every $\bar{X}_a\bar{w}_a$.

Proof: Write $y = y_a y_a'$ as before.

Then $\bar{X}_a\bar{w}_a yv = \sum_{x \in X_a} y(x)x\bar{w}_a v$ with $y(x) \in U^-$.

Thus $\bar{X}_a\bar{w}_a(y-1)v = \sum_{x \in X_a}(y(x)-1)x\bar{w}_a v \in V''$.

(b2) Proof of (b). If this is false, there exists

$v_1 \in V''$, $v_1 \neq 0$, v_1 fixed by X. As usual we may choose v_1 as an eigenvector for H, and then by (b1) and (a3) also an eigenvector for each $\bar{X}_a\bar{w}_a$. Then, as before, $V = KGv_1 = KU^-v_1 \subseteq V''$, a contradiction.

(c) Same proof as for Theorem 44(c).

(d) By Theorem 45(a) applied to $< X_a, Y_a >$.

(e) Let π be the set of simple roots a such that $\mu_a = 0$, and W_π the corresponding subgroup of W. The reader should have no trouble in proving that the left ideal of KG generated by $\sum_{w \in W_\pi w_o} \bar{U} H_\lambda \bar{w} \bar{X}_w$ is an irreducible KG-module whose highest weight is (λ, μ_a).

Corollary: (a) A splitting field for H is also one for G.

(b) Let V be irreducible, of highest weight (λ, μ_a). Then $\dim V = |U|$ if $\lambda = 1$ and all $\mu_a = -1$.

$< |U|$ if not.

(c) For each set π of simple roots, let H_π be the group generated by all $H_a (a \in \pi)$. Then the number of irreducible KG-modules, or, equivalently, of p-regular conjugacy classes of G is $\sum_\pi |H/H_\pi|$.

Proof: (a) Clear.

(b) Write $\bar{U}\bar{w}_o v = \bar{X}_{w_o}\bar{w}_o v = \bar{X}_a\bar{w}_a\bar{X}_b\bar{w}_b \ldots v$, with $w_o = w_a w_b \ldots$ as in Lemma 82, and then proceed as in the proof of Cor. (d) to Theorems 44 and 45.

(c) The given sum counts the number of possible weights (λ, μ_a) according to the set π of simple roots a such that

$\mu_a = -1$.

Exercise: If G is universal, the above number is $\prod_{a \text{ simple}} (|H_a| + 1) = \prod_{\alpha \text{ Simple}} q(\alpha)$, in the notation of Theorem 43. If in addition G is not twisted, then the number is q^{ℓ} .

It remains to prove the following result used (inessentially) in the proof of Lemma 82.

Lemma 83: (a) If $w \in W$, then any two minimal expressions for w as a product of simple reflections can be transformed into each other by the relations

(*) $w_a w_b w_a \cdots = w_b w_a w_b \cdots$ (n terms on each side, n = order $w_a w_b$, with a and b distinct simple roots).

(b) Assume that for each simple root a the corresponding element $\overline{w}_a$ of G (any Chevalley group) is chosen to lie in $< X_a, X_{-a} >$. Let $w = w_a w_b \cdots$ be a minimal expression for $w \in W$. Then $\overline{w} = \overline{w}_a \overline{w}_b \cdots$ is independent of the minimal expression chosen.

Proof: (a) This is a refinement of Appendix IV.38 since the relations $w_\alpha^2 = 1$ are not required. It is an easy exercise to convert the proof of the latter result into a proof of the former, which we shall leave to the reader.

(b) Because of (a) we only have to prove (b) when w has the form of the two sides of (*). For this we can refer to the proof of Lemma 56 since the extra restrictions there, that G is untwisted and that $\overline{w}_a = w_a(1)$ for each a, are not

essential for the proof.

Remark: It would be nice if someone could incorporate in the elementary development just given the tensor product theorem mentioned after Theorem 43 or at least a proof that every irreducible K-module for G can be extended to the including algebraic group, hence also to the other finite Chevalley groups contained in the latter group.

§14. Representations concluded. Now we turn to the complex representations of the groups just considered. Here the theory is in poor shape. Only GL_n (Green, T.A.M.S. 1955) and a few groups of low rank have been worked out completely, then only in terms of the characters. Here we shall consider a few general results which may lead to a general theory.

Henceforth K will denote the complex field. Given a (one-dimensional) character λ on a subgroup B of a group G, realized on a space V_λ, we shall write V_λ^G for the induced module for G. This may be defined by $V_\lambda^G = KG \otimes_{KB} V_\lambda$ (this differs from our earlier version in that we have not switched to a space of functions), and may be realized in KG in the left ideal generated by $B_\lambda = \sum_{b \in B} \lambda(b^{-1})b$ (and will be used in this form). Its dimension is $|G/B|$.

Exercise: Check these assertions.

Lemma 84: Let B, C be subgroups of a finite group G, let λ, μ be characters on B, C, and let V_λ^G, V_μ^G be the corresponding modules for G.

(a) If $x \in G$, then $B_\lambda x C_\mu$ in KG is determined up to multiplication by a nonzero scalar by the (B,C) double coset to which x belongs.

(b) $\mathrm{Hom}_G(V_\lambda^G, V_\mu^G)$ is isomorphic as a K-space to the one generated by all $B_\lambda x C_\mu$.

(c) If $B = C$ and $\lambda = \mu$, then the isomorphism in (b) is one of algebras.

(d) The dimension of $\mathrm{Hom}_G(V_\lambda^G, V_\mu^G)$ is the number of (B,C) double cosets D such that $B_\lambda \times C_\mu \neq 0$ for some, hence for every x in D, or, equivalently, such that the restrictions of λ and $x\mu$ to $B \cap x C x^{-1}$ are equal.

Proof: (a) This is clear.

(b) Assume $T \in \mathrm{Hom}_G(V_\lambda^G, V_\mu^G)$. Since B_λ generates V_λ^G as a KG-module, TB_λ determines T. Let $TB_\lambda = \sum_{x \in G/C} c_x \times C_\mu$. Since $bB_\lambda = \lambda(b)B_\lambda$, we get by averaging over B that $TB_\lambda = \sum_{x \in B\backslash G/C} c_x B_\lambda \times C_\mu$. Thus T is realized on B_λ, hence on all of V_λ^G, by right multiplication by $|B|^{-1} \sum c_x B_\lambda \times C_\mu$. Conversely, any such right multiplication yields a homomorphism, which proves (b).

(c) By discussion in (b).

(d) The first statement follows from (a) and (b). Let $B_1 = B \cap x C x^{-1}$ and $C_1 = x^{-1} B x \cap C$, and $\{y_i\}$ and $\{z_j\}$ systems of representatives for $B_1\backslash B$ and C/C_1. Set $B'_\lambda = \sum \lambda(y_i^{-1}) y_i$ and $C'_\mu = \sum \mu(z_j^{-1}) z_j$. Then $B_\lambda \times C_\mu = B'_\lambda B_1 \lambda B_{1, x\mu} \times C'_\mu$ with $(x\mu)(x c x^{-1}) = \mu(c)$ since $x C_1 x^{-1} = B_1$. If $\lambda \neq x\mu$ on B_1, then $B_1 \lambda B_{1, x\mu} = 0$. If $\lambda = x\mu$, this product is $|B_1| B_{1\lambda}$, and then $B_\lambda \times C_\mu \neq 0$ since the elements $y_i b_1 \times z_j$ are all distinct.

Remarks: (a) This is a special case of a theorem of G. Mackey. (See, e.g., Feit's notes.)

(b) The algebra of (c) is also called the commuting

algebra since it consists of all endomorphisms of V_λ^G that commute with the action of G.

Theorem 47: Let G be a (perhaps twisted) finite Chevalley group.

(a) If λ is a character on H extended to B in the usual way, then V_λ^G is irreducible if and only if $w\lambda \neq \lambda$ for every $w \in W$ such that $w \neq 1$.

(b) If λ, μ both satisfy the conditions of (a), then V_λ^G is isomorphic to V_μ^G if and only if $\lambda = w\mu$ for some $w \in W$.

Proof: (a) V_λ^G is irreducible if and only if its commuting algebra is one-dimensional (Schur's Lemma), i.e., by (c) and (d) of Lemma 84, if and only if λ and $w\lambda$ agree on $B \cap wBw^{-1}$, hence on H, for exactly one $w \in W$, i.e. for only $w = 1$.

(b) Since V_λ^G and V_μ^G are irreducible, they are isomorphic if and only if $\dim \mathrm{Hom}_G(V_\lambda^G, V_\mu^G) = 1$, which, as above, holds exactly when $\lambda = w\mu$ for some (hence for exactly one) $w \in W$.

Exercise: (a) $\dim \mathrm{Hom}_G(V_\lambda^G, V_\mu^G) = |W_\lambda|$ if $\lambda = w\mu$ for some w,

$= 0$ otherwise.

(b) In Theorem 47 the conclusion in (b) holds even if the condition in (a) doesn't.

Here W_λ is the stabilizer of λ in W. We see, in particular, that if $\lambda = 1$ then the commuting algebra of V_λ^G is $|W|$-dimensional. But more is true.

Theorem 48: Let V be the KG-module induced by the trivial one-dimensional KB-module. Then the commuting algebra $\mathrm{End}_G(V)$

is isomorphic to the group algebra KW.

Reformulations:

(a) The multiplicities of the irreducible components of V are just the degrees of the irreducible KW-modules.

(b) The subalgebra, call it A, of KG spanned by the double coset sums $\overline{B}w\overline{X}_w$ is isomorphic to KW.

(c) The algebra of functions $f: G \longrightarrow K$ biinvariant under B ($f(bxb') = f(x)$ for all $b,b' \in B$) with convolution as multiplication is isomorphic to KW.

Proof: The theorem is equivalent to (a) by Schur's Lemma and to (b) by Lemma 84, while (b) and (c) are clearly equivalent. We shall give a proof of (b), due to J. Tits. $\hat{w}$ will denote the average in KG of the elements of the double coset BwB. The elements $\hat{w}$ form a basis of A and $\hat{1}$ is the unit element. If a is a simple root, c_a will denote $|X_a|^{-1}$.

(1) A is generated as an algebra by $\{\hat{w}_a \mid a \text{ simple}\}$ subject to the relations

(α) $\hat{w}_a^2 = c_a\hat{1} + (1-c_a)\hat{w}_a$ for all a.

(β) $\hat{w}_a\hat{w}_b\hat{w}_a \ldots = \hat{w}_b\hat{w}_a\hat{w}_b \ldots$, as in Lemma 83(a).

Proof: We observe that if each c_a is replaced by 1 then these relations go over into a defining set for KW, by Appendix II.38. Since $B \cup Bw_aX_a$ is a group, we have $(\overline{B}w_a\overline{X}_a)^2 = r\overline{B} + s\overline{B}w_a\overline{X}_a$ with $r,s \in K$. Since Bw_aX contains with each of its elements its inverse, we get $r = |Bw_aX_a|$, and then from the total coefficient $s = |Bw_aX_a| - |B|$. Thus (α) holds in A, and so does (β) by

Lemma 25,Cor., which also shows that the $\hat{w}_a$ generate A. Conversely, let A_1 be the abstract associative algebra (with $\hat{1}$) generated by symbols $\hat{w}_a$ subject to (α) and (β). For each $w \in W$ choose a minimal expression $w = w_a w_b \ldots$ and set $\hat{w} = \hat{w}_a \hat{w}_b \ldots$. By Lemma 83(a) and (β) this is independent of the expression chosen. By (α) it follows that

$$\hat{w}_a \hat{w} = \widehat{w_a w} \qquad \text{if } w^{-1}a > 0 ,$$

$$= c_a \widehat{w_a w} + (1 - c_a)\hat{w} \quad \text{if } w^{-1}a < 0.$$

Thus the $\hat{w}$ form a basis for A_1, which, having the same dimension as A, is therefore isomorphic to it.

(2) There exists a positive number $c = c(G)$ such that $c_a = c^{n_a}$ with n_a a positive integer depending only on the type of G. The multiplication table of A in terms of the basis $\{\hat{w}\}$ is given by polynomials in c depending only on the type.

Proof: Consider ${}^2A_4(q^2)$, for example. Here the two possibilities for $|X_a|$ are q^2 and q^3 by Lemma 63(c). If we set $c = q^{-1}$, then the corresponding values of n_a are 2 and 3, which depend only on the type. For each of the other types the verification is similar. From the first statement of (2) and the equations of the proof of (1) the second statement follows.

(3) An associative algebra A_c with multiplication table given by the polynomials of (2) exists for every complex number c. In particular $A_{c(G)} = A$ and $A_1 = KW$.

Proof: Since the type of the group G contains an infinite number

of members, the multiplication table is associative for an infinite set of values of c, hence for all values.

(4) A_c is semisimple for $c = c(G)$, for $c = 1$, and for all but a finite number of values of c.

Proof: A_c is for $c = c(G)$ the commuting algebra of a KG-module and for $c = 1$ a group algebra KW, hence semisimple in both cases. The discriminant of A_c is a polynomial in c, nonzero at $c = 1$ since then A_c is semisimple, hence nonzero for all but a finite number of values of c.

(5) Completion of proof. Since A is semisimple and K is an algebraically closed field, A is a direct sum of complete matric algebras, of certain degrees over K (see, e.g., Jacobson's Structure of Rings or Feit's notes), and similarly for KW. We have to show that the degrees are the same in the two cases. If $\mathcal{a}$ is any finite-dimensional associative algebra which is separable, i.e. which is semisimple when the base field is extended to its algebraic closure, we define the numerical invariants of $\mathcal{a}$ to be the degrees of the resulting matric algebras. The proof of Theorem 48 will be completed by the following lemma.

Lemma 85: Let R be an integral domain, F its field of quotients, and f a homomorphism of R onto a field K. Let $\mathcal{a}$ be a finite-dimensional associative algebra over R, and $\mathcal{a}_F$ and $\mathcal{a}_K$ the resulting algebras over F and K. If $\mathcal{a}_F$ and $\mathcal{a}_K$ are separable, then they have the same numerical

invariants.

In fact, from (3) and the lemma with $R = K[c]$, $\mathcal{A} = A_c$, and first $f : c \longrightarrow c(G)$ and then $f : c \longrightarrow 1$, it follows that A and KW have the same numerical invariants, hence that they are isomorphic.

Proof of the lemma:

(a) Assume that $\mathcal{B}$ is a finite-dimensional semisimple associative algebra over an algebraically closed field L, that $b_1, b_2, \ldots, b_n$ form a basis for $\mathcal{B}/L$, that $x_1, x_2, \ldots, x_n$ are independent indeterminates over L, that $b = \Sigma\, x_i b_i$, and that $P(t)$ is the characteristic polynomial of b acting from the left on $\mathcal{B}_{L(x_1,\ldots,x_n)}$, written as $P(t) = \prod P_i(t)^{p_i}$ with the P_i distinct monic polynomials irreducible over $L(x_1,\ldots,x_n)$. Then:

(a1) The p_i are the numerical invariants of $\mathcal{B}$.

(a2) $p_i = dg_t P_i$ for each i.

(a3) If $P(t) = \prod Q_j(t)^{q_j}$ is any factorization over $L(x_1,\ldots,x_n)$ such that $q_j = dg_t Q_j$ for each j, then it agrees with the one above so that the q_j are the numerical invariants of $\mathcal{B}$.

Proof: For (a1) and (a2) we may assume that $\mathcal{B}$ is the complete matric algebra End L^p and that $b = \Sigma x_{ij} E_{ij}$ in terms of the matric units E_{ij}. If $X = [x_{ij}]$, then $P(t) = \det(tI - X)^p$, so that we have to show that $\det(tI - X)$ is irreducible over $L(x_{ij})$. This is so since specialization to

the set of companion matrices $\begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ x_{p1} & x_{p2} & \cdots & x_{pp} \end{bmatrix}$

yields the general equation
of degree p. In (a3) if some Q_j were reducible or equal to some Q_k with $k \neq j$, then any irreducible factor P_i of Q_j would violate (a2).

(b) Let R^* be the integral closure of R in $\overline{F}$ (consisting of all elements satisfying monic polynomial equations over R), and $x_1, x_2, \ldots, x_n$ indeterminates over $\overline{F}$. Then $R^*[x_1, \ldots, x_n]$ is the integral closure of $R[x_1, \ldots, x_n]$ in $\overline{F}(x_1, \ldots, x_n)$.

Proof: See, e.g., Bourbaki, Commutative Algebra, Chapter V, Prop. 13.

(c) If R^* is as in (b), then any homomorphism of R into K can be extended to one of R^* into $\overline{K}$.

Proof: By Zorn's lemma this can be reduced to the case $R^* = R[\alpha]$, where it is almost immediate since $\overline{K}$ is algebraically closed.

(d) Completion of proof. Let $\{a_i\}$ be a basis for $\mathcal{A}/R$, hence also for $\mathcal{A}_F/F$, and $\{x_i\}$ independent indeterminates over $\overline{F}$ and also over $\overline{K}$. The given homomorphism $f : R \longrightarrow K$ defines a homomorphism $f : \mathcal{A} \longrightarrow \mathcal{A}_K$. By (c) it extends to a homomorphism of R^* into $\overline{K}$ and then naturally to one of $R^*[x_1, \ldots, x_n]$ into $\overline{K}[x_1, \ldots, x_n]$. If $a = \Sigma x_i a_i$ and $P(t) = \prod P_i(t)^{p_i}$ is its characteristic polynomial, factored over $\overline{F}(x_1, \ldots, x_n)$ as before, then the coefficients of each P_i are

integral polynomials in its roots, hence integral over the coefficients of P, hence integral over $R[x_1,x_2,\ldots,x_n]$, hence belong to $R^*[x_1,\ldots,x_n]$ by (b). Thus if $f(a) = \Sigma x_i f(a_i)$, then its character polynomial has a corresponding factorization $F_f(t) = \prod P_{if}(t)^{p_i}$ over $\overline{K}(x_1,\ldots,x_n)$. By (a1) the p_i are the numerical invariants of $\mathcal{A}_F$, and by (a2) they satisfy $p_i = dg_t P_i = dg_t P_{if}$, so that by (a3) with $\mathcal{B} = \mathcal{A}_{\overline{K}}$ they are also the numerical invariants of $\mathcal{A}_K$, which proves the lemma.

Exercise: If λ is a character on H extended to B in the usual way, then $\mathrm{End}_G(V_\lambda^G)$ is isomorphic to KW_λ. (Observe that this result includes both Theorem 47 and Theorem 48.)

Remark: Although A is isomorphic to KW there does not seem to be any natural isomorphism and no one has succeeded in decomposing the module V of Theorem 48 into its irreducible components, except for some groups of low rank. We may obtain some partial results, in terms of characters, by inducing from the parabolic subgroups and using the following simple facts.

Lemma 86: Let π be a set of simple roots, W_π and G_π the corresponding subgroups of W and G (see Lemma 30), and V_π^W and V_π^G the corresponding trivial modules induced to W and G; and similarly for π'.

(a) A system of representatives in W for the $(W_\pi, W_{\pi'})$ double cosets becomes in G a system of representatives for $(G_\pi, G_{\pi'})$ double cosets.

(b) $\dim \mathrm{Hom}_G(V_\pi^G, V_{\pi'}^G) = \dim \mathrm{Hom}_W(V_\pi^W, V_{\pi'}^W)$.

Proof: (a) Exercise.

(b) By Lemma 84(d) and (a).

Corollary 1: Let χ_π^G denote the character of V_π^G and similarly for W. If $\{n_\pi\}$ is a set of integers such that $\chi^W = \Sigma n_\pi \chi_\pi^W$ is an irreducible character of W, then $\chi^G = \Sigma n_\pi \chi_\pi^G$ is, up to sign, one of G.

Proof: Let $(\chi, \psi)_G$ denote the average of $\chi\bar{\psi}$ over G. We have $(\chi_\pi^G, \chi_{\pi'}^G)_G = \dim \mathrm{Hom}_G(V_\pi^G, V_{\pi'}^G)$, and similarly for W. Since χ^W is irreducible, $(\chi^W, \chi^W)_W = 1$, it follows that $(\chi^G, \chi^G)_G = 1$, so that $\pm\chi^G$ is irreducible, by the orthogonality relations for finite group characters.

Remarks: (a) In a beautiful paper in Berliner Sitzungsberichte, 1900, Frobenius has constructed a complete set of irreducible characters for the symmetric group S_n, i.e. the Weyl group of type A_{n-1}, as a set of integral combinations of the characters χ_π^W. Using his method and the preceding corollary one can decompose the character of V in Theorem 48 in case G is of type A_{n-1}. (See R. Steinberg T.A.M.S. 1951).

(b) The situation of (a) does not hold in general. Consider, for example, the group W of type B_2, i.e. the dihedral group of order 8. It has five irreducible modules (of dimensions 1,1,1,1,2), while there are only four χ_π^W's to work with.

(c) A result of a general nature is as follows.

Corollary 2: If the notation is as above and $(-1)^\pi$ is as in Lemma 66(d), then $\chi^G = \Sigma(-1)^\pi \chi_\pi^G$ is an irreducible character

of G and its degree in $|U|$.

Proof: Consider $\chi^W = \Sigma(-1)^\pi \chi^W_\pi$. By (8) on p. 142, extended to twisted groups (check this using the hints given in the proof of Lemma 66), $\chi^W = \det$, an irreducible character. Hence $\pm\chi^G$ is also one by Cor. 1 above. We have $\chi^G(1) = \Sigma(-1)^\pi |G/G_\pi|$. If G is untwisted and the base field has q elements, then by Theorem 4' applied to G and to G_π this can be continued $\Sigma(-1)^\pi W(q)/W_\pi(q) = q^N = |U|$, as in (4) of the proof of Theorem 26. If G is twisted, the proof is similar.

We continue with some remarks on the algebra A of Theorem 48(b).

Lemma 87: The homomorphisms of A onto K are given by: $f(\hat{w}_a) = 1$ or $-c_a$ for each simple root a, subject to the condition that $f(\hat{w}_a)$ is constant on each W-orbit.

Proof: For a and b simple, let $n(a,b)$ denote the order of $w_a w_b$ in W. We claim that (*) a and b belong to the same W-orbit if and only if there exists a sequence of simple roots $a = a_0, a_1, \ldots, a_r = b$ such that $n(a_i, a_{i+1})$ is odd for every i. The equation $\left(w_{a_i} w_{a_{i+1}}\right)^n = 1$ with n odd can be rewritten to show that w_{a_i} and $w_{a_{i+1}}$ are conjugate, so that if the sequence exists then a and b are conjugate. If a and b are conjugate, then so are w_a and w_b, and this remains true when we project into the reflection group obtained by imposing on W the additional relations: $(w_c w_d)^2 = 1$ whenever $n(c,d)$ is even. In this new group w_a and w_b must belong to the same component, so that the

required sequence exists. By (*) the condition of the lemma holds exactly when $f(\hat{w}_a) = f(\hat{w}_b)$ whenever $n(a,b)$ is odd, i.e. exactly when f preserves the relations (β) (of the proof of Theorem 48). Since $f(\hat{w}_a) = 1$ or $-c_a$ exactly when f preserves (α) (solve the quadratic), we have the lemma.

Remark: By finding the annihilator in A of the kernel of each of the homomorphisms of Lemma 87, we get a one-dimensional ideal I in A. This corresponds to an irreducible submodule of multiplicity 1 in V, realized in the left ideal KGI of KG. By working out the corresponding idempotent, the degree of the submodule can be found.

Exercise: (a) If $f(\hat{w}_a) = 1$ for all a, show that $I = K\Sigma\, q_w \hat{w}$ with $q_w = |X_w|$, and that the corresponding KG-module is the trivial one. (Hint: by writing W as a union of right cosets relative to $\{1, w_a\}$ and writing (α) in the form $(\hat{w}_a - 1)(\hat{w}_a + c_a) = 0$, show that I is as indicated.)

(b) If $f(\hat{w}_a) = -c_a$ for all a, show that $I = K\Sigma\,(\det w)\hat{w}$, and that in this case the dimension is $|U|$. (Hint: if e is the given sum and $c_w = q_w^{-1}$, show that $e^2 = me$ with $m = \Sigma c_w = |G/B|/|U|$.)

(c) For $G = B_2(q)$ work out all (four) cases of Lemma 87, hence obtain the degrees of all (five) irreducible components of V.

(d) Same for A_2 and for G_2.

Remark: It can be shown that the module of (b) is isomorphic to the one with character χ^G as in Lemma 86, Cor. 2. If we reduce

the element $\Sigma(\det w)|U/X_w|\overline{B}\, w\, \overline{X}_w$ (which is $|B||U|e$) of I mod p, we see from the proof of Theorem 46(e) that the given module reduces to the one of that theorem for which $\lambda = 1$ and every $\mu_a = -1$. This latter module can itself be shown to be isomorphic to the one in Theorem 43 for which $\langle \lambda, \alpha \rangle = q(\alpha) - 1$ for every α. From these facts and Weyl's formula the character of the original module can be found up to sign and the result used to prove that the number of p-elements (of order a power of p) of G is $|U|^2$. For the details see R. Steinberg, Endomorphisms of linear algebraic groups, to appear.

Finally, we should mention that the algebra A admits an involution given by $\hat{w}_a \longrightarrow 1 - c_a - \hat{w}_a$ for all a (which in case $c_a \longrightarrow 1$ and $A \longrightarrow KW$ reduces to $w \longrightarrow (\det w)w$).

The preceding discussion points up the following

Problem: Develop a representation theory for finite reflection groups and use it to decompose the module V (or the algebra A) of Theorem 48.

It is natural that in studying the complex representations of G we have considered first those induced by characters on B since for representations of characteristic p this leads to a complete set. In characteristic 0, however, this is not the case, as even the simplest case $G = SL_2$ shows. One must delve deeper. Therefore, we shall consider representations of G induced by (one-dimensional) characters λ on U. We can not expect such a representation ever to be irreducible since its degree $|G/U|$ is too large (larger than $|G|^{1/2}$), but what we shall show is that if λ is sufficiently general then at least it is multiplicity-free.

In other words, $\mathrm{End}_G(V_\lambda^G)$ is Abelian, hence a direct sum of fields. (If λ is not sufficiently general, we can expect the Weyl group to play a role, as in Theorem 48.)

Before stating the theorem, we prove two lemmas.

Lemma 88: Let k be a finite field and λ a nontrivial character from the additive group of k into K^*. Then every character can be written uniquely $\lambda_c : t \longrightarrow \lambda(ct)$ for some $c \in k$.

Proof: The map $c \longrightarrow \lambda_c$ is a homomorphism of k into its dual, and its kernel is clearly 0.

Lemma 89: For $w \in W$ the following conditions are equivalent.

(a) If a and wa are positive roots and one of them is simple, then so is the other.

(b) If a is simple and wa is positive, then wa is simple.

(c) $w = w_0 w_\pi$ for some set π of simple roots, with w_0 as usual and w_π the corresponding object of W_π.

There are 2^ℓ possibilities for w.

Proof: (c) $\Rightarrow$ (a) Because w_π maps π onto $-\pi$ and (*) permutes the positive roots with support not in π (same proof as for Appendix I.11).

(a) $\Longrightarrow$ (b) Obvious.

(b) $\Longrightarrow$ (c) Let π be the set of simple roots kept positive, hence simple, by w. We claim: (**) if $a > 0$ and supp $a \not\subseteq \pi$, then $wa < 0$. Write $a = b + c$ with supp $b \subseteq \pi$, supp $c \subseteq \prod - \pi$. Then $wa = wb + wc$. Here $wc < 0$ by the choice of π, and

supp $wc \not\subseteq w\pi \supseteq$ supp wb. Thus $wa < 0$. If a is a simple root not in π then $ww_\pi a < 0$ by (*) and (**), while if a is in π this holds by the definition of π. Thus $ww_\pi = w_o$, whence (c).

Theorem 49: Let G be a finite, perhaps twisted, Chevalley group and $\lambda : U \longrightarrow K^*$ a character such that $\lambda|X_a \neq 1$ if a is simple, $= 1$ if a is positive but not simple. Then V_λ^G is multiplicity-free. In other words, $\mathrm{End}_G(V_\lambda^G)$ is Abelian, or, equivalently, the subalgebra A of KG spanned by the elements $U_\lambda h\bar{w}U_\lambda$ $(h \in H, w \in W)$ is Abelian.

Here $U_\lambda = \sum_{u \in U} \lambda(u^{-1})u$, and we assume that the $\bar{w}$ are chosen as in Lemma 83(b).

Remarks: (a) If a is not simple, then usually $X_a \subseteq \mathcal{D}U$, so that the assumption $\lambda|X_a = 1$ is superfluous, but this is not always the case, e.g. for B_2 or F_4 with $|k| = 2$ or for G_2 with $|k| = 3$. In these latter groups, there are other possibilities, which because of their special nature will not be gone into here.

(b) The proof to follow is suggested by that of Gelfand and Graev, Doklady, 1963, who have given a proof for SL_n and announced the general result for the untwisted groups. T. Yokonuma, C. Rendues, Paris, 1967, has also given a proof for these latter groups, but his details are unnecessarily complicated.

Proof of Theorem 49: The fact that A is Abelian will follow from the existence of an (involutory) antiautomorphism f of G such that

(a) $fU = U$.

(b) $\lambda f = \lambda$ on U.

(c) For each double coset UnU such that $U_\lambda n U_\lambda \neq 0$, we have $f_n = n$ (here $n \in N = \Sigma H\bar{w}$).

For since f extended to KG and then restricted to A is an antiautomorphism and at the same time the identity (by (a), (b), (c)) it is clear that A is Abelian. The existence of f will be proved in several steps.

(1) If $U_\lambda n U_\lambda \neq 0$ and $n \in H\bar{w}$, then $w = w_o w_\pi$ for some set π of simple roots.

Proof: By Lemma 89 we need only prove that if a is simple and wa positive then wa is simple. Writing the first U_λ above with the X_{wa} component on the right, and the second with the X_a component on the left, we get $X_{wa,\lambda} n X_{a,\lambda} n^{-1} \neq 0$. Since λ is nontrivial on X_a it is also so on X_{wa}, whence wa is simple by the assumptions on λ, which proves (1).

The condition in (1) essentially forces the correct definition of f. We set $a^* = -w_o a$. If a is simple, so is a^*. In order to simplify the discussion in one or two spots we assume henceforth that G (i.e. its root system) is indecomposable. If G is untwisted, we start with the graph automorphism corresponding to * (see the Corollary on p. 156), compose it with the inversion $x \longrightarrow x^{-1}$, and finally with a diagonal automorphism so that the result f satisfies, not only $fU = U$ but also $\lambda f = \lambda$ on U. This is possible because of Lemma 89 and the assumptions on λ in the theorem. If G is twisted, then we may omit the graph automorphism (because * is then the identity), and use the explicit isomorphism $X_a / \mathfrak{J} X_a \cong k$ of (2) of the proof of Theorem 36 in combination with Lemma 89 to achieve the second

condition. We see that

(2) f is an involutory antiautomorphism which satisfies the required conditions (a) and (b). We must prove that it also satisfies (c). As consequences of the construction we have:

(3) $fh = \bar{w}_o h \bar{w}_o^{-1}$ for every $h \in H$.

(4) If $a^* = a$, then f is the identity on $X_a / \mathcal{O} X_a$.

(5) If $a^* = a$, there exists a nontrivial element of X_a fixed by f.

Proof: For X_a of type A_1 this follows from (4). For X_a of type ${}^2A_2$ we choose the element (t,u) of Lemma 63(c) with $t = 2$, $u = 2$ if $p \neq 2$, and $t = 0$, $u = 1$ if $p = 2$, since $f(t,u) = (t, -tt^{\theta}u)$ (check this, referring to the construction of f). For types ${}^2C_2$ and ${}^2G_2$ we may choose (0,1) and (0,1,0) since f is the identity on $\{(0,u)\}$ and $\{(0,u,0)\}$.

(6) The elements $\bar{w}_a \in G$ may be so chosen that:

(6a) $f\bar{w}_a = \bar{w}_{a^*}$ for every simple root a.

(6b) If a and b are simple and $n \in N$ is such that $n X_a n^{-1} = X_b$ and $\lambda(nxn^{-1}) = \lambda(x)$ for all $x \in X_a$, then $n\bar{w}_a n^{-1} = \bar{w}_b$.

Proof: Under the action of f and the inner automorphisms i_n by elements n as in (6b) the X_a (a simple) form orbits. From each orbit we select an element X_a. If $a^* = a$, we choose $x_a \in X_a$ as in (5), write it as (*) $x_a = x_1 \bar{w}_a x_2$ with $x_1, x_2 \in X_{-a}$, and choose $\bar{w}_a$ accordingly. Since f is an antiautomorphism and fixes X_{-a}, it also fixes $\bar{w}_a$ by the

uniqueness of the above form. If $a^* \neq a$, we choose $x_a \in X_a, x_a \neq 1$, arbitrarily. We then use the equations $f\bar{w}_a = \bar{w}_{a^*}$ and $i_n\bar{w}_a = \bar{w}_b$ of (6a) and (6b) to extend the definition of $\bar{w}$ to the orbit of a. We must show this can be done consistently, that we always return to the same value. Let $a_1, a_2, \ldots, a_n$ be a sequence of simple roots such that $a_1 = a_n = a$ and for each j either $a_{j+1} = a_j^*$ or else there exists n_j such that the assumptions in (6b) holds with a_j, a_{j+1}, n_j in place of a,b,n. Let g denote the product of the corresponding sequence of f's and i_{n_j}'s. We must show that g fixes $\bar{w}_a$. We have $gX_a = X_a$, $gX_{-a} = X_{-a}$, and in fact g acts on $X_a/\mathcal{D}X_a$, identified with k, by multiplication by a scalar c as follows from the definition of f and the usual formulas for i_n. Since $\lambda g = \lambda$ by the corresponding condition on f and each i_n, it follows from Lemma 89 that $c = 1$, so that g is the identity on $X_a/\mathcal{D}X_a$. If $\mathcal{D}X_a = 0$, then g fixes the element x_a above, hence also $\bar{w}_a$ by (*), whether g is an automorphism or an antiautomorphism. If $\mathcal{D}X_a \neq 0$, then G is twisted so that $a^* = a$. If g is an automorphism, then by the proof of Theorem 36 from (5) on its restriction to $\langle X_a, X_{-a}\rangle$ is the identity so that it fixes $\bar{w}_a$, while if g is an antiautomorphism then by the same result its restriction coincides with that of f so that it fixes $\bar{w}_a$ by the choice of $\bar{w}_a$.

Remark: If G is untwisted, the above proof is quite simple.

We assume henceforth that the $\bar{w}_a$ are as in (6).

(7) If $\bar{w} = \bar{w}_a\bar{w}_b \ldots$ as in Lemma 83(b) and $w^* = w_o w^{-1} w_o^{-1}$,

then $f\bar{w} = \bar{w}^*$.

Proof: Since $w_a w_b \ldots$ is minimal, $\ldots w_{b^*} w_{a^*}$ is also. (Check this.) Since f is an antiautomorphism it follows from (6a) that $f\bar{w} = \ldots \bar{w}_{b^*} \bar{w}_{a^*} = \overline{\ldots w_{b^*} w_{a^*}} = \bar{w}^*$.

(8) If w is as in (1) then $f\bar{w} = \bar{w}$.

Proof: $w^* = w$ in this case (see (7)).

(9) If n is as in (1) then $fn = n$.

Proof: By (1), $n \in \bar{w}H$ with $w = w_o w_\pi$. Assume $a \in \pi$. Then wa is simple and $\lambda(nxn^{-1}) = \lambda(x)$ for all $x \in X_a$, by the inequality in the proof of (1). Thus $n\bar{w}_a n^{-1} = \bar{w}_{wa}$ by (6b), from which we get, on picking a minimal expression for w_π , that (*) $n\bar{w}_\pi n^{-1} = \overline{w_{\pi^*}}$. Since $N(w) = N(w_o w_\pi) = N(w_o) - N(w_\pi)$, it follows that if we put together minimal expressions for w and w_π we will get one for w_o . Thus $\bar{w}_o = \bar{w}\bar{w}_\pi$ by Lemma 83(b), and similarly $\bar{w}_o = \bar{w}_{\pi^*}\bar{w}$, so that (**) $\bar{w}\bar{w}_\pi\bar{w}^{-1} = \bar{w}_{\pi^*}$. If now we write $n = \bar{w}h$, then h commutes with $\bar{w}_\pi$ by (*) and (**). Hence

$fn = fh \cdot f\bar{w}$ since f is an antiautomorphism

$= \bar{w}_o h \bar{w}_o^{-1} w$ by (3) and (8)

$= \bar{w}\bar{w}_\pi h \bar{w}_\pi^{-1}$ since $\bar{w}_o = \bar{w}\bar{w}_\pi$

$= \bar{w}h$ since h commutes with w_π

$= n$.

Thus f satisfies condition (c) and the proof of Theorem 49 is complete.

Exercise: (a) Prove that if $\{\overline{w}_a\}$ is as in (6) and w as in (1), then $U_\lambda \overline{w} U_\lambda \neq 0$.

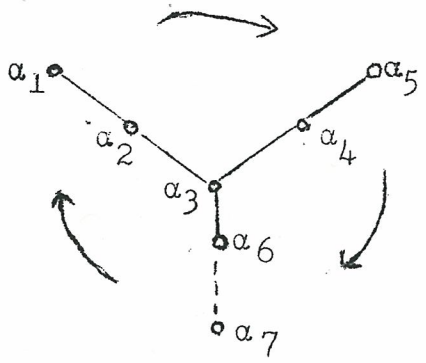
(b) Deduce that if H_π denotes the kernel of the set of simple roots π then the dimension of A, hence the number of irreducible components of V_λ^G, in Theorem 49 is $\Sigma |H_\pi|$.

Remark: The natural group for the preceding theorem seems to be the adjoint group extended by the diagonal automorphisms, a group of the same order as the universal group, but with something extra at the top instead of at the bottom. For this group, G', prove that the dimension above is just $\overline{\prod}(|H_a| + 1) = \overline{\prod} q(\alpha)$ in the notation of the exercise just before Lemma 83. Prove also that in this case V_λ^G is independent of λ.

Remark: The problem now is to decompose the algebra A of Theorem 49 into its simple (one-dimensional) components. If this were done, it would be a major step towards a representation theory for G. As far as we know this has been done only for the group A_1 (see Gelfand and Graev, Doklady, 1962). It would not, however, be the complete story. For not every irreducible G-module is contained in one induced by a character on U, i.e., by Frobenius reciprocity, contains a one-dimensional U-module, as the following, our final, example, due to M. Kneser, shows (although it is for some types of groups such as A_n).

As remarked earlier, reduction mod 3 yields an isomorphism of the subgroup W^+ of elements of determinant 1 of the Weyl group W of type E_6 onto the group $G = SO_5(3)$, the adjoint

group of type $B_2(3)$. If we reverse this isomorphism and extend the scalars we obtain a representation of G on a complex space V. The assertion is that U, i.e. a 3-Sylow subgroup of G, fixes no line of V. Consider the following diagram.



This is the Dynkin diagram of E_6 with the lowest root α_7 adjoined (α_7 is the unique root in $-D$ (see Appendix III.33), unique because all roots are conjugate in the present case. It is connected as shown because of symmetry and the fact that each proper subdiagram must represent a finite reflection group.) We choose as a basis for V the α's with α_3 omitted, a union of three bases of mutually orthogonal planes. w_1w_2 acts as a rotation of 120° in the plane $\langle\alpha_1,\alpha_2\rangle$ and as the identity in the other two planes, and similarly for w_4w_5 and w_6w_7. The group W^+ also contains an element permuting the three planes cyclically as shown, because of the conjugacy of simple systems and the uniqueness of lowest roots, and the four elements generate a 3-subgroup of W^+. It is now a simple matter to prove that this subgroup fixes no line of V.

APPENDIX ON FINITE REFLECTION GROUPS

The results (and some of the terminology in what follows) are motivated by the theory of semisimple Lie algebras, but no knowledge of this theory is assumed. The main results are starred.

I Preliminaries

V will be a finite-dimensional real or rational Euclidean space. By a reflection (on V) is meant a reflection in some hyperplane H. If α is a nonzero vector orthogonal to H, the reflection, denoted σ_α, is given by

(1) $\sigma_\alpha \rho = \rho - 2(\rho,\alpha)/(\alpha,\alpha)\cdot\alpha \qquad (\rho \in V)$.

We observe that σ_α is an automorphism of V, of order 2.

A useful fact is:

(2) If w is an automorphism of V, then $w\sigma_\alpha w^{-1} = \sigma_{w\alpha}$.

To prove this, apply both sides to $\rho \in V$, then use (1) and the invariance of $(\ ,\ )$ under w.

Σ will denote a finite set of nonzero elements of V such that:

(3) $\alpha \in \Sigma \Rightarrow -\alpha \in \Sigma$ and $k\alpha \notin \Sigma$ if $k \neq \pm 1$.

(4) $\alpha \in \Sigma \Rightarrow \sigma_\alpha \Sigma = \Sigma$.

The elements of Σ will be called roots, and W will denote the group generated by all σ_α $(\alpha \in \Sigma)$.

(5) Lemma. The restriction of W to Σ is faithful.

For, each $w \in W$ fixes pointwise the orthogonal complement of Σ.

(6) Cor. W is finite.

(7) Examples. (a) If Σ is the root system of a semisimple Lie algebra over the complex field, then W is the corresponding Weyl group. (b) If W is any finite group generated by reflections, e.g. the group of symmetries of a regular solid, Σ may be taken as the set of unit normals to the hyperplanes in which reflections of W take place.

(8) Definitions. A subset of roots is called a positive system if it consists of the roots which are positive relative to some ordering of V. (Recall that this involves the specification of a subset V^+ of V which is closed under addition and under multiplication by positive scalars and satisfies trichotomy.) A subset of roots, say Π, is a simple system if (a) Π is a linearly independent set, and (b) every root is a linear combination of the elements of Π in which all nonzero coefficients are either all positive or all negative.

(9) Proposition. (a) Each simple system is contained in a unique positive system. (b) Each positive system contains a unique simple system.

If Π is a simple system, then clearly the "all positive" roots in (8b) form the unique positive system containing Π, whence (a). Now let P be any positive system. Let Π be a subset of P which generates P under positive linear

combinations and is minimal relative to this property. Then (*) $\alpha, \beta \in \Pi, \alpha \neq \beta \Longrightarrow (\alpha,\beta) \leq 0$. Assume not, so that $\sigma_\alpha\beta = \beta - c\alpha$ with $c > 0$. Assume $\sigma_\alpha\beta \in P$, so that $\sigma_\alpha\beta = \Sigma c_\gamma \gamma$ $(\gamma \in \Pi, c_\gamma \geq 0)$. If $c_\beta < 1$, the last equation, written suitably, expresses β as a positive combination of the other elements of Π, a contradiction to the minimality of Π, while if $c_\beta \geq 1$, it expresses 0 as a positive combination of elements of Π, hence of P, equally a contradiction. Similarly $-\sigma_\alpha\beta \in P$ leads to a contradiction, whence (*). Now a linear relation on Π may be written $\Sigma a_\alpha\alpha = \Sigma b_\beta\beta$ with the two sums over disjoint parts of Π and $a_\alpha, b_\beta \geq 0$. Writing this as $\rho = \sigma$ and using (*), we get $(\rho,\rho) = (\rho,\sigma) \leq 0$, whence $\rho = 0$ and then every $a_\alpha = 0$ because the α's are all positive. Similarly every $b_\beta = 0$. Thus Π is independent, is a simple system. From the definition of a simple system any simple system contained in P consists of those elements of P which are not positive combinations of others, hence is uniquely determined by P.

(10) Lemma. Let Π be a simple system and P the positive system containing Π. (a) $\alpha, \beta \in \Pi, \alpha \neq \beta \Longrightarrow (\alpha,\beta) \leq 0$. (b) $\rho \in P \Longrightarrow$ there exists $\alpha \in \Pi$ so that $(\rho,\alpha) > 0$.

For (b) write $\rho = \Sigma c_\alpha \alpha (\alpha \in \Pi, c_\alpha \geq 0)$ as in (8b), and then use $0 < (\rho,\rho) = \Sigma c_\alpha (\rho,\alpha)$.

*(11) Main lemma. Let Π, P be as in (10) and $\alpha \in \Pi$. Then $\sigma_\alpha\alpha = -\alpha$ and $\sigma_\alpha(P \setminus \alpha) = P \setminus \alpha$.

Pick $\rho \in P \setminus \alpha$, $\rho = \Sigma c_\beta\beta$ $(c_\beta \geq 0 ; \beta \in \Pi)$. By (3) some

$c_\beta > 0$ $(\beta \neq \alpha)$. Application of σ_α does not change this c_β. Hence $\sigma_\alpha \rho \in P \setminus \alpha$.

(12) Theorem. Any two simple (or positive) systems are conjugate under W.

By (9) we need only consider two positive systems, say P and P'. We use induction on $n = |P \cap (-P')|$. If $n = 0$, $P = P'$. Assume $n > 0$. Then there is a root α simple relative to P such that $\alpha \in P \cap (-P')$. By (11), $|\sigma_\alpha P \cap (-P')| = n-1$, whence $|P \cap -\sigma_\alpha P'| = n-1$. By the inductive assumption $\sigma_\alpha P'$ is conjugate to P; hence so is P'.

Henceforth Π, P will be as in (10) and fixed.

(13) Definition. If $\rho \in \Sigma$, $\rho = \sum_{\alpha \in \Pi} c_\alpha \alpha$ as in (8b), then $\sum c_\alpha$ is called the height of ρ and written ht ρ.

e.g. $\alpha \in \Pi \Rightarrow$ ht $\alpha = 1$.

(14) Lemma. Let W_o be the group generated by $\{\sigma_\alpha | \alpha \in \Pi\}$. If $\rho \in P$, the minimum value of ht on the set $W_o \rho$ is 1 and is taken on only on $W_o \rho \cap \Pi$.

Let ρ' be a minimum point and assume, if possible, that $\rho' \notin \Pi$. By (10b) there is $\alpha \in \Pi$ so that $(\rho', \alpha) > 0$, whence by (1) ht $\sigma_\alpha \rho' <$ ht ρ' and by (11) $\sigma_\alpha \rho' > 0$, a contradiction to the choice of ρ'.

(15) Corollary. (a) If $\rho \in P$, $\rho \notin \Pi$, then ht $\rho > 1$.

(b) $W_o \Pi = \Sigma$. i.e. Every root ρ is conjugate under W_o to a

simple root.

By (14), (a) is clear and so is (b) if $\rho > 0$. If $\rho < 0$, then $-\rho > 0$, whence $-\rho = w\alpha$ ($w \in W_o$, $\alpha \in \Pi$), so that $\rho = (w\sigma_\alpha)\alpha$.

(16) Theorem. W is generated by $\{\sigma_\alpha | \alpha \in \Pi\}$. i.e. $W = W_o$ in (14).

If ρ is a root we have $\rho = w\alpha$ ($w \in W_o$, $\alpha \in \Pi$), by (15b), whence $\sigma_\rho = w\sigma_\alpha w^{-1}$ (see (2)), an element of W_o. Hence $W \subseteq W_o$ and $W = W_o$.

II The function N

(17) Definition. For $w \in W$, $N(w)$ will denote the number of roots ρ such that $\rho > 0$ and $w\rho < 0$. In other words, $N(w) = |P \cap w^{-1}(-P)|$.

e.g. $N(1) = 0$, $N(\sigma_\alpha) = 1$ if $\alpha \in \Pi$, by (11).

(18) Lemma. $w \in W \Rightarrow N(w^{-1}) = N(w)$.

Prove this.

(19) Lemma. Assume $w \in W$, $\alpha \in \Pi$.

(a) If $w^{-1}\alpha > 0$, then $N(\sigma_\alpha w) = N(w) + 1$.

(a') If $w^{-1}\alpha < 0$, then $N(\sigma_\alpha w) = N(w) - 1$.

(b) If $w\alpha > 0$, then $N(w\sigma_\alpha) = N(w) + 1$.

(b') If $w\alpha < 0$, then $N(w\sigma_\alpha) = N(w) - 1$.

Let $S(w) = P \cap w^{-1}(-P)$. Then $S(\sigma_\alpha w) = w^{-1}\alpha \cup S(w)$, whence (a). To get (a') replace w by $\sigma_\alpha w$ in (a), and to get (b) and (b') replace w by w^{-1} and use (18).

(20) Problem. (a) $N(ww') \leq N(w) + N(w')$ and $N(ww') \equiv N(w) + N(w') \bmod 2$. (b) $\det w = (-1)^{N(w)}$. $(w, w' \in W)$.

(21) Lemma Assume $w = w_1 w_2 \cdots w_n$ $(w_i = \sigma_{\alpha_i}, \alpha_i \in \Pi)$. If $N(w) < n$, then for some i, j $(1 \leq i \leq j \leq n-1)$, we have:

(a) $\alpha_i = w_{i+1} w_{i+2} \cdots w_j \alpha_{j+1}$.

(b) $w_{i+1} w_{i+2} \cdots w_{j+1} = w_i w_{i+1} \cdots w_j$.

(c) $w = w_1 w_2 \cdots \overset{\prime}{\cdots} \overset{\prime}{\cdots} \cdots w_n$, with w_i and w_{j+1} missing.

By (19b) and $N(w) < n$, $w_1 w_2 \cdots w_j \alpha_{j+1} < 0$ for some $j \leq n-1$. Since $\alpha_{j+1} > 0$, we have $w_i (w_{i+1} \cdots w_j \alpha_{j+1}) < 0$ and $w_{i+1} \cdots w_j \alpha_{j+1} > 0$ for some $i \leq j$, whence $w_{i+1} \cdots w_j \alpha_{j+1} = \alpha_i$ by (11), which is (a). Using (2) with $w = w_{i+1} \cdots w_j$ and $\alpha = \alpha_{j+1}$, we get (b), and then replacing the left side of (b) by the right side in the product for w and using $w_i^2 = 1$, we get (c).

Problem. Prove, conversely, that (a), (b) or (c) implies $N(w) < n$.

(22) Cor. If $w \in W$, then $N(w)$ is the number of terms in a minimal expression of w as a product of reflections corresponding to simple roots.

Let $w = w_1 w_2 \cdots w_n$ be a minimal expression. By (19) ((a) or (b)), $N(w) \leq n$, and by (2|c), $N(w) \geq n$.

* (23) Theorem. For $w \in W$, if $wP = P$ or $w\Pi = \Pi$ or $N(w) = 0$, then $w = 1$.

The three assumptions are clearly equivalent. Now $N(w) = 0$

implies that the minimal expression of w in (22) is empty, whence $w = 1$.

* (24) Theorem. W is simply transitive on the positive systems, and also on the simple systems.

By (12) and (23).

(25) Problem. (a) For $w \in W$, choose a minimal expression as in (22), $w = w_1 w_2 \cdots w_n$ ($w_i = \sigma_{\alpha_i}$, $\alpha_i \in \Pi$) (so that $n = N(w)$), and set $\rho_i = w_1 w_2 \cdots w_{i-1} \alpha_i$. Prove that $\rho_i (1 \leq i \leq n)$ is a complete list of all roots ρ such that $\rho > 0$ and $w^{-1} \rho < 0$.

(b) Since $-P$ is a positive system, there exists by (24) a unique $w_0 \in W$ such that $w_0 P = -P$. Write $w_0 = w_1 w_2 \cdots w_n$ ($n = N(w_0) = |P|$) as above. Prove that $\rho_i (1 \leq i \leq n)$ is a complete list of all positive roots. (Hint: (19), (21)).

III A fundamental domain for W.

(26) Definition. D will denote the region $\{\rho \in V | (\rho, \alpha) \geq 0, \alpha \in \Pi\}$. Thus D is a closed convex cone, and if Π spans V it is even a simplicial cone with vertex at 0.

(27) Lemma. Every $\rho \in V$ is conjugate to some $\rho' \in D$, in fact to some ρ' in D such that $\rho' - \rho$ is a nonnegative combination of the elements of Π.

Let S be this set of nonnegative combinations (in other words, the dual cone of D). We introduce a partial order in V by the definition $\gamma \succ \gamma'$ if and only if $\gamma - \gamma' \in S$. Among the conjugates ρ' of ρ under W such that $\rho' \succ \rho$, we

pick one which is maximal relative to this partial order. Then $\alpha \in \Pi \Rightarrow \sigma_\alpha \rho' \neq \rho' \Rightarrow (\rho', \alpha) \geq 0$ (by (1)), whence $\rho' \in D$ and (27) follows.

(28) Theorem. Assume $w \in W$, $\rho \in V$, ρ not orthogonal to any root, and $w\rho = \rho$. Then $w = 1$. (Restatement: $w \neq 1, w\rho = \rho \Rightarrow \rho$ is orthogonal to some root.)

By (27) we may assume $\rho \in D$. For $\alpha \in P$, $(w\alpha, \rho) = (\alpha, w^{-1}\rho) = (\alpha, \rho) > 0$. Hence $w\alpha \in P$, for all $\alpha \in P$, so that $wP = P$. Then $w = 1$ by (23).

(29) Cor. If $\rho \in V$ is not orthogonal to any root, its conjugates under W are all distinct. (And conversely, of course.)

(30) Cor. The only reflections in W are those in hyperplanes orthogonal to roots, i.e. those of the form $\sigma_\rho (\rho \in \Sigma)$.

Let u be any reflection in a hyperplane H not orthogonal to any root. The roots being finite in number, there exists $\rho \in H$, ρ not orthogonal to any root. Then $u \neq 1$, $u\rho = \rho \Rightarrow u \notin W$, by (28).

(31) Problem. Let S be a set of roots such that $\{\sigma_\alpha \mid \alpha \in S\}$ generates W. Prove that every root is conjugate, under W, to some $\alpha \in S$, and every reflection in W to some $\sigma_\alpha (\alpha \in S)$.

(32) Lemma. Assume $\rho, \sigma \in D$, $w \in W$, $w\rho = \sigma$. Then (a) w is a product of simple reflections (i.e relative to simple roots) fixing ρ. (b) $\rho = \sigma$.

For (a) we use induction on $N(w)$. If $N(w) = 0$, then

$w = 1$ by (23). Assume $N(w) > 0$. Pick $\alpha \in \Pi$ so that $w\alpha < 0$. Then $0 \geq (\sigma, w\alpha) = (\rho, \alpha) \geq 0$, whence $(\rho, \alpha) = 0$ and $\sigma_\alpha \rho = \rho$. Since $(w\sigma_\alpha)\rho = \sigma$, and $N(w\sigma_\alpha) = N(w) - 1$ by (19b'), the inductive assumption applied to $w\sigma_\alpha$ yields (a). Clearly (a) implies (b).

* (33) Theorem. D is a fundamental domain for W on V. In other words, each element of V is conjugate to exactly one element of D.

By (27) and (32b).

(34) Problem. If $\rho \in D$ and $w \in W$, show that $\rho - w\rho$ is a nonnegative combination of positive roots.

(35) Restatement. The reflecting hyperplanes (those orthogonal to roots) partition V into closed chambers, each of which is a fundamental domain for W. For a given chamber, the roots normal to the walls and inwardly directed form a simple system, and each simple system is obtained in this way. Prove these assertions and also that the angle between two walls of a chamber is always a submultiple of π.

* (36) Theorem. If S is any subset of V, the subgroup of W which fixes S pointwise is a reflection group. In other words, every $w \in W$ which fixes S pointwise is a product of reflections which also do.

Remark. (36) is an extension of (28). Verify this.

For the proof of (36) we may assume that S is indepedent, hence finite, and using induction, reduce to the case where S

has a single element, say ρ, which may be taken in D by (27). Then (32a) with $\sigma = \rho$ yields our result.

(37) Problem. For each subset Π' of Π let $W(\Pi')$ denote the group generated by $\{\sigma_\alpha \mid \alpha \in \Pi'\}$. Prove that $W(\Pi' \cap \Pi'') = W(\Pi') \cap W(\Pi'')$.

IV Generators and relations for W.

* (38) Theorem. For $\alpha,\beta \in \Pi$, let $n(\alpha,\beta)$ denote the order of $\sigma_\alpha\sigma_\beta$ in W. (So $n(\alpha,\alpha) = 1$, while $n(\alpha,\beta) > 1$ if $\alpha \neq \beta$.) Then the group W is defined by the generators $\{\sigma_\alpha \mid \alpha \in \Pi\}$ subject to the relations $\{(\sigma_\alpha\sigma_\beta)^{n(\alpha,\beta)} = 1 \mid \alpha,\beta \in \Pi\}$. In other words, the given elements generate W and the given relations imply all others in W.

By (16) the given elements generate W. Suppose the relation (*) $w_1w_2\cdots w_r = 1$ ($w_i = \sigma_{\alpha_i}$, $\alpha_i \in \Pi$) holds in W. We will show it is a formal consequence of the given relations, by induction on r. By (20b) or by (19) r is even, say $r = 2s$. If $s = 0$ there is nothing to show. Suppose $s > 0$. We start with the observation:

(0) (*) is equivalent to $w_{i+1}w_{i+2}\cdots w_rw_1w_2\cdots w_i = 1 (1 \leq i \leq r)$.

Case 1. Suppose $\alpha_1 \neq w_2w_3\cdots w_s\alpha_{s+1}$. We have $N(w_1w_2\cdots w_{s+1}) = N(w_{2s}w_{2s-1}\cdots w_{s+2}) < s+1$, by (19a). Hence by (21) we have (21a) and (21b) for some i,j such that $1 \leq i \leq j \leq s$. Since $i,j = 1,s$ is excluded in the present case,

both sides of (21b) have length $< s$. By our inductive assumption we may replace the left side of (21b) by the right side in (*). If w_i^2 is then replaced by 1, the inductive assumption can be applied to the resulting relation to complete the proof, in the present case.

Case 2. Suppose $\alpha_1 \neq \alpha_3$. (If $s = 1$, this case doesn't occur.) By the first case we may assume $\alpha_1 = w_2 w_3 \cdots w_s \alpha_{s+1}$ and then by (0) also $\alpha_2 = w_3 w_4 \cdots w_{s+1} \alpha_{s+2}$, whence

(**) $w_2 w_3 \cdots w_{s+1} = w_3 w_4 \cdots w_{s+2}$ by (2).

If (**) is substituted into (*), we can shorten (*), as above. Thus we are reduced to showing that (**) is a consequence of the original relations in (38), i.e. that

$w_3 \underbrace{w_2 w_3 \cdots w_{s+1}} w_{s+2} w_{s+1} \cdots w_4 = 1$ is. Since

$\alpha_3 \neq \alpha_1 = w_2 w_3 \cdots w_s \alpha_{s+1}$, we are back in Case 1. . .

Because of (0) above the only case that remains is:

Case 3. Suppose $\alpha_1 = \alpha_3 = \alpha_5 = \ldots$ and $\alpha_2 = \alpha_4 = \alpha_6 = \ldots$. Then (*) has the form $(\sigma_\alpha \sigma_\beta)^s = 1$ with $\alpha = \alpha_1$, $\beta = \alpha_2$. Here s must be a multiple of $n(\alpha,\beta)$, the order of $\sigma_\alpha \sigma_\beta$, so that (*) is a consequence of the relation $(\sigma_\alpha \sigma_\beta)^{n(\alpha,\beta)} = 1$.

(39) Examples. (a) $W = S_n$. The symmetric group of degree n acts on an n-dimensional space by permuting the coordinates relative to an orthomormal basis ε_i $(1 \leq i \leq n)$. The transposition (ij) corresponds to the reflection in the hyperplane orthogonal to $\varepsilon_i - \varepsilon_j$. We may take $\Sigma = \{\varepsilon_i - \varepsilon_j \mid i \neq j\}$, and relative to a lexicographic ordering, $\Pi = \{\varepsilon_i - \varepsilon_{i+1} \mid 1 \leq i \leq n-1\}$.

Thus S_n is generated by the transpositions $w_i = (i\ i+1)$ $(1 \leq i \leq n-1)$ subject to the relations $w_i^2 = 1$, $(w_i w_{i+1})^3 = 1$, and $(w_i w_j)^2 = 1$ if $|i-j| > 1$. (b) $\underline{W = Oct_n}$. The octahedral group includes sign changes as well as permutations of the coordinates, so has order $2^n n!$. Here we may take $\Sigma = \{ \pm \varepsilon_i \pm \varepsilon_j, \pm \varepsilon_i \mid i \neq j \}$ and $\Pi = \{\varepsilon_i - \varepsilon_{i+1}, \varepsilon_n \mid 1 \leq i \leq n-1\}$. So, comparing with (a), we have one more generator w_n and n more relations $w_n^2 = 1$, $(w_{n-1}w_n)^4 = 1$, $(w_i w_n)^2 = 1$ if $i \leq n-2$. We observe that S_n and Oct_n are the groups of symmetries of the regular simplex and the regular cube.

* (40) Problem. Prove that W is defined by the generators $\{\sigma_\alpha \mid \alpha \in \Sigma\}$ subject to the relations

(A) $\{\sigma_\alpha^2 = 1 \mid \alpha \in \Sigma\}$, (B) $\{\sigma_\alpha \sigma_\beta \sigma_\alpha^{-1} = \sigma_\gamma \mid \alpha, \beta \in \Sigma,\ \gamma = \sigma_\alpha \beta\}$.

(Hint. Using (15b) and (16) show that the group so defined is generated by $\{\sigma_\alpha \mid \alpha \in \Pi\}$ as a consequence of (B), and then using (21) show that any nontrivial relation $w_1 w_2 \cdots w_n = 1$ $(w_i = \sigma_{\alpha_i},\ \alpha_i \in \Pi)$ which holds in W can be shortened as a consequence of (A) and (B).)

(V) Appendix.

We consider some refinements in our results which occur in the crystalographic case, when $2(\alpha,\beta)/(\beta,\beta)$ is an integer for all $\alpha, \beta \in \Sigma$, which we henceforth assume. (This case occurs when we have root systems of Lie algebras.)

(41) Refinement of (8). In the present case, all coefficients

in (8b) are integers.

Prove this, by induction on ht ρ ($\rho \in \Sigma$) (see (13)).

(42) Cor. ht ρ is always an integer.

(43) Problem. Under the assumptions of (34), assume also that $(2\rho, \alpha)/(\alpha,\alpha)$ is an integer for every $\alpha \in \Pi$. Show that $\rho - w\rho$ is a nonnegative integral combination of the elements of Π.

(44) Problem. If α and β are roots, $\alpha \neq -\beta$ and $(\alpha,\beta) < 0$, prove that $\alpha + \beta$ is a root. (Hint: prove that $\alpha + \beta$ equals $\sigma_\alpha\beta$ or $\sigma_\beta\alpha$.)