§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 $V = \{v = (v_1,\ldots,v_n) \in k^n \mid p(v_1,\ldots,v_n) = 0$ 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 $I_k(V) = \{p \in k[x_1,\ldots,x_n] \mid p(v_1,\ldots,v_n) = 0$ 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 <u>homomorphism</u> 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 <u>isomorphism</u> 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 <u>radical of G</u> (rad G) is the maximal connected solvable normal subgroup. G is <u>semisimple</u> if (1) rad $G = \{1\}$ and (2) G is connected.

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

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 $G_a \longrightarrow \mathfrak{X}_\alpha$ 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 $R = \text{rad}\, G$. 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:

<u>Lemma 34</u>: 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 $x_\alpha \colon G_a \longrightarrow \mathfrak{X}_\alpha$ is an isomorphism over k_o.

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

<u>Proof</u>: 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 $x_\alpha(t) = 1 + tX_\alpha + t^2 X_\alpha^2/2 + \cdots$ 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 $\mathfrak{X}_\alpha$ 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 $\mathfrak{X}_\alpha$'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

$G, \mathfrak{X}_\alpha, \ldots$ 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 $\mathcal{H}_{\mathbb{Z}} = \mathcal{H} \cap \mathcal{L}_{\mathbb{Z}}$
$= \{H \in \mathcal{H} \mid \mu(H) \in \mathbb{Z} \text{ for all } \mu \in L\}$.

<u>Lemma 35</u>: 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 φ: $G_m^\ell \longrightarrow H$ 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.

<u>Proof</u>: 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.

<u>Theorem 7</u>: 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:

* si fanno le operazioni elementari x la matrice ad elementi in un PID e poi si ricorda che k^* è divisibile

(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 $\varphi((t_\alpha)_{\alpha<0}, (t_i)_{1\leq i\leq \ell}, (t_\alpha)_{\alpha>0}) = \prod_{\alpha<0} x_\alpha(t_\alpha) \prod h_i'(t_i) \prod_{\alpha>0} x_\alpha(t_\alpha)$ is an isomorphism of varieties over k_o.

Proof: (a) We consider the natural action of G on $\bigwedge^n \mathcal{L}$ 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 $Y_1 = \bigwedge X_\alpha (\alpha > 0)$. 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).

vedere dim alternativa di Tabu 20

(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

(*) *vera perché l'azione è quella aggiunta e $[X_\alpha, X_\beta] = n_{\alpha,\beta} X_{\alpha+\beta}$ se $\beta \neq -\alpha$*

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 $i \le k$, $j \le \ell$ and $ij \ne k\ell$. 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.

<u>Example</u>: 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.

<u>Remark</u> : 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.

<u>Corollary 1</u>: 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 $\varphi: G \longrightarrow G'$ taking $x_\alpha(t) \longrightarrow x'_\alpha(t)$ for all α and t is a homomorphism of algebraic groups over k_o.

<u>Proof</u>: 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 $\varphi_\alpha : SL_2 \longrightarrow \langle \mathfrak{X}_\alpha, \mathfrak{X}_{-\alpha} \rangle$ (of Corollary 6 to Theorem 4') is a homomorphism of algebraic groups over k_0.

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 $t_\alpha, t_i \in K$. Applying φ^{-1} of Theorem 7, we get $(t_\alpha)_{\alpha > 0} \times (t_i) \times (t_\alpha)_{\alpha < 0}$. Since uhu^- is defined over k and φ^{-1} is defined over k_0, all $t_\alpha, t_i \in k$. Hence $uhu^- \in G_k$.

Il fatto che V sia universale si usa perché gli h' e gli h in questo caso coincidono (lemma 35) cioè gli H sono una base di 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 $\{x_\alpha(t) \mid \alpha \in \Sigma,\ t \in k\}$ 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 <u>Colloque sur la théorie des groupes algébriques</u>, Bruxelles, 1962.

<u>Theorem 8</u>: Assume that Σ is orthogonally indecomposable. Then:

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

(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 $\alpha \in \Sigma$, $t \in k$.

<u>Lemma 36</u>: 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 $\mathfrak{X}'_S$ be the subgroup of G' generated by $\{x'_\alpha(t) \mid \alpha \in S, t \in k\}$. Then π maps $\mathfrak{X}'_S$ isomorphically onto the corresponding group in G.

<u>Proof</u>: Using (A) and (B) we can reduce every element of $\mathfrak{X}'_S$ 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 $\mathfrak{X}_S$ can be written uniquely in this form.

<u>Lemma 37</u>: 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) $w'_\alpha(t) w'_\beta(u) w'_\alpha(-t) = w'_\gamma(ct^{-\langle\beta,\alpha\rangle}u)$.

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

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

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

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) $\mathfrak{X}'_S$ is normalized by $\mathfrak{X}'_\alpha$ and $\mathfrak{X}'_{-\alpha}$ and hence by $w'_\alpha(t)$. Thus $w'_\alpha(t)x'_\beta(u)w'_\alpha(-t) \in \mathfrak{X}'_S$. 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 $T = \{mw_\alpha\delta + nw_\alpha\gamma | m,n$ 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 $x'_{\delta+j\gamma}(c_{1j}t\, u^j) \in \mathfrak{X}'_T$. Hence $w'_\alpha(t)x'_{\delta+j\gamma}(c_{1j}t\, u^j)w'_\alpha(-t) \in \mathfrak{X}'_T$, 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.

<u>Lemma 38</u>: 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) $H' = \prod_{i=1}^{\ell} \mathfrak{h}'_i$.

<u>Proof</u>: (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 $w = w_\alpha \cdots$ 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.

<u>Proof of Theorem 8 (b)</u>: 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 $x = 1$.

<u>Remarks</u>: (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).

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

<u>Proof</u>: If $|k| = q$ there are $(q+1)/2$ squares. Since $((q+1)/2)\nmid q$ 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 $t = a/c$, $u = b/c$.

<u>Theorem 9</u>: 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) .

<u>Proof</u>: 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 $f(t,u) = f(t,s^2 u_1) = f(t,u_1) = f(r^2 t_1,u_1)$ $= f(t_1,u_1) = 1$ by Lemma 39(a and d).

<u>Example</u>: 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 $\ker \pi \subseteq$ center of G'.

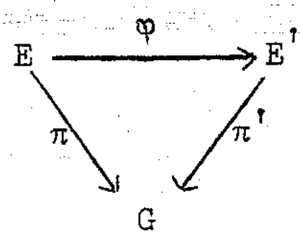
Examples:

(a) π, G', G as in §6.

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

(c) $\pi : G' \to G$ 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 $G \to N$ given by $g \to gng^{-1}$, $g \in G$, has a discrete and connected image, $gng^{-1} = n$ for all $g \in G$.

<u>Definition</u>: A central extension (π,E) of a group G is <u>universal</u> 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.

<u>Proof</u>: 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.

<u>Proof</u>: 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 $\pi : e(x) \rightarrow x$, 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 $\varphi : F \rightarrow E'$ 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, $\Psi : x \rightarrow \varphi(x)\varphi'(x)^{-1}$ is a homomorphism of E into an Abelian group. Since $E = \mathcal{D}E$, Ψ is trivial and $\varphi = \varphi'$.

<u>Remark</u>: 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 $E = \mathcal{D}E$.

<u>Proof</u>: 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) <u>Exercise</u>: 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.

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

(vii) <u>Corollary</u>: 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 $\rho = \text{id}$. 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.

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

<u>Remark</u>: 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 $M(G)$.

<u>Theorem 10</u>: 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.

<u>Remark</u>: 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.

<u>Proof</u>: 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 $v = (2w/(1+w^2))^2$. Then $1 - v = ((1-w^2)/(1+w^2))^2$, 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 $x = \varphi x_\alpha(tc^{-1})\varphi x_\alpha(uc^{-1})(\varphi x_\alpha((t+u)c^{-1}))^{-1}$ 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 $x\varphi x_\alpha(t)\varphi x_\alpha(u)(\varphi x_\alpha(t+u))^{-1}$.

(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.

<u>Exercise</u>: 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.

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

<u>Corollary 2</u>:

(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 G.

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 $G = \mathcal{D}G$, 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 $G = \mathcal{D}G$ (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 $\psi' : E' \to G$ by $\psi'(ec') = \psi(e)$, $e \in E$, $c' \in C'$.

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.

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

<u>Partial Proof</u>:

(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 $|t_i + t_j| \leq \epsilon$.

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) $\varphi x_\alpha(t) \varphi x_\alpha(u) = \varphi x_\alpha(t+u) \quad \alpha \in \Sigma$.

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 $\mathfrak{X}_\alpha$ 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 $h_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t) \cdot w_\alpha(-1) = x_\alpha(t-1)x_{-\alpha}(1-t^{-1})^{x_\alpha(-1)} x_\alpha(t-1)^{w_\alpha(-1)}$ 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 ψ 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.

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

<u>Remarks</u>:

(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 $\pi : G' \to G$ 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 $(1 + t E_{ik}, 1 + E_{kj}) = 1 + t E_{ij}$ 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 $R \to R'$ is onto, then so is the associated map $K_2(R) \to K_2(R')$.

<u>Remark</u>: 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.

<u>Theorem 14</u>: 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 $\pi : U(R) \to E(R)$ is the homomorphism given by $x_{ij}(t) \to 1 + tE_{ij}$, then $(\pi, U(R))$ is a u.c.e. for $E(R)$.

<u>Proof</u>: (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 $U(R) = \mathcal{D}U(R)$. 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 $i,j\leq n$.

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

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

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

<u>Remarks</u>: (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 : $SL_2(4)$, $SL_2(9)$, $SL_3(2)$, $SL_3(4)$, $SL_4(2)$.

* <u>Exercise</u>: 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

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

(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 $n \geq 5$.

<u>Exercise</u>: 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 $BwB = BY_\alpha Y_\beta \ldots Y_\delta$ 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

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