Tôhoku Math. Journ.
28 (1976), 185-198.

ON NORMAL SUBGROUPS OF CHEVALLEY GROUPS OVER COMMUTATIVE RINGS

Dedicated to Professor Ki-ichi Morita on his 60th birthday

EIICHI ABE AND KAZUO SUZUKI

(Received April 4, 1974)

0. Introduction. Let G be a Chevalley-Demazure group scheme associated with a connected complex semi-simple Lie group G_C (as for the definition, see E. Abe [1], 1) and let R be a commutative ring with a unit, $\mathfrak{a}$ an ideal of R. Then the natural ring homomorphism $f: R \rightarrow R/\mathfrak{a}$ induces the group homomorphism $G(f): G(R) \rightarrow G(R/\mathfrak{a})$. The kernel (resp. the inverse image of the center of $G(R/\mathfrak{a})$) of $G(f)$ will be denoted by $G(R, \mathfrak{a})$ (resp. $G^*(R, \mathfrak{a})$) and called the special (resp. general) congruence subgroup modulo $\mathfrak{a}$ of $G(R)$. Any subgroup N of $G(R)$ such that

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

for an ideal $\mathfrak{a}$ of R is a normal subgroup of $G(R)$. Such a normal subgroup of $G(R)$ will be called a congruence subgroup of $G(R)$.

Now let R be a local ring, $\mathfrak{m}$ be the maximal ideal of R and $k = R/\mathfrak{m}$ and let G be simple. One of the authors (cf. E. Abe [1]) has proved that the determination of the normal subgroups of $G(R)$ is reduced to the determination of certain submodules of R except some few cases and that in particular, if G is simply connected, the only normal subgroups of $G(R)$ 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), and that ch. $k \neq 2$ and $k \neq F_3$ if G is of rank 1. This is a generalization of a result given by W. Klingenberg (cf. [5], [6]) for the groups $SL_{n+1}(R)$ and $Sp_{2n}(R)$.

In this note, we shall formulate the problem by some weaker condition than that of the above result and solve the problem for certain class of commutative rings which contains not only local or semi-local rings but also noetherian rings. The main theorem is stated in § 1 with some remarks. In § 2, we shall deal with some important subgroups of $G(R)$ for later use. To prove the theorem, in § 3, we shall first reduce the problem to rings without radicals. Then, in § 4, reduce to m-complete rings (as for the definition cf. § 1). These two reduction theorems lead easily to our main theorem in § 5.

The authors wish to express their thanks to the referee for his careful reading of the original manuscript. By his comment, we can generalize our original result to the present form.

1. Statement of the main theorem. We shall freely use the definitions and notations given in [1], §1. Throughout the paper, G is a simple Chevalley-Demazure group scheme of rank >1 and R is a commutative ring with 1. We denote by $E(R)$ (resp. $G_0(R)$) the subgroup of $G(R)$ generated by $x_\alpha(t)$ for all $t \in R$ and all root $\alpha \in \Delta$ (resp. by $E(R)$ and by $h(\chi)$ for all $\chi \in \mathrm{Hom}(Z[T], R)$) (cf. [1], 1.5). As for the definition of the subgroups $E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ and $E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$, see [1], 1.8. For a given pair (G, R) of simple Chevalley-Demazure group scheme G and a commutative ring R, we are going to find the condition for (G, R) to satisfy the following property:

(N) For any subgroup N of $G_0(R)$ normalized by $E(R)$, there exists a uniquely determined ideal $\mathfrak{a}$ of R and a special submodule $\mathfrak{a}_\lambda$ associated with (G, R) such that

(i) $$E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) \supset N \supset E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$$

(ii) $$G^*(R, \mathfrak{a}_1) \supset N \supset E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$$

(iii) $$E^*(R, \mathfrak{a}_1) \supset N \supset E(R, \mathfrak{a}_1)$$

or

(iv) $$G^*(R, \mathfrak{a}_1) \supset N \supset E(R, \mathfrak{a}_1) .$$

We don't know whether $G(R) = G_0(R)$ for any commutative ring. However, if R is semi-local, then it is true (cf. 2.4). In this case, a subgroup of $G(R)$ normalized by $E(R)$ is a normal subgroup of $G(R)$ and $E(R)$ contains the commutator subgroup of $G(R)$. If G is simply connected and R is local, then for any ideal $\mathfrak{a}$ of R, $G(R, \mathfrak{a}) = E(R, \mathfrak{a})$ (cf. 2.3). Therefore, the conditions (N-iii) and (N-iv) are equivalent in this case. It is an interesting problem to find the condition for R to satisfy $G(R, \mathfrak{a}) = E(R, \mathfrak{a})$ for any ideal $\mathfrak{a}$ of R. Condition (N-ii) is weaker than (N-i). Therefore, it is desirable to characterize the subgroups N by (N-i) rather than by (N-ii).

Now, we shall first state some necessary conditions for (G, R) to verify the condition (N). Let R be a commutative ring and $\mathrm{Spm}\, R = \{\mathfrak{m}_\mu; \mu \in M\}$ be the set of all maximal ideals of R, where M is the set of indices corresponds bijectively to $\mathrm{Spm}\, R$. For any $\mu \in M$, we denote by k_μ the residue class field $R/\mathfrak{m}_\mu$.

(a) If G is of type B_2 or G_2, then $k_\mu \neq F_2$ for any $\mu \in M$, where F_2 is a finite field with two elements.

(b) The characteristic of k_μ is different from the length λ of long roots of Δ for any $\mu \in M$.

From [1], 2.3, we see the following:

1.1. PROPOSITION. *Assume* (G, R) *satisfies* (*a*). *If* (G, R) *verifies* (*N-i*) *or* (*N-ii*) *and further satisfies* (*b*), *then* (G, R) *verifies* (*N-iii*) *or* (*N-iv*) *respectively.*

Note that if (G, R) does not satisfy (b), Proposition 1.1 is not true in general (cf. Example 5.3). Therefore, we restrict our attention to the condition (N-i) or (N-ii).

We shall prove the following fundamental reduction theorem in § 3, whose proof is analogous to that of the groups over local rings.

1.2. PROPOSITION. *Let* J *be the Jacobson radical of* R. *If* $(G, R/J)$ *verifies the condition* (*a*) *and* (*N-i*), *then* (G, R) *verifies also* (*N-i*).

Now, we shall introduce further conditions of R. Let $\mathscr{I}$ be the family of ideals of R which are the intersection of finite numbers of powers of maximal ideals. Namely, $\mathscr{I}$ is the set of the ideals

$$\mathfrak{a}_\alpha = \bigcap_{i=1}^{n} \mathfrak{m}_{\mu_i}^{e_i}, \qquad \mu_i \in M \ (1 \leqq i \leqq n)$$

for any finite set of maximal ideals $\mathfrak{m}_{\mu_1}, \cdots, \mathfrak{m}_{\mu_n}$ and of natural numbers $\alpha = \{e_1, \cdots, e_n\}$. We denote by A the set of all indices α which corresponds bijectively to the ideals of $\mathscr{I}$. We set up the following condition for R.

(c) For any ideal $\mathfrak{a}$ of R, $\mathfrak{a} = \bigcap_{\alpha \in A} (\mathfrak{a} + \mathfrak{a}_\alpha)$.

We denote by $\tilde{R} = \varprojlim_{\alpha} R/\mathfrak{a}_\alpha$ the completion of R with respect to the family of the ideals of $\mathscr{I}$. We shall call an ideal in $\mathscr{I}$ an m-ideal and $\tilde{R}$ the m-completion of R. $\tilde{R}$ is a topological ring by natural way and the condition (c) means that any ideal of R is relatively closed in R. We shall say that a ring R which satisfies the condition (c) is m-complete if $\tilde{R} = R$. Note that any noetherian ring and the direct product of arbitrary numbers of fields satisfy condition (c). Then, we shall prove the following second reduction theorem in § 4.

1.3. PROPOSITION. *Assume* R *satisfies* (*c*) *and let* $\tilde{R}$ *be the* m-*completion of* R. *If* G *is simply connected and* $(G, \tilde{R})$ *verifies* (*N-ii*), *then* (G, R) *also verifies* (*N-ii*).

From these reduction theorems, we shall prove the following in the last section.

1.4. THEOREM. *Let G be simple of rank >1. Assume that R/J is m-complete and $(G, R/J)$ satisfies (a). Then (G, R) verifies (N-i). In particular, if R is a local or semi-local ring and (G, R) satisfies (a), then (G, R) verifies (N-i).*

1.5. THEOREM. *Let G be simple, simply connected of rank >1. Assume $(G, R/J)$ satisfies (a) and (c). Then (G, R) verifies (N-ii). In particular, if R/J is a noetherian ring and $(G, R/J)$ satisfies (a), then (G, R) verifies (N-ii).*

From 1.5 and 1.1, we have the following.

1.6. COROLLARY. *Let G be simple, simply connected of rank >1. Assume $(G, R/J)$ satisfies (a), (b) and (c). Then (G, R) verifies condition (N-iv).*

Recently, J. Wilson [9] has shown that for the general linear group $GL_n(R)$ $(n \geqq 4)$ over a commutative ring R with a unit, the following holds: For a normal subgroup N of $GL_n(R)$, there exists a uniquely determined ideal $\mathfrak{a}$ of R such that

$$GL_n^*(R, \mathfrak{a}) \supset N \supset E(R, \mathfrak{a}) .$$

It is a problem whether our result can be generalized for any commutative ring not necessarily noetherian and any normal subgroups of $G(R)$.

Finally, in the case of Dedekind domain of arithmetic type, using the Matsumoto's result [7] on a problem of congruence subgroups, we can refine our theorem as follows.

1.7. COROLLARY. *Let G be a simply connected, simple Chevalley-Demazure group scheme of rank >1, R a Dedekind domain of arithmetic type and k the quotient field of R. Assume (G, R) satisfies (a) and (b) and k is not totally imaginary, then for any subgroup N of $G_0(R)$ normalized by $E(R)$, there exists a uniquely determined ideal $\mathfrak{a}$ of R such that*

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

2. Certain subgroups of $G(R)$. Let R be a commutative ring with a unit and with the Jacobson radical J. We shall deal with the structure of certain sub-groups of $G(R)$ with respect to J which are analogous to those of the group over a local ring with respect to its maximal ideal given in [1], 2. We shall use the same definitions and notations as in [1], 2.

2.1. PROPOSITION. *Let $\mathfrak{a}_1$ be an ideal of R contained in J and $\mathfrak{a}_2$*

be a special submodule of R associated with $(G, \mathfrak{a}_1)$. Then

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

PROOF. For convenience, denote by $UT'V$ the set in the right side of the above equation. First, we claim that $UT'V$ is normalized by $E(R)$. By the same way as [1], 2.13, 2.14, 2.15, we can prove that $UT'V$ is normalized by $x_{\pm\alpha}(t)$ for any root $\alpha_i \in \Pi$ and any $t \in R$. Therefore, it is normalized by $w_{\alpha_i} = x_{\alpha_i}(1)x_{-\alpha_i}(-1)x_{\alpha_i}(1)$, and then also by $E(R)$. Next, we claim that $x_\alpha(t)UT'V \in UT'V$ for all $x_\alpha(t) \in E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. If $\alpha > 0$, it is obvious and if $\alpha = -\alpha_i$, $\alpha_i \in \Pi$, then it is proved by the same way as [1], 2.13. Now, let $-\alpha$ be any negative root. Since there is an element w of $E(R)$ such that $wx_{-\alpha}(t)w^{-1} = w_{-\alpha_i}(t')$ for some $\alpha_i \in \Pi$, we have

$$\begin{aligned} x_{-\alpha}(t)UT'V &= w^{-1}x_{-\alpha_i}(t')(wUT'Vw^{-1})w = w^{-1}(x_{-\alpha_i}(t')UT'V)w \\ &= w^{-1}(UT'V)w = UT'V . \end{aligned}$$

Thus $UT'V$ is a normal sub-group of $E(R)$. It is the minimal normal subgroup of $E(R)$ containing $x_\alpha(t)$ for all root $\alpha \in \Delta$ and all $t \in \mathfrak{a}_{\lambda(\alpha)}$ and therefore we have $UT'V = E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$.*) q.e.d.

2.2. COROLLARY. *$P(R) = U(R, J)T(R)V(R)$ is a subgroup of $G(R)$.*

PROOF. $E(R, J) = U(R, J)T'(R, J)V(R, J)$ is normalized by $E(R)$ and by $T(R)$. If we set $B(R) = T(R)V(R)$, then we have

$$P(R) = E(R, J)B(R) = B(R)E(R, J) .$$

Therefore, $P(R)$ is a subgroup of $G(R)$.

2.3. PROPOSITION. *Let $\mathfrak{a}$ be an ideal of R contained in J. Then we have*

$$G(R, \mathfrak{a}) = U(R, \mathfrak{a})T(R, \mathfrak{a})V(R, \mathfrak{a}) \subset G_0(R) .$$

In particular, if G is simply connected, then $G(R, \mathfrak{a}) = E(R, \mathfrak{a})$.

PROOF. In the same way as [1], 3.2, if $\mathfrak{a} \subset J$, then we have that $G(R, \mathfrak{a}) \subset G_0(R)$, and any element g of $G(R, \mathfrak{a})$ is uniquely expressed by $g = utv$ for some $u \in U(R, \mathfrak{a})$, $t \in T(R, \mathfrak{a})$ and $v \in V(R, \mathfrak{a})$. If G is simply connected, then $T(R, \mathfrak{a}) = T'(R, \mathfrak{a}) \subset E(R, \mathfrak{a})$. Thus $G(R, \mathfrak{a}) = E(R, \mathfrak{a})$.

2.4. COROLLARY. *Let R be semi-local. Then $G(R) = G_0(R)$ and in particular, if G is simply connected, then $G(R) = E(R)$.*

---

*) In Lemma 2.14 of [1], the condition with respect to y fails, and the proof of 2.18 must be corrected as this proof.

PROOF. Since R is semi-local, $G(R/J)=\prod_{\mu\in M}G(k_\mu)$ where M is a finite set. We have $G(R/J)=G_0(R/J)$ for $G(k_\mu)=G_0(k_\mu)$. On the other hand, from Proposition 2.3, $G(R,J)\subset G_0(R)$. Therefore, we have $G(R)=G_0(R)$. If G is simply connected, then $T(R)=T'(R)\subset E(R)$, and so $G(R)=E(R)$. q.e.d.

3. **Reduction to rings without radicals.** To prove the theorem, we shall reformulate the condition (N-i) (resp. (N-ii)) as follows:

3.1. PROPOSITION. *(N-i) (resp. (N-ii)) is equivalent to the following*
(N′) *Let N be a subgroup of $G_0(R)$ normalized by $E(R)$ such that*

(i) $$E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)\not\supset N\supset E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$$

resp.

(ii) $$G^*(R,\mathfrak{a}_1)\not\supset N\supset E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)\,.$$

Then N contains a unipotent element $x_\alpha(t)$ such that $x_\alpha(t)\notin E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$.

This can be proved in the same way as [1], 3.20. Thus, in § 3 and § 4, we shall prove (N′-i) or (N′-ii) instead of (N-i) or (N-ii) in each cases.

In the present section, we shall prove 1.2. Let J be the Jacobson radical of R. Assume R/J satisfies (a) and $(G,R/J)$ verifies (N-i). We shall prove that (G,R) also satisfies (N-i). Let N be a sub-group of $G_0(R)$ normalized by $E(R)$ with the condition (N′-i). For convenience, we denote by $E_1^*=E^*(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$, $E_1=E(R,\mathfrak{a}_1,\mathfrak{a}_\lambda)$ and $N'=N-E_1^*$. Then 1.2 follows immediately from the following two Propositions 3.2 and 3.3.

3.2. PROPOSITION. *We set $P(R)=U(R,J)T(R)V(R)$. Then*

$$N'\cap P(R)\neq\varnothing\,.$$

PROOF. Let $\pi\colon R\to R/J$ be the natural homomorphism and denote by $\bar R$, $\bar{\mathfrak{a}}_1$ and $\bar{\mathfrak{a}}_\lambda$ the images of R, $\mathfrak{a}_1$ and $\mathfrak{a}_\lambda$ respectively. If $\bar N=NG(R,J)/G(R,J)$ is a central subgroup of $G(\bar R)$, then

$$N\subset NG(R,J)\subset G^*(R,J)\subset P(R)\,.$$

Therefore, we may assume that $\bar N$ is not a central subgroup of $G(\bar R)$. First, assume

$$E^*(\bar R,\bar{\mathfrak{a}}_1,\bar{\mathfrak{a}}_\lambda)\not\supset \bar N\supset E(\bar R,\bar{\mathfrak{a}}_1,\bar{\mathfrak{a}}_\lambda)\,,$$

then by the condition (N′-i) for $(G,\bar R)$, we can conclude that there exists a unipotent element $x_\alpha(t)$ of $N\cdot G(R,J)$ such that $x_\alpha(t)\notin E_1^*\cdot E(R,J)$. Without loss of generality, we may assume α is negative. If we write

$x_\alpha(t) = g \cdot h$ for some $g \in N$ and $h \in G(R, J)$, then $g = x_\alpha(t) \cdot h^{-1} \in N' \cap P(R)$.

Next, assume $E_1(\bar{R}, \bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_\lambda) \supset \bar{N}$. Then $(E_1 \cdot E(R, J))^* \supset N$ and there are $g \in G_0(R)$ and $h \in N$ such that $(g, h) = g_1 g_2 \notin E_1$ where $g_1 \in E_1$ and $g_2 \in E(R, J)$. Since $G_0(R) = E(R)T(R)$, we can choose such an element g from $E(R)$ or $T(R)$. If $g \in T(R)$, then $h \notin T(R)$. Therefore, $g_2 \notin T(R)$ and so $g_2 \notin E_1^*$. Now, assume $g \in E(R)$ and claim $g_2 \notin E^*$. Then, we have $g_1^{-1} \cdot (g, h) \in N' \cap E(R, J) \subset N' \cap P(R)$. This shall complete the proof of Proposition in this case. We shall first give a lemma.

LEMMA. *Let A be a group such that $A = (A, A)$ and B be a normal subgroup of A. If (A, B) is a central subgroup of A, then $(A, B) = \{1\}$.*

PROOF. Let x, y be any elements of A, z be any element of B and denote ${}^z x = zxz^{-1}$. Then

$$({}^z x, (y, z))({}^y z, (x, y))({}^x y, (z, x)) = 1 .$$

Thus $({}^y z, (x, y)) = 1$ for any $x, y \in A$ and $z \in B$. Since $(A, A) = A$, we have $(A, B) = 1$. Lemma q.e.d.

We set $A = E(R)/E_1$ and $B = N/E_1$, then $(A, A) = A$. Applying the above lemma, we have $(A, B) = \{1\}$, namely $(E(R), N) \subset E_1$. This is a contradiction and it must be $g_2 \notin E_1^*$. q.e.d.

We shall use here the notations and definitions of [1], 3 and prove the following.

3.3. PROPOSITION. *Assume that (G, R) satisfies (a). Let N be a subgroup of $G_0(R)$ normalized by $E(R)$.*

(i) If $N' \cap P(R) \neq \emptyset$, then $N' \cap x_\beta(R)x_{\beta'}(R) \neq \emptyset$ where β, β' are dominant roots of Δ.

(ii) If $N' \cap x_\beta(R)x_{\beta'}(R) \neq \emptyset$ where β, β' are dominant roots of Δ, then $N' \cap x_\alpha(R) \neq \emptyset$ for some root α of Δ. (Definition of dominant roots is given in [1] 3.5.)

As for the proof of (ii), see [1] 3.18. To prove (i), we follow the same way as [1] 3.13 and it is sufficient to prove the following.

(P_n) Assume that the rank of G is > 1. If there exists an element $z = xhy$ of $N' \cap P(R)$ such that $x \in U(\Delta') \cap U(R, J)$, $h \in T(R)$, $y \in V(\Delta')$ 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'.

We proceed by induction on n. As for the proof of (P_2) see [1], 3.14, 3.15 and 3.17. We shall give here a proof of $(\mathrm{P}_{n-1}) \Rightarrow (\mathrm{P}_n)$ $(n \geqq 3)$ for the proof given in [1] 3.16 has some gaps.

Without loss of generality, we may assume $n = l$. Denote $z = x_1 x_0 h y_0 y_1$ where $x_1 \in U(\Delta_1)$, $x_0 \in U(\Delta_0)$, $h = h(x) \in T(R)$, $y_0 \in V(\Delta_0)$ and $y_1 \in V(\Delta_1)$.

(i) First, we shall show to be able to assume without loss of generality that $z = x_1 y_1$.

Suppose that $z_0 = x_0 h y_0 \notin E_1^*$ and $x_0 \notin E_1$ or $y_0 \notin E_1$. We note that $U(\Delta_1)$ and $V(\Delta_1)$ are normalized by $G_0(\Delta_0)$. Therefore, by (P_{n-1}), we obtain an element $z' = x_1' x_\gamma(s) x_{\gamma'}(s') y_1'$ of N' such that $x_1' \in U(\Delta_1)$, $y_1' \in V(\Delta_1)$, $x_0' = x_\gamma(s) x_{\gamma'}(s') \in U(\Delta_0)$ where γ, γ' are dominant roots of Δ_0 and $x_\gamma(s) \notin E_1$ or $x_\gamma(s') \notin E_1$. We set $\Delta(x_1')$ (resp. $\Delta(y_1')$) the set of roots β in Δ_1 (resp. $-\Delta_1$) such that x_1' (resp. y_1') is a product of $x_\beta(t) \notin E_1$. If $\Delta(y_1') = \varnothing$, then z has already required property. So that we may assume $\Delta(y_1') \neq \varnothing$. We note that $\gamma - \alpha_1 \notin \Delta$, $\gamma + \alpha_1 \in \Delta$, $\gamma' - \alpha_1 \notin \Delta$ and $\gamma' + \alpha_1 \in \Delta$, and we shall treat two cases separately. Case 1. $x_0' = x_\gamma(s)$ *where* γ *is the highest root of* Δ_0. Suppose that there are roots $\beta \in \Delta(x_1')$ and $\alpha_i \in \Pi$ $(i > 1)$ such that $\beta + \alpha_i \in \Delta$, $\beta - \alpha_i \notin \Delta$ or that there are roots $-\beta \in \Delta(y_1')$ and $\alpha_i \in \Pi$ $(i > 1)$ such that $-\beta + \alpha_i \notin \Delta$, $-\beta - \alpha_i \in \Delta$. Then, since $\gamma + \alpha_i \notin \Delta$ for any α_i $(i > 1)$, a conjugate of $(z', x_{\alpha_i}(1))$ has a form $x_1 y_1$. Otherwise, if $\beta \in \Delta(x_1')$, then $\beta - \alpha_1 \notin \Delta$, $\beta + \alpha_1 \in \Delta$ and if $-\beta \in \Delta(y_1')$, then $-\beta + \alpha_1 \notin \Delta$, $-\beta - \alpha_1 \in \Delta$ and further $\gamma - \alpha_1 \notin \Delta$. Thus $(z', x_{-\alpha_1}(1))$ has a form $x_1' \cdot y_1'$. Case 2. $x_0' = x_\gamma(s) x_{\gamma'}(s')$. In this case, Δ_0 is of type B_{n-1} or C_3. If Δ_0 is of type B_{n-1}, then $\gamma = \alpha_2 + 2\alpha_3 + \cdots + 2\alpha_n$, $\gamma' = \alpha_2 + \alpha_3 + \cdots + \alpha_n$.*) If $2s' \in \mathfrak{a}_1$, then the assertion is obvious and otherwise a conjugate of $(z', x_{\alpha_1 + \cdots + \alpha_n}(1))$ is reduced to the Case 1.

(ii) We may suppose that $z = x_\beta(t) x_{\beta'}(t') x_{\beta''}(t'') y_1'$ where β, β' are dominant roots of Δ such that $\beta'' \in \Delta^+$ and $\alpha_1 + \beta'' = \beta'$ is the highest root of Δ.

This follows from (i) and Lemma 3.11, [1].

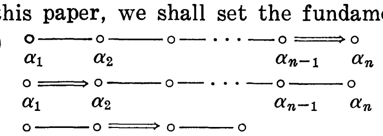
(iii) We shall show to be able to assume that $z' \in U(R) \cap N'$.

Case 1. $\Delta(x_1') = \{\beta'\}, \{\beta''\}$ or $\{\beta', \beta''\}$. If there exist $-\gamma \in \Delta(y_1')$ and $\alpha_i \in \Pi$ $(i > 1)$ such that $-\gamma + \alpha_i \in \Delta$ and $-\gamma - \alpha_i \notin \Delta$, then $(z', x_{\alpha_i}(1)) \in V(R) \cap N'$, for $\beta' + \alpha_i \notin \Delta$, $\beta'' + \alpha_i \notin \Delta$ for any $i > 1$. Otherwise, we may assume that if $-\gamma \in \Delta(y_1')$, then $-\gamma = -\alpha_1$ or $-\gamma + \alpha_1 \in \Delta$ and $-\gamma - \alpha_1 \notin \Delta$. Therefore,

---

*) In this paper, we shall set the fundamental root system as follows:

(B_n), (C_n), (F_4)



$$(z', x_{-\alpha_1}(1)) = x_{\beta''}(\pm t) \in U(R) \cap N' , \quad \text{if} \quad \beta' \in \Delta(x_1')$$

and

$$(z', x_{-\beta'}(1)) = x_{-\alpha_1}(t) \in V(R) \cap N' , \quad \text{if} \quad \beta' \notin \Delta(x_1') .$$

Case 2. $\beta \in \Delta(x_1')$. In this case, Δ is of type B_n, C_n or F_4. Let Δ be of type B_n or C_n. Then we have

$$\beta' = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_n , \quad \beta = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

or

$$\beta' = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_n , \quad \beta = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_{n-1} + \alpha_n$$

respectively. If $2t \in \mathfrak{a}_1$, then a conjugate of $(z', x_{\alpha_1+\cdots+\alpha_n}(1))$ or $(z', x_{\alpha_n}(1))$ is reduced to the Case 1. If $2t \in \mathfrak{a}_1$, then we may assume that α_n is orthogonal to β, β', β'' and to $\Delta(y_1')$. Thus, z' is reduced to the case (P_{n-1}). Now, let Δ be of type F_4. Then we have

$$\beta = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 , \quad \beta' = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 ,$$
$$\beta'' = \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 .$$

These are orthogonal to α_3 and z' is reduced to the case (P_3).

From (iii), again applying Lemma 3.11 [1], we have completed the proof $(\mathrm{P}_{n-1}) \Rightarrow (\mathrm{P}_n)$.

4. **Reduction to m-complete rings.** In this section, we shall prove 1.3. Let R be a commutative ring with condition (c) and $\tilde{R}$ be its m-completion of R, and G be simply connected. Assume $(G, \tilde{R})$ verifies (N-ii) and we shall show that (G, R) also verifies (N-ii). From (c), $\bigcap_{\alpha \in A} \mathfrak{a}_\alpha = 0$. Therefore R is imbedded in $\tilde{R}$ as a dense subring.

4.1. LEMMA. *Let R_μ be the $\mathfrak{m}_\mu$-adic completion of R. Then*

$$\tilde{R} = \prod_{\mu \in M} R_\mu .$$

PROOF. Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{m}_{\mu_i}^{e_i}$ for $\mathfrak{a} \in \mathscr{F}$, and we set $R_{\mu_{i,\alpha}} = R/\mathfrak{m}_{\mu_i}^{e_i}$. Then

$$R/\mathfrak{a}_\alpha = \prod_{i=1}^n R_{\mu_{i,\alpha}} .$$

The natural homomorphism

$$f_{\alpha\beta}\colon R/\mathfrak{a}_\beta \longrightarrow R/\mathfrak{a}_\alpha \quad \text{for} \quad \mathfrak{a}_\beta \subset \mathfrak{a}_\alpha$$

gives a natural local homomorphism

$$f_{\alpha\beta}^\mu\colon R_{\mu,\beta} \longrightarrow R_{\mu,\alpha} \quad \text{for} \quad \mathfrak{a}_\alpha \subset \mathfrak{m}_\mu .$$

We write $f_{\alpha\beta}^\mu = 0$ if $\mathfrak{a}_\beta \subset \mathfrak{m}_\mu$ but $\mathfrak{a}_\alpha \not\subset \mathfrak{m}_\mu$. We set

$$I = \{(\mu, \alpha) \in M \times A; \mathfrak{a}_\alpha \subset \mathfrak{m}_\mu\}$$

and consider the product $\prod_{(\mu,\alpha)\in I} R_{\mu,\alpha}$. Each $R/\mathfrak{a}_\alpha$ is identified with the subalgebra of that product consisting of the partial product of $R_{\mu,\alpha}$ for all μ such that $(\mu, \alpha) \in I$. If $\alpha \leqq \beta$, then for any $\mu \in M$ such that $(\mu, \beta) \in I$ the diagram

$$\begin{array}{ccc} R/\mathfrak{a}_\beta & \xrightarrow{f_{\alpha\beta}} & R/\mathfrak{a}_\alpha \\ \downarrow & & \downarrow \\ R_{\mu,\beta} & \xrightarrow[f^\mu_{\alpha\beta}]{} & R_{\mu,\alpha} \end{array}$$

is commutative. Now, by the above identification, we have

$$\begin{aligned} \tilde{R} &= \left\{z = (z_\alpha) \in \prod_{\alpha\in A} (R/\mathfrak{a}_\alpha); f_{\alpha\beta}(z_\beta) = z_\alpha,\ \alpha \leqq \beta\right\} \\ &= \left\{x = (x_{\mu,\alpha}) \in \prod_{(\mu,\alpha)\in I} R_{\mu,\alpha}; f_{\alpha\beta}(x_{\mu,\beta}) = x_{\mu,\alpha},\ \alpha \leqq \beta\right\} . \end{aligned}$$

But for each $\mu \in M$, the set $I_\mu = \{\alpha \in M, (\mu, \alpha) \in I\}$ is confinal to M and we see $R_\mu = \varprojlim_\alpha R_{\mu,\alpha}$. Since we may write

$$\prod_{(\mu,\alpha)\in I} R_{\mu,\alpha} = \prod_{\mu\in M} \left(\prod_{\alpha\in I} R_{\mu,\alpha}\right) ,$$

$\tilde{R}$ is identified with the product $\prod_{\mu\in M} R_\mu$. q.e.d.

4.2. COROLLARY. *The Jacobson radical* $J(\tilde{R})$ *of* $\tilde{R}$ *is isomorphic to* $\prod_{\mu\in M} \mathfrak{m}_\mu$ *and* $\tilde{R}/J(\tilde{R})$ *is m-complete.*

PROOF. We set $\mathfrak{a} = \prod_{\mu\in M} \mathfrak{m}_\mu$, then $\mathfrak{a}$ is an ideal of $\tilde{R} = \prod_{\mu\in M} R_\mu$. If $m = (m_\mu) \in \mathfrak{a}$, then $1 + m$ is invertible in R_μ for each $\mu \in M$ which implies that $1 + m$ is invertible in $\tilde{R}$. Thus we have $J(\tilde{R}) = \mathfrak{a}$. Further, $\tilde{R}/J(\tilde{R}) = \prod_{\mu\in M} k_\mu$ shows that $\tilde{R}/J(\tilde{R})$ is m-complete. q.e.d.

4.3. PROOF OF 1.3. Let N be a subgroup of $G_0(R)$ normalized by $E(R)$ such that

$$G^*(R, \mathfrak{a}_1) \not\supset N \supset E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) .$$

We must show that there exists a unipotent element $x_\alpha(t) \in N$ such that $x_\alpha(t) \notin E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. By definition, $G(\tilde{R}) = \varprojlim_\alpha G(R/\mathfrak{a}_\alpha)$. Since G is simply connected and $R/\mathfrak{a}_\alpha$ is semi-local for all $\alpha \in A$, we have $G(R/\mathfrak{a}_\alpha) = E(R/\mathfrak{a}_\alpha)$ from 2.4. Therefore, the natural homomorphism $G(R) \to G(R/\mathfrak{a}_\alpha)$ is onto for all $\alpha \in A$ and we see

$$G(\tilde{R}) = \varprojlim_\alpha G(R)/G(R, \mathfrak{a}_\alpha) .$$

Denote by $\tilde{\mathfrak{a}}$ (resp. $\tilde{N}$) the closure of $\mathfrak{a}$ in $\tilde{R}$ (resp. of N in $G(\tilde{R})$). Then

$$G(\tilde{R}, \tilde{\mathfrak{a}}) = \varprojlim_{\alpha} G(R, \mathfrak{a} + \mathfrak{a}_\alpha)/G(R, \mathfrak{a}_\alpha)$$

and we claim that

$$E^*(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda) \not\supset \tilde{N} \supset E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda) .$$

In fact, $\tilde{N} \supset E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda)$ is obvious. Suppose $E^*(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda) \supset \tilde{N}$. Then

$$(\tilde{N}, G(\tilde{R})) \subset E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda)$$

which implies for any ideal $\mathfrak{a}_\alpha$ of $\mathscr{I}$,

$$(N, G(R)) \subset (E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda) \cap G(R)) \cdot G(R, \mathfrak{a}_\alpha) .$$

Therefore, $(N, G(R)) \subset G(R, \mathfrak{a}_1 + \mathfrak{a}_\alpha)$ for any ideal $\mathfrak{a}_\alpha \in \mathscr{I}$. Thus, we have

$$(N, G(R)) \subset \bigcap_{\alpha \in M} G(R, \mathfrak{a}_1 + \mathfrak{a}_\alpha) = G(R, \mathfrak{a}_1) .$$

This contradicts to our assumption, namely, we have $E^*(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda) \not\supset \tilde{N}$. Now, from the condition (N'-i) for m-complete rings with 1.2 and 4.2, we have $\tilde{R}$ also verifies (N'-i), and since $\tilde{N}$ is normalized by $E(\tilde{R})$, there exists a unipotent element $x_\alpha(t) \in \tilde{N}$ such that $x_\alpha(t) \notin E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda)$ for some $t \in \tilde{R}$. We set $\tilde{N}' = \tilde{N} - E(\tilde{R}, \tilde{\mathfrak{a}}_1, \tilde{\mathfrak{a}}_\lambda)$ and $N' = N - E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. Since $x_\alpha(\tilde{R}) = \widetilde{x_\alpha(R)}$, we see $x_\alpha(\tilde{R}) \cap G(R) = x_\alpha(R)$. Therefore, $x_\alpha(\tilde{R}) \cap N' = x_\alpha(R) \cap N'$ is a dense subset of $x_\alpha(\tilde{R}) \cap \tilde{N}' \neq \emptyset$ which is not empty as shown above. Thus we have $x_\alpha(R) \cap N' \neq \emptyset$ which completes the proof. q.e.d.

5. Conclusion of the proof and an example.

5.1. PROOF OF 1.4. Assume that R/J is m-complete and $(G, R/J)$ satisfies (a). We shall show that (G, R) verifies (N-i). From 1.2, we may assume that $J = 0$. Since R is m-complete, $\tilde{R} = R = \prod_{\mu \in M} k_\mu$. Therefore $G(R) \cong \prod_{\mu \in M} G(k_\mu)$. Now, let N be a non-central subgroup of $G_0(R)$ normalized by $E(R)$ such that

$$E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) \not\supset N \supset E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) .$$

For any $\mu \in M$, we have the natural homomorphism

$$\psi_\mu \colon G(R) \to G(k_\mu) .$$

Let $Z(R)$ (resp. $Z(k_\mu)$) be the center of $G(R)$ (resp. $G(k_\mu)$). Then $Z(R) \simeq \prod_{\mu \in M} Z(k_\mu)$. The images by ψ_μ of N, $E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ and $E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$ are normal subgroups of $G(k_\mu)$ and either contained in $Z(k_\mu)$ or contain $E(k_\mu)$, in fact $E(k_\mu)$ is simple over its center. (cf. J. Tits [8])

Now, we set

$$K = \{\mu \in M;\ \psi_\mu(E(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)) \supset E(k_\mu)\}$$
$$L = \{\mu \in M;\ \psi_\mu(N) \supset E(k_\mu)\}\ .$$

Then we have $L \supsetneqq K \neq \varnothing$. In fact, $K \neq \varnothing$ follows from the fact that N is not central and $L \supsetneqq K$ follows from $E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda) \not\supset N$.

If we take an index $\mu \in L - K$, we have

$$N \supset (N, E(k_\mu)) \supset (E(k_\mu), E(k_\mu)) = E(k_\mu)\ .$$

Therefore, there exists an element $x_\alpha(t) \in E(k_\mu)$ in N which is not contained in $E^*(R, \mathfrak{a}_1, \mathfrak{a}_\lambda)$. q.e.d.

5.2. Proof of 1.5. Assume G is simply connected and $(G, R/J)$ satisfies (a) and (c). We shall show that (G, R) verifies (N-ii). From 1.2, we may assume $J = 0$. Let $\tilde{R}$ be m-completion of R. Then from 1.4, $(G, \tilde{R})$ verifies (N-i) and in particular (N-ii). Since R satisfies (c), from 1.3, (G, R) also verifies (N-ii). q.e.d.

5.3. Example. *A normal subgroup of symplectic modular groups.* We shall give an example of a normal subgroup of $Sp_{2n}(Z)$ for which the condition (N-iv) does not hold when (G, R) does not satisfy (b). $Sp_{2n}(Z)$ is by definition, the group of all $2n \times 2n$ matrices x with entries in Z such that ${}^t xJx = J$, where $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, I being the unit matrix of degree n. An element $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $GL_{2n}(Z)$ is contained in $Sp_{2n}(Z)$ if and only if ${}^t a\, d - {}^t c\, b = I$, ${}^t a\, c = {}^t c\, a$ and ${}^t d\, b = {}^t b\, d$, where $a = (a_{ij})$, $b = (b_{ij})$, $c = (c_{ij})$ and $d = (d_{ij})$ are $n \times n$ matrices with entries in Z. For an integer $q \geqq 1$, define $Sp_{2n}(Z, qZ)$ and $Sp^*_{2n}(Z, qZ)$ as in introduction.

Now, let $n \geqq 2$ and let N be the set of all elements of $Sp_{2n}(Z, 2Z)$ such that

$$(*) \qquad b_{ii} \equiv c_{ii} \equiv 0 \pmod 4\ (1 \leqq i \leqq n)\ .$$

We shall show that N is a normal subgroup of $Sp_{2n}(Z)$ and it contains the subgroup $Sp_{2n}(Z, 4Z)$ but not contained in $Sp^*_{2n}(Z, 4Z)$. We denote by $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ or $x_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ $(i = 1, 2)$ elements of $Sp_{2n}(Z)$. We claim that if $x_i \in Sp_{2n}(Z, 2Z)$ $(i = 1, 2)$ and $x = x_1 x_2$ then

$$b \equiv b_1 + b_2\ , \quad c \equiv c_1 + c_2 \pmod 4\ .$$

We set $a_i = I + 2a_i'$, $d_i = I + 2d_i'$ $(i = 1, 2)$, then

$$b = a_1 b_2 + b_1 d_2 = b_1 + b_2 + 2(a_1' b_2 + b_1 d_2')\ .$$

Since $b_1 \equiv b_2 \equiv 0 \pmod 2$, we see $b \equiv b_1 + b_2 \pmod 4$. Similarly, we have $c \equiv c_1 + c_2 \pmod 4$. This shows that if $x_1, x_2 \in N$, then $x_1 x_2 \in N$ and if

$x \in N$, then $x^{-1} \in N$, i.e., N is a subgroup of $Sp_{2n}(Z)$. Next, we claim that N is normal. We note that $Sp_{2n}(Z)$ is generated by the matrices

$$y = \begin{pmatrix} u & 0 \\ 0 & t_u^{-1} \end{pmatrix}, \quad z = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \text{ and } z' = \begin{pmatrix} 1 & 0 \\ v' & 1 \end{pmatrix}$$

where $u \in GL_n(Z)$ and v, v' are symmetric $n \times n$-matrices with entries in Z (cf. for example, J. Mennicke: Zur Theorie der Siegelishen Module Gruppe, Math. Ann. 159, 1965, p. 115–p. 129). Therefore, to prove that N is normal, it is enough to show that yxy^{-1}, zxz^{-1} and $z'xz'^{-1} \in N$ for any $x \in N$. Let first $x \in N$ and $x_1 = yxy^{-1}$. Since ${}^tb \equiv b \pmod 4$, (i, i)-component of $b_1 = ub{}^tu$ is $\sum_{j,k} u_{ik}b_{kj}u_{ij} \equiv 2\sum_{k<j} u_{ik}b_{kj}u_{ij} + u_{ik}b_{kk}u_{ik} \equiv 0 \pmod 4$. Thus, b_1 and also c_1 have the property (*) and we have $x_1 \in N$. Next, let $x \in N$ and $x_2 = zxz^{-1}$. Denote $a = I + 2a'$, $d = I + 2d'$. Then ${}^ta' + d' \equiv 0 \pmod 2$, for ${}^ta \cdot d \equiv I + 2({}^td' + d') \equiv I + {}^tc \cdot b \equiv I \pmod 4$. Now, we have

$$b_1 = -av - vcv + b + vd = -2(a'v - vd') - vcv + b .$$

Here, $a'v - vd' \equiv a'v + v{}^ta' \pmod 2$ and $a'v + v{}^ta'$ is symmetric. Further, vcv is symmetric mod 4 and its (i, i)-component is

$$\sum_{j,k} v_{ij}c_{jk}v_{ki} = 2\sum_{j<k} v_{ij}c_{jk}v_{ki} + v_{ik}c_{kk}v_{ki} \equiv 0 \pmod 4 .$$

Thus, b_1 and also c_1 have the property (*) and $x_1 \in N$. Similary, we see $z'xz'^{-1} \in N$ for any $x \in N$. Thus we have proved that N is a normal subgroup of $Sp_{2n}(Z)$.

It is easy to see that N contains $Sp_{2n}(Z, 4Z)$ but not contained in $Sp^*_{2n}(Z, 4Z)$. Moreover, if q is a multiple of 4, then $Sp^*_{2n}(Z, qZ) \not\supset N$ and if q is not a multiple of 4, then $N \not\supset Sp_{2n}(Z, qZ)$. Therefore, there exists no integer $q \geqq 0$ such that $Sp^*_{2n}(Z, qZ) \supset N \supset Sp_{2n}(Z, qZ)$.

References

[1] E. Abe, Chevalley groups over local rings, Tôhoku Math. J. 21 (1969), 474–494.

[2] H. Bass, J. Milnor and J. P. Serre, Solution of the congruence subgroup problem for $SL_n(n \geqq 3)$, $Sp_{2n}(n \geqq 2)$, Pub. Math. I.H.E.S. No. 33 (1967).

[3] C. Chevalley, Sur certain groups simples, Tôhoku Math. J. 7 (1955), 14–66.

[4] C. Chevalley, Certains schemas des groups semi-simples, Sem. Bourbaki, No. 217 (1960–61).

[5] W. Klingenberg, Linear Gruppen über lokalen Ringen, Amer. J. Math. 83 (1961), 137–157.

[6] W. Klingenberg, Symplectic groups over local rings, Amer. J. Math. 83 (1963), 232–240.

[7] H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployes, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 1–62.

[8] J. TITS, Algebraic and abstruct simple groups, Ann. of Math. 80 (1964), 313-329.
[9] J. WILSON, The normal and subnormal structure of general linear groups, Proc. Camb. Phil. 71 (1972), 163-177.

DEPARTMENT OF THE FOUNDATIONS
OF MATHEMATICAL SCIENCES
TOKYO UNIVERSITY OF EDUCATION
OTSUKA 3-29-1, BUNKYO-KU, TOKYO
AND
DEPARTMENT OF MATHEMATICS
FACULTY OF GENERAL EDUCATION
KUMAMOTO UNIVERSITY
KUROKAMI-CHO, KUMAMOTO