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.

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.

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

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 roots. 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

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

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

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

$$= H_j - \langle \alpha_i,\alpha_j \rangle H_i$$

$$= H_{w_i \alpha_j}$$

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) $[H_i, X_\alpha] = \langle \alpha, \alpha_i \rangle X_\alpha$

(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 $[H_\beta, X_\alpha] = \alpha(H_\beta) X_\alpha = \langle \alpha, \beta \rangle X_\alpha$. (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 $\mathcal{H} = \{\text{diagonal matrices}\}$ is a Cartan subalgebra. For $i,j = 1, \ldots, \ell+1$, $i \neq j$, define $\alpha = \alpha(i,j)$ by $\alpha(i,j)\colon \operatorname{diag}(a_1, \ldots, a_{\ell+1}) \longrightarrow a_i - a_j$. 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 $X_\alpha = E_{i,j}$, $X_{-\alpha} = E_{j,i}$, $H_\alpha = E_{i,i} - E_{j,j}$ 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 $\theta : \mathcal{U} \to \mathcal{A}$ 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_α, $X_{-\alpha}$, H_α, 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 $\mathcal{L}_{\mathbb{Z}} \otimes \mathcal{L}_{\mathbb{Z}} \otimes \ldots$, any number of factors.

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

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

$X_\alpha \cdot X_{-\alpha} = H_\alpha$, $(X_\alpha^2/2)\cdot X_{-\alpha} = -X_\alpha$, $X_\alpha \cdot H_i = -<\alpha,\alpha_i> X_\alpha$, 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 $\{X_\alpha \mid \alpha \in S\}$ 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 $\beta, \gamma, \beta + \gamma, \ldots$ 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 $b, c, \ldots$ 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 $b + c + d + \ldots$, 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 weight vector 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 weight of the representation.

Lemma 11: 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 $X_\alpha v \neq 0$.

Proof: 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 $\{\prod_{\alpha<0} X_\alpha^{m(\alpha)} \prod_{i=1}^{\ell} H_i^{n_i} X_\alpha^{p(\alpha)}\}$ 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 $\beta(H_\alpha) = <\beta,\alpha> \in \mathbb{Z}$ 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.

Corollary 2: 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 $\langle x, iy^* \rangle = - \langle ix, y^* \rangle$ where $x \in V$, $y \in V^*$, $i \in \mathcal{L}$ and where $\langle x, y^* \rangle$ denotes the value of the linear function y^* at x. If M^* is the dual lattice in V^* of M; i.e., $\langle M, M^* \rangle \subset \mathbb{Z}$; then clearly $i \in \mathcal{L}$ preserves M^* if and only if i 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 $i: A \to [i, A]$ ($i \in \mathcal{L}$, $A \in \mathrm{End}(V)$) 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^m 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 $\pm\mu, 0$ 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

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

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 $C_{11} = N_{\alpha,\beta}$. $[X_\alpha, X_\beta] = N_{\alpha,\beta} X_{\alpha+\beta}$

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

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

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

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

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 $c_{11} = N_{\alpha,\beta}$.

Carter I p 16 Π syst fondam di radici $\Rightarrow \alpha = \sum \lambda_i \alpha_i$
$ht(\alpha) = \sum \lambda_i$

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).

segue ad es dalla Lemma 36.3 p 50 Carter Nella kpo Ax se $i\alpha + j\beta$ è radice, con $ij \neq 0$, allora $i=j=1$, I casi Br e G_2 non capitano perché in loro 2α lunghezza

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) $P_r = \{\alpha \mid ht\,\alpha \geq r,\ r \geq 1\}$.

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 $\mathcal{X}_\alpha$ ($\alpha \in S$ 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.

se

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 $\mathcal{X}_S = \mathcal{X}_{\alpha_1} \mathcal{X}_{S-\{\alpha_1\}}$. Using induction on the size of S, we see $\mathcal{X}_S = \prod \mathcal{X}_\alpha$.

Now suppose $y \in \mathcal{X}_S$, $y = \prod x_\alpha(t_\alpha)$. Since $X^k_{\alpha_1} \neq 0$, 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 $x_{\alpha_1}(t_{\alpha_1})^{-1} y \in \mathcal{X}_{S-\{\alpha_1\}}$, we may complete the proof of this case by induction.

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

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

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

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

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

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

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

Corollary 2: Let P be the set of all positive roots and let $U = \mathcal{X}_P$. Then $U = \prod \mathcal{X}_\alpha$ 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, $U^- = \mathcal{X}_{-P}$ 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 $\mathcal{X}_\alpha$ 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 $U = \mathcal{X}_Q \mathcal{X}_R$ and $\mathcal{X}_Q \cap \mathcal{X}_R = 1$. (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 $H \in \mathfrak{H}$. By linearity it suffices to prove this for $-H_\alpha$, 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 $\chi_\alpha(t)$ and $w_\alpha(t)$, is an element of the three dimensional algebra $\langle X_\alpha, Y_\alpha, H_\alpha \rangle$ whose value depends on calculations within this algebra, not on the representation chosen. Taking the usual representation in s_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 $h_\alpha(t)$ 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 $H \in \mathfrak{H}$, $Hv'' = Hw_\alpha(t)v = w_\alpha(t)w_\alpha(t)^{-1}Hw_\alpha(t)v = w_\alpha(t)(w_\alpha H)v = \mu(w_\alpha H)v'' = (w_\alpha \mu)(H)v''$. Hence v'' corresponds to the weight $w_\alpha\mu = \mu - \langle \mu, \alpha \rangle \alpha$. Thus the only nonzero term in the sum occurs for $i = -\langle \mu, \alpha \rangle$.

IMPORTANTE:
per il Lemma 24
si ha che:

By (b) applied to the adjoint representation a usa il Lemma 14
$w_\alpha(t)\, X_\beta w_\alpha(t)^{-1} = ct^{-\langle\beta,\alpha\rangle} X_{w_\alpha\beta}$ 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) $\omega_c x_\beta(t)\omega_\alpha^{-1} = x_{w_\alpha\beta}(ct)$ 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 $v \in V^k_\mu$.

$\omega_\alpha h_\beta(t)\omega_\alpha^{-1} v = \omega_\alpha t^{\langle w_\alpha\mu,\beta\rangle} \omega_\alpha^{-1} v$ (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) $$x_\alpha(t) x_\alpha(u) = x_\alpha(t + u) .$$

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

with the c_{ij} as in Lemma 15.

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

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

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

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 $\mathcal{X}_\alpha$ $(\alpha > 0)$, 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 $\mathcal{X}_\beta$ (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)

$\omega_\alpha(-1) = x_\alpha(-1)\, x_{-\alpha}(1)\, x_\alpha(-1)$

$\omega_\alpha(1) = x_\alpha(1)\, x_{-\alpha}(-1)\, x_\alpha(1)$

(R2) $x_\alpha(-1)\, x_\alpha(1) = x_\alpha(-1+1) = 1$

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 $\omega_\alpha \omega_\beta \omega_\alpha^{-1} = \omega_\alpha \chi_\beta(1)\chi_{-\beta}(-1)\chi_\beta(1)\,\omega_\alpha^{-1}$ (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 χ_α by $w_{\alpha_1}(1)w_{\alpha_2}(1) \ldots$ we get $\chi_{w\alpha}$ (R4) and conjugating by h we get χ_α (R8). Hence $\chi_{w\alpha} = \chi_\alpha$ 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 $\chi_\alpha \neq \chi_\beta$.

Proof: We know that χ_α 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) $BwB \cdot Bw_\alpha B = Bw\, \mathfrak{X}_\alpha\, \mathfrak{X}_{P-\{\alpha\}} H w_\alpha B =$

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

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

(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) $BwB \cdot Bw_\alpha B = Bw' w_\alpha B \cdot Bw_\alpha B = Bw' B \cdot Bw_\alpha B \cdot Bw_\alpha B \subseteq Bw' B\ (B \cup Bw_\alpha B)$ (by Lemma 24) = $Bw' B \cup Bw' w_\alpha B = BwB \cup Bww_\alpha B$.

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

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 $\mathfrak{L} = s\ell_n$ 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 standard flag. 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 simplex 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 incident 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 $A = \begin{bmatrix} & & & 1 \\ & & \iddots & \\ & 1 & & \\ \hline & -1 & & \\ & \iddots & & \\ -1 & & & \end{bmatrix}$ in the first case

and $A = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$ 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 $G \subseteq Sp_m$, in the second and third cases $G \subseteq SO_m$ (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 $x'x'_\beta(u)x'^{-1} = x'_\beta(\prod_\alpha t_\alpha^{\langle\beta,\alpha\rangle} u)$ by (R8). Applying φ we see that $\prod_\alpha t_\alpha^{\langle\beta,\alpha\rangle} = 1$. 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_0 be the element of W making all positive roots negative. Then $x = \omega_{w_0} x \omega_{w_0}^{-1}$ is both superdiagonal and subdiagonal. Since h is diagonal, u is diagonal, and also unipotent.

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

* Lemma 20 (b) $\omega_\alpha x_\beta(t)\omega_\alpha^{-1} = x_{w_\alpha\beta}(\pm t)$

(a) $\omega_\alpha h_\beta(t)\omega_\alpha^{-1} = h_{w_\alpha\beta}(t)$

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 rôle 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, $(<\alpha_i, \alpha_j>)$ $i, j = 1, 2, \ldots,$ 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 $\prod_{i=1}^{\ell} t_i^{<\beta,\alpha_i>} =$ 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 $L_V = L_0$, 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 φ: $G' \to G$ 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 $\omega_i : \mathrm{diag}(a_1, \ldots, a_n) \to a_i$. 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 $\varphi_\alpha \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} = x_\alpha(t)$, $\varphi_\alpha \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$

$= x_{-\alpha}(t)$, $\omega_\alpha \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \omega_\alpha$, and $\omega_\alpha \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} = h_\alpha(t)$. Moreover, $\ker \omega_\alpha = \{1\}$ 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 $\ker \omega \subseteq \{\pm 1\}$ by Corollary 5.

Exercise: If G is universal, each ω_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 the

Proof: Part (a) follows from $BwB \cdot Bw_\alpha B \subseteq B\, ww_\alpha B \cup BwB$. lemma 25

(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_α, w_β, $\ldots \in A$. Hence, α, β, $\ldots \in \pi$ $w \in W_\pi$, 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 $n \times n$ 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 $w_\beta\, bw_\alpha w_\beta^{-1} \in N \cap (Bw_\alpha w_\beta B \cup Bw_\beta w_\alpha w_\beta$ 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 $(x_\beta(t), x_\gamma(u)) = x_{\beta+\gamma}(\pm tu)\, x_{\beta+2\gamma}(\pm tu^2)$

↓

contu

quindi $\in G'$

Proof: By Lemma 14, we have

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

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

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 $G = G_1 \cdot G_2 \cdot \cdots \cdot G_r$ 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.