

PRODUCTS OF CONJUGACY CLASSES IN CHEVALLEY GROUPS OVER LOCAL RINGS

N. GORDEEV AND J. SAXL

ABSTRACT. Estimates of extended covering numbers are obtained for Chevalley groups over local rings.

§1. INTRODUCTION

In this paper we continue the investigation of products of conjugacy classes in finite groups and in algebraic groups; see [GS1, GS2].

Here we consider a different type of perfect groups: Chevalley groups over rings. Namely, let \tilde{G} be a simple and simply connected algebraic group over \mathbb{C} . Then, for every commutative ring A , the group $\tilde{G}(A)$ ([Ab, St]) can be defined — this is the Chevalley group over A . We treat the case where A is a local ring. We prove (Theorem 1) that if A is a complete local ring and $\tilde{G}(K)$ is a quasisimple group over the residue field K of A , then

$$\text{ecn}(\tilde{G}(A)) \leq 6 \text{ecn}(\tilde{G}(K)).$$

This fact was announced in [GS1]. (For a group G , the symbol $\text{ecn}(G)$ denotes the *extended covering number* of G ,

$$\text{ecn}(G) = \min\{n \in \mathbb{N} \mid C_1 C_2 \cdots C_n = G \text{ for any } n \text{ conjugacy classes } C_1, \dots, C_n \text{ of } G \text{ such that } \langle C_1 \rangle = \langle C_2 \rangle = \cdots = \langle C_n \rangle = G\};$$

see [GS1].)

This inequality implies

$$\text{ecn}(\tilde{G}(A)) \leq d \cdot \text{rank } \tilde{G},$$

where d is a general constant that does not depend on \tilde{G} or A (Corollary 1). For a general local ring A , in Theorem 2 we prove that if the residue field K is large, then

$$\text{ecn}(\tilde{G}(A)) \leq 8 \text{ecn}(\tilde{G}(K)).$$

In the final part of the paper we consider problems similar to those treated by J. Thompson and O. Ore for a group $\tilde{G}(A)$ over a local ring A (see [EG2]). In the case of a large residue field K , we show the existence of a real conjugacy class $C \subset \tilde{G}(A)$ such that the set C^2 contains all generating conjugacy classes of $\tilde{G}(A)$. In particular, every element in a generating conjugacy class of $\tilde{G}(A)$ is a single commutator (Theorem 3).

2000 *Mathematics Subject Classification*. Primary 14L15, 14L17, 20G35.

Key words and phrases. Products of conjugacy classes, Chevalley groups.

The first author was supported by EPSRC (grant GR/R79081/01), by Russian Ministry of Education (grant E02-1.0-15), by RTF Network (grant HPRN-CT-2002-00287), and by RFBR (grant no. 03-01-00349).

§2. NOTATION, TERMINOLOGY, CONVENTIONS

2.1. Let G be a group. Then:

- (a) $Z(G)$ is the center of the group G ;
- (b) a *generating conjugacy class* C of the group Γ is a class such that $\langle C \rangle = \Gamma$;
- (c) the union of all generating conjugacy classes is denoted by $\text{GN}(\Gamma)$.

2.2. Let A be a commutative ring, and let V be an $A[G]$ -module.

Let $I_{A[G]} = \{a_1(g_1 - 1) + a_2(g_2 - 1) + \dots + a_n(g_n - 1) \mid a_i \in A, g_i \in G\}$ be the *augmentation ideal* of $A[G]$. If $A = \mathbb{Z}$, we shall write I_G instead of $I_{\mathbb{Z}[G]}$. An $A[G]$ -module V is said to be *augmentative* if $I_{A[G]}V = V$. Obviously, $I_{A[G]}V = I_G V$; therefore, an $A[G]$ -module V is augmentative if and only if it is augmentative as a $\mathbb{Z}[G]$ -module.

2.3. All algebraic groups treated here are linear algebraic groups defined over a field K (see [Bo]). We omit the field of definition K if it is assumed to be algebraically closed.

§3. CHEVALLEY GROUPS OVER COMPLETE LOCAL RINGS

Let \tilde{G} be a simple simply connected algebraic group over \mathbb{C} corresponding to a root system R , and let \tilde{G}_Z be the corresponding group scheme over \mathbb{Z} (see [Ab, St]). Then for every commutative ring A the group $\tilde{G}_Z(A)$ will be denoted by $\tilde{G}(A)$.

Next, let A be a local ring, M its maximal ideal, and $K = A/M$ its residue field. Consider the groups $\tilde{G}(A/M^n)$. Then

$$(3.1) \quad \tilde{G}(A) = \langle x_\alpha(a) \mid \alpha \in R, a \in A \rangle,$$

where $x_\alpha(a)$ is an element of the corresponding root subgroup (see [Ab]).

Denote by

$$\tilde{G}(M^n) = \text{Ker}(\tilde{G}(A) \longrightarrow \tilde{G}(A/M^n))$$

the corresponding congruence subgroup. Then (see [Ab])

$$(3.2) \quad \tilde{G}(M^n) = \langle h_\alpha(t), x_\alpha(m) \mid t \in A, t \equiv 1n \pmod{M^n}, m \in M^n, \alpha \in R \rangle$$

(here $h_\alpha(t), t \in A^* = A \setminus M$, is a root semisimple element defined in [St]).

The following result was formulated (without proof) in [GS1].

Theorem 1. *Let A be a complete local ring, and let $\tilde{G}(K)$ be a quasisimple group. Then*

$$\text{ecn}(\tilde{G}(A)) \leq 6 \text{ecn}(\tilde{G}(K)).$$

Proof. Consider the group $L(n) = \tilde{G}(M^n)/\tilde{G}(M^{n+1})$. The Chevalley commutator formula and (3.2) show that $L(n)$ is an Abelian group isomorphic to a vector space over K . Let $\{m_i\}_{i \in I}$ be a basis of the K -vector space M^n/M^{n+1} , and let

$$L_i = \langle x_\alpha(m), h_\delta(1 + m) \mid m \equiv dm_i \pmod{M^{i+1}} \text{ for some } d \in K \rangle.$$

Then

$$(3.3) \quad L(n) \cong \sum_{i \in I} L_i.$$

The action of $\tilde{G}(A)$ on $\tilde{G}(M^n)$ by conjugation gives the structure of a $\tilde{G}(K)$ -module on $L(n)$.

Lemma 1. *The decomposition (3.3) is a decomposition into a sum of $\tilde{G}(K)$ -modules, where each L_i is isomorphic as a $\tilde{G}(K)$ -module to the corresponding Lie algebra $L(K)$ with adjoint action of $\tilde{G}(K)$ on it.*

Proof. Let $L = L(K) = \sum_{\alpha \in R} Ku_\alpha \oplus \sum_{\delta \in \Delta} K\mathfrak{h}_\delta$ be a Lie algebra corresponding to the Chevalley group $\tilde{G}(K)$, where Δ is a simple root subsystem of R and $\{u_\alpha, \mathfrak{h}_\delta\}$ is a Chevalley basis of L . Note that the construction of the group $\tilde{G}(A)$ presupposes that this group is acting as an automorphism group on a free module A^s for some s (see [Ab, St]). Moreover, the Lie ring $L(A) = \sum_{\alpha \in R} Au_\alpha \oplus \sum_{\delta \in \Delta} A\mathfrak{h}_\delta$ is embedded in $\text{End}_A A^s$, and $x_\alpha(a) = \exp(au_\alpha)$, $a \in A$.

We view the group $\tilde{G}(M^n)/\tilde{G}(M^{n+1})$ as a subgroup of $\text{Aut}_A(A/M^{n+1})^s$. Let $m \in M$, $m \equiv dm_i \pmod{M^{n+1}}$, $d \in K$. Then the operator $x_\alpha(m) \pmod{\tilde{G}(M^{n+1})}$ in $\text{Aut}(A/M^{n+1})^s$ is equal to $1 + mu_\alpha = 1 + dm_i u_\alpha$ (in spite of the fact that the residue field K is not necessarily contained in A , we can identify multiplication by m with multiplication by dm_i , because the operator we consider is in $(A/M^{n+1})^s$). Next, $h_\delta(1 + m) \pmod{\tilde{G}(M^{n+1})} = 1 + dm_i \mathfrak{h}_\delta$ (this can be checked by considering $(Au_\delta + Au_{-\delta} + A\mathfrak{h}_\delta) \pmod{M^{n+1}}$). Now we have a $\tilde{G}(K)$ -isomorphism of $\tilde{G}(K)$ -modules

$$\exp \cdot m_i : L \longrightarrow L_i$$

(here $\exp \cdot m_i(l) = \exp(m_i l)$). □

Lemma 2. $L(n)$ is an augmentative $K[\tilde{G}(K)]$ -module.

Proof. This follows from Lemma 1 and the fact that the adjoint action of a Chevalley group is augmentative (see [GS2, Theorem 3.C]). □

Lemma 3. If A is a complete local ring, then

$$\tilde{G}(A) = \varprojlim \tilde{G}(A/M^n).$$

Proof. Let

$$\theta : \tilde{G}(A) \longrightarrow \varprojlim \tilde{G}(A/M^n)$$

be the homomorphism induced by the natural homomorphisms

$$\theta_n : \tilde{G}(A) \longrightarrow \tilde{G}(A/M^n).$$

From (3.2) we see that $\bigcap_n \tilde{G}(M^n) = \{1\}$. Therefore, θ is a monomorphism.

We prove that θ is an epimorphism. Every element

$$g \in \varprojlim \tilde{G}(A/M^n)$$

is a sequence $\{g_n\}_n$ such that $g_n \in \tilde{G}(A/M^n)$ and $\theta_{n,m}(g_n) = g_m$ for every $n \geq m$, where

$$\theta_{n,m} : \tilde{G}(A/M^n) \longrightarrow \tilde{G}(A/M^m)$$

is the natural epimorphism. Let \tilde{g}_1 be a preimage of g_1 in $\tilde{G}(A)$. Then there exists a sequence $\{h_n\}_n$, $n \geq 2$, of elements of $\tilde{G}(M)$ such that

$$(3.4) \quad g_n \equiv \tilde{g}_1 h_n \pmod{\tilde{G}(M^n)}$$

for every $n \geq 2$. Let R^-, R^+, Δ be (respectively) the sets of negative, positive, and simple roots that correspond to \tilde{G} . Then

$$(3.5) \quad h_n = \left(\prod_{\alpha \in R^-} x_\alpha(a_{\alpha,n}) \right) \left(\prod_{\delta \in \Delta} h_\delta(b_{\delta,n}) \right) \left(\prod_{\alpha \in R^+} x_\alpha(c_{\alpha,n}) \right),$$

where $a_{\alpha,n}, c_{\alpha,n} \in M$, $b_{\delta,n} \equiv 1 \pmod{M}$ (see [Ab]). Since $\theta_{n,m}(g_n) = g_m$ for every $n \geq m$, the congruences (3.4) imply that $\theta_{n,m}(\theta_n(h_n)) = \theta_m(h_m)$ for every $n \geq m$. Consequently,

$$(3.6) \quad a_{\alpha,n} \equiv a_{\alpha,m} \pmod{M^m}, \quad b_{\delta,n} \equiv b_{\delta,m} \pmod{M^m}, \quad c_{\alpha,n} \equiv c_{\alpha,m} \pmod{M^m}$$

for every $n \geq m$. Since A is a complete local ring, (3.6) implies the existence of elements $a_\alpha, c_\alpha \in M$ and $b_\delta \in 1 + M$ such that

$$(3.7) \quad a_\alpha \equiv a_{\alpha,n} \pmod{M^n}, \quad b_\delta \equiv b_{\delta,n} \pmod{M^n}, \quad c_\alpha \equiv c_{\alpha,n} \pmod{M^n}$$

for every n (see [B2]). Putting

$$(3.8) \quad h = \left(\prod_{\alpha \in R^-} x_\alpha(a_\alpha) \right) \left(\prod_{\delta \in \Delta} h_\delta(b_\delta) \right) \left(\prod_{\alpha \in R^+} x_\alpha(c_\alpha) \right),$$

from (3.4)–(3.8) we obtain

$$\theta(\tilde{g}_1 h) = \{g_n\}_n.$$

Thus, θ is a surjection and, therefore, an isomorphism. □

Now we can finish the proof of Theorem 1. Let G be a group containing a normal subgroup $N \triangleleft G$ such that

- (i) there exists a sequence $\{N_i\}_{i=1}^{i=\infty}$ of subgroups of N with the following properties: $N_i \triangleleft G$ for every i , $[N_i, N] \leq N_{i+1}$ for every i , and N_{i+1}/N_i is an augmentative $\mathbb{Z}[G/N]$ -module for every i ;
- (ii) $N = \varprojlim N/N_i$.

Then $\text{ecn}(G) \leq 3k \text{ecn}(G/N)$, where $k \leq \text{gen}(G/N)$ (see [GS1, Proposition 3]). Now the claim follows from this inequality, Lemmas 1, 2, 3, and the fact that $\text{gen}(\tilde{G}(K)) = 2$. □

In [GS1] it was proved that there exists a constant c such that $\text{ecn}(G) \leq c \cdot \text{rank}(G)$ for every Chevalley group G . Theorem 1 shows that this result extends to all Chevalley groups over complete local rings.

Now, let $c(\tilde{G})$ be a constant such that

$$\text{ecn}(\tilde{G}) \leq c(\tilde{G}) \cdot \text{rank}(\tilde{G})$$

for every field K .

Corollary 1. *Let $A = \prod_{i \in I} A_i$ be a direct product of complete local rings. Then*

$$\text{ecn}(\tilde{G}(A)) \leq 6c(\tilde{G}) \cdot \text{rank}(\tilde{G}).$$

Proof. We have $\tilde{G}(A) = \prod_{i \in I} \tilde{G}(A_i)$. Obviously, we have $\text{ecn}(\tilde{A}) \leq \max\{\text{ecn}(\tilde{G}(A_i))\}$, and the claim follows from Theorem 1. □

Corollary 2. *If*

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z},$$

then

$$\text{ecn}(\tilde{G}(\mathbb{Z}/n\mathbb{Z})) \leq \text{ecn}(\tilde{G}(\widehat{\mathbb{Z}})) \leq 6c(\tilde{G}) \cdot \text{rank}(\tilde{G})$$

for every n .

Proof. This follows from Corollary 1. □

§4. CHEVALLEY GROUPS OVER LOCAL RINGS WITH A LARGE RESIDUE FIELD

For general local rings, we can give an estimate if the residue field is large (below we keep the previous notation). Let \tilde{T} be a maximal split torus of \tilde{G} , and let $T = \tilde{T}(A)$. An element $t \in T$ is said to be *regular* if $tx_\alpha(a)t^{-1} \neq x_\alpha(a)$ for every $\alpha \in R$ (where R is the root system for \tilde{G}) and every $a \in A, a \neq 0$. Let \tilde{U} (respectively, \tilde{U}^-) be the subgroup of \tilde{G} generated by all positive (respectively, negative) root subgroups, and let $U = \tilde{U}(A), U^- = \tilde{U}^-(A)$.

We need the following proposition, which is an analog of the main result in [EG1] for fields.

Proposition 1. *Let $t \in T$ be a regular element such that $\bar{t} = t \pmod{\tilde{G}(M)}$ is a regular element of $\tilde{G}(K)$. Then every generating conjugacy class C of $\tilde{G}(A)$ has a representative g of the form*

$$g = vtu, \quad v \in U^-, \quad u \in U.$$

Proof. Let \bar{C} be the image of C in $\tilde{G}(K)$. Then there exists an element $\bar{g}' \in \bar{C}$ such that

$$(4.1) \quad \bar{g}' = \bar{v}'\bar{t}\bar{u}'$$

for some $\bar{v}' \in \bar{U}^-$ and $\bar{u}' \in \bar{U}$, where \bar{U}^- and \bar{U} are the images of the groups U^- and U in $\tilde{G}(K)$, and \bar{t} is the image of t in $\tilde{G}(K)$ (see [EG1]). Let $g' \in C, v' \in U^-,$ and $u' \in U$ be preimages of $\bar{g}, \bar{v},$ and $\bar{u},$ respectively. From (4.1) we obtain

$$(4.2) \quad g' = v'tu'm, \quad m \in \tilde{G}(M).$$

On the other hand,

$$(4.3) \quad m = u''t'v'', \quad u'' \in U \cap \tilde{G}(M), \quad v'' \in U^- \cap \tilde{G}(M), \quad t' \in \tilde{T}(A) \cap \tilde{G}(M).$$

Putting $g_1 = v''g'v''^{-1},$ from (4.2) and (4.3) we see that

$$(4.4) \quad g_1 = vt't'u \quad \text{for some } v \in V, \quad u \in U.$$

We shall show that tt' in (4.4) can be replaced by $t.$ This is done by conjugating tt' by an appropriate element of $\tilde{G}(A).$

Lemma 4. *Let σ be a diagonal automorphism of $\tilde{G}(A),$ i.e., $\sigma(x_\alpha(a)) = x_\alpha(\omega_\alpha a),$ $\sigma(x_{-\alpha}(a)) = x_{-\alpha}(\omega_\alpha^{-1}a)$ for some $\omega_\alpha \in A^* = A \setminus M.$ Let $\tau \in \tilde{G}(A)$ be an element of the form $\tau = vhh'u$ for some $v \in U^-, u \in U$ and some $h \in \tilde{T}(A), h' \in \tilde{T}(A) \cap \tilde{G}(M).$ Suppose*

$$\sigma((hh')x_\alpha(a)(hh')^{-1}) \not\equiv x_\alpha(a) \pmod{\tilde{G}(M)}$$

for every $\alpha \in R$ and every $a \in A, a \neq 0.$ Then there exists an element $g \in \tilde{G}(A)$ such that

$$g\sigma\tau g^{-1} = v'\sigma hu'$$

for some $v' \in U^-, u' \in U.$ (We view $\sigma\tau$ as an element of the group $E = \langle \sigma, \tilde{G}(A) \rangle.$)

Proof. If the rank of R is one, then the proof is almost the same as in the case where A is a field; see [EG1, Part I, Lemma 1].

We assume that the statement of the lemma is valid for every Chevalley group of rank less than r and consider the case where the rank of R is $r.$

Let

$$(4.5) \quad h = \prod_{\delta \in \Delta} h_\delta(s_\delta), \quad h' = \prod_{\delta \in \Delta} h_\delta(s'_\delta),$$

where $s_\delta, s'_\delta \in A^*$, $s'_\delta \equiv 1 \pmod{M}$, and $\Delta = \{\delta_1, \dots, \delta_r\}$ is a simple root system for \tilde{G} . Put

$$(4.6) \quad \tilde{h} = \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i}).$$

The element $\sigma\tau$ can be written in the form

$$(4.7) \quad \sigma\tau = v_1 \sigma \tilde{h} x_{-\delta_1}(c) h_{\delta_1}(s_{\delta_1} s'_{\delta_1}) x_{\delta_1}(b) u_1,$$

where v_1 (respectively, u_1) is a product of elements of the form $x_\alpha(d)$, $d \in A$, $\alpha \in R^-$ (respectively, $\alpha \in R^+$) and $\alpha \neq -\delta_1$ (respectively, $\alpha \neq \delta_1$), and where $c, b \in A$ (this follows from Chevalley's commutator formula). We put $\tau_1 = x_{-\delta_1}(c) h_{\delta_1}(s_{\delta_1} s'_{\delta_1}) x_{\delta_1}(b)$. Then the element $\sigma \tilde{h} h_{\delta_1}(s_{\delta_1} s'_{\delta_1}) = \sigma h h'$ satisfies the condition of the lemma for the root δ_1 . Applying this lemma to the rank one group $\langle x_{\pm\delta_1}(a) \mid a \in A \rangle$ and to $\sigma \tilde{h}$ instead of σ , we get an element $f \in \langle x_{\pm\delta_1}(a) \mid a \in A \rangle$ such that

$$(4.8) \quad f \sigma \tau_1 f^{-1} = x_{-\delta}(p) \sigma \tilde{h} h_{\delta_1}(s_{\delta_1}) x_{\delta_1}(q)$$

for some $p, q \in A$. Observe that the elements $f v f^{-1}$ and $f u f^{-1}$ are also products of negative (positive) root elements except for those corresponding to $\pm\delta_1$ (because $f \in \langle x_{\pm\delta_1}(a) \mid a \in A \rangle$). Now (4.5)–(4.8) imply

$$(4.9) \quad f \sigma \tau f^{-1} = v' \sigma h_{\delta_1}(s_{\delta_1}) \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i}) u'$$

for some $v' \in U^-, u' \in U$. We rewrite (4.9) as

$$(4.10) \quad f \sigma \tau f^{-1} = v_1 \sigma h_{\delta_1}(s_{\delta_1}) \left(v_2 \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i}) u_2 \right) u_1,$$

where v_2, u_2 are products of negative (respectively, positive) root subgroup elements corresponding to roots in the root system R_2 generated by $\delta_2, \dots, \delta_r$, and v_1, u_1 are products of negative (respectively, positive) root subgroup elements corresponding to the roots that do not belong to R_2 . Now we put $\tau_2 = v_2 \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i}) u_2$. Since the element $\sigma h_{\delta_1}(s_{\delta_1}) \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i})$ differs from $\sigma h h'$ only by the factor $h_{\delta_1}(s'_{\delta_1})$, which belongs to the group $\tilde{G}(M)$, the condition of the lemma is still true for the element $\sigma h_{\delta_1}(s_{\delta_1}) \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i} s'_{\delta_i})$ and the root subgroup elements corresponding to R_2 . Applying the statement of the lemma to the element τ_2 and to $\sigma h_{\delta_1}(s_{\delta_1})$ instead of σ , and using the induction hypothesis, from (4.10) we get

$$l f \sigma \tau f^{-1} l^{-1} = v'' \sigma h_{\delta_1}(s_{\delta_1}) \prod_{i \geq 2} h_{\delta_i}(s_{\delta_i}) u'' = v'' \sigma h u''$$

for some element l in the Chevalley group generated by the root subgroup elements corresponding to the root system R_2 and for some $v'' \in U^-$ and $u'' \in U$ (note that $l v_1 l^{-1} \in U^-$ and $l u_1 l^{-1} \in U$).

The lemma is proved. □

Now, Proposition 1 follows from (4.4) and Lemma 4 if we put $\sigma = 1$, $h = t$, and $h' = t'$. □

We turn to estimating $\text{ecn}(\tilde{G}(A))$.

Theorem 2. *Suppose A is a local commutative ring and $|K| \geq 8|R| + 1$. Then*

$$\text{ecn}(\tilde{G}(A)) \leq 8 \text{ecn}(\tilde{G}(K)).$$

Proof. We shall need the following two lemmas.

Lemma 5. *Under the conditions of Theorem 2 there exists an element $t \in \tilde{T}(A)$ such that $t^4 \pmod{\tilde{G}(M)}$ is a regular semisimple element of $\tilde{G}(K)$.*

Proof. We shall show that there is an element $\bar{t} \in \tilde{T}(K)$ such that

$$(4.11) \quad \bar{t}^4 \notin \bigcup_{\alpha \in R} \text{Ker } \alpha.$$

For an infinite field K this is obvious. Let K be a finite field; then $|\tilde{T}(K)| = |K^*|^r$. We have $K^{*2} \subset \text{Im } \alpha$. Consequently, $K^{*8} \subset \text{Im } \alpha^4$, whence $|\text{Ker } \alpha^4| \leq 8|K^*|^{r-1}$. If $|R| \leq |K^*|/8$, then $|\bigcup_{\alpha \in R} \text{Ker } \alpha^4| < |K^*|^r$, and we have (4.11). Any element $\bar{t} \in \tilde{T}(K)$ satisfying (4.11) is a regular element of the group $\tilde{G}(K)$. Now we can take any preimage of \bar{t} in $\tilde{T}(A)$. □

Lemma 6. *Suppose $t \in \tilde{T}(A)$ is an element as in Lemma 5. Then*

$$[t^2, U] = [U, t^2] = U, \quad [t^2, U^-] = [U^-, t^2] = U^-.$$

Proof. Let $U = U_1 \geq U_2 = [U_1, U_1] \geq U_3 = [U_1, U_2] \geq \dots$ be the natural filtration. We may view U_i/U_{i+1} as a free A -module and write the operation $t^2ut^{-2}u^{-1}$ on U_i/U_{i+1} additively, as an A -module homomorphism

$$\phi_t : U_i/U_{i+1} \longrightarrow U_i/U_{i+1}, \quad \phi_t(u) = t^2(u) - u,$$

where $t^2(u) = t^2ut^{-2}$. Since $t^2 \pmod{\tilde{G}(M)}$ is a regular element of $\tilde{G}(K)$, the operator ϕ_t is invertible on U_i/U_{i+1} . This gives us the statement for U (by induction on i), and in the same way for U^- . □

Now we prove Theorem 2. Put $e = \text{ecn}(\tilde{G}(K))$. In the product of any e generating conjugacy classes of $\tilde{G}(A)$ we can find elements of the form

$$(4.12) \quad t_1 \dot{w}_0 m_1, \quad m_2 \ddot{w}_0 t_2,$$

where $t_1, t_2 \in \tilde{T}(A)$ are elements satisfying the condition of Lemma 5,

$$(4.13) \quad t_1 \equiv t_2 \pmod{\tilde{G}(M)},$$

the elements \dot{w}_0, \ddot{w}_0 are preimages in $N_{\tilde{G}(A)}(\tilde{T}(A))$ of the longest element w_0 of the Weyl group of R , satisfying the condition $\dot{w}_0 \ddot{w}_0 \in \tilde{T}(A) \cap \tilde{G}(M)$, and $m_1, m_2 \in \tilde{G}(M)$. The elements m_1, m_2 can be written in the form

$$(4.14) \quad m_1 = \dot{w}_0^{-1} v_1 \dot{w}_0 h_1 u_1, \quad m_2 = u_2 h_2 \ddot{w}_0 v_2 \ddot{w}_0^{-1},$$

where $v_1, v_2, u_1, u_2 \in U \cap \tilde{G}(M)$ and $h_1, h_2 \in \tilde{T}(A) \cap \tilde{G}(M)$ (see [Ab]). Now (4.12) and (4.14) imply that, conjugating (4.12) by appropriate elements, we can get elements of the form

$$(4.15) \quad u'_1 t'_1 \dot{w}_0, \quad \ddot{w}_0 t'_2 u'_2,$$

where $u'_1, u'_2 \in U \cap \tilde{G}(M)$, $t'_1, t'_2 \in \tilde{T}(A)$, and

$$(4.16) \quad t'_1 \equiv t_1 \pmod{\tilde{G}(M)}, \quad t'_2 \equiv t_2 \pmod{\tilde{G}(M)}.$$

From (4.13), (4.15), and (4.16) we see that in the product of $2e$ generating conjugacy classes we can find an element of the form $u_1 t u_2$, where $u_1, u_2 \in U$, $t \in \tilde{T}(A)$, and $t^2 \pmod{\tilde{G}(M)}$ is a regular semisimple element of $\tilde{G}(K)$. Thus, by Lemma 6, in this product we can also find every element of the form tu , where t is our fixed element and u runs through all elements of U . In the same way, in another product of $2e$ generating conjugacy classes we can find all the elements of the form vt' , where t' is a fixed element of $\tilde{T}(A)$ such that $t' \equiv t \pmod{\tilde{G}(M)}$ and v runs through all elements of U^- . Now

in the product of $4e$ generating conjugacy classes we can find all elements of the form $\mathfrak{U} = \{vt''u\}$, where t'' is fixed, $t'' \pmod{\tilde{G}(M)}$ is a regular element of $\tilde{G}(K)$, and v and u run through the elements of U^- and U , respectively. By Proposition 1, in the product of $4e$ generating conjugacy classes we can find every element of $\tilde{G}(A)$ such that its image in $\tilde{G}(K)$ is not in the center of that group. Since every element of $\tilde{G}(A)$ can be written as the product of two such elements, our statement is proved. \square

Remark. We have $\text{ecn}(\tilde{G}(A)) \leq c \cdot \text{rank}(\tilde{G})$ with some general constant c for every commutative local ring A with a large residue field. Presumably, the latter condition is not necessary.

§5. ANALOGS OF THE CONJECTURES OF ORE AND THOMPSON

Using Proposition 1, we can get results about products of conjugacy classes in Chevalley groups over commutative local rings, which are analogs of the results of [EG2] on the conjectures of Ore and Thompson for finite simple groups.

Theorem 3. *Let $\text{GN}(\tilde{G}(A))$ be the set of all elements in all generating conjugacy classes of $\tilde{G}(A)$. Assume that $|K| \geq 4|R| + 1$. Then there exists a real generating conjugacy class C of $\tilde{G}(A)$ such that*

$$\text{GN}(\tilde{G}(A)) \subset C^2.$$

Moreover, every element of $\text{GN}(\tilde{G}(A))$ is a single commutator.

Proof. We shall need the following lemma.

Lemma 7. *Under the condition of Theorem 3, there exists a real element $t \in \tilde{T}(A)$ such that $t^2 \pmod{\tilde{G}(M)}$ is a regular element of $\tilde{G}(K)$.*

Proof. If R is not one of A_r , D_r ($r = 2k + 1$), and E_6 , then the corresponding Weyl group has an element -1 , so that the condition of reality is fulfilled automatically. We get the regularity condition in the same way as in Lemma 5.

Consider the case where $R = A_r$. Here $\tilde{G}(A) = SL_{r+1}(A)$. Put $s = [(r + 1)/2]$. The condition of the lemma implies that we can find elements $\{\epsilon_i\}_{i=1}^{i=s} \subset K^*$ such that $\epsilon_i^2 \neq \epsilon_j^{-2}, \epsilon_j^{\pm 2}, \pm 1$ for every $i \neq j$. (Indeed, this is obvious if $\text{rank } G = 1$. If $\text{rank}(\tilde{G}) \geq 2$, then

$$|K^{*2}| \geq 2|R| > r + 3 = 2\frac{r + 1}{2} + 2 \geq 2s + 2,$$

and we can find s pairs of elements $\epsilon_i^2, \epsilon_i^{-2}$ that are different from each other and from ± 1 .) Now we fix preimages ω_i, ω_i^{-1} of $\epsilon_i, \epsilon_i^{-1}$ in the group A^* for every i and put

$$t = \text{diag}(\omega_1, \omega_1^{-1}, \omega_2, \omega_2^{-1}, \dots).$$

Obviously, t satisfies the requirement of the lemma.

We pass to the case where $R = D_r$, $r = 2k + 1$. Let $R = \langle \alpha_1, \dots, \alpha_r \rangle$, let $R_1 = \langle \alpha_2, \dots, \alpha_r \rangle = D_{r-1}$, and let $\tilde{T}_1 \leq \tilde{T}$ be the subtorus corresponding to R_1 . Since in R there are no roots orthogonal to all roots of R_1 , in the subtorus \tilde{T}_1 we can find a regular element of \tilde{G} . Now all elements in \tilde{T}_1 are real. Thus, we can find an appropriate element in $\tilde{T}_1(A)$.

Finally, let $R = E_6$. Consider the group of $\tilde{T}(K)$,

$$H = \{h_{\epsilon_2 - \epsilon_3}(v_1)h_{\epsilon_2 + \epsilon_3}(v_2)h_{\epsilon_4 - \epsilon_5}(v_3)h_{\epsilon_4 + \epsilon_5}(v_4) \mid v_1, v_2, v_3, v_4 \in K^*\}$$

(here the notation for roots corresponds to [B1]). It can be checked that $K^* \subset \alpha(H)$ for every root $\alpha \in R = E_6$. Consequently, we can argue as above to find a regular element in H^2 and then take an appropriate preimage that is a real element of $\tilde{G}(A)$. \square

Now we can prove Theorem 3. Let $t \in \tilde{T}(A)$ be a real element satisfying the condition of Lemma 7, and let C be its conjugacy class. By Lemma 6,

$$(5.1) \quad \begin{aligned} U^{-}t^2U &= [U^{-}, t]tt[t^{-1}, U] \\ &= \{vtv^{-1} \mid v \in U^{-}\}\{utu^{-1} \mid u \in U\} \subset C \cdot C = C^2. \end{aligned}$$

By Proposition 1 and (5.1), we have $\text{GN } \tilde{G}(A) \subset C^2$. Since C is real, every element of C^2 is a commutator. \square

REFERENCES

- [Ab] E. Abe, *Chevalley groups over local rings*, Tôhoku Math. J. (2) **21** (1969), 474–494. MR0258837 (41:3483)
- [Bo] A. Borel, *Linear algebraic groups*, 2nd ed., Grad. Texts in Math., vol. 126, Springer-Verlag, New York, 1991. MR1102012 (92d:20001)
- [B1] N. Bourbaki, *Éléments de mathématique*. Fasc. XXXIV. *Groupes et algèbres de Lie*. Chapitres IV, V, VI, Actualités Sci. Indust., No. 1337, Hermann, Paris, 1968. MR0240238 (39:1590)
- [B2] ———, *Commutative algebra*. Chapters 1–7, Springer-Verlag, Berlin, 1998. MR1727221 (2001g:13001)
- [EG1] E. W. Ellers and N. Gordeev, *Gauss decomposition with prescribed semisimple part in Chevalley groups*. I, II, III, Comm. Algebra **22** (1994), 5935–5950; **23** (1995), 3085–3098; **24** (1996), 4447–4475. MR1298758 (95m:20052); MR1332168 (96f:20064); MR1421200 (98a:20048)
- [EG2] ———, *On the conjectures of J. Thompson and O. Ore*, Trans. Amer. Math. Soc. **350** (1998), 3657–3671. MR1422600 (98k:20022)
- [GS1] N. Gordeev and J. Saxl, *Products of conjugacy classes in Chevalley groups*. I. *Extended covering numbers*, Israel J. Math. **130** (2002), 207–248. MR1919378 (2003e:20050)
- [GS2] ———, *Products of conjugacy classes in Chevalley groups*. II. *Covering and generation*, Israel J. Math. **130** (2002), 249–258. MR1919379 (2003e:20051)
- [St] R. Steinberg, *Lectures on Chevalley groups*, Yale Univ., New Haven, Conn., 1968. MR0466335 (57:6215)

DEPARTMENT OF MATHEMATICS, RUSSIAN STATE PEDAGOGICAL UNIVERSITY, MOÏKA 48, ST. PETERSBURG 191186, RUSSIA

E-mail address: nickgordeev@mail.ru

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS, UNIVERSITY OF CAMBRIDGE, WILBERFORCE ROAD, CAMBRIDGE CB3 0WB, UNITED KINGDOM

E-mail address: J.Saxl@dpms.cam.ac.uk

Received 20/MAY/2004
Originally published in English