$(n+1)\times(n+1)$ 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 $G_\alpha = \langle X_\alpha , X_{-\alpha} \rangle$, 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 $w = w_\alpha w_\beta \dots w_\delta$ as a product of reflections relative to simple roots $\alpha, \beta \dots$. Then $BwB = BY_\alpha Y_\beta \dots Y_\delta$ 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

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

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

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

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

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

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

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

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

Thus $SL_2(k) = B_2(k)SL_2(\mathfrak{o})$, and (c) follows.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Applying Theorem 4', Cor. 5 to the Chevalley groups (both equal to G) constructed from the representations ρ and $\rho_0 \tau_1$ of $\mathcal{L}$, we get an automorphism of G which aside from complex conjugation satisfies the equations of (a), hence composed with conjugation satisfies these equations. From Theorem 7 adapted to the present situation (see the remark at the end of § 5) it follows that σ is analytic, whence (a). We observe that if G is defined by the adjoint representation of $\mathcal{L}$, then σ is effected by conjugation by the semiautomorphism σ_0 of Lemma 44.

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

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

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

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

= maximal torus in K.

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) We have isomorphisms and central extensions,

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

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

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

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

Corollary 2: The group K is connected.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$K_\alpha, K_\beta = \{$rotations around the z-axis, x-axis$\}$,

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

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

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

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

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

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

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

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

This easily follows from the uniqueness in Theorem 4'.

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

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

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

(a) $A \subset P$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Corollary 2: K is generated by the groups K_α.

Proof: By Lemma 49 and Cor. 1.

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

Proof: Since the corresponding result holds for $SL_2(\Theta)$, this follows from Lemma 49(d) and Cor. 2.

Example: Assume $\Theta = \mathbb{Z}$, $k = \mathbb{Q}$. We get that $G_{\mathbb{Z}}$ is generated by $\{x_\alpha(1)\}$. The normal form in Cor. 1 can be used to extend Nielsen's theorem (see (1) on p. 96) from $SL_3(\mathbb{Z})$ to $G_{\mathbb{Z}}$ whenever Σ has rank ≥ 2, is indecomposable, and has all roots of equal length (W. Wardlaw, Thesis, U. C. L. A. 1966). It would be nice if the form could be used to handle $SL_3(\mathbb{Z})$ itself since Nielsen's proof is quite involved. The case of unequal root lengths is at present in poor shape. In analogy with the fact that in the earlier development K is a simple compact group if Σ is indecomposable, we have here: Every normal subgroup of $G_{\mathbb{Z}}$ is

finite or of finite index if Σ is indecomposable and has rank ≥ 2. The proof isn't easy.

Exercise: Prove that $G_{\mathbb{Z}}/\mathcal{D}G_{\mathbb{Z}}$ is finite, and is trivial if Σ is indecomposable and not of type A_1, B_2 or G_2.

Returning to the general set up, if p is a prime in o, we write $|\ |_p$ for the p-adic norm defined by $|0|_p = 0$ and $|x|_p = 2^{-r}$ if $x = p^r a/b$ with a and b prime to p.

Theorem 19: (Approximation theorem): Let o and k be as above, a principal ideal domain and its quotient field, S a finite set of inequivalent primes in o, and for each $p \in S$, $t_p \in k$. Then for any $\varepsilon > 0$ there exists $t \in k$ such that $|t - t_p|_p < \varepsilon$ for all $p \in S$ and $|t|_q \leq 1$ for all primes $q \notin S$.

Proof: We may assume every $t_p \in o$. To see this write $t_p = p^r a/b$ as above. By choosing $s \geq -r$ and c and d so that $a = cp^s + db$ and replacing a/b by d, we may assume $b = 1$. If we then multiply by a sufficiently high power of the product of the elements of S, we achieve $r \geq 0$, for all $p \in S$. If we now choose n so that $2^{-n} < \varepsilon$, $e = \prod_{p \in S} p^n$, $e_p = e/p^n$, then f_p, g_p so that $f_p p^n + g_p e_p = 1$, and finally $t = \Sigma\, g_p e_p t_p$, we achieve the requirements of the theorem.

Now given a matrix $x = (a_{ij})$ over k, we define $|x|_p = \max|a_{ij}|_p$. The following properties are easily verified.

(1) $|x + y|_p \leq \max|x|_p, |y|_p$.

(2) $|xy|_p \leq |x|_p|y|_p$.

(3) If $|x_i|_p = |y_i|_p$ for $i = 1,2,\ldots,n$, then

$$|\prod x_i - \prod y_i|_p \leq \max_i |y_1|_p \ldots \widehat{|y_i|_p} \ldots |y_n|_p |x_i - y_i|_p .$$

Theorem 20: (Approximation theorem for split groups): Let e,k,S,ε be as in Theorem 19, G a Chevalley group over k, and $x_p \in G$ for each $p \in S$. Then there exists $x \in G$ so that $|x - x_p|_p < \varepsilon$ for all $p \in S$ and $|x|_q \leq 1$ for all $q \notin S$.

Proof: Assume first that all x_p are contained in some $\mathcal{X}_\alpha$, $x_p = x_\alpha(t_p)$ with $t_p \in k$. If $x = x_\alpha(t)$, $t \in k$, then $|x|_q \leq \max |t|_q, 1$ because $x_\alpha(t)$ is an integral polynomial in t and similarly $|xx_p^{-1} - 1|_p \leq |t - t_p|_p$, so that $|x - x_p|_p \leq |x_p|_p|t - t_p|_p$ by (1) and (2) above. Thus our result follows from Theorem 19 in this case. In the general case we choose a sequence of roots $\alpha_1,\alpha_2,\ldots$ so that $x_p = x_{p1}x_{p2}\cdots$ with $x_{pi} \in \mathcal{X}_{\alpha_i}$ for all $p \in S$. By the first case there exists $x_i \in \mathcal{X}_{\alpha_i}$ so that

$$|x_i - x_{pi}|_p < |x_{pi}|_p \quad \text{and} \quad \varepsilon|x_{pi}|_p/|x_{p1}|_p|x_{p2}|_p\cdots$$

if $p \in S$ and $|x_i|_q \leq 1$ if $q \notin S$. We set $x = x_1x_2\cdots$. Then the conclusion of the theorem holds by (3) above.

With Theorem 20 available we can now prove:

Theorem 21: (Elementary divisor theorem): Assume e,k,G, $K = G_e$ are as before. Let A^+ be the subset of H defined by: $\hat{\alpha}(h) \in e$ for all positive roots $\hat{\alpha}$.

(a) $G = KA^+K$ (Cartan decomposition).

(b) The A^+ component in (a) is uniquely determined mod $H \cap K$, i.e. mod units (see Lemma 49); in other words, the set of numbers $\{\hat{\mu}(h) | \hat{\mu}$ weight of the representation defining $G\}$ is.

Example: The classical case occurs when $G = SL_n(k)$, $K = SL_n(\mathfrak{o})$, and A^+ consists of the diagonal elements $\mathrm{diag}(a_1, a_2, \ldots, a_n)$ such that a_i is a multiple of a_{i+1} for $i = 1, 2, \ldots$.

Proof of theorem: First we reduce the theorem to the local case, in which $\mathfrak{o}$ has a single prime, modulo units. Assume the result ture in this case. Assume $x \in G$. Let S be the finite set of primes at which x fails to be integral. For $p \in S$, we write $\mathfrak{o}_p$ for the local ring at p in $\mathfrak{o}$, and define K_p and A_p^+ in terms of $\mathfrak{o}_p$ as K and A^+ are defined for $\mathfrak{o}$. By the local case of the theorem we may write $x = c_p a_p c_p'$ with $c_p, c_p' \in K_p$ and $a \in A_p^+$, for all $p \in S$. Since we may choose a_p so that $\hat{\mu}(a_p)$ is always a power of p and then replace all a_p by their product, adjusting the c's accordingly, we may assume that a_p is independent of p, is in A^+, and is integral outside of S. We have $c_p a c_p' x^{-1} = 1$ with $a = a_p$ for $p \in S$. By Theorem 20 there exist $c, c' \in G$ so that $|c - c_p|_p < |c_p|_p$ for $p \in S$ and $|c|_q \leq 1$ for $q \notin S$, the same equations hold for c' and c_p', and $|cac'x^{-1} - 1|_p \leq 1$ for all $p \in S$. By properties (1), (2), (3) of $|\ |_p$, it is now easily verified that $|c|_p \leq 1$, $|c_p'| \leq 1$ and $|cac'x^{-1} - 1|_p \leq 1$,

whether p is in S or not. Thus $c \in K$, $c' \in K$ and $cac'x^{-1} \in K$, so that $x \in KA^+K$ as required. The uniqueness in Theorem 21 clearly also follows from that in the local case.

We now consider the local case, p being the unique prime in $\mathfrak{o}$. The proof to follow is quite close to that of Theorem 17. Let A be the subgroup of all $h \in H$ such that all $\hat{\mu}(h)$ are powers of p, and redefine A^+, casting out units, so that in addition all $\hat{\alpha}(h)$ $(\hat{\alpha} > 0)$ are nonnegative powers of p.

Lemma 50: For each $a \in A$ there exists a unique $H \in \mathcal{H}_{\mathbb{Z}}$, the $\mathbb{Z}$-module generated by the elements H_α of the Lie algebra $\mathcal{L}$, such that $\hat{\mu}(a) = p^{\mu(H)}$ for all weights μ.

Proof: Write $a = \prod h_\alpha(c_\alpha p^{n_\alpha})$ with $c_\alpha \in \mathfrak{o}^*$, $n_\alpha \in \mathbb{Z}$. Then $\hat{\mu}(a) = \prod (c_\alpha p^{n_\alpha})^{\mu(H_\alpha)}$. Since $\hat{\mu}(a)$ is a power of p the c_α, being units, may be omitted, so that $\hat{\mu}(a) = p^{\mu(H)}$ with $H = \Sigma\, n_\alpha H_\alpha$. If H' is a second possibility for H, then $\mu(H') = \mu(H)$ for all μ, so that $H' = H$.

If a and H are as above, we write $H = \log_p a$, $a = p^H$, and introduce a norm: $|a| = |H|$, the Killing norm. This norm is invariant under the Weyl group. Now assume $x \in G$. We want to show $x \in KA^+K$. From the definitions if $T = H \cap K$ then $H = AT$. Thus by Theorem 18 there exists $y = ua \in KxK$ with $u \in U$, $a \in A$. There is only a finite number of possibilities for a: if $a = p^H$, then $\{\mu(H) \mid \mu$ a weight in the given representation$\}$ is bounded below (by $-n$ if n is chosen so that the matrix of $p^n x$ is integral, because $\{p^{\mu(H)}\}$ are the

diagonal entries of y), and also above since the sum of the weights is 0, so that H is confined to a bounded region of the lattice $\mathcal{H}_{\mathbb{Z}}$. We choose $y = ua$ above so as to maximize $|a|$. If $u = \prod u_\alpha$ ($u_\alpha \in \mathcal{H}_\alpha$), we set $\operatorname{supp} u = \{\alpha \mid u_\alpha \neq 1\}$ and then minimize $\operatorname{supp} u$ subject to a lexicographic ordering of the supports based on an ordering of the roots consistent with addition (thus $\operatorname{supp} u < \operatorname{supp} u'$ means that the first α in one but not in the other lies in the second). We claim $u = 1$. Suppose not. We claim (*) $u_\alpha \notin K$ and $a^{-1}u_\alpha a \notin K$ for $\alpha \in \operatorname{supp} u$. If u_α were not in K, we could move it to the extreme left in the expression for y and then remove it. The new terms introduced by this shift would, by the relations (B), correspond to roots higher than α, so that $\operatorname{supp} u$ would be diminished, a contradiction. Similarly a shift to the right yields the second part of (*). Now as in the proof of Theorem 17 we may conjugate y by a product of $w_\beta(1)$'s (all in K) to get $u_\alpha \neq 1$ for some simple α, as well as (*). We write $a = p^H$, choose c so that $H' = H - cH_\alpha$ is orthogonal to H_α, set $a_\alpha = p^{cH_\alpha}$, $a' = p^{H'}$, $a = a_\alpha a'$. We only know that $2c = \langle H, H_\alpha \rangle \in \mathbb{Z}$, so that this may involve an adjunction of $p^{1/2}$ which must eventually be removed. If we bear this in mind, then after reducing (*) to the rank 1 case, exactly as in the proof of Theorem 17, what remains to be proved is this:

Lemma 51: Assume $y = ua = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p^c & \\ & p^{-c} \end{bmatrix}$ with $2c \in \mathbb{Z}$, $t \in k$,

$t \notin \mathfrak{o}$ and $tp^{-2c} \notin \mathfrak{o}$. Then c can be increased by an integer by multiplications by elements of K.

Proof: Let $t = \varepsilon p^{-n}$ with $\varepsilon \in \mathfrak{o}^*$. Then $n \in \mathbb{Z}$, $n > 0$ and $n + 2c > 0$ by the assumptions, so that $c + n > c$, $c + n > -c$ and $|c + n| > |c|$. If we multiply y on the left by $\begin{bmatrix} p^n & \varepsilon \\ -\varepsilon^{-1} & 0 \end{bmatrix}$, on the right by $\begin{bmatrix} 1 & 0 \\ -\varepsilon^{-1} p^{n+2c} & 1 \end{bmatrix}$, both in K, we get $\begin{bmatrix} p^{c+n} & 0 \\ 0 & p^{-c-n} \end{bmatrix}$, which proves the lemma, hence that $u = 1$. Thus $y = a \in A$, so that $x \in KAK$. Thus $G = KAK$. Finally every element of A is conjugate to an element of A^+ under the Weyl group, which is fully represented in K (every $w_\alpha(1) \in K$). Thus $G = KA^+K$. It remains to prove the uniqueness of the A^+ component. If G' is the universal group of the same type as G and π is the natural homomorphism, it follows from Lemma 49(d) and Theorem 18, Cor. 2 that $\pi K' = K$ and from Lemma 49 that π maps A'^+ isomorphically onto A^+. Thus we may assume that G is universal. Then G is a direct product of its indecomposable factors so that we may also assume that G is indecomposable. Let λ_i be the i^{th} fundamental weight, V_i an $\mathcal{L}$-module with λ_i as highest weight, G_i the corresponding Chevalley group, $\pi_i : G \longrightarrow G_i$ the corresponding homomorphism, and μ_i the corresponding lowest weight. Assume now that $x = cac' \in G$, with $c, c' \in K$ and $a \in A^+$. Set $\hat{\mu}_i(a) = p^{-n_i}$. Each weight on V_i is μ_i increased by a sum of positive roots, Thus n_i is the smallest integer such that $p^{n_i}\pi_i a$ is integral, i.e. such

that $p^{n_i}\pi_i x$ is since $\pi_i c$ and $\pi_i c'$ are integral, thus is uniquely determined by x. Since $\{\mu_i\}$ is a basis of the lattice of weights $(\mu_i = w_o\lambda_i)$, this yields the uniqueness in the local case and completes the proof of Theorem 21.

Corollary 1: If o is not a field, the group K is maximal in its commensurability class.

Proof: Assume K' is a subgroup of G containing K properly. By the theorem there exists $a \in A^+ \cap K'$, $a \notin K$. Some entry of the diagonal matrix a is nonintegral so that by unique factorization $|K'/K|$ is infinite.

Remark: The case $o = \mathbb{Z}$ is of some importance here.

Corollary 2: If $o = \mathbb{Z}_p$ and $k = \mathbb{Q}_p$ (p-adic integers and numbers) and the p-adic topology is used, then K is a maximal compact subgroup of G.

Proof: We will use the fact that $\mathbb{Z}_p$ is compact. (The proof is a good exercise.) We may assume that G is universal. Let $\bar{k}$ be the algebraic closure of k and $\bar{G}$ the corresponding Chevalley group. Then $G = \bar{G} \cap SL(V,k)$ (Theorem 7, Cor. 3), so that $K = \bar{G} \cap SL(V,o)$. Since o is compact, so is $End(V,o)$, hence also is K, the set of solutions of a system of polynomial equations since $\bar{G}$ is an algebraic group, by Theorem 6. If K' is a subgroup of G containing K properly, there exists $a \in A^+ \cap K'$, $a \notin K$, by the theorem. Then $\{|a^n|_p \mid n \in \mathbb{Z}\}$ is not bounded so that K' is not compact.

Remark: We observe that in this case the decompositions $G = BK$ and $G = KA^+K$ are relative to a maximal compact subgroup just as in Theorems 16 and 17. Also in this case the closure formula of Theorem 16, Cor. 7 holds.

Exercise (optional): Assume that G is a Chevalley group over $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$ and that K is the corresponding maximal compact subgroup discussed above. Prove the commutativity under convolution of the algebra of functions on G which are complex-valued, continuous, with compact support, and invariant under left and right multiplications by elements of K. (Such functions are sometimes called zonal functions and are of importance in the harmonic analysis of G.) Hint: prove that there exists an antiautomorphism φ of G such that $\varphi x_\alpha(t) = x_{-\alpha}(t)$ for all α and t, that φ preserves every double coset relative to K, and that φ preserves Haar measure. A much harder exercise is to determine the exact structure of the algebra.

Next we consider a double coset decomposition of $K = G_\Theta$ itself in the local case. We will use the following result, the first step in the proof of Theorem 7.

Lemma 52: Let $\mathcal{L}$ be the Lie algebra of G (the original Lie algebra of S_1 with its coefficients transferred to k), N the number of positive roots, and $\{Y_1, Y_2, \ldots, Y_r\}$ a basis of $\wedge^N \mathcal{L}$ made up of products of X_α's and H_i's with $Y_1 = \bigwedge_{\alpha>0} X_\alpha$. For $x \in G$ write $xY_1 = \Sigma\, c_j(x) Y_j$. Then $x \in U^- HU$ if and only if $c_1(x) \neq 0$.

Theorem 22: Assume that $\mathfrak{o}$ is a local principal ideal domain, that p is its unique prime, and that k and G are as before.

(a) $B_I = U^- H_{\mathfrak{o}} U_{\mathfrak{o}}$ is a subgroup of $G_{\mathfrak{o}}$.

(b) $G_{\mathfrak{o}} = \bigcup_{w \in W} B_I w B_I$ (disjoint), if the representatives for W in G are chosen in $G_{\mathfrak{o}}$.

(c) $B_I w B_I = B_I w U_{w,\mathfrak{o}}$ with the last component of the right uniquely determined mod $U_{w,p}$.

Proof: Let $\bar{\mathfrak{o}}$ denote the residue class field $\mathfrak{o}/p\mathfrak{o}$, $G_{\bar{\mathfrak{o}}}$ the Chevalley group of the same type as G over $\bar{\mathfrak{o}}$, and $B_{\bar{\mathfrak{o}}}, H_{\bar{\mathfrak{o}}}, \ldots$ the usual subgroups. By Theorem 18, Cor. 3 reduction mod p yields a homomorphism π of $G_{\mathfrak{o}}$ onto $G_{\bar{\mathfrak{o}}}$.

(1) $\pi^{-1}(U_{\bar{\mathfrak{o}}}^- H_{\bar{\mathfrak{o}}} U_{\bar{\mathfrak{o}}}) \subseteq U^- HU$. We consider G acting on $\wedge^N \mathfrak{L}$ as in Lemma 52. As is easily seen $G_{\mathfrak{o}}$ acts integrally relative to the basis of Y's. Now assume $\pi x \in U_{\bar{\mathfrak{o}}}^- H_{\bar{\mathfrak{o}}} U_{\bar{\mathfrak{o}}}^-$. Then $c_1(\pi x) \neq 0$ by the lemma applied to $G_{\bar{\mathfrak{o}}}$, whence $c_1(x) \neq 0$ and $x \in U^- HU$ again by the lemma.

(2) Corollary: $\ker \pi \subseteq U^- HU$.

(3) $B_I = \pi^{-1} B_{\bar{\mathfrak{o}}}$. Assume $x \in \pi^{-1} B_{\bar{\mathfrak{o}}}$. Then $x \in U^- BU$ by (1). From this and $x \in G_{\mathfrak{o}}$ it follows as in the proof of Theorem 7(b) that $x \in U_{\mathfrak{o}}^- H_{\mathfrak{o}} U_{\mathfrak{o}}$, and then that $x \in B_I$.

(4) Completion of proof: By (3) we have (a). To get (b) we simply apply π^{-1} to the decomposition in $G_{\bar{\mathfrak{o}}}$ relative to $B_{\bar{\mathfrak{o}}}$. We need only remark that a choice as indicated is always possible since each $w_\alpha(1) \in G_{\mathfrak{o}}$. From (b) the equation in (c) easily

follows. (Check this.) Assume $b_1 w u_1 = b_2 w u_2$ with $b_i \in B_I$, $u_i \in U_{w,\theta}$. Then $b_1^{-1} b_2 = w u_1 u_2^{-1} w^{-1} \in B_I \cap U_\theta^- = U_p^-$, whence $u_1 u_2^{-1} \in U_{w,p}$ and (c) follows.

Remark: The subgroup B_I above is called an Iwahori subgroup. It was introduced in an interesting paper by Iwahori and Matsumoto (Pabl. Math. I.H.E.S. No. 25 (1965)). There a decomposition which combines those of Theorems 21(a) and 22(b) can be found. The present development is completely different from theirs.

There is an interesting connection between the decomposition $G_\theta = \bigcup B_I w B_I$ above and the one, $G_\theta = \bigcup (BwB)_\theta$, that G_θ inherits as a subgroup of G, namely:

Corollary: Assume $w \in W$, that $S(w)$ is as in Theorem 16, Cor. 9, and that $\pi: G_\theta \longrightarrow G_{\bar\theta}$ is, as above, the natural projection. Then $\pi(B_I w B_I) = B_{\bar\theta} w B_{\bar\theta}$, and $\pi(BwB)_\theta = \bigcup_{w' \in S(w)} B_{\bar\theta} w' B_{\bar\theta}$. Hence if $\bar\theta$ is a topological field, e.g. $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$, then $\pi(BwB)_\theta$ is the topological closure of $\pi(B_I w B_I)$.

Proof: The first equation follows from $\pi^{-1} B_{\bar\theta} = B_I$, proved above. Write $w = w_\alpha w_\beta \ldots$ as in Lemma 25, Cor. Then

(*) $(BwB)_\theta = (Bw_\alpha B)_\theta (Bw_\beta B)_\theta \ldots$ by Theorem 18, Cor. 1. Now $(Bw_\alpha B)_\theta \supseteq x_{-\alpha}(p)$ and $w_\alpha(1)$ and is a union of B_θ double cosets. Thus $\pi(Bw_\alpha B)_\theta \supseteq B_{\bar\theta} \cup B_{\bar\theta} w_\alpha B_{\bar\theta} = B_\theta G_{\alpha,\bar\theta}$. The reverse inequality also holds since $(Bw_\alpha B)_\theta \subseteq B_\theta G_{\alpha,\theta}$ by Theorem 18, Cor. 1. From this, (*), the definition of $S(w)$, and Lemma 25, the required expression for $\pi(BwB)_\theta$ now follows.

Appendix. Our purpose is to prove Theorem 23 below which gives the closure of BwB under very general conditions. We will write $w' \leq w$ if $w' \in S(w)$ with $S(w)$ as in Theorem 16, Cor. 9; i.e. if w' is a subexpression (i.e. the product of a subsequence) of some minimal expression of w as a product of simple reflections.

Lemma 53: The following are true.

(a) If w' is a subexpression of some minimal expression for w, it is a subexpression of all of them.

(b) In (a) the subexpressions for w' can all be taken to be minimal.

(c) The relation $\leq$ is transitive.

(d) If $w \in W$ and α is a simple root such that $w\alpha > 0$ (resp. $w^{-1}\alpha > 0$), then $ww_\alpha > w$ (resp. $w_\alpha w > w$).

(e) $w_o \geq w$ for all $w \in W$.

Proof: (a) This was proved in Theorem 16, Cor. 7 and 9 in a rather roundabout way. It is a direct consequence of the following fact, which will be proved in a later section: the equality of two minimal expressions for w (as a product of simple reflections) is a consequence of the relations $w_1w_2\ldots = w_2w_1\ldots$ (w_1, w_2 distinct simple reflections, n terms on each side, n = order w_1w_2).

(b) If $w' = w_1w_2\ldots w_r$ is an expression as in (b) and it is not minimal, then two of the terms on the right can be cancelled by Appendix II 21.

(c) By (a) and (b).

(d) If $w\alpha > 0$ and $w_1 w_2 \dots w_s$ is a minimal expression for w, then $w_1 \dots w_s w_\alpha$ is one for ww_α by Appendix II 19, so that $ww_\alpha > w$, and similarly for the other case.

(e) This is proved in Lemma 46.

Now we come to our main result.

Theorem 23: Let G be a Chevalley group. Assume that k is a nondiscrete topological field and that the topology inherited by G as a matric group over k is used. Then the following conditions on w, w' are equivalent.

(a) $Bw'B \subseteq \overline{BwB}$.

(b) $w' \leq w$.

Proof: Let Y_1 be as in Lemma 52 and more generally $Y_w = \bigwedge_{\alpha>0} X_{w\alpha}$ for $w \in W$. For $x \in G$ let $c_w(x)$ denote the coefficient of Y_w in xY_1. We will show that (a) and (b) are equivalent to:

(c) $c_{w'}$ is not identically 0 on BwB.

(a) => (c). We have $x_\beta(t)X_\alpha = X_\alpha + \Sigma\, t^j X_j$ with X_j of weight (0 or a root) $\alpha + j\beta$, and $n_w X_\alpha = cX_{w\alpha}$ $(c \neq 0)$ if n_w represents w in W in N/H. Thus (*) $BwBY_1 \subseteq k^* Y_w +$ higher terms in the ordering given by sums of positive roots. Thus $c_{w'}$ is not identically 0 on $Bw'B$, hence also not on BwB, by (a).

(c) => (b). We use downward induction on $N(w')$. If this is maximal then $w' = w_0$, the element of W making all positive

roots negative, and then $w = w_o$ by (c) and (*) above. Assume $w' \neq w_o$. Choose α simple so that $w'^{-1}\alpha > 0$, hence $N(w_\alpha w') > N(w')$. Since $c_{w'}(BwB) \neq 0$ and $Bw_\alpha BwB \subset BwB \cup Bw_\alpha wB$, we see that $c_{w_\alpha w'}(BwB) \neq 0$ or $c_{w_\alpha w'}(Bw_\alpha wB) \neq 0$, so that $w_\alpha w' \leq w$ or $w_\alpha w' \leq w_\alpha w$. In the first case $w' < w$ by Lemma 53(c) and (d). In the second case if $w^{-1}\alpha < 0$ then $w_\alpha w < w$ by Lemma 53(d) which puts us back in the first case, while if not we may choose a minimal expression for w starting with w_α and conclude that $w' \leq w$.

(b) ⟹ (a). By the definitions and the usual calculus of double cosets, this is equivalent to: if α is simple, then $\overline{Bw_\alpha B} = B \cup Bw_\alpha B$. The left side is contained in the right, an algebraic group, hence a closed subset of G. Since $Bw_\alpha B$ contains $\chi_\alpha - 1$ and the topology on k is not discrete, its closure contains 1, hence also B, proving the reverse inequality and completing the proof of the theorem.

Remark: In case k above is $\mathbb{C}, \mathbb{R}$ or $\mathbb{Q}_p$, the theorem reduces to results obtained earlier. In case k is infinite and the Zariski topology on k and G are used it becomes a result of Chevalley (unpublished). Our proof is quite different from his.

Exercise: (a) If $w \in W$ and α is a positive root such that $w\alpha > 0$, prove that $ww_\alpha > w$ (compare this with Lemma 53(d)), and conversely if $w' \leq w$ then (*) there exists a sequence of positive roots $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that if $w_i = w_{\alpha_i}$ then

$w' w_1 \ldots w_{i-1} \alpha_i > 0$ for all i and $w' w_1 \ldots w_r = w$. Thus $w' \leq w$ and (*) are equivalent.

(b) It seems to us likely that $w' \leq w$ is also equivalent to: there exists a permutation π of the positive roots such that $w' \pi\alpha - w\alpha$ is a sum of positive roots for every $\alpha > 0$; or even to: $\sum_{\alpha>0} (w'\alpha - w\alpha)$ is a sum of positive roots.

§9. The orders of the finite Chevalley groups. Presently we will prove:

Theorem 24: Let W be a finite reflection group on a real space V of finite dimension ℓ, S the algebra of polynomials on V, $I(S)$ the subalgebra of invariants under W. Then:

(a) $I(S)$ is generated by ℓ homogeneous algebraically independent elements $I_1,\dots,I_\ell$.

(b) The degrees of the I_j's, say $d_1,\dots,d_\ell$, are uniquely determined and satisfy $\sum_j (d_j - 1) = N$, the number of positive roots.

(c) For the irreducible Weyl groups the d_i's are as follows:

W	d_i's
A_ℓ	$2, 3, \dots, \ell + 1$
B_ℓ, C_ℓ	$2, 4, \dots, 2\ell$
D_ℓ	$2, 4, \dots, 2\ell - 2, \ell$
E_6	2, 5, 6, 8, 9, 12
E_7	2, 6, 8, 10, 12, 14, 18
E_8	2, 8, 12, 14, 18, 20, 24, 30
F_4	2, 6, 8, 12
G_2	2, 6

Our main goal is:

Theorem 25: (a) Let G be a universal Chevalley group over a field k of q elements and the d_i's as in Theorem 24. Then

$|G| = q^N \prod_i (q^{d_i} - 1)$ with $N = \Sigma(d_i - 1)$ = the number of positive roots.

(b) If G is simple instead, then we have to divide by $c = |\mathrm{Hom}(L_1/L_0, k^*)|$, given as follows:

G	A_ℓ	B_ℓ, C_ℓ	D_ℓ	E_6	E_7	E_8	F_4	G_2
c	$(\ell+1, q-1)$	$(2, q-1)$	$(4, q^\ell - 1)$	$(3, q-1)$	$(2, q-1)$	1	1	1

Remark: We see that the groups of type B_ℓ and C_ℓ have the same order. If $\ell = 2$ the root systems are isomorphic so the groups are isomorphic. We will show later that if $\ell \geq 3$ the groups are isomorphic if and only if q is even.

The proof of Theorem 25 depends on the following identity.

Theorem 26: Let W and the d_i's be as in Theorem 24 and t an indeterminate. Then $\sum_{w \in W} t^{N(w)} = \prod_i (1 - t^{d_i})/(1 - t)$.

We show first that Theorem 25 is a consequence of Theorems 24 and 26.

Lemma 54: If G is as in Theorem 25(a) then $|G| = q^N (q - 1)^\ell \sum_{w \in W} q^{N(w)}$.

Proof: Recall that, by Theorems 4 and 4', $G = \bigcup_{w \in W} BwB$ (disjoint) and $BwB = UHwU_w$ with uniqueness of expression. Hence $|G| = |U||H| \cdot \sum_{w \in W} |U_w|$. Now by Corollary 1 to the proposition of §3, $|U| = q^N$ and $|U_w| = q^{N(w)}$. By Lemma 28, $|H| = (q - 1)^\ell$.

Corollary: U is a p-Sylow subgroup of G, if p denotes the characteristic of k.

Proof: $p \mid q^{N(w)}$ unless $N(w) = 0$. Since $N(w) = 0$ if and only if $w = 1$, $p \nmid \Sigma\, q^{N(w)}$.

Proof of Theorem 25: (a) follows from Lemma 54 and Theorem 26. (b) follows from the fact that the center of the universal group is isomorphic to $\mathrm{Hom}(L_1/L_0, k^*)$ and the values of L_1/L_0 found in S_3.

Before giving general proofs of Theorems 24 and 26 we give independent (case by case) verifications of Theorems 24 and 26 for the classical groups.

Theorem 24: Type A_ℓ: Here $W \cong S_{\ell+1}$ permuting $\ell + 1$ linear functions $\omega_1, \ldots, \omega_{\ell+1}$ such that $\sigma_1 = \Sigma\, \omega_i = 0$. In this case the elementary symmetric polynomials $\sigma_2, \ldots, \sigma_{\ell+1}$ are invariant and generate all other polynomials invariant under W.

Types B_ℓ, C_ℓ: Here W acts relative to a suitable basis $\omega_1, \ldots, \omega_\ell$ by all permutations and sign changes. Here the elementary symmetric polynomials in $\omega_1^2, \ldots, \omega_\ell^2$ are invariant and generate all other polynomials invariant under W.

Type D_ℓ: Here only an even number of sign changes can occur. Thus we can replace the last of the invariants for B_ℓ, $\omega_1^2 \ldots \omega_\ell^2$ by $\omega_1 \ldots \omega_\ell$.

Theorem 26: Type A_ℓ: Here $W \cong S_{\ell+1}$ and $N(w)$ is the number

of inversions in the sequence $(w(1),\ldots,w(\ell+1))$. If we write $P_\ell(t) = \sum_{w\in W\cong S_{\ell+1}} t^{N(w)}$ then $P_{\ell+1}(t) = P_\ell(t)(1 + t + t^2 +\ldots+ t^{\ell+1})$, as we see by considering separately the $\ell+2$ values that $w(\ell+2)$ can take on. Hence the formula $P_\ell(t) = \prod_{j=2}^{\ell+1}(1 - t^j)/(1 - t)$ follows by induction.

Exercise: Prove the corresponding formulas for types B_ℓ, C_ℓ and D_ℓ. Here the proof is similar, the induction step being a bit more complicated.

Part (a) of Theorem 24 follows from:

Theorem 27: Let G be a finite group of automorphisms of a real vector space V of finite dimension ℓ and I the algebra of polynomials on V invariant under G. Then:

(a) If G is generated by reflections, then I is generated by ℓ algebraically independent homogeneous elements (and 1).

(b) Conversely, if I is generated by ℓ algebraically independent homogeneous elements (and 1) then G is generated by reflections.

Example: Let $\ell = 2$ and V have coordinates x,y. If $G = \{\pm \text{id.}\}$, then G is not a reflection group. I is generated by x^2, xy, and y^2 and no smaller number of elements suffices.

Notation: Throughout the proof we let S be the algebra of all polynomials on V, S_o the ideal in S generated by the homogeneous elements of I of positive degree, and Av stand for

average over G (i.e. $AvP = |G|^{-1} \sum_{g \in G} gP$) .

Proof of (a): (Chevalley, Am. J. of Math. 1955.)

(1) Assume $I_1, I_2, \ldots$ are elements of I such that I_1 is not in the ideal in I generated by the others and that $P_1, P_2, \ldots$ are homogeneous elements of S such that $\Sigma P_i I_i = 0$. Then $P_1 \in S_o$.

Proof: Suppose $I_1 \in$ ideal in S generated by $I_2, \ldots$. Then $I_1 = \sum_{i \geq 2} R_i I_i$ for some $R_2, \ldots \in S$ so that $I_1 = AvI_1 = \sum_{i \geq 2} (AvR_i) I_i$ belongs to the ideal in I generated by $I_2, \ldots$, a contradiction. Hence I_1 does not belong to the ideal in S generated by $I_2, \ldots$.

We now prove (1) by induction on $d = \deg P_1$. If $d = 0$, $P_1 = 0 \in S_o$. Assume $d > 0$ and let $g \in G$ be a reflection in a hyperplane $L = 0$. Then for each i, $L | (P_i - gP_i)$. Hence $\Sigma((P_i - gP_i)/L) I_i = 0$, so by the induction assumption $P_1 - gP_1 \in S_o$, i.e. $P_1 \equiv gP_1 \pmod{S_o}$. Since G is generated by reflections this holds for all $g \in G$ and hence $P_1 \equiv AvP_1 \pmod{S_o}$. But $AvP_1 \in S_o$ so $P_1 \in S_o$.

We choose a minimal finite basis $I_1, \ldots, I_n$ for S_o formed of homogeneous elements of I . Such a basis exists by Hilbert's Theorem.

(2) The I_i's are algebraically independent.

Proof: If the I_i are not algebraically independent, let $H(I_1, \ldots, I_n) = 0$ be a nontrivial relation with all monomials in

the I_i's of the same minimal degree in the underlying coordinates $x_1,\ldots,x_\ell$. Let $H_i = \partial H(I_1,\ldots,I_n)/\partial I_i$. By the choice of H not all H_i are 0. Choose the notation so that $\{H_1,\ldots,H_m\}$ $(m \leq n)$ but no subset of it generates the ideal in I generated by all the H_i. Let $H_j = \sum_{i=1}^{m} V_{j,i} H_i$ for $j = m+1,\ldots,n$ where $V_{j,i} \in I$ and all terms in the equation are homogeneous of the same degree. Then for $k = 1, 2,\ldots,\ell$ we have $0 = \partial H/\partial x_k = \sum_{i=1}^{n} H_i \partial I_i/\partial x_k$ $= \sum_{i=1}^{m} H_i(\partial I_i/\partial x_k + \sum_{j=m+1}^{n} V_{j,i} \partial I_j/\partial x_k)$. By (1) $\partial I_1/\partial x_k$ $+ \sum_{j=m+1}^{n} V_{j,1} \partial I_j/\partial x_k \in S_o$. Multiplying by x_k, summing over k, using Euler's formula, and writing $d_j = \deg I_j$ we get $d_1 I_1 + \sum_{j=m+1}^{n} V_{j,1} d_j I_j = \sum_{i=1}^{n} A_i I_i$ where A_i belongs to the ideal in S generated by the x_k. By homogeneity $A_1 = 0$. Thus I_1 is in the ideal generated by $I_2,\ldots,I_n$, a contradiction.

(3) The I_i's generate I as an algebra.

Proof: Assume $P \in I$ is homogeneous of positive degree. Then $P = \Sigma P_i I_i$, $P_i \in S$. By averaging we can assume that each $P_i \in I$. Each P_i is of degree less than the degree of P, so by induction on its degree P is a polynomial in the I_i's.

(4) $n = \ell$.

Proof: By (2) $n \leq \ell$. By Galois theory $\mathbb{R}(I)$ is of finite index in $\mathbb{R}(x_1, x_2,\ldots,x_n)$, hence has transcendence degree ℓ over $\mathbb{R}$, whence $n \geq \ell$.

By (2), (3) and (4) (a) holds.

Proof of (b): (Todd, Shephard Can. J. Math. 1954.)

Let $I_1,\dots,I_\ell$ be algebraically independent generators of I of degrees $d_1,\dots,d_\ell$, respectively.

(5) $\prod_{i=1}^{\ell}(1-t^{d_i})^{-1} = \operatorname{Av}_{g\in G} \det(1-gt)^{-1}$, as a formal identity in t.

Proof: Let $\varepsilon_1,\dots,\varepsilon_\ell$ be the eigenvalues of g and $x_1,\dots,x_\ell$ the corresponding eigenfunctions. Then $\det(1-gt)^{-1}$ $= \prod_i (1+\varepsilon_i t+\varepsilon_i^2 t^2+\dots)$. The coefficient of t^n is $\sum_{p_1+p_2+\dots=n} \varepsilon_1^{p_1}\varepsilon_2^{p_2}\dots$, i.e. the trace of g acting on the space of homogeneous polynomials in $x_1,\dots,x_\ell$ of degree n, since the monomials $x_1^{p_1}x_2^{p_2}\dots$ form a basis for this space. By averaging we get the dimension of the space of invariant homogeneous polynomials of degree n. This dimension is the number of monomials $I_1^{p_1}I_2^{p_2}\dots$ of degree n, i.e., the number of solutions of $p_1d_1+p_2d_2+\dots=n$, i.e. the coefficient of t^n in $\prod_{i=1}^{\ell}(1-t^{d_i})^{-1}$.

(6) $\prod d_i = |G|$ and $\Sigma(d_i-1) = N$ = number of reflections in G.

Proof: We have $\det(1-gt) = \begin{cases} (1-t)^\ell & \text{if } g=1, \\ (1-t)^{\ell-1}(1+t) & \text{if } g \text{ is a reflection,} \\ \text{a polynomial not divisible by } (1-t)^{\ell-1} & \text{otherwise.} \end{cases}$

Substituting this in (5) and multiplying by $(1-t)^{\ell}$, we have $\prod (1 + t + \ldots + t^{d_i-1})^{-1} = |G|^{-1}(1 + N(1-t)/(1+t) + (1-t)^2 P(t))$ where $P(t)$ is regular at $t = 1$. Setting $t = 1$ we get $\prod d_i^{-1} = |G|^{-1}$. Differentiating and setting $t = 1$ we get $(\prod d_i^{-1})\Sigma(-(d_i-1)/2) = |G|^{-1}(-N/2)$, so $\Sigma(d_i-1) = N$.

(7) Let G' be the subgroup of G generated by its reflections. Then $G' = G$ and hence G is a reflection group.

Proof: Let I_i', d_i', and N' refer to G'. The I_i' can be expressed as polynomials in the I_i with the determinant of the corresponding Jacobian not 0. Hence after a rearrangement of the I_i, $\partial I_i/\partial I_i' \neq 0$ for all i. Hence $d_i \geq d_i'$. But $\Sigma(d_i - 1) = N = N' = \Sigma(d_i' - 1)$ by (6). Hence $d_i = d_i'$ for all i, so, again by (6), $|G| = \prod d_i = \prod d_i' = |G'|$, so $G = G'$.

Corollary: The degrees $d_1, d_2, \ldots$ above are uniquely determined and satisfy the equations (6).

Thus Theorem 24(b) holds.

Exercise: For each reflection in G choose a root α. Then $\det \frac{\partial(I_1, I_2, \ldots)}{\partial(x_1, x_2, \ldots)} = \prod \alpha$ up to multiplication by a nonzero number.

Remark: The theorem remains true if $\mathbb{R}$ is replaced by any field of characteristic 0 and "reflection" is replaced by "automorphism of V with fixed point set a hyperplane".

For the proof of Theorem 24(c) (determination of the d_i) we use:

Proposition: Let G and the d_i be as in Theorem 27 and $w = w_1 \ldots w_\ell$, the product of the simple reflections (relative to an ordering of V (see Appendix I.8)) in any fixed order. Let h be the order of w. Then:

(a) $N = \ell h/2$.

(b) w contains $\omega = \exp 2\pi i/h$ as an eigenvalue, but not 1.

(c) If the eigenvalues of w are $\{\omega^{m_i} | 1 \leq m_i \leq h - 1\}$ then $\{m_i + 1\} = \{d_i\}$.

Proof: This was first proved by Coxeter (Duke Math. J. 1951), case by case, using the classification theory. For a proof not using the classification theory see Steinberg, T.A.M.S. 1959, for (a) and (b) and Coleman, Can. J. Math. 1958, for (c) using (a) and (b).

This can be used to determine the d_i for all the Chevalley groups. As an example we determine the d_i for E_8. Here $\ell = 8$, $N = 120$, so by (a) $h = 30$. Since w acts rationally $\{\omega^n | (n, 30) = 1\}$ are all eigenvalues. Since $\varphi(30) = 8 = \ell$ these are all the eigenvalues. Hence the d_i are $1, 7, 11, 13, 17, 19, 23, 29$ all increased by 1, as listed previously. The proofs for G_2 and F_4 are exactly the same. E_6 and E_7 require further argument.

Exercise: Argue further.

Remark: The d_i's also enter into the following results, related to Theorem 24:

(a) Let $\mathcal{L}$ be the original Lie algebra, k a field of characteristic 0, G the corresponding adjoint Chevalley group. The algebra of polynomials on $\mathcal{L}$ invariant under G is generated by ℓ algebraically independent elements of degree $d_1, \ldots, d_\ell$, the d_i's as above.

This is proved by showing that under restriction from $\mathcal{L}$ to $\mathcal{H}$ the G-invariant polynomials on $\mathcal{L}$ are mapped isomorphically onto the W-invariant polynomials on $\mathcal{H}$. The corresponding result for the universal enveloping algebra of $\mathcal{L}$ then follows easily.

(b) If G acts on the exterior algebra on $\mathcal{L}$, the algebra of invariants is an exterior algebra generated by ℓ independent homogeneous elements of degrees $\{2d_i - 1\}$.

This is more difficult. It implies that the Poincaré polynomial (whose coefficients are the Betti numbers) of the corresponding compact semisimple Lie group (the group K constructed from $\mathbb{C}$ in §8) is $\prod (1 + t^{2d_i - 1})$.

Proof of Theorem 26: (Solomon, Journal of Algebra, 1966.)

Let $\prod$ be the set of simple roots. If $\pi \subseteq \prod$ let W_π be the subgroup generated by all w_α, $\alpha \in \pi$.

(1) If $w \in W_\pi$ then w permutes the positive roots with support not in π.

Proof: If β is a positive root and supp $\beta \not\subset \pi$ then $\beta = \sum_{\alpha \in \prod} e_\alpha \alpha$ with some $e_\alpha > 0$, $\alpha \notin \pi$. Now $w\beta$ is β plus a

vector with support in π, hence its coefficient of α is positive, so $w\beta > 0$.

(2) Corollary: If $w \in W_\pi$ then $N(w)$ is unambiguous (i.e. it is the same whether we consider $w \in W$ or $w \in W_\pi$).

(3) For $\pi \subseteq \Pi$ define $W_\pi' = \{w \in W \mid w\pi > 0\}$. Then:

(a) Every $w \in W$ can be written uniquely $w = w'w''$ with $w' \in W_\pi'$ and $w'' \in W_\pi$.

(b) In (a) $N(w) = N(w') + N(w'')$.

Proof: (a) For any $w \in W$ let $w' \in W_\pi w$ be such that $N(w')$ is minimal. Then $w'\alpha > 0$ for all $\alpha \in \pi$ by Appendix II.19(a'). Hence $w' \in W_\pi'$ so that $w \in W_\pi' W_\pi$. Suppose now $w = w'w'' = u'u''$ with $w', u' \in W_\pi'$ and $w'', u'' \in W_\pi$. Then $w'^{-1}u' = w''u''^{-1}$. Hence $w'^{-1}u'\pi > 0$. Now $w'^{-1}(-\pi) < 0$ so $w'^{-1}u'\pi$ has support in π. Hence $w''u''^{-1}\pi \subseteq \pi$ so by Appendix II.23 (applied to W_π) $w''u''^{-1} = 1$. Hence $w' = u'$, $w'' = u''$.

(b) follows from (a) and (1).

(4) Let $W(t) = \sum_{w \in W} t^{N(w)}$, $W_\pi(t) = \sum_{w \in W_\pi} t^{N(w)}$. Then $\sum_{\pi \subseteq \Pi} (-1)^\pi W(t)/W_\pi(t) = t^N$, where N is the number of positive roots and $(-1)^\pi = (-1)^{|\pi|}$.

Proof: We have, by (3), $W(t)/W_\pi(t) = \sum_{w \in W_\pi'} t^{N(w)}$. Therefore the contribution of the term for w to the sum in (4) is $c_w t^{N(w)}$ where $c_w = \sum_{\substack{\pi \subseteq \Pi \\ w\pi > 0}} (-1)^\pi$. If w keeps positive exactly k elements

of $\prod$ then $c_w = \begin{cases} (1-1)^k = 0 & \text{if } k \neq 0 \\ 1 & \text{if } k = 0 . \end{cases}$

Therefore the only contribution is made by w_o, the element of w which makes all positive roots negative, so the sum in (4) is equal to t^N as required.

Corollary: $\Sigma(-1)^{\pi}|W|/|W_\pi| = 1$.

Exercise: Deduce from (4) that if α and β are complementary subsets of $\prod$ then $\sum_{\pi \supseteq \alpha} (-1)^{\pi-\alpha}/W_\pi(t) = \sum_{\pi \supseteq \beta} (-1)^{\pi-\beta}/W_\pi(t^{-1})$.

Set $D = \{v \in V | (v, \alpha) \geq 0 \text{ for all } \alpha \in \prod\}$, and for each $\pi \subseteq \prod$ set $D_\pi = \{v \in V | (v, \alpha) = 0 \text{ for all } \alpha \in \pi, (v, \beta) > 0 \text{ for all } \beta \in \prod - \pi\}$. D_π is an open face of D.

(5) The following subgroups of W are equal:

(a) W_π .

(b) The stabilizer of D_π .

(c) The point stabilizer of D_π .

(d) The stabilizer of any point of D_π .

Proof: (a) $\subseteq$ (b) because π is orthogonal to D_π . (b) $\subseteq$ (c) because D is a fundamental domain for W by Appendix III.33. Clearly (c) $\subseteq$ (d) . (d) $\subseteq$ (a) by Appendix III.32.

(6) In the complex cut on real k-space by a finite number of hyperplanes let n_i be the number of i-cells. Then $\Sigma(-1)^i n_i = (-1)^k$.

Proof: This follows from Euler's formula, but may be proved

directly by induction. In fact, if an extra hyperplane H is added to the configuration, each original i-cell cut in two by H has corresponding to it in H an $(i-1)$-cell separating the two parts from each other, so that $\Sigma(-1)^i n_i$ remains unchanged.

(7) In the complex K cut from V by the reflecting hyperplanes let $n_\pi(w)$ $(\pi \subseteq \prod, w \in W)$ denote the number of cells W-congruent to D_π and w-fixed. Then $\sum_{\pi \subseteq \prod} (-1)^\pi n_\pi(w) = \det w$.

Proof: Each cell of K is W-congruent to exactly one D_π. By (5) every cell fixed by w lies in V_w $(V_w = \{v \in V | wv = v\})$. Applying (6) to V_w and using $\dim D_\pi = i - |\pi|$ we get $\sum_{\pi \subseteq \prod} (-1)^\pi n_\pi(w) = (-1)^{i-k}$, where $k = \dim V_w$. But w is orthogonal, so that its possible eigenvalues in V are $+1$, -1 and pairs of conjugate complex numbers. Hence $(-1)^{i-k} = \det w$.

If χ is a character on W_1, a subgroup of W, then χ^W denotes the induced character defined by (*) $\chi^W(w) = |W_1|^{-1} \sum_{\substack{x \in W \\ xwx^{-1} \in W_1}} \chi(xwx^{-1})$. (See, e.g., W. Feit, Characters of finite groups.)

(8) Let χ be a character on W and $\chi_\pi = (\chi | W_\pi)^W$ $(\pi \subseteq \prod)$. Then $\sum_{\pi \subseteq \prod} (-1)^\pi \chi_\pi(w) = \chi(w) \det w$ for all $w \in W$.

Proof: Assume first that $\chi \equiv 1$. Now $xwx^{-1} \in W_\pi$ if and only if xwx^{-1} fixes D_π (by (5)) which happens if and only if w fixes $x^{-1}D_\pi$. Therefore $1_\pi(w) = n_\pi(w)$ by (*). By (7) this gives the result for $\chi \equiv 1$. If χ is any character then

$\chi_\pi = \chi \cdot 1_\pi$ so (8) holds.

(9) Let M be a finite dimensional real W-module, $I_\pi(M)$ be the subspace of W_π-invariants, and $\hat{I}(M)$ be the space of W-skew-invariants (i.e. $\hat{I}(M) = \{m \in M \mid wm = (\det w)m \text{ for all } w \in W\}$). Then $\sum_{\pi \subseteq \prod} (-1)^\pi \dim I_\pi(M) = \dim \hat{I}(M)$.

Proof: In (8) take χ to be the character of M, average over $w \in W$, and use (*).

(10) If $p = \prod \alpha$, the product of the positive roots, then p is skew and p divides every skew polynomial on V.

Proof: We have $w_\alpha p = -p = (\det w_\alpha)p$ if α is a simple root by Appendix I.11. Since W is generated by simple reflections p is skew. If f is skew and α a root then $w_\alpha f = (\det w_\alpha)f = -f$ so $\alpha \mid f$. By unique factorization $p \mid f$.

(11) Let $P(t) = \prod (1 - t^{d_i})/(1 - t)$ and for $\pi \subseteq \prod$ let $\{d_{\pi i}\}$ and P_π be defined for W_π as $\{d_i\}$ and P are for W. Then $\sum_{\pi \subseteq \prod} (-1)^\pi P(t)/P_\pi(t) = t^N$.

Proof: We must show (*) $\sum_{\pi \subseteq \prod} (-1)^\pi \prod_i (1 - t^{d_{\pi i}})^{-1}$ $= t^N \prod_i (1 - t^{d_i})^{-1}$. Let $S = \sum_{k=0}^{\infty} S_k$ be the algebra of polynomials on V, graded as usual. As in (5) of the proof of Theorem 27 the coefficient of t^k on the left hand side of (*) is $\sum_{\pi \subseteq \prod} (-1)^\pi \dim I_\pi(S_k)$. Similarly, using (10), the coefficient of t^k on the right hand side of (*) is $\dim \hat{I}(S_k)$. These are equal by (9).

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

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

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

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

(a) Σ^* is a root system.

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

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

extends to a homothety.

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

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

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

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