Tôhoku Math. Journ.
21(1969), 474-494

CHEVALLEY GROUPS OVER LOCAL RINGS

EIICHI ABE

Dedicated to Professor Tadao Tannaka on his 60th birthday

(Received April 8, 1969)

Introduction.

0.1. Let G_C be a connected complex semi-simple Lie group. Following Chevalley (cf. [2] and [3]), we have a uniquely determined affine group scheme (i.e. a representable covariant functor G from the category of commutative rings with a unit into the category of groups) such that

(1) $G(C)$ is a connected complex semi-simple Lie group isomorphic to G_C, where C is the field of complex numbers.

(2) For any algebraically closed field k, $G(k)$ is a connected semi-simple algebraic group defined and split over the prime field of k and its type is the same with that of G_C.

We call G the Chevalley-Demazure group scheme associated with G_C and we shall say that G is simple, of rank r or simply connected if the Lie group G_C is so. In Section 1, we shall introduce briefly the definition of G.

0.2. Let R be a commutative ring with a unit, $\mathfrak{a}$ be an ideal of R, f: $R \rightarrow R/\mathfrak{a}$ be the natural homomorphism. Then, there is a group homomorphism $G(f): G(R) \rightarrow G(R/\mathfrak{a})$. Denote by $G(R, \mathfrak{a})$ (resp. $G^*(R, \mathfrak{a})$) the kernel (resp. the inverse image of the center of $G(R/\mathfrak{a})$) of $G(f)$ and we call it the special (resp. general) congruence subgroup modulo $\mathfrak{a}$ of $G(R)$. Any subgroup N of $G(R)$ such that $G^*(R, \mathfrak{a}) \supseteqq N \supseteqq G(R, \mathfrak{a})$ for an ideal $\mathfrak{a}$ of R is a normal subgroup of $G(R)$. Such a normal subgroup of $G(R)$ we shall call a *congruence subgroup* of $G(R)$.

0.3. Now, let R be a local ring, $\mathfrak{m}$ be the maximal ideal and k be the residue class field $R/\mathfrak{m}$, p be the characteristic of k. W. Klingenberg has proved (cf. [5], [6]) that if $G=SL_{n+1}$ or Sp_{2n}, the only normal subgroups of $G(R)$ are the congruence subgroups provided that the characteristic of k is $\neq 2$

and $k \neq F_3$ for the groups $G = SL_2$ and $G = Sp_{2n}$. In this note, for a simple Chevalley-Demazure group scheme and a local ring R, we shall reduce the determination of the normal subgroups of $G(R)$ to the determination of certain submodules of R, except the following cases:

(a) G is of type A_1 and $p = 2$ or $k = F_3$

(b) G is of type B_2 or G_2 and $k = F_2$,

where F_q is the finite field with q elements. In particular, if G is simply connected, we have that the only normal subgroups are the congruence subgroups provided that the characteristic of k is $\neq 2$ (resp. $\neq 3$) if G is of type B_n, C_n or F_4 (resp. of type G_2). The main theorem is stated in Section 1 with the preliminary definitions. In Section 2, we give some basic properties of certain subgroups of $G(R)$ for our later use and, in Section 3, we prove a key proposition (2.17) and then prove our main theorem (1.9).

The author wishes to express his hearty thanks to Mr. H. Hijikata for his valuable advises.

1. Chevalley-Demazure group scheme, Statement of the main theorem. In this section, we shall introduce the Chevalley-Demazure group scheme associated with a connected complex semi-simple Lie group (cf. [2], [3]) and then state our main theorem.

1.1. Let G_C be a connected complex semi-simple Lie group, T_C a maximal torus of G_C. Denote by g_C, t_C the Lie algebras of G_C and T_C respectively. Let Δ be the system of roots of g_C with respect to t_C, $\Pi = \{\alpha_1, \cdots, \alpha_l\}$ be a fundamental root system of Δ, g_Z be a Chevalley lattice of g_C generated by $\{H_{\alpha_1}, \cdots, H_{\alpha_l}, X_\alpha, \alpha \in \Delta\}$. For each $\alpha \in \Delta$, the element $H_\alpha = [X_\alpha, X_{-\alpha}]$ is contained in the submodule $t_Z = g_Z \cap t_C$. We have

(1) $$\alpha(H_\alpha) = 2,$$

(2) if α, β are roots, then $\beta(H_\alpha) = \nu - \mu$, where ν, μ are non-negative integers such that $\beta + i\alpha$ is a root for each integer $-\nu \leqq i \leqq \mu$, or

(3) if α, β and $\alpha+\beta$ are roots, $[X_\alpha, X_\beta] = N_{\alpha\beta} X_{\alpha+\beta}$, where $N_{\alpha\beta} = \pm(\nu+1)$.

1.2. Let ρ be a faithful representation of G_C in an n-dimensional vector space V over C, $d\rho$ the differential of ρ which is a representation of g_C in V. Then, there exists a Z-free module V_Z generated by $\{v_1, \cdots, v_n\}$ in V such that

(4) $(m!)^{-1} d\rho(X_\alpha)^m V_Z \subset V_Z$ for all integers $m \geqq 0$ and all roots $\alpha \in \Delta$,

(5) $d\rho(H_\alpha) v_i = \Lambda_i(H_\alpha) v_i$, $\Lambda_i(H_\alpha) \in Z$, for all roots $\alpha \in \Delta$ and all i $(1 \leqq i \leqq n)$.

Such a module V_Z is called to be admissible (cf. [2] and [7]). The base $\{v_1, \cdots, v_n\}$ of V_Z determines the coordinates x_{ij} $(1 \leqq i, j \leqq n)$ on $GL(V)$ and the restrictions of x_{ij} to G_C generate a subring $Z[G]$ of the affine algebra $C[G]$ of G_C. The ring $Z[G]$ has a structure of a Hopf algebra and defines a group scheme G over Z. Namely,

$$R \longrightarrow G(R) = \mathrm{Hom}(Z[G], R)$$

is a covariant functor from the category of commutative rings with 1 into the category of groups. We shall call G the Chevalley-Demazure group scheme associated with G_C. In particular, if G_C is simply connected of type A_n (resp. of type C_n), then G is isomorphic to the functor SL_{n+1} (resp. $S_{p_{2n}}$).

1.3. For any $t \in C$, $x_\alpha(t) = \exp t\, d\rho(X_\alpha)$ is an element of G_C and the coordinates of $x_\alpha(t)$ are polynomial functions on t with coefficients in Z. Let $Z[\xi]$ be the algebra over Z generated by one variable ξ. Then we have a homomorphism of $Z[G]$ onto $Z[\xi]$ which assigns to each x_{ij} the (i, j)-coordinate of $x_\alpha(\xi)$. The homomorphism induces an injective homomorphism of groups

$$G_\alpha(R) = \mathrm{Hom}(Z[\xi], R) \longrightarrow G(R) = \mathrm{Hom}(Z[G], R).$$

We denote also by $x_\alpha(t)$, $t \in R$, the element of $G(R)$ corresponding to an element of $G_\alpha(R)$ such that $\xi \to t$.

1.4. Let P (resp. X, P_r) the additive group generated by the weights of all representations of G (resp. the weights of ρ, the roots of g_C). Then, these are free abelian groups of rank l such that $P \supseteqq X \supseteqq P_r$; X is generated by $\Lambda_1, \cdots, \Lambda_n$ over Z; if G is simply connected, then $P = X$. For any $\chi \in \mathrm{Hom}(X, C^*)$, $h(\chi) = \mathrm{diag}(\chi(\Lambda_1), \cdots, \chi(\Lambda_n))$ is an element of G_C. Let $Z[T]$ be the algebra generated by $\Lambda_1, \Lambda_1^{-1}, \cdots, \Lambda_n, \Lambda_n^{-1}$ over Z. Then, we have a homomorphism of $Z[G]$ onto $Z[T]$ which assigns to each x_{ij} the (i, j)-coordinate of $h(\chi)$. The homomorphism induces an injective homomorphism of groups

$$T(R) = \mathrm{Hom}(Z[T], R) \longrightarrow G(R) = \mathrm{Hom}(Z[G], R).$$

We denote by $h(\chi)$ the element of $G(R)$ corresponding to an element $\chi \in \mathrm{Hom}(Z[T], R)$.

1.5. DEFINITION. Let R be a commutative ring with 1 and G be a Chevalley-Demazure group scheme. We denote by $G_0(R)$ the subgroup of $G(R)$ generated by $x_\alpha(t)$ for all $t \in R$ and all $\alpha \in \Delta$ and by $h(\chi)$ for all $\chi \in \mathrm{Hom}(Z[T], R)$, and denote by $E(R)$ the subgroup of $G(R)$ generated by $x_\alpha(t)$

for all $t \in R$ and all $\alpha \in \Delta$. We know that if R is a field or the ring of integers of a field with a non-archimedean discrete valuation, then $G(R)=G_0(R)$. Further, if G is simple, simply connected of rank >1 and if R is a semi-local ring, then $G(R)=E(R)$ (cf. [8]). However, we don't know whether, in general, $G(R)=G_0(R)$ for a group scheme G (not necessarily simply connected) and a semi-local ring R. We shall show in Section 3 the following.

1.6. PROPOSITION. *Let G be a Chevalley-Demazure group scheme and R be a local ring, then $G(R)=G_0(R)$. In particular, if G is simply connected, then $G(R)=E(R)$.*

1.7. For a root $\alpha \in \Delta$, let $(\alpha,\alpha)=\sum_{\gamma\in\Delta}\gamma(H_\alpha)^2$. The length $\lambda(\alpha)$ of α is defined to be 1 if $(\alpha,\alpha)\leqq(\beta,\beta)$ for any root $\beta\in\Delta$, and is defined to be λ if $(\alpha,\alpha)/(\beta,\beta)=\lambda$ for some root β of length 1. If G is of type A_n $(n\geqq 1)$, D_n $(n\geqq 4)$ or E_n $(n=6, 7$ or $8)$, then $\lambda(\alpha)=1$ for all roots α; if G is of type B_n $(n\geqq 2)$, C_n $(n\geqq 2)$ or F_4 (resp. of type G_2), there are roots of lengths 1 and 2 (resp. 1 and 3).

1.8. DEFINITION. Let G be a simple Chevalley-Demazure group scheme. We call G is *of symplectic type* if G is of type C_n $(n\geqq 2)$ and simply connected. Let R be a commutative ring with 1, $\mathfrak{a}$ be an ideal of R and for a positive integer λ, $\mathfrak{a}_{(\lambda)}$ be the ideal of R generated by λa, a^λ for all $a\in\mathfrak{a}$. We shall call *a special submodule associated* with $(G,\mathfrak{a})$ a submodule $\mathfrak{b}$ of R such that

(a) $\mathfrak{a}\supseteqq\mathfrak{b}\supseteqq\mathfrak{a}_{(\lambda)}$, where λ is the length of the long root in Δ,

(b) if G is of symplectic type, $r^2b\in\mathfrak{b}$ for any $r\in R$ and $b\in\mathfrak{b}$,

(b′) if G is not of symplectic type, $\mathfrak{b}$ is an ideal of R.

For convenience, we shall denote $\mathfrak{a}$ (resp. $\mathfrak{b}$) by $\mathfrak{a}_1$ (resp. $\mathfrak{a}_\lambda$). Thus, by our notation, for an element $x_\alpha(t)$ of $G(R)$, $t\in\mathfrak{a}_{\lambda(\alpha)}$ means that $t\in\mathfrak{a}$ or $\mathfrak{b}$ according as $\lambda(\alpha)=1$ or λ. Now, we shall define certain subgroups of $G(R)$. $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ is the normal subgroup of $E(R)$ generated by $x_\alpha(t)$ for all roots α and $t\in\mathfrak{a}_{\lambda(\alpha)}$; $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ is the normal subgroup of $G(R)$ consisting of the elements x of $G(R)$ such that $(x,G(R))\subseteqq E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, where for any subsets A, B of $G(R)$, (A,B) is the subgroup of $G(R)$ generated by $a^{-1}b^{-1}ab$ for $a\in A$, $b\in B$. In particular, if $\mathfrak{a}_1=\mathfrak{a}_\lambda$, we denote $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ (resp. $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$) by $E(R,\mathfrak{a}_1)$ (resp. $E^*(R,\mathfrak{a}_1)$) and if $\mathfrak{a}_1=\mathfrak{a}_\lambda=R$, by definition $E(R,\mathfrak{a}_1)=E(R)$. Then, our main theorem is the following which is proved in Section 3.

1. 9. THEOREM. *Let G be a simple Chevalley-Demazure group scheme. Let R be a local ring, $\mathfrak{m}$ be the maximal ideal of R, $k=R/\mathfrak{m}$ be the residue class field, p be the characteristic of k. Assume that if G is of type A_1 then $p\neq 2$ and $k\neq F_3$ and if G is of type B_2 or G_2 then $k\neq F_2$. Let N be a subgroup of $G(R)$ normalized by $E(R)$. Then N is normal and there exist uniquely determined ideal $\mathfrak{a}$ of R and a special submodule $\mathfrak{b}$ associated with $(G, \mathfrak{a})$ such that*

$$E^*(R, \mathfrak{a}, \mathfrak{b}) \supseteqq N \supseteqq E(R, \mathfrak{a}, \mathfrak{b}).$$

1. 10. COROLLARY. *Under the same conditions as* (1. 9), *if, in particular, G is simply connected, then $G(R, \mathfrak{a})=E(R, \mathfrak{a})$ for any ideal $\mathfrak{a}$ of R.*

1. 11. COROLLARY. *Under the same conditions as* (1. 9), *if, in particular, G is simply connected and the characteristic p of k is different from the length λ of the long root, then, for any normal subgroup N of $G(R)$, there exists an ideal $\mathfrak{a}$ of R such that*

$$G^*(R, \mathfrak{a}) \supseteqq N \supseteqq G(R, \mathfrak{a}).$$

2. Certain subgroups of $G(R)$. In this section, we shall deal with the structure of certain subgroups of $G(R)$. We assume that R is a local ring and G is simple. Notations and definitions are the same as those in the previous sections.

2. 1. DEFINITION. $U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ (resp. $V(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$) is the subgroup of $G(R)$ generated by $x_\alpha(t)$, $t\in\mathfrak{a}_{\lambda(\alpha)}$ for all positive (resp. negative) roots $\alpha\in\Delta$. In particular, if $\mathfrak{a}_1=\mathfrak{a}_\lambda$, we denote it by $U(R, \mathfrak{a}_1)$ (resp. $V(R,\mathfrak{a}_1)$), and if $\mathfrak{a}_1=\mathfrak{a}_\lambda=R$, we denote it by $U(R)$ (resp. $V(R)$). Note that U and V are subgroup schemes of G. $T(R)$ is the subgroup of $G(R)$ consisting of all $h(\chi)$ for all $\chi\in\mathrm{Hom}(Z[T], R)$ which is isomorphic to $\mathrm{Hom}(Z[T], R)$ the direct product of l copies of $G_m(R)$. $T'(R)$ is the subgroup of $T(R)$ generated by $h(\chi_{\alpha,u})$ for all roots $\alpha\in\Delta$ and $u\in R^*$ (the group of units of R) where $\chi_{\alpha,u}(\Lambda_i)=u^{\Lambda_i(H_\alpha)}$ $(1\leqq i\leqq n)$. $T(R, \mathfrak{a})$ is the subgroup of $T(R)$ generated by all $h(\chi)$ such that $\chi(\alpha)\equiv 1 \pmod{\mathfrak{a}}$ for all root α. Now, we denote by $T'(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ the subgroup of $T'(R)$ generated by $h(\chi_{\alpha,u})$ for all pairs (α, u) of $\alpha\in\Delta$ and $u\in R^*$ such that $u=1+st$ for $s\in R$ and $t\in\mathfrak{a}_{\lambda(\alpha)}$.

2. 2. As for the relations of generators for $G(R)$, we know the following (cf. [1], [3]).

(1) $$h(\chi_{\alpha,u})=x_{-\alpha}(u^{-1}-1)\,x_\alpha(1)\,x_{-\alpha}(u-1)\,x_\alpha(1)^{-1}x_\alpha(1-u^{-1}), \quad u\in R^*.$$

(2) $$h(\chi)\,x_\alpha(t)\,h(\chi)^{-1} = x_\alpha(\chi(\alpha)\,t)\,, \quad t \in R\,.$$

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

(3) $$\omega_\alpha x_\beta(t)\,\omega_\alpha^{-1} = x_{w_\alpha(\beta)}(\pm t)\,, \qquad t \in R\,,$$

where w_α is the reflection in the hyperplane orthogonal to α and it is an element of the Weyl group.

Let Δ^+ be the set of the positive roots. If Δ is of type A_2,

(4) $$\Delta^+ = \{\alpha, \beta, \alpha+\beta\};\ \lambda(\alpha) = \lambda(\beta) = \lambda(\alpha+\beta) = 1$$

and we have

(5) $$(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(\pm tu) \qquad \text{for any} \quad t, u \in R\,.$$

If Δ is of type B_2,

(6) $$\Delta^+ = \{\alpha, \beta, \alpha+\beta, 2\alpha+\beta\};\ \lambda(\alpha) = \lambda(\alpha+\beta) = 1,\ \lambda(\beta) = \lambda(2\alpha+\beta) = 2$$

and we have

(7) $$(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(\pm tu)\,x_{2\alpha+\beta}(\pm t^2 u)$$

(8) $$(x_\alpha(t), x_{\alpha+\beta}(u)) = x_{2\alpha+\beta}(\pm 2tu) \qquad \text{for any} \quad t, u \in R\,.$$

If Δ is of type G_2,

(9) $$\Delta^+ = \{\alpha, \beta, \alpha+\beta, 3\alpha+\beta, 3\alpha+2\beta\};$$
$$\lambda(\alpha) = \lambda(\alpha+\beta) = \lambda(2\alpha+\beta) = 1,\ \lambda(\beta) = \lambda(3\alpha+\beta) = \lambda(3\alpha+2\beta) = 3$$

and we have

(10) $$(x_\alpha(t), x_\beta(u)) = x_{\alpha+\beta}(\pm tu)\,x_{2\alpha+\beta}(\pm t^2 u)\,x_{3\alpha+\beta}(\pm t^3 u)\,x_{3\alpha+2\beta}(\pm t^3 u^2)\,,$$

(11) $$(x_{\alpha+\beta}(t), x_\alpha(u)) = x_{2\alpha+\beta}(\pm 2tu)\,x_{3\alpha+\beta}(\pm 3tu^2)\,x_{3\alpha+2\beta}(\pm 3t^2 u)\,,$$

(12) $$(x_{\alpha+\beta}(t), x_{2\alpha+\beta}(u)) = x_{3\alpha+2\beta}(\pm 3tu) \qquad \text{for any} \quad t, u \in R\,.$$

Now, we prove the following.

2.3. PROPOSITION. *For any ideal* $\mathfrak{a}$ *of* R, *denote by* $E_1(R, \mathfrak{a})$ (*resp.* $E_\lambda(R, \mathfrak{a})$) *the normal subgroup of* $E(R)$ *generated by* $x_\alpha(t)$, $t \in \mathfrak{a}$, *for all roots*

α such that $\lambda(\alpha)=1$ resp. $\lambda(\alpha)=\lambda$). Then

$$E(R, \mathfrak{a}, \mathfrak{b}) = E_1(R, \mathfrak{a})$$

for any special submodule $\mathfrak{b}$ associated with $(G, \mathfrak{a})$

PROOF. Since the Weyl group W is generated by w_α, $\alpha \in \Delta$ and W is transitive on the set of roots of the same length, from (3), it is sufficient to show that $x_\beta(t) \in E_1(R,\mathfrak{a})$ for some root β of length λ and for all $t \in \mathfrak{a}$. Therefore, no loss of generality, we may assume that G is of type B_2 or G_2. First, let G be of type B_2, and let Δ^+ be the roots (6). From (7) and (8), we have that $x_{2\alpha+\beta}(\pm t^2 u)$ and $x_{2\alpha+\beta}(\pm 2tu)$ are in $E_1(R, \mathfrak{a})$ for all $t \in \mathfrak{a}$ and $u \in R$. Thus, by definition, we have $E(R, \mathfrak{a}, \mathfrak{b}) = E_1(R, \mathfrak{a})$. Secondly, let G be of type G_2 and let Δ^+ be the roots (9).

From (10) and (11) we have $z = x_{3\alpha+\beta}(\pm t^3 u) x_{3\alpha+2\beta}(\pm t^3 u^2)$ and $x_{3\alpha+2\beta}(\pm 3tu)$ are in $E_1(R,\mathfrak{a})$ for all $t \in \mathfrak{a}$ and $u \in R$. Further, $(x_\beta(1), z) = x_{3\alpha+2\beta}(\pm t^3 u) \in E_1(R, \mathfrak{a})$ for all $t \in \mathfrak{a}$, and $u \in R$. Thus by definition, we have $E(R,\mathfrak{a},\mathfrak{b}) = E_1(R, \mathfrak{a})$. q.e.d.

2.4. PROPOSITION. *Under the same notation as in* (2.3),

(i) *If $p \neq \lambda$, then $E_1(R, \mathfrak{a}) = E(R, \mathfrak{a}) = E(R, \mathfrak{a}, \mathfrak{b})$.*

(ii) *$E_\lambda(R, \mathfrak{a}) = E(R, \mathfrak{a})$ provided that, if G is of type G_2, $k \neq F_2$.*

PROOF. It suffices to prove for the groups of type B_2 and G_2.

(i) Let Δ^+ be the positive roots (6) of type B_2. Since $p \neq 2$, 2 is a unit. (8) for $t = 2^{-1}$ and $u \in \mathfrak{a}$ shows that $x_{2\alpha+\beta}(\pm u) \in E_1(R, \mathfrak{a})$. Now, let Δ^+ be the positive roots (9) of type G_2. Since $p \neq 3$, 3 is a unit. (12) for $t = 3^{-1}$ and $u \in \mathfrak{a}$ shows that $x_{3\alpha+2\beta}(\pm u) \in E_1(R, \mathfrak{a})$.

(ii) Let Δ^+ be the positive roots (6) of type B_2. Then from (8) for $t=1$ and $u \in \mathfrak{a}$, we have $x_{\alpha+\beta}(u) \in E_\lambda(R, \mathfrak{a})$. Now, let Δ^+ be the positive roots (9) of type G_2. Then from (10) for $t=1$ and $u \in \mathfrak{a}$, we have $z = x_{\alpha+\beta}(\pm u) x_{2\alpha+\beta}(\pm u^2) \in E_\lambda(R, \mathfrak{a})$ and $z = \omega_\beta z \omega_\beta^{-1} = x_\alpha(\pm u) x_{2\alpha+\beta}(\pm u^2) \in E_\lambda(R, \mathfrak{a})$. Since $k \neq F_2$, there exists an element χ of $\mathrm{Hom}(Z[T], R)$ such that $\chi(\alpha) = 1$ and $\chi(\beta) = v$ where v and $v-1$ are units of R. Then $h(\chi) z' h(\chi)^{-1} = x^\alpha(\pm u) x_{2\alpha+\beta}(\pm v u^2) \in E_\lambda(R, \mathfrak{a})$. Therefore, $z'^{-1} h(\chi) z' h(\chi)^{-1} = x_{2\alpha+\beta}(\pm(v-1)u^2) \in E_\lambda(R, \mathfrak{a})$. This shows $x_{2\alpha+\beta}(u^2) \in E_\lambda(R, \mathfrak{a})$ and we have also $x_\alpha(u) \in E_\lambda(R, \mathfrak{a})$. q. e. d.

2.5. PROPOSITION. *Each element of $U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ is expressible in the form*

$$x_{\beta_1}(s_1) x_{\beta_2}(s_2) x_{\beta_3}(s_3) \cdots\cdots x_{\beta_N}(s_N)$$

where $s_i \in \mathfrak{a}_{\lambda(\beta_i)} (1 \leqq i \leqq N)$ and $\beta_1, \beta_2, \cdots, \beta_N$ are the positive roots of Δ, the *ordering of the roots is arbitrary chosen and fixed once for all.*

Let U' be the set of elements expressible in the form as stated in the proposition. We call the order of the positive roots (or the negative roots) is regular if the heigt $h(\alpha)=\sum_{i=1}^{l} m_i$ of $\alpha=\sum_{i=1}^{l} m_i d_i$ is an increasing function of α. First, we prove the following lemma.

2.6. LEMMA. *Let α, β be two positive roots. For any elements $x_\alpha(t)\in E(R)$ and $x_\beta(u)\in U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$, the commutator $(x_\alpha(t), x_\beta(u))$ is an element of U' which is expressible by the product of $x_\gamma(s)$ for roots $\gamma>\alpha, \beta$, by a regular order.*

PROOF. If $\alpha+\beta\notin\Delta$, then $(x_\alpha(t), x_\beta(u))=1$ and the lemma is trivial. We assume that $\alpha+\beta\in\Delta$. Let Δ_2 be a subsystem of roots in Δ of rank 2 consisting of the roots $i\alpha+j\beta$, $i, j\in Z$.

(i) If $\alpha-\beta\notin\Delta$, $\{\alpha, \beta\}$ is a fundamental system of roots of Δ_2. When Δ_2 is of type A_2, we have $(x_\alpha(t), x_\beta(u))=x_{\alpha+\beta}(\pm tu)$. If $u\in\mathfrak{a}_{\lambda(\beta)}$ then tu is also an element of $\mathfrak{a}_{\lambda(\beta)}$. When Δ_2 is of type B_2, we have $(x_\alpha(t), x_\beta(u))=x_{\alpha+\beta}(\pm tu)x_{2\alpha+\beta}(\pm t^2u)$ or $x_{\alpha+\beta}(\pm tu)x_{\alpha+2\beta}(\pm tu^2)$ according as $\lambda(\alpha)=1$ or 2. If $\lambda(\beta)=1$ (resp. $=2$), then $tu\in\mathfrak{a}$ and $t^2u\in\mathfrak{a}_2$ (resp. $tu^2\in\mathfrak{a}_2$). Finally, when Δ_2 is of type G_2, $(x_\alpha(t), x_\beta(u))=x_{\alpha+\beta}(\pm tu)x_{2\alpha+\beta}(\pm t^2u)x_{3\alpha+\beta}(\pm t^3u)x_{3\alpha+2\beta}(\pm t^3u^2)$ or $=x_{\alpha+\beta}(\pm tu)x_{\alpha+2\beta}(\pm tu^2)x_{\alpha+3\beta}(\pm tu^3)x_{2\alpha+3\beta}(\pm t^2u^3)$ according as $\lambda(\alpha)=1$ or 3. If $\lambda(\beta)=1$ (resp. $=3$), then tu, $tu^2\in\mathfrak{a}_1$ and tu^3, $t^2u^3\in\mathfrak{a}_3$(resp. $t^3u, t^3u^2\in\mathfrak{a}_3$), for $\mathfrak{a}_1$ and $\mathfrak{a}_3$ are ideals of R.

(ii) If $\alpha-\beta=\gamma\in\Delta$ and $\alpha-2\beta\notin\Delta$, then $\{\beta, \gamma\}$ is a fundamental root system of Δ_2 which is of type B_2 or G_2. When Δ_2 is of type B_2, we have $\alpha=\gamma+\beta$, $\alpha+\beta=\gamma+2\beta$ and $\lambda(\alpha)=\lambda(\beta)=1$, $\lambda(\alpha+\beta)=\lambda(\gamma)=2$. Thus, $(x_\alpha(t), x_\beta(u))=x_{\alpha+\beta}(\pm 2tu)$. If $u\in\mathfrak{a}_1$, then $2tu\in\mathfrak{a}_2$. When Δ_2 is of type G_2, we have $\alpha=\gamma+\beta$, $\alpha+\beta=\gamma+2\beta$ and $\lambda(\beta)=\lambda(\alpha)=\lambda(\alpha+\beta)=1$, $\lambda(\gamma)=\lambda(\alpha+2\beta)=\lambda(2\alpha+\beta)=3$. Thus, $(x_\alpha(t),x_\beta(u))=x_{\alpha+\beta}(\pm 2tu)x_{\alpha+2\beta}(\pm 3tu^2)x_{2\alpha+\beta}(\pm 3t^2u)$. If $u\in\mathfrak{a}_1$, then $2tu\in\mathfrak{a}_1$, $3tu^2\in\mathfrak{a}_3$ and $3t^2u\in\mathfrak{a}_3$.

(iii) If $\alpha-2\beta=\gamma\in\Delta$ and, $\alpha-3\beta\notin\Delta$, then $\{\beta, \gamma\}$ is a fundamental root system of Δ_2 which is of type G_2. We have $\alpha=\gamma+2\beta$, $\alpha+\beta=\gamma+3\beta$ and $\lambda(\alpha)=\lambda(\beta)=1$, $\lambda(\alpha+\beta)=3$. Thus $(x_\alpha(t), x_\beta(u))=x_{\alpha+\beta}(\pm 3tu)$. If $u\in\mathfrak{a}_1$, then $3tu\in\mathfrak{a}_3$. q. e. d.

2.7. PROOF OF (2.5). We shall show that U' is a subgroup of $G(R)$. This proves that $U'=U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. It suffices to prove that $x_\alpha(t)x\in U'$ for any $x_\alpha(t)\in U$ and $x\in U'$. We claim this by induction on a regular order of the roots α. If α is the highest root then $x_\alpha(t)=xx_\alpha(t)$ and the assertion is trivial. Assume that $x_\alpha(t)x\in U'$ for any $x_\alpha(t)$ and $x\in U'$ such that $\alpha>\beta$. We must show that $x_\beta(t)x\in U'$ for any $t\in\mathfrak{a}_{\lambda(\beta)}$ and $x\in U'$. Let $x_i=x_{\beta_i}(s_i)x_{\beta_{i+1}}(s_{i+1})\cdots$

$x_{\beta_N}(s_N)$ be an element of U'. Then $x_\beta(t)x_N \in U'$ is trivial by (2.6). Now assume $x_{\beta_j}(t)u_k \in U'$ for any $u_k(k>i)$ and we show that $x_\beta(t)x_i \in U'$. If $\beta \neq \beta_j$ for any $i \leqq j \leqq N$, then this is trivial. Therefore, we may assume that $\beta = \beta_j$ for some $j > i$. From (2.6), we have

$$x_{\beta_j}(t)x_i = x_{\beta_j}(t)x_{\beta_i}(s_i)x_{i+1} = x_{\beta_i}(s_i)x_{\beta_j}(s_j)zx_{i+1}$$

where z is an element of U' expressible by a product of $x_\alpha(t) \in U'$ for $\alpha > \beta$. Further, by our assumption, $x_{\beta_j}(s_j)zx_{i+1} \in U'$. Thus, we have proved $x_{\beta_j}(t)x_i \in U'$. q. e. d.

2. 8. PROPOSITION. *If $\mathfrak{a}_1$ is a proper ideal of R and $\mathfrak{a}_\lambda$ is a special submodule associated with $(G, \mathfrak{a}_1)$, then*

(13) $$E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) = U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)T'(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)V(R, \mathfrak{a}_1, \mathfrak{a}_\lambda).$$

First, we prove some lemmas.

2. 9. LEMMA. *For any root α and a unit element u of R, there exists $h(\chi) \in T'(R)$ such that $\chi(\alpha) = u^2$. Further, let Δ be of rank>1, then there exists $h(\chi) \in T'(R)$ such that $\chi(\alpha) = u$ if and only if G is not of symplectic type or $\lambda(\alpha) = 1$.*

PROOF. Since $\chi_{\alpha,u}(\alpha) = u^2$, the first assertion is trivial. If $X = P_r$, the second assertion is also trivial. We may assume that α is in $\Pi = \{\alpha_1, \cdots \alpha_l\}$, say $\alpha = \alpha_1$ and let α_2 be not orthogonal to α_1. If $\Delta_2 = \{\alpha_1, \alpha_2\}$ is of type G_2, then $\Delta = \Delta_2$ and the lemma holds from $P = X = P_r$. If Δ_2 is of type A_2(resp. of type B_2 and $\lambda(\alpha_1) = 1$), then $\chi = \chi_{\alpha,u^{-1}}$ (resp. $= \chi_{\alpha_1,u}\chi_{\alpha_2,u}$) has the value u at α. Thus, we can find $h(\chi) \in T'(R)$ such that $\chi(\alpha) = u$ except the case G is of symplectic type and $\lambda(\alpha) = 2$. q. e. d.

2. 10. COROLLARY. *If $\mathfrak{a}_1$ is a proper ideal and $x_\alpha(t) \in E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$, then $h(\chi)x_\alpha(t)h(\chi)^{-1} \in E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ for any $h(\chi) \in T(R)$.*

PROOF. This follows from (2) and the above lemma.

2. 11. LEMMA. *Let Δ be of rank>1 and $\mathfrak{a}_1$ be proper. If $u = 1 + st$ where $s \in R$ and $t \in \mathfrak{a}_{\lambda(\alpha)}$, then $\chi_{\alpha,u}(\beta) \equiv 1 (mod\ \mathfrak{a}_1)$ for any root β such that $\lambda(\beta) = 1$ and $\chi_{\alpha,u}(\beta) \equiv 1 (mod\ \mathfrak{a}_{(\lambda)})$ for any root β such that $\lambda(\beta) = \lambda$.*

PROOF. Note that $\chi_{\alpha,u}(\beta) = (1+st)^{\beta(H_\alpha)}$ where $t \in \mathfrak{a}_{\lambda(\alpha)}$. If $\lambda(\beta) = 1$, then $\mathfrak{a}_{\lambda(\beta)} = \mathfrak{a}_1$ is an ideal such that $\supsetneqq \mathfrak{a}_{\lambda(\alpha)}$. Therefore, the assertion is trivial. If

$\lambda(\beta)=\lambda$ and $\lambda(\alpha)=1$, then we have $\chi_{\alpha,u}(\beta)=(1+st)^{\pm\lambda}\equiv 1(\mathrm{mod}\ \mathfrak{a}_{(\lambda)})$. Finally, let $\lambda(\beta)=\lambda(\alpha)=\lambda$. If G is not of symplectic type, then the assertion follows from the fact that $\mathfrak{a}_{\lambda(\alpha)}=\mathfrak{a}_{\lambda(\beta)}$ is an ideal of R. If G is of symplectic type, then we have $\beta(H_\alpha)=2$ or 0 according as $\alpha=\beta$ or $\alpha\neq\beta$. Therefore, we have also $\chi_{\alpha,u}(\beta)\equiv 1(\mathrm{mod}\ \mathfrak{a}_{(\lambda)})$. q. e. d.

2.12. COROLLARY. *If $\mathfrak{a}_1$ is a proper ideal and $h(\chi)\in T(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, then $x_\alpha(s)h(\chi)x_\alpha(s)^{-1}\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ for any $x_\alpha(s)\in E(R)$.*

PROOF. This follows from the relation $x_\alpha(s)h(\chi)x_\alpha(s)^{-1}=x_\alpha((1-\chi(\alpha))s)h(\chi)$ (cf. (2)) and the above lemma.

2.13. LEMMA. *If $\mathfrak{a}_1$ is a proper ideal and $x_\alpha(t)\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, then*

$$x_{-\alpha}(s)x_\alpha(t)x_{-\alpha}(s)^{-1}=x_\alpha(v)h(\chi_{\alpha,u})x_{-\alpha}(w) \tag{14}$$

for any $x_{-\alpha}(s)$, where $x_\alpha(v)$ and $x_{-\alpha}(w)$ are elements of $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and $h(\chi_{\alpha,u})$ is an element of $T'(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$.

PROOF. Since $t\in\mathfrak{m}$, $1+st$ *is a unit in R. Therefore, the equation*

$$\begin{pmatrix}1&0\\s&1\end{pmatrix}\begin{pmatrix}1&t\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-s&1\end{pmatrix}=\begin{pmatrix}1&v\\0&1\end{pmatrix}\begin{pmatrix}u&0\\0&u^{-1}\end{pmatrix}\begin{pmatrix}1&0\\w&1\end{pmatrix}$$

has a solution, i.e., we have $u=(1+st)^{-1}$, $v=t(1+st)^{-1}$ and $w=-s^2t(1+st)^{-1}$. Thus, we have (14) where $h(\chi_{\alpha,u})\in T'(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ by definition. Further, if G is not of symplectic type, $x_\alpha(v)$, $x_{-\alpha}(w)\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ for $\mathfrak{a}_1$ and $\mathfrak{a}_\lambda$ are ideals. If G is of symplectic type, since $(1+st)^{-1}\equiv 1-st(\mathrm{mod}\ \mathfrak{a}_\lambda)$, $v\equiv t(1-st)\equiv 0$, $w\equiv -s^2t(1-st)\equiv 0(\mathrm{mod}\ \mathfrak{a}_\lambda)$ (cf. 1.8.(b)). Therefore, we have also $x_\alpha(v)$, $x_{-\alpha}(w)\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. q. e. d.

2.14. LEMMA. *If $\mathfrak{a}_1$ is a proper ideal, $x_\alpha(t)\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and β is a positive root $\neq\alpha$, then*

$$x_{-\beta}(s)x_\alpha(t)x_{-\beta}(s)^{-1}=xy \text{ for any } x_{-\beta}(s)\in E(R), \tag{15}$$

where $x\in U(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and y is a product of $x_{-\gamma}(u)$'s in $V(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ such that $-\gamma>-\beta$.

PROOF. Since α and $-\beta$ are linearly independent, there exists an element w which is a product of ω_γ for some roots $\gamma\in\Delta$, such that $wx_\alpha(t)w^{-1}$ and $wx_{-\beta}(s)w^{-1}$ are in $U(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Therefore, $x_{-\beta}(s)x_\alpha(t)x_{-\beta}(s)^{-1}\in w^{-1}U(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)w$.

From (2.5), any element of $U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ can be expressed by the form $x_{\beta_1}(s_1)x_{\beta_2}(s_2)\cdot\cdots\cdot x_{\beta_N}(s_N)$, where $s_i \in \mathfrak{a}_{\lambda(\beta_i)}$ and $\beta_1, \cdots, \beta_N$ are the positive roots. If we arrange the order of the roots in such a way that $w(\beta_i)>0$ for $1\leqq i\leqq j$ and $w(\beta_i)<0$ for $j+1\leqq i\leqq N$, then we have $w^{-1}U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)w \subseteqq U(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)V(R_1, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. Since x and y are products of $x_\gamma(u)$'s where γ are linear combinations of α and $-\beta$, we have our assertion. q. e. d.

2. 15. PROOF OF (2. 8). For convenience, denote by $UT'V$ the set in the right side of the equation (13). First, we claim that $UT'V$ is a subgroup of $E(R)$. It suffices to prove that $zUT'V \subset UT'V$ for any element z of $UT'V$ of the form $x_\beta(t)$, $h(\chi_{\beta,u})$ and $x_{-\beta}(t)$. If $z=x_\beta(t)$, then by (2. 5), we have $x_\beta(t) U \subset U$. If $z=h(\chi_{\beta,u}) \in T'$, then from (2. 10), we have $h(\chi_{\beta,u})U \subset UT'$. Finally, if $z=x_{-\beta}(t)$, we show by induction on a regular order of the roots that

$$(16) \qquad x_{-\beta}(t)U \subset UT'V \quad \text{for any} \quad x_{-\beta}(t) \in V.$$

If $-\beta$ is the largest negative root, from (2. 13) and (2. 14), (16) is true. Assume that (16) holds for any negative root larger than $-\beta$. We must show that $x_{-\beta}(t)x \in UT'V$ for any $x \in U$. If $x=x_{\beta_N}(s)$, it is clear from (2. 14). Now, assume that it is true for $x'=x_{\beta_{i+1}}(s_{i+1})\cdots x_{\beta_N}(s_N) \in U$, and let $x=x_{\beta_i}(s_i)x' \in U$. Then we have again by (2. 14), $x_{-\beta}(t)x_{\beta_i}(s_i)x'=x_{\beta_i}(s_i)x''yx'$ and by our assumption $yx' \in UT'V$. Thus we have $x_{-\beta}(t)x \in UT'V$. This completes the proof of (16). Secondly, we claim that $UT'V$ is normal in $E(R)$. It suffices to show that $x_{\pm\alpha_i}(t)UT'Vx_{\pm\alpha_i}(t)^{-1} \in UT'V$ for any root $\alpha_i \in \Pi$ and any $t \in R$. We have $x_{\alpha_i}(t)Ux_{\alpha_i}(t)^{-1} \subset U$ (cf. 2. 6) and $x_{\alpha_i}(t)h(\chi_{\beta,u})x_{\alpha_i}(t)^{-1} \subset UT'$ for any $h(\chi_{\beta,u}) \in T'$ and any $t \in R$(cf. 2. 12). The elements of V is expressible by a product of $x_{-\alpha_i}(u)$ and an element of $V^{(i)}$ consisting of elements expressible by a product of $x_\gamma(s)$ such that γ are negative roots different from $-\alpha_i$ and that $s \in \mathfrak{a}_{\lambda(\gamma)}$. Since $x_{\alpha_i}(t)x_{-\alpha_i}(u)x_{\alpha_i}(t)^{-1} \in UT'V$ *and* $x_{\alpha_i}(t)V^{(i)}x_{\alpha_i}(t)^{-1} \in V^{(i)}$ (cf. 2. 14), we have $x_{\alpha_i}(t)Vx_{\alpha_i}(t)^{-1} \subset UT V$. Therefore, we have $x_{\alpha_i}(t)UT'Vx_{\alpha_i}(t)^{-1} \subset UT'V$. A similar calculation applies to $x_{-\alpha_i}(t)$. q. e. d.

2. 16. PROPOSITION. *$B(R)=U(\mathfrak{m})T(R)V(R)$ (resp. $B'(R)=U(\mathfrak{m})T'(R)V(R)$) is a subgroup of $G(R)$ (resp. $E(R)$), where $U(\mathfrak{m})$ is the subgroup of $U(R)$ generated by $x_\alpha(t)$ for all $t \in \mathfrak{m}$ and all positive root α.*

PROOF. Iwahori-Matsumoto ([4], Theorem 2. 5) have proved this in the case that R is the ring of integers of a field with a non-trivial, non-archimedean discrete valuation and G is an adjoint group. However, their proof remains valid also in our case.

The following proposition plays a fundamental role in the proof of our main theorem.

2.17. PROPOSITION. *Let G be a simple Chevalley-Demazure group scheme, R be a local ring and $\mathfrak{a}$ a proper ideal of R and $\mathfrak{b}$ a special submodule associated with $(G,\mathfrak{a})$. Assume that $p\neq 2$ and $k\neq F_3$ if G is of type A_1 and that $k\neq F_2$ if G is of type B_2 or G_2. Let N be a subgroup of $G(R)$ normalized by $E(R)$ such that $E^*(R,\mathfrak{a},\mathfrak{b})\not\supset N\supset E(R,\mathfrak{a},\mathfrak{b})$. Then N contains an element $x_\alpha(t)$ not contained in $E(R,\mathfrak{a},\mathfrak{b})$.*

The proof will be divided into several steps. We set

$$E_0^*(R,\mathfrak{a},\mathfrak{b})=U(R,\mathfrak{a},\mathfrak{b})T^*(R,\mathfrak{a},\mathfrak{b})V(R,\mathfrak{a},\mathfrak{b})$$

where $T^*(R,\mathfrak{a},\mathfrak{b})=T(R)\cap E^*(R,\mathfrak{a},\mathfrak{b})$. Then $E_0^*(R,\mathfrak{a},\mathfrak{b})$ is a subgroup of $G(R)$ normalized by $E(R)$ such that $E^*(R,\mathfrak{a},\mathfrak{b})\supset E_0^*(R,\mathfrak{a},\mathfrak{b})\supset E(R,\mathfrak{a},\mathfrak{b})$. We denote by $N'=N-E_0^*(R,\mathfrak{a},\mathfrak{b})$. Then, (2.17) follows immediately from the following which we shall prove in the next section.

2.18. Assume that $k\neq F_2, F_3$ if G is of type A_1. If $N'\neq\emptyset$, then $N\cap B(R)\neq\emptyset$.

2.19. Assume that $p\neq 2$ and $k\neq F_3$ if G is of type A_1 and that $k\neq F_2$ if G is of type G_2. If $N'\cap B(R)\neq\emptyset$, then $N'\cap x_\beta(R)x_{\beta'}(R)\neq\emptyset$, where β, β are dominant roots of Δ (for the definition, see 3.5).

2.20. Assume that $k\neq F_2$ if G is of type B_2 or G_2. If $N'\cap x_\beta(R)x_{\beta'}(R)\neq\emptyset$, then $N'\cap x_\alpha(R)\neq\emptyset$ for some root α.

2.21. Assume that $p\neq 2$ and $k\neq F_3$ if G is of type A_1 and that $k\neq F_2$ if G is of type B_2 or G_2, then $E_0^*(R,\mathfrak{a},\mathfrak{b})=E^*(R,\mathfrak{a},\mathfrak{b})$.

3. Proof of the main theorem. In this section, we prove (1.6), (2.17) and then prove our main theorem (1.9) and its corollaries. We use notations and definitions same as those in the previous sections.

3.1. PROPOSITION. *Let G be a Chevalley-Demazure group scheme. Then $\Omega(C)=U(C)T(C)V(C)$ is an affine open subset of $G(C)$ and there exists a rational representation ϕ of $G(C)$ into a general linear group $GL_N(C)$ such that the coordinate function $d_{ij}(g)$ $(1\leqq i,j\leqq N)$ of $\phi(g)$ is in $Z[G]$ and that the affine ring of $\Omega(C)$ is $C[G][d_{11}^{-1}]$. Further, the mapping*

$$\theta(C): U(C)\times T(C)\times V(C)\rightarrow G(C)$$

defined by $\theta(C)(x,h,y)=xhy$ induces a ring isomorphism

$$\widetilde{\theta} : Z[G][d_{11}^{-1}] \to Z[U] \otimes Z[T] \otimes Z[V],$$

where $Z[U]$ *(resp.* $Z[V]$*) is the affine ring of the subgroup* U *(resp.* V*) of* G*.*

This proposition follows from a theorem in [2].

3.2. PROOF OF (1.6). In (3.1), we denote by G' the group scheme defined by the subring $Z[G']$ of $Z[G]$ generated by $d_{ij}(1 \leqq i, j \leqq N)$. The homomorphism ϕ defines a homomorphism of group schemes $G \to G'$ which we denote also by ϕ. Since $\theta(R) : U(R) \times T(R) \times V(R) \to \Omega(R) = \mathrm{Hom}(Z[G][d_{11}^{-1}], R)$ defined by $\theta(R)(x, h, y) = xhy$ is bijective, we have $\Omega(R) \subset G_0(R)$. On the other hand, if $g \in G(R, \mathfrak{m})$, then $\phi(g) \in G'(R, \mathfrak{m})$. This shows that $d_{11}(g) \equiv 1 \pmod{\mathfrak{m}}$ and $d_{11}(g)$ is a unit in R. Therefore, $g \in \Omega(R)$. Thus, we have $G(R, \mathfrak{m}) \subset \Omega(R) \subset G_0(R)$. Now, let φ be the homomorphism of groups $G(R) \to G(R/\mathfrak{m})$ induced by the canonical homomorphism of rings $R \to R/\mathfrak{m}$. For any element $g \in G(R)$, $\varphi(g)$ is an element of $G_0(k) = G(k)$. Therefore, $g = g_1 g_2$ where $g_1 \in G(R, \mathfrak{m})$ and g_2 is an element of $G_0(R)$ such that $\varphi(g) = g_2$. Thus, we have $g \in G_0(R)$. This shows that $G(R) = G_0(R)$. If G is simply connected, then $T(R) = T'(R) \subset E(R)$. Therefore, we have $G(R) = E(R)$. q. e. d.

3.3. COROLLARY. *Let* $\mathfrak{a}$ *be a proper ideal of* R*, then*

$$G(R, \mathfrak{a}) = U(R, \mathfrak{a})T(R, \mathfrak{a})V(R, \mathfrak{a})$$

$$G^*(R, \mathfrak{a}) = U(R, \mathfrak{a})T^*(R, \mathfrak{a})V(R, \mathfrak{a}),$$

where $T^*(R, \mathfrak{a}) = G^*(R, \mathfrak{a}) \cap T(R)$.

This follows easily from the above proposition.

3.4. PROOF OF (2.18). If $N \subset G^*(R, \mathfrak{m})$, then $N \subset B(R)$ and the assertion is trivial. If $N \not\subset G^*(R, \mathfrak{m})$, then $\varphi(N)$ is a subgroup of $G(k)$ normalized by $E(k)$ not contained in the center of $G(k)$. Therefore, we have $\varphi(N) \cap T(k)V(k) \neq 1$ (cf. [1], p. 50. We assume that if G is of type $A_1, k \neq F_2, F_3$). Thus, there exists an element $g \in N$ such that $\varphi(g) = \varphi(h)\varphi(y) \in T(k)V(k)$ for some elements $h \in T(R)$ and $y \in V(R)$ and that $\varphi(g)$ is not contained in the center of $G(k)$. This means that $g = g'hy$ for some $g' \in G(R, \mathfrak{m})$. Since g' is expressed by the form $x'h'y$ where $x \in U(R, \mathfrak{m})$, $h' \in T(R, \mathfrak{m})$ and $y' \in V(R, \mathfrak{m})$, we have $g \in B(R)$ and $g \notin G^*(R, \mathfrak{m})$. This shows that $N \cap B(R) \neq \emptyset$.

3.5. Now, we proceed to prove (2.19). First, we give some preliminary lemmas on irreducible root systems. Let Δ be an irreducible root system and

$\Pi=\{\alpha_1,\cdots,\alpha_l\}$ be a fundamental system of rcots. A root $\beta\in\Delta$ is called to be *dominant* if $\beta(H_{\alpha_i})\geqq 0$ for all $\alpha_i\in\Pi$. By definition, the highest root is dominant. Further, if $\lambda(\alpha)=1$ for all root $\alpha\in\Delta$, then the highest root is the only dominant root. On the other hand, if Δ has a root of length 2 or 3, there exist exactly two dominant roots and the length of these two roots are different each other (cf. [1]. Lemma 13, p. 60).

3.6. LEMMA. *Let Δ be not of type G_2, then*

(i) *For any positive root $\alpha\in\Delta$ which is not in Π, there exists a root $\alpha_i\in\Pi$ such that $\alpha-\alpha_i\in\Delta$ and $\alpha+\alpha_i\notin\Delta$.*

(ii) *For any positive root $\alpha\in\Delta$ which is not dominant, there exists a root $\alpha_i\in\Pi$, such that $\alpha+\alpha_i\in\Delta$ and $\alpha-\alpha_i\notin\Delta$.*

PROOF. We claim that for any positive root α which is not in Π, there exists a root $\alpha_i\in\Pi$ such that $\alpha(H_{\alpha_i})>0$. We see $\lambda(\beta)\alpha(H_\beta)=\lambda(\alpha)\beta(H_\alpha)$ for any root $\alpha,\beta\in\Delta$. If $\alpha=\sum_{i=1}^{l} m_i\alpha_i$, then $2\lambda(\alpha)=\lambda(\alpha)\alpha(H_\alpha)=\lambda(\alpha)\sum_{j=1}^{l} m_j\lambda(\alpha_j)\alpha(H_{\alpha_j})$ >0. Since $\lambda(\alpha)>0$, $m_j\geqq 0$ and $\lambda(\alpha_j)>0$, $\alpha(H_{\alpha_i})>0$ for some α_i. Thus $\alpha-\alpha_i$ is a root. As for a positive root which is not dominant, by definition, there exists a root $\alpha_i\in\Pi$, such that $\alpha(H_{\alpha_i})<0$. Thus $\alpha+\alpha_i$ is a root. Now, let Δ be not of type G_2. Assume $\alpha\pm\alpha_i$ are roots. Then $\pm\alpha$, $\pm\alpha_i\pm(\alpha+\alpha_i)$ and $\pm(\alpha-\alpha_i)$ are the only linear combinations of α and α_i which are roots (cf. [1], Lemma 2, p. 20). This contradicts to $\alpha(H_{\alpha_i})\neq 0$. Thus we have our lemma. q. e. d.

3.7. Let $\alpha_0=\sum_{i=1}^{l} m_i\alpha_i$ be the highest root. We know that if Δ is of type A_n, B_n, C_n, D_n, E_6 or E_7, then Min $m_i=1$ and if Δ is of type E_8, F_4 or G_2, then Min $m_i=2$. In the former case, we set α_1 one of the roots α_i in Π such that $m_i=1$ and further, if Δ is of type A_n, α_i is not orthogonal to α_0 and the latter case, we set α_1 one of the roots α_i in Π such that $m_i=2$ and that α_0 is not orthogonal to α_i and orthogonal to all roots in Π different from α_i. (There exists exactly one root which has these properties.) Then, the diagram of $\Pi-\{\alpha_1\}$ is connected. Further, we have

LEMMA. *Let Δ be of type E_8, F_4 or G_2 and $\alpha=\sum_{i=1}^{l} m_i\alpha_i$ be a root. Then, $m_1=2$ if and only if α is the highest root.*

PROOF. If $\alpha=\alpha_0$, then $m_1=2$. Conversely, if $\alpha=\sum_{i=1}^{l} m_i\alpha_i$ is a root such that $m_1=2$ and $\alpha\neq\alpha_0$, then we have $\alpha_0-\alpha_{i(1)}-\cdots-\alpha_{i(k)}=\beta$ for some $\alpha_{i(j)}$ where $i(j)\neq 1$ $(1\leqq j\leqq k)$. This is a contradiction, for $\alpha_0-\alpha_i\notin\Delta$ for all $i>1$. q. e. d.

3. 8. We define a subset Δ_1 of Δ closed under addition of roots and an irreducible subsystem Δ_0 of Δ as follows

$$\Delta_1=\left\{\alpha\in\Delta\ ;\ \alpha=\sum_{i=1}^{l}m_i\alpha_i,\quad m_1>0\right\},$$

$$\Delta_0=\left\{\alpha\in\Delta\ ;\ \alpha=\sum_{i=1}^{l}m_i\alpha_i,\quad m_1=0\right\}.$$

Let $\Delta_1=\{\beta_1,\beta_2,\cdots,\beta_m\}$ where $\beta_i<\beta_{i+1}$ and $\beta_m=\alpha_0$ by a regular order of Δ. Then from (3. 7), we have

COROLLARY. *In a group $G(R)$ whose root system is Δ, for any roots β_i and β_j of Δ_1 and for any elements s and t of R,*

$$(x_{\beta_i}(s),\ x_{\beta_j}(t))=1\quad or\ x_{\alpha_0}(u)\ for\ some\ u\in R.$$

3. 9. LEMMA. *Let γ be a dominant root in Δ_0, then $\gamma-\alpha_1\notin\Delta$ and $\gamma+\alpha_1\in\Delta$.*

PROOF. Since γ is positive and is not a dominant root in Δ, from (3. 6), $\gamma+\alpha_i$ is a root for some $\alpha_i\in\Pi$. On the other hand, $\gamma+\alpha_i$ is not a root for all $\alpha_i\in\Pi$, $i>1$, for γ is a dominant root in Δ_0. Thus $\alpha+\alpha_1$ is a root. It is clear that $\alpha-\alpha_1$ is not a root. q.e.d.

3. 10. Now, let N be a subgroup of $G(R)$ and N' be its subset stated in (2. 16). Let $x=x_{\gamma_1}(s_1)x_{\gamma_2}(s_2)\cdots x_{\gamma_n}(s_n)$ be an element of N where $\gamma_i\in\Delta(1\leqq i\leqq n)$ and $\{i(1), i(2),\cdots,i(k)\}$ be the set of all indices such that $s_{i(j)}\notin\mathfrak{a}_{\lambda(\gamma_{i(j)})}(1\leqq j\leqq k)$, $1\leqq i(1)<i(2)<\cdots<i(k)\leqq n$. Then a simple calculation shows that $x=x_{\gamma_{i(1)}}(s_{i(1)})\cdots x_{\gamma_{i(k)}}(s_{i(k)})$ is also an element of N'. We call x' *the reduced form of* x. For a subset Δ of Δ, we denote by $U(\Delta')$ the subgroup of $U(R)$ generated by $x_\alpha(t)$ for all positive roots α in Δ' and for all $t\in R$. Then, we have

3. 11 LEMMA. *Let G be not of type G_2. If there exists an element $x\in N\cap U(\Delta_1)$, then starting from x by a finite process of taking a commutator with an element of $U(\Delta_0)$ (resp. $U(\Delta)$) and taking its reduced form, we obtain an element of N' of the form $x_\beta(t)x_{\beta'}(t')_{\beta''}(t'')$ (resp. $x_\beta(t)x_{\beta'}(t')$), where β, β are dominant roots of Δ, β' the highest root and β'' is a positive root such that $\beta''+\alpha_1=\beta'$.*

PROOF. We may assume that x is of the form $x_{\beta_i}(t_i)x_{\beta_{i+1}}(t_{i+1})\cdots x_{\beta_m}(t_m)$ where $1\leqq i\leqq m$ and $t_i\notin \mathfrak{a}_{\lambda(\beta_i)}$. We prove the lemma by induction on i. If $i=m$, then the assertion is trivial. Suppose $i<m$ and assume that for any element

$$(1)\qquad x=x_{\beta_k}(t_k)x_{\beta_{k+1}}(t_{k+1})\cdots x_{\beta_m}(t_m),\ k>i,\ t_k\notin \mathfrak{a}_{\lambda(\beta_k)},$$

of N the lemma is true. If β_i is not dominant, then, by (3.6. ii), there exists a root $\alpha_i\in\Pi$ such that $\alpha+\alpha_i\in\Delta$ and $\alpha-\alpha_i\notin\Delta$. Therefore, if $\alpha_i\neq\alpha_1$, then, by (3.8), $(x_{\alpha_i}(1),x)=x'$ can be reduced to an element of N' of the form (1). If $\alpha_i=\alpha_1$ or β_i is dominant, we may assume that $(x_{\beta_i}(t_i),x_{\alpha_j}(1))\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ for all $\alpha_j\in\Pi\cap\Delta_0$. For, if there exists a root $\alpha_j(j>1)$ such that $x'=(x_{\beta_i}(t_i), x_{\alpha_j}(1))\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, then x' can be reduced to an element of N' of the form (1). Now, we set $x=x_{\beta_i}(t_i)x'$ where $x'=x_{\beta_{i+1}}(t_{i+1})\cdots x_{\beta_m}(t_m)$. Then we may apply induction assumption to x'. Thus we obtain an element stated in the lemma. q. e. d.

3.12. COROLLARY. *Let G be not of type G_2. If there exists an element $x\in N\cap U(\Delta)$, then starting from x by a finite process of taking a commutator with an element of $U(\Delta)$ and taking its reduced form, we obtain an element of N' of the form $x_\beta(t)x_{\beta'}(t')$ where β, β' are dominant roots of Δ.*

PROOF. We prove by induction on the rank of Δ. If Δ is of rank $=1$, then this is trivial. Assume that the lemma holds for the groups of rank less than that of Δ. We set $x=x_1x_0$ with $x_1\in U(\Delta_1)$ and $x_0\in U(\Delta_0)$ (cf. 2.5). If $x_0\in N'$, then by induction assumption, we obtain an element $x'=x_1'x_\gamma(s)x_{\gamma'}(s')$ of N' where $x_1'\in U(\Delta_1)$ and γ, γ' are dominant roots of Δ_0. For, the group $U(\Delta_1)$ is stable by taking a commutator with an element of $U(\Delta_0)$. Then, by (3.9), $(x', x_{\alpha_1}(1))=x''$ is an element of $U(\Delta_1)\cap N'$. Thus, we may apply (3.11) to x' If. $x_0\notin N$, then $x_1\in U(\Delta_1)\cap N'$. We may also apply (3.11) to x_1. q .e. d.

3.13. PROOF OF (2.19) FOR THE GROUP OF NOT TYPE G_2. If G is of type A_1, it is known by Klingenberg (cf. [5], 2.7). Therefore, we assume that the rank of G is >1. Let $z=xhy\in B(R)\cap N$, where $x\in U(\mathfrak{m})$, $h\in T(R)$ and $y\in V(R)$. If x and y are in $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, then $z=h(\chi)\in N'$. Therefore, there exists a root α such that $\chi(\alpha)\not\equiv 1 \pmod{\mathfrak{a}_{\lambda(\alpha)}}$. Then, $(x_\alpha(1),h(\chi))=x_\alpha(\chi(\alpha)^{-1}-1)$ is an element of N'. Thus, we may assume that $x\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ or $y\notin E(E,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Note that, for an element $z=xhy\in N'$, if x and y' are the reduced forms of x and y, then $z'=x'hy'$ is also an element of N' which we call the reduced form of z. For a subsystem Δ' of Δ, denote by $G(\Delta')$ the subgroup of $G(R)$ generated by $x_\alpha(t)$ for all $\alpha\in\Delta'$ and all $t\in R$ and by $T(R)$. Now, we prove the following (P_n) $(n\geqq 2)$ by induction on n.

(P_n) Let G be not of type G_2. Suppose there exists an element $z=xhy$ of $N'\cap B(R)$ such that $x\in U(\Delta')\cap U(\mathfrak{m})$, $h\in T(R)$ and $y\in V(\Delta')$ and that $x\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ or $y\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, where Δ' is a subsystem of Δ of rank n. Then, starting from z, by a finite process of taking its reduced form, taking a conjugate in $G(\Delta')$ or taking a commutator with an element of $G(\Delta')$, we obtain an element of the form $x_\gamma(s)x_{\gamma'}(s')$ in N', where γ, γ' are dominant roots of Δ'.

3.14. PROOF OF (P_2) FOR THE GROUP OF TYPE A_2. Let Δ^+ be the roots (4) and denote

$$z=x_\alpha(s_1)x_\beta(s_2)x_{\alpha+\beta}(s_3)h(\chi)x_{-\alpha-\beta}(t_3)x_{-\beta}(t_2)x_{-\alpha}(t_1).$$

By (3.12), it suffices to show that we obtain an element of $U(R)\cap N'$ or $V(R)\cap N'$. If $x\in E(R,\mathfrak{a}_1)$, the argument is clear. Suppose $x\notin E(R,\mathfrak{a}_1)$.

(i) If $s_1\in\mathfrak{a}_1$ and $s_3\notin\mathfrak{a}_1$, we have

$$x_{-\alpha}(1)^{-1}z'x_{-\alpha}(1)=x_\beta(s_2\pm s_3)x_{\alpha+\beta}(s_3)h(\chi)x_{-\alpha}(1-\chi(\alpha))x_{-\alpha-\beta}(t_3\pm t_2)x_{-\beta}(t_2)x_{-\alpha}(t_1).$$

Therefore $(z',\ x_{-\beta}(1))$ is conjugate to $z''=x_\beta(\pm s_3)x_{-\alpha-\beta}(u)x_{-\alpha}(v)$ for some u, $v\in R$. Then $z'''=\omega_\beta\omega_\alpha z'\omega_\alpha^{-1}\omega_\beta^{-1}$ is an element of $U(R)\cap N'$.

(ii) If $s_1\in\mathfrak{a}_1$ and $s_3\in\mathfrak{a}_1$, then we have $(z',\ x_{-\alpha-\beta}(1))$ is conjugate to $x_{-\alpha}(\pm s_2)x_{-\alpha-\beta}(w)$ for some $w\in R$ which is an element of $V(R)\cap N'$.

(iii) If $s_1\notin\mathfrak{a}_1$, then we have

$$x_\beta(1)^{-1}z\,x_\beta(1)=x_\alpha(s_1)x_\beta(s_2)x_{\alpha+\beta}(s_3\pm s_1)x_\beta(\chi(\beta)-1)h(\chi)$$
$$x_{-\alpha-\beta}(t_3)x_{-\alpha}(\pm t_3)x_\beta(v)h(\chi_{\beta,u})x_{-\beta}(w)x_{-\alpha}(t_1).$$

Therefore, $(z,\ x_\beta(1))$ is conjugate to $z'=x_{\alpha+\beta}(\pm s_1)x_\beta(v')h'y'$ for some $y'\in V(R)$ and $v'\in R$. Then z'' is an element of N' and a similar calculation as one of the above cases applies to z''. q. e. d.

3.15. PROOF OF (P_2) FOR THE GROUPS OF TYPE B_2. Let Δ^+ be the roots (6) and we denote

$$z=x_\alpha(s_1)x_\beta(s_2)x_{\alpha+\beta}(s_3)x_{2\alpha+\beta}(s_4)h(\chi)x_{-2\alpha-\beta}(t_4)x_{-\alpha-\beta}(t_3)x_{-\beta}(t_2)x_{-\alpha}(t_1).$$

Suppose $x\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. (i) If $s_1\in\mathfrak{a}_1$ and $s_4\notin\mathfrak{a}_2$, then a direct calculation shows that $(z',x_{-\alpha}(1))$ is conjugate to $z''=x_\beta(\pm 2s_3\pm s_4)x_{\alpha+\beta}(s_4)y'$ for some $y'\in V(R)$ and $(z'',\ x_{-2\alpha-\beta}(1))$ is conjugate to $z''=x_{-\alpha}(\pm s_4)x_\beta(\pm s_4^2)$. Then $\omega_\alpha z''\omega_\alpha^{-1}\in U(R)\cap N'$.

(ii) If $s_1\in\mathfrak{a}_1$, $s_3\notin\mathfrak{a}_1$ and $s_4\in\mathfrak{a}_2$, then we have

$$x_{-2\alpha-\beta}(1)^{-1}z'x_{-2\alpha-\beta}(1)=x_{\beta}(s_2)x_{\alpha+\beta}(s_3)x_{-\alpha}(\pm s_3)x_{\beta}(\pm s_3^2)h(\chi)x_{-2\alpha-\beta}(1-\chi(2\alpha+\beta))y\ ,$$

and $(z',\ x_{-2\alpha-\beta}(1))$ is conjugate to $z''=x_{-\alpha}(\pm s_3)x_{\beta}(\pm s_3^2)x_{-2\alpha-\beta}(u)$ for some $u\in R$. Then $\omega_{2\alpha+\beta}z''\omega_{2\alpha+\beta}^{-1}\in U(R)\cap N$.

(iii) If $s_1\in\mathfrak{a}_1$, $s_2\notin\mathfrak{a}_2$, $s_3\in\mathfrak{a}_1$ and $s_4\in\mathfrak{a}_2$, then $(z',x_{-\alpha-\beta}(1))$ is conjugate to $x_{-\alpha}(\pm t_2)x_{-2\alpha-\beta}(u)$ for some $u\in R$ which is an element of $V(R)\cap N'$.

(iv) If $s_1\notin\mathfrak{a}_1$, we have

$$x_{\beta}(1)^{-1}z'x_{\beta}(1)=x_{\alpha}(s_1)x_{\alpha+\beta}(\pm s_1)x_{2\alpha+\beta}(\pm s_1^2)x_{\beta}(s_2)x_{\alpha+\beta}(s_3)x_{2\alpha+\beta}(s_4)$$

$$x_{\beta}(\chi(\beta)-1)h(\chi)x_{-2\alpha-\beta}(t_4)x_{-\alpha-\beta}(t_3)x_{-2\alpha-\beta}(\pm 2t_3)x_{\beta}(v)h(\chi_{\beta,u})x_{-\beta}(w)x_{-\alpha}(t_1)$$

and $(z,\ x_{\beta}(1))$ is conjugate to $z''=x_{\alpha+\beta}(\pm s_1)x_{2\alpha+\beta}(\pm s_1^2)x_{\beta}(v')h\,y'$, for some $v'\in R$, $h\in T(R)$ and $y'\in V(R)$. A similar caluculation as one of the above cases applies to z .

3.16. PROOF OF $(P_{n-1})\Longrightarrow(P_n)$ for $n\geqq 3$. No loss of generality, we may assume $n=l$. Denote $z=x_1x_0hy_0y_1$ where $x_1\in U(\Delta_1)$, $x_0\in U(\Delta_0)$, $h=h(\chi)\in T(R)$, $y_0\in V(\Delta_0)$ and $y_1\in V(\Delta_1)$ (cf. 2.5, 3.7 and 3.8). Suppose $z_0=x_0hy_0\notin E_0^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and $x_0\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ or $y_0\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Then, by (P_{n-1}), we obtain an element $x_1'x_\gamma(s)x_{\gamma'}(s)y_1'$ of N' such that $x_\gamma(s)x_\gamma(s')\in E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ where γ, γ' are dominant roots in Δ_0. For $U(\Delta_1)$ and $V(\Delta_1)$ are stable by taking a conjugate by an element of $G(\Delta_0)$or a commutator with an element of $G(\Delta_0)$. Therefore, we may assume that $z=x_1y_1$ for $x_1\in U(\Delta_1)$ and $y_1\in V(\Delta_1)$. Then, by (3.11), we obtain an element $z'=x_\beta(t)x_{\beta'}(t')x_{\beta''}(t'')y_1'$ where β, β' are dominant roots and β'' is a positive root such that $\alpha_1+\beta''=\beta'$ is the highest root and where $y_1'\in V(\Delta_1)$, for $V(\Delta_1)$ is stable by taking a commutator with an element of $U(\Delta_0)$ or taking a reduced form. Further, we may assume that x_1' is commutative modulo $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ for all $x_{\alpha_i}(1)$, $i>1$, (cf.proof of 3.11) and that z' is a reduced form. Now, let Δ' be the set of roots γ such that $x_{-\gamma}(u)$ is a factor of y_1' for $u\notin\mathfrak{a}_{\lambda(\gamma)}$. If $\Delta'=\emptyset$, then $z'\in U(R)\cap N'$. If $\Delta'\neq\emptyset$, we may assume that there exists a root $\gamma\neq\alpha_1$ of Δ'. For, otherwise, $\omega_{\alpha_1}z'\omega_{\alpha_1}^{-1}\in U(R)\cap N'$. For a root $\gamma\in\Delta'$, if there exists $\alpha_i\in\Pi(i>1)$ such that $-\gamma+\alpha_i\in\Delta$ and $-\gamma\ -\alpha_i\notin\Delta$, then $(z',x_{\alpha_i}(1))\in V(R)\cap N'$. Otherwise, by (3. 6. i), for any root $\gamma\neq\alpha_1$ of Δ', $-\gamma+\alpha_1\in\Delta$ and $-\gamma-\alpha_1\notin\Delta$. Therefore, we may assume that $x_1=x_\beta(t)$. For, if $x_{\beta'}(t')$ is a factor of x_1', $(z',x_{-\alpha_1}(1))\in U(R)\cap N'$ and further if $x_{\beta''}(t'')$ is a factor of x_1', $(z,x_{-\alpha'}(1))$ is conjugate to an element of $V(R)\cap N'$. Thus we have $(z',x_{\alpha_1}(1))\in V(R)\cap N$, since $\beta+\alpha_1$ is not a root. Thus we have proved (P_n). This completes the proof of (2.19) for the groups of not type G_2.

3.17. PROOF OF (2.19) FOR THE GROUP OF TYPE G_2. Let $z=xhy\in B(R)\cap N'$. We may assume that $x\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ or $y\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Further, since $k \neq F_2$, we may assume that $h=1$. Let Δ^+ be the roots (9) and denote

$$x = x_\alpha(s_1)x_\beta(s_2)x_{\alpha+\beta}(s_3)x_{2\alpha+\beta}(s_4)x_{3\alpha+\beta}(s_5)x_{3\alpha+2\beta}(s_6)$$

$$y = x_{-3\alpha-2\beta}(t_6)x_{-3\alpha-\beta}(t_5)x_{-2\alpha-\beta}(t_4)x_{\alpha-\beta}(t_3)x_{-\beta}(t_2)x_{-\alpha}(t_1).$$

Let u be a unit of R such that $u-1$ is also a unit, and $\chi'_{\alpha,u}$(resp. $\chi'_{\beta,u}$) be an element of Hom$(Z[T], R)$ such that $\chi'_{\alpha,u}(\alpha)=u$, $\chi'_{\alpha,u}(\beta)=1$ (resp. $\chi'_{\beta,u}(\alpha)=1$, $\chi'_{\beta,u}(\beta)=u$). We denote by z' the reduced form of z.

(i) If $s_1 \in \mathfrak{a}_1$, $s_2 \in \mathfrak{a}_3$ and $s_3 \in \mathfrak{a}_1$, then $(h(\chi_{\beta,u}), z)$ is conjugate to $z = x_{3\alpha+\beta}((u^{-1}-1)s_5)x_{3\alpha+2\beta}((u-1)s_6)y'$, for some $y' \in V(R)$. Therefore, if $s_6 \notin \mathfrak{a}_3$, then $(x_{-\beta}(1), z'')$ is conjugate to $z''' = x_{3}{}_{+}(\pm(u-1)s_6)y''$ and $(x_{-3\alpha-2\beta}(1), z''')$ is conjugate to $x_{-\beta}(\pm(u-1)s_6)$. If $s_6 \in \mathfrak{a}_3$ and $s_5 \notin \mathfrak{a}_3$, $(x_{-3\alpha-2\beta}(1), z')$ is conjugate to $x_{-\beta}(\pm(u^{-1}-1)s_5)$. Finally, if $s_4 \notin \mathfrak{a}_1$ and $s_5, s_6 \in \mathfrak{a}_3$, then $(x_{-3\alpha-2\beta}(1), z')$ is conjugate to

$$z'' = x_{-\alpha-\beta}(\pm s_4)x_\alpha(\pm s_4^2)x_{3\alpha+\beta}(\pm s_4^3)x_{-\beta}(\pm s_4^3)$$

and we have

$$z''' = \omega_{\alpha+\beta}z''\omega_{\alpha+\beta}^{-1} = x_{\alpha+\beta}(\pm s_4)x_{2\alpha+\beta}(\pm s_4^2)x_{3\alpha+\beta}(\pm s_4^3)x_{3\alpha+2\beta}(\pm s_4^3).$$

Then, $(h(\chi_{\beta,u}), z''')$ is conjugate to $z^{(4)} = x_{\alpha+\beta}(\pm(u-1)s_4)$. $x_{3\alpha+\beta}(v)x_{3\alpha+2\beta}(w)$ and $(h(\chi_{\alpha,u}), z^{(4)})$ is conjugate to $z^{(5)} = x_{\alpha+\beta}(\pm s'_4)x_{3\alpha+\beta}(v')$ where $s'_4 \notin \mathfrak{a}_1$. If $v' \notin \mathfrak{a}_1$, we have $(x_\beta(1), z^{(5)}) = x_{3\alpha+2\beta}(\pm v')$.

(ii) If $s_1 \in \mathfrak{a}_1$, $s_2 \in \mathfrak{a}_3$ and $s_3 \notin \mathfrak{a}_1$, we may assume that $s_4 \in \mathfrak{a}$, $s_5 \in \mathfrak{a}_3$ and $s_6 \in \mathfrak{a}_3$. For, if it does not hold, then $(h(\chi_{3\alpha+2\beta,u}), z')$ has the form of the case (i). Now let $z' = x_{\alpha+\beta}(s_3)y$, then $(x_{-3\alpha-2\beta}(1), z')$ is conjugate to

$$z'' = x_{-2\alpha-\beta}(\pm s_3)x_{-\alpha}(\pm s_3^2)x_\beta(\pm s_3^3)x_{-3\alpha-\beta}(\pm s_3^3)$$

and we have

$$z''' = \omega_{2\alpha+\beta}z''\omega_{2\alpha+\beta}^{-1} = x_{2\alpha+\beta}(\pm s_3)x_{\alpha+\beta}(\pm s_3^2)x_\beta(\pm s_3^3)x_{3\alpha+2\beta}(\pm s_3^3).$$

Then, $(h(\chi_{3\alpha+\beta,u})z''')$ is conjugate to $z^{(4)} = x_{2\alpha+\beta}(\pm(u^{-1}-1)s_3)x_\beta(v)x_{3\alpha+2\beta}(w)$ and $(h(\chi_{\alpha,u}), z^{(4)})$ is conjugate to $z^{(5)} = x_{2\alpha+\beta}(s'_3)x_\beta(v')$, where $s'_3 \notin \mathfrak{a}_1$. If $v' \notin \mathfrak{a}_1$, we have $(x_{3\alpha+\beta}(1), z^{(5)})$ is conjugate to $x_{3\alpha+2\beta}(\pm v')$.

(iii) If $s_1 \notin \mathfrak{a}_1$ or $s_2 \notin \mathfrak{a}_3$, taking a conjugate of $(h(\chi'_{\alpha,u}), z')$ or $(h(\chi'_{\beta,u}), z')$ if necessary, we may assume that either $s_1 \notin \mathfrak{a}_1$ and $s_3 \in \mathfrak{a}_3$ or $s_1 \in \mathfrak{a}_1$ and $s_3 \notin \mathfrak{a}_3$. Then a conjugate of $(x_\alpha(1), z')$ or $(x_\beta(1), z')$ has the form of the case (ii). q. e. d.

3.18. PROOF OF (2.20). If the roots of Δ have all length 1, then it is clear. Assume that Δ has two roots whose lengths are different. If G is of rank >2, then there exists a root γ linearly independent to β, β' such that (arranging β, β' in a suitable order) $\beta+\gamma$ is a root and $\beta-\gamma$, $\beta+2\gamma$, $2\beta+\gamma$ $\beta'-\gamma$ and $\beta'+\gamma$ are not roots (cf. [1], Lemma 13, P. 60). Then, if $t\notin \mathfrak{a}_{\lambda(\beta)}$, we have $(x_\gamma(1),\ x_\beta(t)x_{\beta'}(t'))=x_{\beta+\gamma}(\pm t)\in N'$. Now, let G be of type B_2. Since $k\neq F_2$, there exists a unit u of R such that $u-1$ is also a unit. Let $x=x_{\alpha+\beta}(t)x_{2\alpha+\beta}(t')$. If $t\notin \mathfrak{a}_{\lambda(\alpha+\beta)}$, we have $y=\omega_\beta x\omega_\beta^{-1}=x_\alpha(\pm t)x_{2\alpha+\beta}(\pm t')$ and $(h(\chi_{\beta,u}),y)=x_{\alpha+\beta}(\pm(u-1)t)$ $\in N'$. If G is of type G_2, since $X=P_r$, we can prove easily. q. e. d.

3.19. PROOF OF (2.21). Since $G^*(R,\mathfrak{m})\supset E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, by (3.3), we have $B(R)\supset E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Now, assume that $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)\supsetneqq E_0^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Then, (2.18), (2.19) and (2.20) apply to $N=E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, we have an element $x_\alpha(t)$ of $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ not contained in $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. This is a contradiction. q. e. d.

3.20. PROOF OF (1.9). If R is a field, then the theorem is a well known result of Chevalley (cf. [1], [10]). Further, if the rank of G is $=1$, the result has been given by Klingenberg (cf. [5]). If N is a central subgroup of $G(R)$, the theorem is trivial, for $E^*(R,\{0\})$ contains the center of $G(R)$ and $E(R,\{0\})=1$. Therefore, we may assume that the rank of G is >1, R is not a field and N is not central. Let $\mathfrak{a}_1$ and $\mathfrak{a}_\lambda$ be the ideal of R and the special submodule of R associated with $(G,\mathfrak{a}_1)$ which are maximal satisfying $N\supset E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. If $\mathfrak{a}_1=R$, then by definition $\mathfrak{a}_\lambda=R$ and we have $E^*(R)=G(R)\supset N\supset E(R)$. Therefore, we may assume $\mathfrak{a}_1$ is proper. Now, assume that $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)\not\supset N$. Then, by (2.17), there exists an element $x_\alpha(t)\in N$ which is not contained in $E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Further, if G is of symplectic type and $\lambda(\alpha)=\lambda$, then $x_\alpha(r^2t)\in N$ for any $r\in R$ and otherwise, we have $x_\alpha(rt)\in N$ for any $r\in R$. Now, let $\mathfrak{a}_1'$ be the ideal of R generated by $\mathfrak{a}_1$ and t, and $\mathfrak{a}_\lambda'$ be the special submodule associated with $\mathfrak{a}_1'$ generated by $\mathfrak{a}_\lambda$ and t. Then N contains $E(R,\mathfrak{a}_1',\mathfrak{a}')$ (cf. 2.4). This contradicts to the maximality of $\mathfrak{a}_1$ and $\mathfrak{a}_\lambda$. Thus, we have $E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)\supset N\supset E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$. Note that if $N\supset E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and $N\supset E(R,\mathfrak{b}_1,\mathfrak{b}_\lambda)$ where $\mathfrak{a}_1$, $\mathfrak{b}_1$ are ideals of R and $\mathfrak{a}_\lambda$, $\mathfrak{b}_\lambda$ are special submodules associated with $\mathfrak{a}_1$, $\mathfrak{b}_1$ respectively, then $N\supset E(R,\mathfrak{c}_1,\mathfrak{c}_\lambda)$ where $\mathfrak{c}_1$ is the ideal generated by $\mathfrak{a}_1$ and $\mathfrak{b}_1$, and $\mathfrak{c}_\lambda$ is the special submodule associated with $\mathfrak{c}_1$ generated by $\mathfrak{a}_\lambda$ and $\mathfrak{b}_\lambda$. Therefore, $\mathfrak{a}_1$ and $\mathfrak{a}_\lambda$ are uniquely determined by N. Finally, the result shows that N is a normal subgroup of $G(R)$. q. e. d.

3.21. PROOF OF (1.10) AND (1.11). From (1.9), we have $E^*(R,\mathfrak{a})$ $\supset G(R,\mathfrak{a})\supset E(R,\mathfrak{a})$. If G is simply connected, $T(R,\mathfrak{a})=T'(R,\mathfrak{a})$. Therefore, from (3.3), we have $G(R,\mathfrak{a})=E(R,\mathfrak{a})$. This shows (1.10). (1.11) follows from (1.10) and (2.4). q.e.d.

REFERENCES

[1] C. CHEVALLEY, Sur certains groupes simples, Tôhoku Math. J., 27(1955), 14–66.
[2] C. CHEVALLEY, Certains schémas des groupes semi-simples, Sém. Bourbaki, exp. 219(1960/61).
[3] M. DEMAZURE AND A. GROTHENDIECK, Séminaire de géométrie algébrique, Schémas en groupes, Inst. Hautes Études Sci., (1963–64).
[4] N. IWAHORI AND H, MATSUMOTO, On some Bruhat decomposition and the structure of Hecke ring of p-adic Chevalley groups, Inst. Hautes Etudes Sci. Publ. Math. 25(1965), 5–48.
[5] W. KLINGENBERG, Lineare Gruppen über lokalen Ringen, Amer. J. Math., 83(1961), 137–153.
[6] W. KLINGENBERG, Symplectic groups over local rings, Amer. J. Math., 85(1963), 232–240.
[7] B. KOSTANT, Groups over Z, Proc. Sym. Pure Math. Amer. Math. Soc., 9(1966), 71–83.
[8] H. MATSUMOTO, Subgroups of finite index in certain arithmetic groups, Proc. Sym. Pure Math., Amer. Math. Soc. 9(1966), 99–103.
[9] H. MATSUMOTO, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, to appear.
[10] J. TITS. Algebraic and abstract simple groups, Ann. of Math., 80(1964), 313–329.

DEPARTMENT OF THE FOUNDATIONS OF MATHEMATICAL SCIENCES
TOKYO UNIVERSITY OF EDUCATION
TOKYO, JAPAN