Generalized Tits System (Bruhat Decomposition) on $\mathfrak{p}$-Adic Semisimple Groups

BY

NAGAYOSHI IWAHORI

1. **Generalized Tits system.** In order to describe the situation where the algebraic group G is not simply connected (cf. Bruhat's talk; also see **[3]**, **[8]**), we have to generalize the notion of *Tits system* (or *BN*-pair, see Tits **[13]**) as follows.

Let G be a group and B, N subgroups of G. The triple (G, B, N) is called a *generalized Tits system* if the following conditions (i) $\sim$ (vi) are all satisfied.

(i) $H = B \cap N$ is a normal subgroup of N.

(ii) The factor group N/H is a semidirect product of a subgroup Ω and a normal subgroup $W: N/H = \Omega \cdot W$.

(iii) There exists a system of generators of W consisting of involutive elements $w_i\,(i \in I)$ with the following properties (iii; α) and (iii; β). [We assume that $w_i \neq 1$ and that $w_i \neq w_j$ (for $i \neq j$). We also identify the index set I with the generator system $\{w_i\,; i \in I\}$].

(iii; α) For any σ in ΩW and for any w_i in I,

$$\sigma B w_i \subset B\sigma w_i B \cup B\sigma B.$$

(For any element σ and τ in ΩW, $\sigma B\tau$ is defined as the set $\tilde{\sigma}B\tilde{\tau}$ where $\tilde{\sigma}$ and $\tilde{\tau}$ are elements of N projecting to σ, τ respectively. Obviously $\sigma B\tau$ is thus well defined. Similarly $B\sigma B$ is defined.)

(iii; β) $w_i B w_i^{-1} \neq B$ for all w_i in I.

(iv) Any element ρ in Ω normalizes $I: \rho I \rho^{-1} = I$.

(v) $\rho B \rho^{-1} = B$ for all ρ in Ω; $B\rho \neq B$ for any $\rho \in \Omega - \{1\}$.

(vi) G is generated by B and N.

W is called the Weyl group of (G, B, N); $\Omega W = N/H$ is called the generalized Weyl group of (G, B, N).

Let now (G, B, N) be a generalized Tits system. Then, Tits **[13]** (cf. also Iwahori and Matsumoto [**8**, §2]), one can prove the following main properties of the generalized Tits system (G, B, N).

(a) $G = \bigcup_{\sigma \in \Omega W} B\sigma B$ (disjoint union)

(b) The normalizer $N(B)$ of B in G is given by

$$N(B) = \bigcup_{\rho \in \Omega} B\rho B = B\Omega B = B\Omega = \Omega B.$$

Furthermore, $N(B)/B$ is isomorphic with Ω.

(c) For any subgroup H of G containing B, there exist a unique subgroup Ω_H of Ω and a unique subset J_H of I such that $H = B(\Omega_H W(J_H))B$; where $W(J_H)$ means the subgroup of W generated by J_H. Moreover, J_H is normalized by every element ρ in $\Omega_H: \rho J_H \rho^{-1} = J_H$. The pair (Ω_H, J_H) is called *associated* with the subgroup H.

(d) Conversely, let (Ω', J) be a pair of a subgroup Ω' of Ω and a subset J of I such that J is normalized by every element of Ω'. (Such a pair will be called an *admissible pair.*) Then there exists a unique subgroup H such that $G \supset H \supset B$ and that $\Omega' = \Omega_H$, $J = J_H$. Thus the mapping $H \to (\Omega_H, J_H)$ is a bijection from the set of all subgroups between G and B onto the set of all admissible pairs.

(e) Let L be the normalizer in G of a subgroup H containing B. Let (Ω_H, J_H), (Ω_L, J_L) be the admissible pairs associated to H, L respectively. Then,

$$J_L = J_H, \Omega_L = \{\rho \in \Omega; \rho\Omega_H\rho^{-1} = \Omega_H, \rho J_H \rho^{-1} = J_H\}.$$

(f) Let H_i $(i = 1, 2)$ be subgroups of G containing B and (Ω_i, J_i) $(i = 1, 2)$ the admissible pairs associated to H_1, H_2 respectively. Then the following conditions (α)–(γ) are equivalent:

(α) H_1 and H_2 are conjugate in G,

(β) H_1 and H_2 are conjugate by an element in $N(B)$,

(γ) $\rho\Omega_1\rho^{-1} = \Omega_2$ and $\rho J_1 \rho^{-1} = J_2$ for some ρ in Ω.

(g) $G_0 = BWB$ is a normal subgroup of G and (G_0, B, N_0) is a Tits system with W as its Weyl group, where $N_0 = N \cap G_0$. Moreover $G/G_0 \cong \Omega$.

(h) For any element g in G, the automorphism of G_0 defined by $x \to gxg^{-1}$ preserves the Tits system (G_0, B, N_0) up to the conjugacy in G_0, i.e., there exists an element g_0 in G_0 such that $gBg^{-1} = g_0Bg_0^{-1}$, $gN_0g^{-1} = g_0N_0g_0^{-1}$.

According to a remark of Tits, (g) and (h), provide the following alternative description of generalized Tits systems, which make them appear as sort of nonconnected analogues of the usual ones.

To begin with, let us recall the notion of saturation for a Tits system. In general, a generalized Tits system (G,B,N) is called *saturated* if

$$B \cap N = \bigcap_{n \in N} nBn^{-1}.$$

Note that any generalized Tits system (G, B, N) can be modified into a saturated one (G, B, N^*) without changing the factor group $N/B \cap N$. In fact, N^* is given as $N^* = N \cdot H^*$ where $H^* = \bigcap_{n \in N} nBn^{-1}$. Conversely, starting from a saturated system (G, B, N^*) one gets other systems by replacing N^* by any subgroup N such that $N \cdot H^* = N^*$.

Suppose now that G_0 is a normal subgroup of a group G and let (G_0, B_0, N_0) be a saturated Tits system on G_0. We assume that, for any element g in G, the automorphism $x \to gxg^{-1}$ of G_0 preserves the Tits system (G_0, B_0, N_0) up to the conjugacy in G_0 (cf. (h) above). Then we get a saturated, generalized Tits system (G, B, N) on G, where $N = \Gamma N_0$, $\Gamma = N_G(B) \cap N_G(N_0)$, $B = B_0$. $(N_G(X)$

means the normalizer of X in G.) Furthermore, $N/B \cap N$ is isomorphic to the semidirect product $\Omega \cdot W$, where W is the Weyl group of (G_0, B_0, N_0) and $\Omega = N_G(B)/B$. This procedure exhausts all saturated generalized Tits systems.

2. **Existence of a generalized Tits system on $\mathfrak{p}$-adic semisimple algebraic groups.** (Supplements to Bruhat's talk.) Let k be a *local field*, i.e., a field with nontrivial, nonarchimedean, discrete valuation. We denote by $\mathfrak{O}$ (resp. $\mathfrak{p}$, resp. π) the ring of integers (resp. the unique maximal ideal in $\mathfrak{O}$, resp. a generator of the ideal $\mathfrak{p}$). We also denote by κ the residue class field $\mathfrak{O}/\mathfrak{p}$.

Now let G be a connected, semisimple algebraic group of Chevalley type over the local field k. Let A be a maximal k-split torus of G and Φ the root system of (G, A). We denote by P_r (resp. by P) the $\boldsymbol{Z}$-module generated by all roots (resp. by all weights). Note that P_r and P are lattices of the vector space $\langle\Phi\rangle_{\boldsymbol{R}}$ spanned by Φ over $\boldsymbol{R}$. We recall also that an element λ in $\langle\Phi\rangle_{\boldsymbol{R}}$ is in P if and only if $2(\lambda, \alpha)/(\alpha, \alpha)$ is in $\boldsymbol{Z}$ for all α in Φ, where $(\ ,\ )$ is a suitable inner product in $\langle\Phi\rangle_{\boldsymbol{R}}$ (cf. Borel's talk p. 13). In particular, one has $P \supset P_r$ and P/P_r is a finite abelian group.

Now it is known that there is associated canonically a sublattice Γ such that $P \supset \Gamma \supset P_r$ and that $A_k \cong \mathrm{Hom}(\Gamma, k^*)$ (cf. [3]). We denote by $h\ (\chi)$ the element in A_k which corresponds to χ in $\mathrm{Hom}(\Gamma, k^*)$. Also for each root α, there is associated a rational homomorphism $x_\alpha: G_a \to G$ defined over k, where G_a is the additive group of the universal domain. (Note that G is simply connected (resp. the adjoint group, i.e., centerless) if and only if the associated lattice Γ coincides with P (resp. with P_r).)

Now let N be the normalizer of A in G. We shall now construct a generalized Tits system (G_k, B, N_k) on G_k by taking a certain subgroup B. Let $\mathfrak{G}_{\mathfrak{O}}$ be the Chevalley lattice in the Lie algebra $\mathfrak{G}_k$ of G over k (cf. Bruhat's talk and also Cartier's talk). We denote by $G_{\mathfrak{O}}$ the stabilizer of the Chevalley lattice $\mathfrak{G}_{\mathfrak{O}}$ in G_k:

$$G_{\mathfrak{O}} = \{g \in G_k;\, \mathrm{Ad}(g)\mathfrak{G}_{\mathfrak{O}} = \mathfrak{G}_{\mathfrak{O}}\}.$$

Then one can show [8] that $G_{\mathfrak{O}}$ is generated by the following elements in G_k:

$$x_\alpha(t) \qquad (t \in \mathfrak{O};\, \alpha \in \Phi) \quad \text{and}$$
$$h(\chi) \qquad (\chi \in \mathrm{Hom}(\Gamma, \mathfrak{O}^*)),$$

where $\mathfrak{O}^*$ means the group of invertible elements in $\mathfrak{O}$. Thus it is seen that the homomorphism ϕ of $G_{\mathfrak{O}}$ defined by the reduction mod $\mathfrak{p}$ maps $G_{\mathfrak{O}}$ onto the Chevalley group G_κ over κ associated to the lattice Γ. Thus one gets a "good reduction" (cf. Bruhat's talk).

Now let us fix a linear ordering in Φ. Then this determines a Borel subgroup B_κ of G_κ. Put

$$B = \phi^{-1}(B_\kappa).$$

As in the case where G is simply connected, the subgroup B thus defined is unique up to the conjugacy by elements in G_k (see Bruhat's talk). Now one can show [8] that our subgroup B is generated by the following elements in G_k:

$$\begin{array}{ll} x_\alpha(t) & (t \in \mathfrak{p}, \alpha \in \Phi_+) \\ x_\beta(t) & (t \in \mathfrak{O}, \beta \in \Phi_-) \\ h(\chi) & (\chi \in \operatorname{Hom}(\Gamma, \mathfrak{O}^*)). \end{array}$$

Note that one gets $A_{\mathfrak{O}} = N_k \cap B$, and $A_{\mathfrak{O}}$ is generated by the elements $h(\chi)$, $\chi \in \operatorname{Hom}(\Gamma, \mathfrak{O}^*)$.

Our main purpose here is the following:

THEOREM. *(G_k, B, N_k) is a generalized Tits system on G_k.*

For the proof of this theorem together with other properties of B, see [**8**]. Let us describe here the structure of the factor group $N_k/B \cap N_k = N_k/A_{\mathfrak{O}}$. To begin with, we recall the notion of *the affine Weyl group* $\tilde{W}(\Phi)$ associated to the root system Φ. We denote by $w_{\alpha,\nu}$ $(\alpha \in \Phi, \nu \in \boldsymbol{Z})$ the reflection mapping of the Euclidean space $\langle\Phi\rangle_{\boldsymbol{R}}$ with respect to the hyperplane $\{x \in \langle\Phi\rangle_{\boldsymbol{R}}; (\alpha, x) = \nu\}$, i.e.,

$$w_{\alpha,\nu}(x) = x - (x, \alpha) \cdot \alpha^* + \nu\alpha^*,$$

where $\alpha^* = 2\alpha/(\alpha, \alpha)$. We denote by $\tilde{W}(\Phi)$ the group generated by the reflections $w_{\alpha,\nu}$ $(\alpha \in \Phi, \nu \in \boldsymbol{Z})$, and call it the affine Weyl group associated to Φ. Note that the Weyl group $W(\Phi)$ is the subgroup of $\tilde{W}(\Phi)$ generated by the reflections $w_{\alpha,0}$ $(\alpha \in \Phi)$, and that $\tilde{W}(\Phi)$ is the semidirect product of $W(\Phi)$ and the normal subgroup D consisting of the translations of the following form: $x \to x + d$, where d is in the lattice $\Gamma^\perp = \{d \in \langle\Phi\rangle_{\boldsymbol{R}}; (d, \gamma) \in \boldsymbol{Z} \text{ for all } \gamma \in \Gamma\}$. Thus $\tilde{W}(\Phi) = W(\Phi) \cdot D$, $D \cong \Gamma^\perp \cong \operatorname{Hom}(\Gamma, \boldsymbol{Z})$.

Now one gets [**8**] $N_k/A_{\mathfrak{O}} \cong \Omega \cdot \tilde{W}(\Phi)$ (semidirect product) where Ω is a finite abelian group isomorphic with P/Γ. The set I of generating involutive elements of $\tilde{W}(\Phi)$ appearing in the structure of the generalized Tits system (G_k, B, N_k) is given as follows [**8**]: let $\Phi = \Phi_1 \cup \cdots \cup \Phi_r$ be the decomposition of the root system Φ into irreducible components Φ_i. Let $\Delta_i = \{\alpha_1^{(i)}, \cdots, \alpha_{l_i}^{(i)}\}$ be the set of all simple roots in Φ_i (relative to the given ordering) and $\alpha_0^{(i)}$ the highest root in Φ_i. Then I is given by

$$I = \{w_{\alpha_j^{(i)},0}\ (1 \leqq i \leqq r, 1 \leqq j \leqq l_i),\quad w_{\alpha_0^{(i)},1}\ (1 \leqq i \leqq r)\}.$$

We refer to [**8**, §1] as for the more detailed description of the groups $\Omega \cdot \tilde{W}(\Phi)$, $\tilde{W}(\Phi)$.

We note that the analogue of the above theorem is also true for a reductive algebraic group G defined over a local field k which has a k-split maximal torus.

EXAMPLE. Let $G = GL_n$. Then $G_k = GL(n, k)$ and $G_{\mathfrak{O}} = GL(n, \mathfrak{O})$. With respect to the usual ordering of roots, we get

$$B = \begin{pmatrix} \mathfrak{O}^* & & \mathfrak{p} \\ & \ddots & \\ \mathfrak{O} & & \mathfrak{O}^* \end{pmatrix}, \quad A_k = \begin{pmatrix} k^* & & 0 \\ & \ddots & \\ 0 & & k^* \end{pmatrix}.$$

Moreover we have $N_k = A_k \cdot S_n$, where S_n is the subgroup of G_k consisting of all permutation matrices. (Hence S_n may be regarded as the symmetric group of degree n.) Put

$$D = \left\{ \begin{pmatrix} \pi^{\nu_1} & & 0 \\ & \ddots & \\ 0 & & \pi^{\nu_n} \end{pmatrix} ; \nu_1, \cdots, \nu_n \in \boldsymbol{Z} \right\}.$$

Then $A_k = A_{\mathfrak{D}} \cdot D$ (direct product) with $A_{\mathfrak{D}} = A_k \cap B$, and one gets $N_k = A_{\mathfrak{D}}(DS_n)$ (semidirect product). Thus one gets **[4]** a generalized Tits system (G_k, B, N_k) with the following factor group:

$$N_k/B \cap N_k \cong \Omega \cdot \tilde{W},$$

where $\Omega \cong N(B)/B \cong \boldsymbol{Z}$ and $\tilde{W}$ is generated by involutive elements $w_1, \cdots, w_n$ in DS_n given by

$$w_i = \left(\begin{array}{c|cc|c} I_{i-1} & & & 0 \\ \hline & 0 & 1 & \\ & 1 & 0 & \\ \hline 0 & & & I_{n-i-1} \end{array}\right) \quad (1 \leqq i \leqq n-1), \quad w_n = \left(\begin{array}{c|ccc|c} 0 & & 0 & & \pi \\ \hline & 1 & & & \\ 0 & & \ddots & & 0 \\ & & & 1 & \\ \hline \pi^{-1} & & 0 & & 0 \end{array}\right).$$

Note that $N(B) = \{\omega\}B$ is a semidirect product where ω is an element in DS_n given by

$$\omega = \begin{pmatrix} 0 & & & & \pi \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}.$$

Furthermore we have $\omega w_i \omega^{-1} = w_{i+1}$ $(1 \leqq i \leqq n;\ w_{n+1} = w_1)$.

3. **A characterization of the subgroup** B **(cf. §2) for locally compact ground fields.** In this section we assume that k is a locally compact field with the (finite) residue class field κ of characteristic p.

Let G be a semisimple algebraic group defined over k. One sees then that for any open compact subgroup K of G_k, the normalizer $N(K)$ of K in G_k is also open and compact. Using this fact, one can prove the following theorem:

THEOREM (SYLOW). *Let G be a semisimple algebraic group defined over k. Then G_k has a maximal pro-p-subgroup S. Furthermore, any pro-p-subgroup of G_k is contained in a conjugate of S.*

We recall the terminologies used above: pro-finite group means the projective limit of finite groups; pro-p-group means the projective limit of finite p-groups.

Thus any two maximal pro-p-subgroup of G_k are conjugate. A maximal pro-p-subgroup of G_k is called a *Sylow subgroup* of G_k.

COROLLARY. *Let B be the normalizer in G_k of a Sylow subgroup S of G_k. Then, distinct subgroups of G_k containing B are never mutually conjugate in G_k, and each of them equals its own normalizer in G_k.*

Now for simply connected, semisimple groups of Chevalley type, we have the following

PROPOSITION (MATSUMOTO). *Let G be a connected, simply connected, semisimple group of Chevalley type over k. Then our subgroup B of G_k introduced in §2 is the normalizer of a Sylow subgroup of G_k.*

This proposition gives in a certain sense a "p-analytic" characterization of our BN-pair structure in G_k.

4. **Applications.**

4.1. *Maximal compact subgroups.* Let G be a connected, semisimple algebraic group of Chevalley type over a local field k. Then, since we have a generalized Tits system (G_k, B, N_k) on G_k (cf. §2), we can determine the conjugacy classes of subgroups of G_k containing a conjugate of B. Thus, in particular, when k is locally compact, we can determine the conjugacy classes of maximal compact subgroups of G_k. As an example, we shall give a table of the number s of conjugacy classes of the maximal compact subgroups of G_k containing B, when G is the adjoint group of simple groups [**8**].

Type of G	s
A_l	the number of (positive) divisors of $l + 1$
B_l and C_l	$l + 1$
D_l $(l = 2m + 1)$	l
D_l $(l = 2m)$	$l + 2$
E_6	5
E_7	8
E_8	9
F_4	5
G_2	3

Also, if G is simply connected and simple, then $s = l + 1$, when l is the rank of G [**8**].

We note that these values of s are shown to be the number of conjugacy classes of maximal compact subgroups of G_k by Hijikata [**5**], when G is of classical type. Thus it is an interesting question to prove (or disprove) this fact in general. Or one may formulate in the following way:

CONJECTURE 1. *Let G be a connected, semisimple algebraic group of Chevalley type over a locally compact field k. Then, every maximal compact subgroup K of G_k contains a conjugate of B (the subgroup introduced in* §2).

In other words, B has a fixed point on the homogeneous space G_k/K. In this respect, the following conjecture concerning the structure of the homogeneous space G_k/B seems to be interesting.

Let G_C be a connected, simply connected, complex semisimple Lie group (which is an algebraic linear group as is well known). Let k be the formal power series field $C((t))$ of one variable over C and $\mathfrak{O}$ be the ring of integral power series in k:

$$\mathfrak{O} = \left\{ \sum_{i=0}^{\infty} a_i t^i ; a_0, a_1, \cdots, \in C \right\}.$$

Then $\mathfrak{p} = t \cdot \mathfrak{O}$. Thus we can consider our subgroup B (in §2) in G_k. One has $G_k = \bigcup_{\sigma \in \tilde{W}} B\sigma B$. Hence G_k/B is a disjoint union of the sets $B\sigma B/B$. Now it is easy to show that $B\sigma B/B$ has the structure of a complex affine cell of dimension $\lambda(\sigma)$, where $\lambda(\sigma)$ is the word-length of σ relative to the generators given in §2 of the affine Weyl group $\tilde{W}$ (cf. [**8**]). The subset $G_{\mathfrak{O}}/B$ of G_k/B is easily identified with the generalized flag manifold G_C/B_C, where B_C is a Borel subgroup of G_C, because $G_C \subset G_k$ and $G_C \cap B = B_C$. Under this setting, let us state the following

CONJECTURE 2. *There exists a structure of a topological space of G_k/B with the following properties*:

(i) *G_k/B is an infinite dimensional* CW*-complex.*

(ii) *$G_k/B = \bigcup_{\sigma \in W} (B\sigma B/B)$ is a cellular decomposition of G_k/B. Each cell $B\sigma B/B$ is homeomorphic to $R^{2\lambda(\sigma)}$.*

(iii) *The Poincaré series $P(G_k/B, t)$ of G_k/B is equal to the product of the Poincaré polynomial $P(G_C/B_C, t)$ of G_C/B_C with Poincaré series $P(\Omega(G_C), t)$ of the loop space on G_C. Note that these Poincaré series are given by Bott as follows, using the exponents $m_1, \cdots, m_l$ of G_C*:

$$P(G_C/B_C, t) = \prod_{i=1}^{l} (1 + t^2 + t^4 + \cdots + t^{2m_i}) = \sum_{\sigma \in W} t^{2\lambda(\sigma)},$$

$$P(\Omega(G_C), t) = \prod_{i=1}^{l} (1 - t^{m_i})^{-1}.$$

Or, more strongly,

(iii)′ *G_k/B is homeomorphic to the product space $G_C/B_C \times \Omega(G_C)$. (Or G_k/B has the same homotopy type as the above product space.)*

(iv) (*Tits*) *G_k/B is the inductive limit of projective varieties of finite dimension.* (*A more precise statement of this conjecture has been given by Tits in his talk.*)

4.2. *Elementary divisor theorem.* Let $\mathfrak{O}$ be a Dedekind domain with the quotient field k. Then each prime ideal $\mathfrak{p}$ of $\mathfrak{O}$ defines a nontrivial, discrete, nonarchimedian valuation $x \to |x|_{\mathfrak{p}}$ of the quotient field k of $\mathfrak{O}$. The localization of $\mathfrak{O}$ relative to $\mathfrak{p}$ is denoted by $\mathfrak{O}_\mathfrak{p}$, i.e., $\mathfrak{O}_\mathfrak{p}$ is the ring of integers of k relative to the valuation $x \to |x|_\mathfrak{p}$. Then $\mathfrak{O}$ is the intersection of all localizations $\mathfrak{O}_\mathfrak{p}$ of $\mathfrak{O}$.

Now let G be a connected, semisimple algebraic group of Chevalley type over k. Then, fixing a Chevalley lattice in the Lie algebra $\mathfrak{G}_k$, one has the subgroups $G_\mathfrak{O}, G_{\mathfrak{O}_\mathfrak{p}}$ of G_k. Let A be the associated maximal k-split torus. Then by the structure of generalized Tits system on G_k with respect to the valuation $x \to |x|_\mathfrak{p}$, one sees that [8] $G_k = G_{\mathfrak{O}_\mathfrak{p}} A_k G_{\mathfrak{O}_\mathfrak{p}}$ for all prime ideal $\mathfrak{p}$ in $\mathfrak{O}$. Thus a natural question arises: can one replace $G_{\mathfrak{O}_\mathfrak{p}}$ by $G_\mathfrak{O} = \bigcap_\mathfrak{p} G_{\mathfrak{O}_\mathfrak{p}}$, i.e., does one get

$$G_k = G_\mathfrak{O} A_k G_\mathfrak{O}?$$

Now, this is not true in general. A counter example is obtained by Y. Ihara for the case $G = \mathrm{SL}_2$, $k = Q(\sqrt{(-5)})$, $\mathfrak{O}$ = "the principal order in k." On the other hand, this fact is known to be valid together with some uniqueness property when $\mathfrak{O}$ is a principal ideal domain and G is of classical type. (It is called the elementary divisor theorem.) In this respect, it is seen that a similar theorem is true for any semisimple groups of Chevalley type.

Thus, let k be the quotient field of a principal ideal domain $\mathfrak{O}$. Let G be a connected, semisimple algebraic group of Chevalley type over k. Let Γ be the lattice between the weight-lattice P and the root lattice P_r associated to G (cf. §2). We denote $\chi \to h(\chi)$ the isomorphism from $\mathrm{Hom}(\Gamma, k^*)$ onto A_k, where A is a k-split maximal torus of A. Fixing a Chevalley lattice associated to A, the subgroup $G_\mathfrak{O}$ is defined. Now, fixing an ordering in the root system Φ of (G, A), one gets the notion of a *dominant element* in A_k; i.e., an element $h(\chi) \in A_k$ with $\chi \in \mathrm{Hom}(\Gamma, k^*)$ is called dominant if $\chi(\Phi_+) \subset \mathfrak{O}$. We denote by A_k^+ the set of all dominant elements in A_k. Then, A_k^+ is a semigroup in A_k. A_k^+ contains a subgroup $A_\mathfrak{O} = \{h(\chi); \chi(\Gamma) \subset \mathfrak{O}^*\}$. Under these settings, we get the following elementary divisor theorem.

THEOREM (MATSUMOTO). $G_k = G_\mathfrak{O} A_k^+ G_\mathfrak{O}$. *Moreover, the space* $G_\mathfrak{O}\backslash G_k/G_\mathfrak{O}$ *of double cosets of* $G_k \bmod G_\mathfrak{O}$ *is bijective with* $A_k^+/A_\mathfrak{O}$ *by the natural mapping* $a \cdot A_\mathfrak{O} \to G_\mathfrak{O} \cdot a \cdot G_\mathfrak{O}$.

5. **Hecke rings associated to a generalized Tits system.** (Cf. Shimura's talk.) Let us recall the notion of the Hecke ring $\mathscr{H}(G, B)$ associated to a pair of a group G and a subgroup B of G such that B is commensurable with any of its conjugates, i.e., $[B : B \cap \sigma B \sigma^{-1}] < \infty$ for all σ in G. Let $\mathscr{H} = \mathscr{H}(G, B)$ be the free Z-module spanned by the double cosets $S_\sigma = B\sigma B$ $(\sigma \in G)$. Then a multiplication is defined in $\mathscr{H}$ as follows:

$$S_\sigma S_\tau = \sum_\rho m_{\sigma,\tau}^\rho S_\rho,$$

where $m_{\sigma,\tau}^\rho$ is the number of cosets of the form Bx contained in $(B\sigma^{-1}B\rho) \cap (B\tau B)$. It is seen that $m_{\sigma,\tau}^\rho$ is independent of the choice of the representatives σ, τ, ρ in the double coset; moreover, given σ, τ, the number of the double cosets $B\rho B$ satisfying $m_{\sigma,\tau}^\rho \neq 0$ is finite. Furthermore, it is shown that $\mathscr{H}(G, B)$ becomes an associative algebra with the unit element over $\mathbf{Z}$ (see e.g. [7]). K being any field (or commutative ring), $\mathscr{H}(G, B) \otimes_{\mathbf{Z}} K$ is denoted by $\mathscr{H}_K(G, B)$ and is called the Hecke algebra of the pair (G, B) over K.

Now let us assume that (G, B, N) be a generalized Tits system on G with the factor group $\Omega W = N/B \cap N$ and standard involutive generators $I = \{w_i\}$ of W. For any $\sigma \in W$, we denote by $\lambda(\sigma)$ the length of a reduced expression of σ in terms of I. Consider the normal subgroup $G_0 = BWB$ of G and the induced Tits system (G_0, B_0, N_0) on G_0 where $B_0 = B$, $N_0 = N \cap G_0$. Then, as is seen easily, B is commensurable with any conjugate in G if and only if B_0 is commensurable with any conjugate in G_0. Moreover, when this is the case, $\mathscr{H}(G, B)$ is obtained from $\mathscr{H}(G_0, B_0)$ as follows: we note that Ω acts on the ring $\mathscr{H}(G_0, B_0)$ as a group of automorphisms as follows: for $\rho \in \Omega$ and for $\sigma \in W$, $B_0\sigma B_0 \to B_0(\rho\sigma\rho^{-1})B_0$, or putting $S_\sigma = B_0\sigma B_0$, we express this automorphism by $S_\sigma \to \rho(S_\sigma) = S_{\rho\sigma\rho^{-1}}$. Now introduce a new multiplication in the tensor product $\mathbf{Z}[\Omega] \otimes_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$ as follows ($\mathbf{Z}[\Omega]$ means the group ring of Ω over $\mathbf{Z}$):

$$(\rho \otimes S_\sigma)(\rho' \otimes S_{\sigma'}) = \rho\rho' \otimes (\rho')^{-1}(S_\sigma)S_{\sigma'}$$

for any ρ, $\rho' \in \Omega$ and σ, $\sigma' \in W$. Then one obtains a new ring structure on

$$\mathbf{Z}[\Omega] \otimes_{\mathbf{Z}} \mathscr{H}(G_0, B_0).$$

The ring thus obtained is denoted by $\mathbf{Z}[\Omega] \tilde{\otimes}_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$, and is called the *twisted tensor product* of $\mathbf{Z}[\Omega]$, $\mathscr{H}(G_0, B_0)$. Now we get

PROPOSITION. $\mathscr{H}(G, B) \cong \mathbf{Z}[\Omega] \tilde{\otimes}_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$.

Thus the question about the structure of the Hecke ring $\mathscr{H}(G, B)$ for a generalized Tits system (G, B, N) is reduced to the case where (G, B, N) is a usual Tits system; and in this case, the question was settled by [10] as follows.

Let (G, B, N) be a Tits system with the Weyl group W, and let $I = \{w_i\}$ the standard involutive generators of W. Suppose that B is commensurable with $w_iBw_i^{-1}$ for any $w_i \in I$. Then B is commensurable with any of its conjugates in G. Furthermore, for a reduced expression $\sigma = w_{i_1} \cdots w_{i_r}$ $(r = \lambda(\sigma))$ of $\sigma \in W$, one has

$$S_\sigma = S_{i_1} \cdots S_{i_r} \qquad (\text{where } S_j = S_{w_j}).$$

Thus the first half of the following theorem is obtained.

THEOREM [10]. *The set $\{S_i; i \in I\}$ generates the ring $\mathscr{H}(G, B)$. A system of defining relations for this generator $\{S_i\}$ is given as follows:*

$$S_i^2 = q_i \cdot 1 + (q_i - 1) \cdot S_i \quad (\textit{for all } i \in I),$$
$$(S_iS_j)^{m_{ij}} = (S_jS_i)^{m_{ij}}, \textit{ if the order of } w_iw_j \textit{ is } 2m_{ij} < \infty,$$
$$(S_iS_j)^{m_{ij}}S_i = (S_jS_i)^{m_{ij}}S_j, \textit{ if the order of } w_iw_j \textit{ is } 2m_{ij} + 1 < \infty.$$

where q_i is the number of cosets of the form Bx contained in Bw_iB.

EXAMPLE 1. Let k be a local field such that $\kappa = \mathfrak{O}/\mathfrak{p}$ is finite. Let G be a simply connected, semisimple algebraic group of Chevalley type over k. Then the Tits system (G_k, B, N_k) in §2 satisfies the assumption made above relative to the commensurability of B with its conjugates. More precisely, for $\sigma \in W$, $B\sigma B$ contains $q^{\lambda(\sigma)}$ cosets of the form Bx, where q is the cardinality of the residue class field κ. In particular, all q_i's in the above theorem are equal to q in this case. Furthermore, the order of any $w_i w_j$ is always finite. [Especially, if G is SL_2, then it is seen (this is due to Oscar Goldman) that $\mathscr{H}_{\boldsymbol{Q}}(G_k, B) \cong \boldsymbol{Q}[\tilde{W}]$, where $\tilde{W}$ is the affine Weyl group of SL_2. (Note that $\tilde{W}$ is isomorphic with the free product of two copies of $\boldsymbol{Z}_2$ (= cyclic group of order 2).)

In this case, $G_{\mathfrak{O}}$ is also commensurable with any of its conjugate in G_k. Moreover, one can show that the Hecke ring $\mathscr{H}(G_k, G_{\mathfrak{O}})$ is commutative and is isomorphic with the polynomial ring in l variables over $\boldsymbol{Z}$ (l being the rank of G) (see **[1]**, **[11]**, **[12]**). We note the following formula for the number of cosets of the form $G_{\mathfrak{O}} \cdot x$ in $G_{\mathfrak{O}} \cdot h(\chi) \cdot G_{\mathfrak{O}}$ (with $h(\chi) \in A_k^+$). We may assume that $\chi(\lambda) = \pi^{(d,\lambda)}$ for some $d \in D = P^\perp = \{x \in \langle \Phi \rangle_{\boldsymbol{R}}; (x, P) \subset \boldsymbol{Z}\}$. Then the number $\#$ desired is given by

$$\# = q^{\varepsilon(d)} \sum_{\sigma \in W_d^1} q^{\lambda(\sigma)},$$

where (regarding $D \subset \tilde{W}$ as in §2),

$$\begin{aligned} \varepsilon(d) &= \operatorname*{Min}_{w \in W} \lambda(dw) \\ &= \sum_{\alpha \in \Phi_+;\, (\alpha,d) > 0} |(d,\alpha) - 1| + \sum_{\alpha \in \Phi_+;\, (\alpha,d) \leqq 0} |(d,\alpha)|, \end{aligned}$$

and W_d^1 is the following subset of W. Let W_d be the subgroup of W defined by $W_d = \{\sigma \in W; \sigma(d) = d\}$. Then W_d is generated by the $w_{\alpha_i,0}$ with $(\alpha_i, d) = 0$ ($\alpha_1, \cdots, \alpha_l$ being the simple roots). Now W_d^1 is defined by

$$W_d^1 = \{\sigma \in W; \lambda(w\sigma) \geqq \lambda(\sigma) \text{ for any } w \in W_d\}.$$

(See Kostant **[9]**.)

We note also that, if k is the quotient field of a principal ideal domain $\mathfrak{O}$, the Hecke ring $\mathscr{H}(G_k, G_{\mathfrak{O}})$ of a simply connected, semisimple algebraic group G of Chevalley type over k is isomorphic with the tensor product of the Hecke rings $\mathscr{H}(G_k, G_{\mathfrak{O}_\mathfrak{p}})$:

$$\mathscr{H}(G_k, G_{\mathfrak{O}}) \cong \otimes_{\mathfrak{p}} \mathscr{H}(G_k, G_{\mathfrak{O}_\mathfrak{p}}).$$

EXAMPLE 2. Let G be a *finite* group and (G, B, N) be a Tits system on G with the Weyl group W. Then one has

THEOREM (TITS). *Let k be an algebraically closed field whose characteristic does not divide the orders of G, W. Then $\mathscr{H}_k(G, B) \cong k[W]$.*

See the appendix for the proof.

Appendix: Proof After Tits of $\mathscr{H}_k(G, B) \cong k[W]$ for a Finite Tits System

1. **Rings obtained by a specialization.** Let A be an associative algebra over a commutative ring $\mathfrak{O}$. Let ϕ be a homomorphism of $\mathfrak{O}$ into a commutative ring $\mathfrak{O}'$. Then one has an $\mathfrak{O}$-module structure on $\mathfrak{O}'$ by $\alpha \cdot \beta = \phi(\alpha)\beta$ ($\alpha \in \mathfrak{O}, \beta \in \mathfrak{O}'$). Thus one may consider the tensor product

$$A_\phi = A \otimes_{\mathfrak{O}} \mathfrak{O}',$$

which has an obvious algebra-structure over $\mathfrak{O}'$. Note that if ϕ is surjective, then the homomorphism $\phi^* : A \to A_\phi$ defined by $\phi^*(a) = a \otimes 1$ is also surjective and $\operatorname{Ker}(\phi^*) = \operatorname{Ker}(\phi)$. Thus

$$A_\phi \cong A/A \cdot \operatorname{Ker}(\phi).$$

In particular, if A is a free $\mathfrak{O}$-module of finite rank with a basis $\{u_\lambda\}$, then A_ϕ is also a free $\mathfrak{O}'$-module with a basis $\{\phi^*(u_\lambda)\}$. The structure constants $\{C^\nu_{\lambda\mu}\}$ of A relative to $\{u_\lambda\}$ are mapped by ϕ into the structure constants $\{\phi(C^\nu_{\lambda\mu})\}$ of A_ϕ relative to $\{\phi^*(u_\lambda)\}$. Hence, Δ, Δ' being the discriminants of A, A_ϕ respectively, one has $\phi(\Delta) = \Delta'$.

For the special case where $\mathfrak{O}$ is a polynomial ring $k[t_1, t_2, \cdots t_r]$ over a field k and ϕ is the specialization $\mathfrak{O} \to k$ over k defined by $\phi(t_i) = \alpha_i$, we denote A_ϕ also by $A(\alpha_i)$ for brevity.

PROPOSITION 1. *Let $\mathfrak{O} = k[t_1, \cdots, t_r]$ be the polynomial ring over an algebraically closed field k. Suppose that A is an associative algebra over $\mathfrak{O}$ such that*

(i) *A is a free $\mathfrak{O}$-module of finite rank, and*

(ii) *the discriminant $\Delta(t_1, \cdots, t_r)$ of A (relative to a basis of A) is not zero. Then for any $(\alpha_i) \in k^r$, $(\beta_i) \in k^r$ such that $\Delta(\alpha_i) \neq 0$, $\Delta(\beta_i) \neq 0$, one has $A(\alpha_i) \cong A(\beta_i)$ as k-algebra.*

For the proof, we note that $A(\alpha_i)$ is separable, semisimple and refer to Gerstenhaber [14]. Also we note that an elementary proof is possible for this particular case. In fact, Ω being the algebraic closure of the quotient field of $\mathfrak{O}$, one gets the following isomorphism as Ω-algebra

$$A \otimes_{\mathfrak{O}} \Omega \cong A(\alpha_i) \otimes_k \Omega.$$

2. **An algebra associated with a Coxeter group.** By Proposition 1 above, in order to prove $\mathscr{H}_k(G, B) \cong k[W]$, it is enough to show the existence of an algebra A over some polynomial ring $\mathfrak{O} = k[t_1, \cdots, t_r]$ with above conditions and the existence of two points $(\alpha_i) \in k^r$, $(\beta_i) \in k^r$ such that

$$\Delta(\alpha_i) \neq 0,\ \Delta(\beta_i) \neq 0,\ A(\alpha_i) \cong \mathscr{H}_k(G, B),\ A(\beta_i) \cong k[W].$$

Now such an algebra was constructed by Tits as follows.

Let W be an Coxeter group with a fundamental generating involution $R = \{r\}$, i.e., the defining relations for R are obtained by $(rs)^{n_{rs}} = 1$ (n_{rs} being the order of

rs for all r and s in R; $n_{rr} = 1$). Denote by $l(w)$ the length of $w \in W$ relative to R. Then

LEMMA 1. *If $r, s \in R$ and $w \in W$ satisfy $l(rws) = l(w)$, $l(rw) = l(ws)$, then $s = w^{-1}rw$.*

Now let k be any commutative ring. Let C be the set of conjugacy classes represented by elements in R, and let $\{u_c, v_c; c \in C\}$ be indeterminates over k. We write also u_r, v_r for u_c, v_c for r in c. Denote by $\mathfrak{O}$ the polynomial ring

$$k[u_c, v_c; c \in C].$$

PROPOSITION 1. *Let V be the free $\mathfrak{O}$-module spanned by W. Then there exists a K-bilinear, associative multiplication $*$ in V such that*

$$\begin{aligned} r*w &= rw \qquad \text{if } l(rw) > l(w), \\ &= u_r rw + v_r w, \qquad \text{if } l(rw) < l(w). \end{aligned}$$

Moreover, such a multiplication is unique.

PROOF. Uniqueness is obvious. Let us prove the existence. Define

$$P_r, \lambda_r \in \mathrm{End}_{\mathfrak{O}}(V) \qquad (r \in R)$$

as follows:

$$\begin{aligned} P_r(w) &= rw & &\text{if } l(rw) > l(w), \\ &= u_r rw + v_r w, & &\text{if } l(rw) < l(w), \\ \lambda_r(w) &= wr & &\text{if } l(rw) > l(w), \\ &= u_r wr + v_r w, & &\text{if } l(rw) < l(w). \end{aligned}$$

Then, using Lemma 1, one can check $P_r\lambda_s = \lambda_s P_r$ for any $r, s \in R$. Let $\mathfrak{R}$ (resp. $\mathfrak{L}$) be the $\mathfrak{O}$-subalgebras of $\mathrm{End}_{\mathfrak{O}}(V)$ generated by $\{P_r; r \in R\}$ (resp. by $\{\lambda_r; r \in R\}$). It is seen that the mappings $\rho^*: \mathfrak{R} \to V$, $\lambda^*: \mathfrak{L} \to V$ defined by $\rho^*(\phi) = \phi(1)$ $(\phi \in \mathfrak{R})$, $\lambda^*(\psi) = \psi(1)$ $(\psi \in \mathfrak{L})$ are both bijective.

In fact, for any reduced expression $w = r_1 \cdots r_n$, one has

$$\rho^*(\rho_{r_1} \cdots \rho_{r_n}) = w.$$

Thus ρ^* is surjective. Same is true for λ^*. Injectivity of ρ^* is seen as follows from the commutativity of P_r, λ_s above: let $\rho^*(\phi) = 0$. Then $\phi(1) = 0$. Hence

$$0 = \psi(\phi(1)) = \phi(\psi(1))$$

for all $\psi \in \mathfrak{L}$. Hence $\phi = 0$ by the surjectivity of λ^*.

Now define the product $v*v'(v, v' \in V)$ by

$$\begin{aligned} v*v' &= \rho^*\{\rho^{*-1}(v) \cdot \rho^{*-1}(v')\} \\ &= \{\rho^{*-1}(v)\}(v'). \end{aligned}$$

Then one sees that $*$ defines an algebra structure on V such that $r*w = P_r(w)$, which completes the proof.

Now let us return to the given Tits structure (G, B, W). We assume that k is an algebraically closed field whose characteristic does not divide the orders of G, W. Using above notations, one sees that the $\mathfrak{O}$-algebra $A = (V, *)$ associated to the Coxeter group W (cf. **[10]**) has the following properties:

(1) The discriminant $\Delta(u_c, v_c; c \in C)$ of A (note that this is a polynomial in the u_c, v_c) is not zero.

(2) By the specialization $u_c \to \alpha_c, v_c \to \beta_c$ $(c \in C; \alpha_c, \beta_c \in k)$, A gives rise to an algebra $A(\alpha_c, \beta_c)$ over k. In particular, by the theorem above one obtains

$A(q_c, q_c - 1) \cong \mathscr{H}_k(G, B)$ where q_c is the number of B-cosets in BrB, where $r \in c$,

$$A(1, 0) \cong k[W].$$

Note that $\mathscr{H}_k(G, B)$ and $k[W]$ are both semisimple algebras over k (cf. **[7]**). Thus, by our assumption on the characteristic of k, we get $\Delta(\alpha_i) \neq 0$, $\Delta(\beta_i) \neq 0$ for $(\alpha_i) = (q_c, q_c - 1)$, $(\beta_i) = (1, 0)$. This completes the proof.

References

1. F. Bruhat, *Sur une classe de sous-groupes compacts maximaux des groupes de Chevalley sur un corps* $\mathfrak{p}$*-adique*, Publ. Math., I.H.E.S., No. 23 (1964), 46–74.

2. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. **7** (1955), 14–66.

3. C. Chevalley, *Classification des groupes de Lie algébriques*, Séminaire E.N.S., Paris, 1956–1958.

4. O. Goldman and N. Iwahori, *On the structure of Hecke rings associated to general linear groups over* $\mathfrak{p}$*-adic fields* (unpublished).

5. H. Hijikata, *Maximal compact subgroups of some* $\mathfrak{p}$*-adic classical groups*, Mimeographed Notes from Yale University, (1964).

6. ———, *On arithmetic of* $\mathfrak{p}$*-adic Steinberg groups*, Mimeographed Notes from Yale University, 1964.

7. N. Iwahori, *On the structure of a Hecke ring of a Chevalley group over a finite field*, J. Fac. of Sci. Univ. Tokyo **10** (1964), 215–236.

8. N. Iwahori and H. Matsumoto, *On some Bruhat decomposition and the structure of the Hecke rings of the* $\mathfrak{p}$*-adic Chevalley groups*, Publ. Math., I.H.E.S., No. 25 (1965), 5–48.

9. B. Kostant, *Lie algebra cohomology and the generalized Borel–Weil theorem*, Ann. of Math. **74** (1961), 328–380.

10. H. Matsumoto, *Générateurs et relations des groupes de Weyl généralisés*, C. R. Paris **258** (1964), 3419–3422.

11. I. Satake, *Theory of spherical functions on reductive algebraic groups over* $\mathfrak{p}$*-adic fields*, Publ. Math., I.H.E.S., No. 18 (1964), 5–69.

12. T. Tamagawa, *On the* ζ*-functions of a division algebra*, Ann. of Math. **77** (1963), 387–405.

13. J. Tits, *Théorème de Bruhat et sous-groupes paraboliques*, C. R. Paris **254** (1962), 2910–2912.

14. M. Gerstenhaber, *On the deformation of rings and algebras*, Ann. of Math. **79** (1964), 59–103.

On Rational Points on Projective Varieties Defined Over a Complete Valuation Field[1]

BY

TSUNEO TAMAGAWA

1. Let k be a field with a nonarchimedean valuation $|\ |$, k^{n+1} denote the vector space over k of all $(n+1)$-tuples of elements of k and $\boldsymbol{P}_k^n$ denote the projective space of all one-dimensional subspaces of k^{n+1}. The one-dimensional subspace spanned by $x \in k^{n+1}$ will be denoted by $\langle x \rangle$. The norm of $x = (x_0, \cdots, x_n)$ is defined by $\|x\| = \mathrm{Max}(|x_0|, \cdots, |x_n|)$. Let $f(X_0, \cdots, X_n)$ be a homogeneous polynomial of degree d in k. Then the value $\|x\|^{-d}|f(x)|$ is uniquely determined by the point $P = \langle x \rangle \in \boldsymbol{P}_k^n$, so we denote it by $|f(P)|$. If $f(x) = 0$, we simply write $f(P) = 0$. The norm $\|f\|$ of a polynomial $f(X_0, \cdots, X_n) = \sum c_{i0} \cdots {}_{in} X_0^{i_1} \cdots X_n^{i_n}$ is defined by $\|f\| = \mathrm{Max}(|c_{i0} \cdots {}_{in}|)$. Obviously we have $|f(P)| \leqq \|f\|$ for all $P \in \boldsymbol{P}_k^n$. A set of homogeneous polynomials $f_1, \cdots, f_N$ in k will be called a zero set if we have

$$M(f_1, \cdots, f_N) = \mathrm{Inf}_{P \in \boldsymbol{P}_k^n} \mathrm{Max}(|f_1(P)|, \cdots, |f_N(P)|) = 0.$$

Let Ω be a universal domain containing k. Namely Ω is an algebraically closed field containing k such that there exist infinitely many elements in Ω which are algebraically independent over k. We denote the projective space $\boldsymbol{P}_\Omega^n$ by $\boldsymbol{P}^n$.

We will prove the following theorems:

THEOREM 1. *Assume that k is complete and perfect. If a set $\{f_1, \cdots, f_N\}$ of homogeneous polynomials $f_1, \cdots, f_N$ in k is a zero set, then there exists a point $P_0 \in \boldsymbol{P}_k^n$ such that $f_1(P_0) = 0, \cdots, f_N(P_0) = 0$.*

THEOREM 2. *Assume that k is complete and perfect. Let $V \subset \boldsymbol{P}^n$ be a variety defined over k, and V_k denote the set of all k-rational points on V. Let ϕ be a rational function on V defined over k. If ϕ is defined at all points of V_k, then $|\phi(P)|$ is bounded on V_k.*

An immediate consequence of Theorem 2 is the following:

THEOREM 3. *Assume that k is complete and perfect. Let G be a reductive algebraic group defined over k such that there is no subtorus of G which splits over k. Then the group G_k of all k-rational elements of G is bounded.*

[1] This work is partly supported by NSF Contract No. 4428.