Newton Institute Institute for this support.

Freedom in Conjugacy Classes of Simple Algebraic Groups and Identeties with Constants

Nikolai Gordeev

Department of Mathematics of Russian State Pedagogical University,

Moijka 48, St.Petersburg, 191-186 Russia.

e-mail: algebra@ivt.rgpu.spb.ru

Isaac Newton Institute for Mathematical Sciences

CAMBRIDGE

21 February, 1997

Preprint number: NI 97010

Abstract.

Let G be a simple algebraic group defined over a field k and let K/k a field extension. Further, let C_1,...,C_n be non-central conjugacy classes of $G(K)$. If the transcendence degree $tr.degK/k$ is big enough we show that almost always (except in the cases described) the elements $g_1 \in C_1$,..., $g_n \in C_n$ in general position generate a subgroup of $G(K)$ which is isomorphic to the free-product $\langle g_1\rangle * \langle g_2\rangle * \ldots * \langle g_n\rangle$ (modulo the centre $Z(G(K))$. We deduce this result from another which deals with identities with constants in the group $G(K)$. At the end we discuss the situation when $K = \overline{Q}$ is the algebraic closure of the field Q of rational numbers.

1. Introduction

Let G be a simple algebraic group defined over a field k. Then G is unirational over k ([2, 18.2]). Thus there exists a dominant rational map

$$\varphi : A_k^m \longrightarrow G_k. \tag{1.1}$$

The smallest possible m in (1.1) we denote by $d(G)$. Further, let K/k be an extension of fields. If $tr.degK/k$ is big enough with respect to n (actually, if $tr.degK/k \geq nd(G)$) then according to a theorem of A.Borel, [1], any n elements in "general position" generate a free subgroup of $G(K)$ (here "general position" means that elements do not belong to some fixed countable set of proper closed subsets of $G^n(K)$, see [1]).

Here we consider subgroups of $G(K)$ generated by elements from fixed conjugacy classes in general position. Namely, let $C_1, \ldots, C_n$ be non-central conjugacy classes of $G(K)$ and let $g_1, \ldots, g_n$ be their elements in "general position". The natural expectation is that the group generated by these elements is isomorphic to the free product $\langle g_1 \rangle * \ldots * \langle g_n \rangle$ (modulo the center $Z(G(K))$). But this is not true in general. However, if we exclude some special conjugacy classes we obtain "freedom" in general position.

We need the following

Definition 1. *Let T be a maximal torus of $G(\overline{K})$ (here $\overline{K}$ is the algebraic closure of K). Further, let $s \in T$ be a non-central element. We say that the element s is small if $\alpha(s) = 1$ for every long root $\alpha : T \longrightarrow \overline{K}^*$.*

Definition 2. *Let G be a group corresponding to a root system containing roots with different length.Further, let $u \in G(\overline{K})$ be a nontrivial unipotent element and let C_u be its conjugacy class. We say that u is a small element if the Zariski closure of its conjugacy class $\overline{C_u}$ does not contain both short and long root elements. We say that a small unipotent element belongs to the first class if the Zariski closure of its conjugacy class contains a long root element. Otherwise we say that such element belongs to the second class.*

Definition 3. *Let $g \in G(K)$. We say that g is small if g is a small semisimple element or a small unipotent element in $G(\overline{K})$ (here we consider the group $G(K)$ as a subgroup of $G(\overline{K})$).*

Now we formulate the main result of this paper.

Theorem 1. *Let G be a group of adjoint type. Further, let $C_1, \dots, C_n$ be nontrivial conjugacy classes of $G(K)$ which are also defined over the field k. Assume that $tr.deg K/k \geq nd(G)$ and one of the following conditions holds:*

1. All roots of the root system corresponding to G have the same length.

2. There cannot be both small semisimple and small unipotent elements among the powers of elements from the conjugacy classes $C_1, \dots, C_n$; and $char k \neq 2$ for the cases of root systems B_l, C_l, F_4 and $char k \neq 3$ for the case of the root system G_2.

3. There cannot be small unipotent elements of both first and second class among the powers of elements from the conjugacy classes $C_1, \ldots, C_n$; and $\mathrm{char} k = 2$ for the cases of root systems B_l, C_l, F_4 and $\mathrm{char} k = 3$ for the case of the root system G_2.

Then there exists a Zariski dense subset $M \subset C_1 \times \ldots \times C_n$ such that for every sequence $(g_1, \ldots, g_n) \in M$ the group $\Gamma = \langle g_1, \ldots, g_n \rangle$ generated by $g_1, \ldots, g_n$ is isomorphic to the free-product $\langle g_1 \rangle * \ldots * \langle g_n \rangle$.

Remark 1. *If G is not a group of adjoint type then we can change in the conditions 2.and 3. small unipotent elements for elements of the form zu where u is a small unipotent element and $z \in Z(G(\overline{K}))$. We will call such elements* small almost unipotent *elements. Theorem 1 gives us an isomorphism $\overline{\Gamma} \approx \langle \overline{g_1} \rangle * \ldots * \langle \overline{g_n} \rangle$ where $\overline{\Gamma}$ and $\overline{g_1}, \ldots, \overline{g_n}$ are the images of Γ and $g_1, \ldots, g_n$ in the group $G(K)/Z(G(K)$.*

Theorem 1 will follow from another which deals with identities with constants in simple groups.

Definition 4. *Let $D \subset GL(V)$ be a linear group and let $d_0, \ldots, d_m$ be fixed elements of $GL(V)$. Further, let $x_1, \ldots, x_n$ be letters. The expression:*

$$f(x_1, \ldots, x_n) = d_0 x_{i_1}^{l_1} d_1 \ldots x_{i_m}^{l_m} d_m$$

where l_i are integers is called a generalized monomial (see, [5], [12]*) if the condition $i_k = i_{k+1}$ and $l_k l_{k+1} < 0$ implies $d_k \notin C_{GL(V)}(D)$. We say that we have a generalized* *identity in D if $f(g_1, \ldots, g_n) = 1$ for every $g_1, \ldots, g_n \in D$ (here 1 is the identity of GL(V)). If $d_1, \ldots, d_m \in D$ we say that the identity with constants $d_0, \ldots, d_m$ holds in the group D.*

Generalized identities were considered by I.Z.Golubchik and A.V.Mikhalev, [5], and by G.M.Tomanov, [12]. It was shown in [12] that there are no such identities if $SL(V) \subset D$. If $D \subset GL_m(K)$ is an algebraic group then there is no generalized identity only if $SL_m(K) \subset D$, [12]. In [5], [12] there are examples of generalized identities for the cases $D = SO_n(K), Sp_n(K)$.

Here we obtain the following result using the approach of G.M.Tomanov ,[12] which is based on the method of attracting and repulsing points which is due to J.Tits, [11].

Theorem 2. *Let $f = f(x_1, \ldots, x_n)$ be a generalized monomial with coefficients from the group $G(K)$. Assume that K is an infinite field and one of the following conditions holds:*

1. All roots of the root system corresponding to G have the same length.

2. There cannot be both small semisimple and small almost unipotent elements among the coefficients of f; and $chark \neq 2$ for the cases of root systems B_l, C_l, F_4 and $chark \neq 3$ for the case of the root system G_2.

3. There cannot be small almost unipotent elements of both first and second class among the coefficients of f; and $chark = 2$ for the cases of root systems B_l, C_l, F_l and $chark = 3$ for the case of the root system G_2.

Then there is no identity $f(x_1, \ldots, x_n) \equiv 1$ in $G(K)$.

We show here that in all cases of root systems with different length of roots there exist identities with constants.

Theorem 3. *Let G be a group of type B_l, C_l, F_4, G_2. Let s be a small semisimple element and $u = x_\alpha(v), u' = x_\alpha(v')$ be two long root elements of $G(K)$. Then the following identities hold in $G(K)$:*

a. $[\,[x_1ux_1^{-1}, x_2sx_2^{-1}x_1ux_1^{-1}x_2s^{-1}x_2^{-1}], [x_1u'x_1^{-1}, x_2sx_2^{-1}x_1u'x_1^{-1}x_2s^{-1}x_2^{-1}]\,] \equiv 1$ *;*

b. $[x_1ux_1^{-1}, x_2sx_2^{-1}x_1ux_1^{-1}x_2s^{-1}x_2^{-1}] \equiv 1$ *if G is of the type B_l or C_l;*

c. $[\,[x_1ux_1^{-1}, x_2u_0x_2^{-1}x_1ux_1^{-1}x_2u_0^{-1}x_2^{-1}], [x_1u'x_1^{-1}, x_2u_0x_2^{-1}x_1u'x_1^{-1}x_2u_0^{-1}x_2^{-1}]\,] \equiv 1$ *where u_0 is a short root element of $G(K)$ and when G is of the type B_l, C_l, F_4 and $char k = 2$ or G is of the type G_2 and $char k = 3$;*

d. $[x_1ux_1^{-1}, x_2u_0x_2^{-1}x_1ux_1^{-1}x_2u_0^{-1}x_2^{-1}] \equiv 1$ *when G is of the type B_l or C_l and $char k = 2$.*

Remark 2. *The identity a. is the most general here and it holds for all cases where the corresponding general monomial exists, but in cases of bad characteristic we cannot find small semisimple elements. In such cases we may use c.*

Remark 3. *The identities of Theorem 3 show nontrivial relations which take place in groups generated by elements taken from some special conjugacy classes even in general position.*

Remark 4. *In* [12] *there are example of identities in the group G for the cases B_l, C_l which can be written in our notations as* $(\star)$ $([\,[u, xsx^{-1}], [u', xsx^{-1}]\,] \equiv 1$*. These identities follow from b. Indeed, put* $x_1 \equiv 1$*,* $x_2 \equiv x$ *then we obtain from b.* $[u, xsx^{-1}uxs^{-1}x^{-1}] \equiv 1$ *for every long root element* u*. This implies* $[X_\alpha, sX_\alpha s^{-1}] = 1$ *for every long root subgroup* X_α *and and every small semisimple element* s*. Now we have* $(\star)$*.*

The method which we use here to obtain Theorem 1 from Theorem 2 is due to A.Borel, [1]. It is based on the procedure of removing "the subsets of relations" from $G^n(K)$. It works only if the transendence degree $tr.deg K/k$ is big enough. At the end of the paper we consider a quite different situation when $k = K = \overline{Q}$ is the algebraic closure of the field of rational numbers. Presumably, the results here should be the same as above. Here we present an observation on the group $PSL_2(\overline{Q})$ which can show the different level of the complexity of such questions when the transcendence degree $tr.deg K/k$ is small.

Theorem 4. *Let C_1, C_2 be fixed nontrivial conjugacy classes of elements of finite order in $PSL_2(\overline{Q})$. Then there exists a Zariski dense subset $M \subset C_1 \times C_2$ such that $,\ = \langle g_1, g_2 \rangle \approx \langle g_1 \rangle * \langle g_2 \rangle$ for every pair $(g_1, g_2) \in M$.*

Corollary 1. *Let G be a semisimple algebraic group of adjoint type defined over $\overline{Q}$ and let C_1, C_2 be fixed nontrivial conjugacy classes of elements of primary orders in $G(\overline{Q})$. Then there exists a subset $M \subset C_1 \times C_2$ such that $,\ = \langle g_1, g_2 \rangle \approx \langle g_1 \rangle * \langle g_2 \rangle$ for every pair $(g_1, g_2) \in M$.*

Theorem 5. *Let C be a fixed nontrivial conjugacy class of elements of finite order in $PSL_2(\overline{Q})$. Then for every natural number n there exists a Zariski dense subset $M \subset C^n$ such that $,\ = \langle g_1, \dots, g_n \rangle \approx \langle g_1 \rangle * \dots * \langle g_n \rangle$ for every sequence $(g_1, \dots, g_n) \in M$.*

Corollary 2. *Let G be a semisimple algebraic group of adjoint type defined over $\overline{Q}$ and let C be a fixed nontrivial conjugacy class of elements of primary orders in $G(\overline{Q})$. Then for every natural number n there exists a subset $M \subset C^n$ such that $,\ = \langle g_1, \dots, g_n \rangle \approx \langle g_1 \rangle * \dots * \langle g_n \rangle$ for every sequence $(g_1, \dots, g_n) \in M$.*

Remark 5. *The statement of Corollary 2 also holds if C is not a semisimple class. Indeed, let $g = g_s g_u$ be the Jordan decomposition of an element from C. Since the centralizer $C_G(g_s)$ is a reductive group (see,* [9]*) and since $g_u \in C_G(g_s)$ we may assume $g = g_u$. According to the Morozov-Jacobson theorem we may consider g as a unipotent element of $SL_2(\overline{Q})$ or $PSL_2(\overline{Q})$. It is a well known fact that there exist two unipotent elements in $SL_2(Z)$ generating the free group of rank two. Since every* *subgroup of a free group is free we can easily construct a free group of any rank generated by unipotent elements of* $SL_2(Z)$ *or* $PSL_2(Z)$.

2. Small elements in simple groups

Here we consider small elements in $G(\overline{K})$ where $\overline{K}$ is the algebraic closure of the field K.

We denote by R the root system corresponding to G. If $\alpha \in R$ then we denote by X_α the corresponding root subgroup of $G(\overline{K})$ (i.e. $X_\alpha = \langle x_\alpha(v) \,|\, v \in \overline{K} \rangle$); and by $h_\alpha(t)$ where $t \in \overline{K^*}$ a corresponding semisimple element of the group $\langle X_{\pm\alpha} \rangle$, see [10]. We use the notation of N.Bourbaki [3] for roots. Further, by i and ω we denote the primitive fourth and third roots of unity.

Let T be a maximal torus of $G(\overline{K})$ and let $s \in T$ be a small semisimple element. One can easely check (using the tables I - X of [3]):

I. if $R = B_l$ then $char k \neq 2$ and

$s = h_{\epsilon_1}(\pm i) \ldots h_{\epsilon_l}(\pm i)$;

II. if $R = C_l$ then $char k \neq 2$ and

$s = h_{2\epsilon_i}(-1)$ $(i = 1, \ldots, l)$;

III. if $R = F_4$ then $char k \neq 2$ and

$s = h_{\epsilon_1}(\pm i) h_{\epsilon_2}(\pm i) h_{\epsilon_3}(\pm i) h_{\epsilon_4}(\pm i)$;

IV. if $R = G_2$ then $chark \neq 3$ and

$s = h_\alpha(\omega)h_\beta(\omega^2)$,

where α, β are long roots of R such that $\alpha + \beta \in R$.

Now we consider small unipotent elements in $G(\overline{K})$. In cases when the characteristic is not bad we get the possibilities for such elements from the classification of the unipotent elements in simple algebraic groups (see, R.W.Carter, [4], N.Spaltenstein, [8]). Namely, if u is a small unipotent element of $G(\overline{K})$ then:

V. if $chark \neq 2$ and $R = C_l, F_4$ or if $chark \neq 3$ and $R = G_2$ then u is conjugate to a long root element;

VI. if $chark \neq 2$ and $R = B_l$ then in the natural representation of $G(\overline{K})$ as the group $SO_{2l+1}(\overline{K})$ the elementary divisors of u are (2,... ,2,1,..., 1).

Thus if $chark \neq 2$ for cases B_l, C_l, F_4 and $chark \neq 3$ for the case G_2 then all small unipotent elements are in the first class. In cases of a bad characteristic there are small elements in the second class. The Zariski closure of the conjugacy class of a small unipotent element belonging to the second class contains a short root element. This fact follows from the classification, [8].

3. Proof of theorem 2

First of all we formulate Tomanov's criterion, [12], for the coefficients of generalized monomials which can give generalized identities.

Let $D \subset GL(V)$ be a linear group and let

$$f = f(x_1, \dots, x_n) = d_0 x_{i_1}^{l_1} d_1 \dots x_{i_m}^{l_m} d_m$$

be a generalized monomial where $\{d_k\}$ are elements of $GL(V)$. Put

$$I(f) = \{d_k \mid i_k = i_{k+1}, l_k l_{k+1} < 0\}.$$

Assume that $D = G(\overline{K})$ and V is an irreducible $G(\overline{K})$-module. Let $e_1, \dots, e_r$ be a basis of V consisting of weight-vectors where e_1 is a vector corresponding to the highest weight and e_r is a vector corresponding to the lowest weight. Further, let V' be the subspace of V generated by vectors $e_1, \dots, e_{r-1}$. Define

$$\Lambda(G(\overline{K}), V) = \{g \in GL(V), g \notin Z(GL(V)) \mid \sigma g \sigma^{-1} e_1 \in V' \text{ for every } \sigma \in G(\overline{K})\}.$$

It has been proved in [12] :

$$f \equiv 1 \,\text{in}\, G(\overline{K}) \Longrightarrow \Lambda(G(\overline{K}) \cap I(f) \neq \emptyset. \tag{3.1}$$

Now we apply the criterion (3.1) to the coefficients $d_0, \dots, d_m$ of f. Since K is an infinite field the identity $f \equiv 1$ holds in $G(K)$ if and only if it holds in $G(\overline{K})$ because $G(K)$ is dense in G, see [2, 18.3]. Thus we may consider our identity in $G(\overline{K})$. Let $d_k = s_k u_k$ be the Jordan decomposition of a coefficient and let $C_{d_k}, C_{s_k}, C_{u_k}$ be conjugacy classes of d_k, s_k, u_k in $G(\overline{K})$. If $C_{d_k}e_1 \subset V'$ then $\overline{C}_{d_k}e_1 \subset V'$ (here V, V', e_1 are as above; $\overline{C}_{d_k}$ is the Zariski closure of C_{d_k}). Thus

$$d_k \in \Lambda(G(\overline{K}), V) \Longrightarrow \overline{C}_{d_k} \subset \Lambda(G(\overline{K}), V) \tag{3.2}$$

We need the following

Lemma 1. *Let $V = V(\alpha_0)$ be an irreducible $G(\overline{K})$-module corresponding to the weight α_0 where α_0 be the maximal positive root of R. Suppose one of the following conditions holds:*

1). $s_k \notin Z(G(\overline{K}))$ and s_k is a non-central and non-small element;

2). $u_k \neq 1$ and $char k \neq 2$ if $R = B_l, C_l, F_4$ and $char k \neq 3$ if $R = G_2$.

Then $d_k \notin \Lambda(G(\overline{K}), V)$.

Proof. Here we have $e_1 = e_{\alpha_0}, e_r = e_{-\alpha_0}$. Further,

$$x_{-\alpha_0}(v)e_{\alpha_0} = e_{\alpha_0} + v^2 e_{-\alpha_0} + \dots$$

([10], Lemma 72). Thus

$$t_1 x_{-\alpha_0}(v) t_2 \notin \Lambda(G(\overline{K}), V) \tag{3.3}$$

for every $t_1, t_2 \in T$. If $t \in T$ is not a small element then it is conjugate to an element $t' \in T$ such that $[x_{-\alpha_0}(v), t'] = x_{-\alpha_0}(v') \neq 1$. From (3.3) we obtain

$$x_{-\alpha_0}(v') t' x^{-1}_{-\alpha_0}(v') = x_{-\alpha_0} t' \notin \Lambda(G(\overline{K}), V)$$

and therefore

$$t \notin \Lambda(G(\overline{K}), V). \tag{3.4}$$

Consider case 1). Since $C_{s_k} \subset \overline{C}_{d_k}$ ([9], II.3.) the implication (3.2) and the non-inclusion (3.4) implies $d_k \notin \Lambda(G(\overline{K}), V)$.

Consider case 2). Let $F = C_{G(\overline{K})}(s_k)$. Then F is a reductive subgroup of $G(\overline{K})$ generated by a maximal torus T, some root subgroups and some elements from the Weyl group ([4, Theorem 3.5.3]). Moreover, $u_k \in F$. Further, we may assume that $u_k \in F^0$ where F^0 is the connected component of the group F. (Indeed, we may consider the situation in the simply connected form of the group G. The centralizers of semisimple elements are connected in this case, [4, 3.5.6.]. Then we can return to the adjoint group considering the image of the adjoint representation.) Let $\overline{Q}_{u_k}$ be the Zariski closure of the conjugacy class of u_k in F^0. Then there exists a unipotent element $u_0 \neq 1$ belonging to a simple component F_0 of the group F^0 such that $\overline{Q}_{u_0} \subset \overline{Q}_u$ where $\overline{Q}_{u_0}$ is the Zariski closure of the conjugacy class of the element u_0 in the group F_0. In the Zariski closure of any unipotent conjugacy class of a simple group one can find a long root element except cases $char k = 2$ for root systems B_l, C_l, F_4 or $char k = 3$ for G_2. This follows from the classification of unipotent classes in simple algebraic groups, [8]. Since the connected component F^0 of the group F is generated by T and some root subgroups of $G(\overline{K})$ one can find a long root element x_α of the group $G(\overline{K})$ contained in $\overline{Q}_{u_0}$ and therefore in $\overline{C}_{u_k}$. Moreover the element

x_α commutes with s_k and $s_k x_\alpha \in \overline{C}_{d_k}$. Acting on $s_k x_\alpha$ by an appropriate element of the Weyl group we obtain $tx_{-\alpha_0} \in \overline{C}_{d_k}$ for some $t \in T$ and for some long root element $x_{-\alpha_0}$. Now our assertion follows from (3.2) and (3.4). □

Now we return to the proof of the theorem.

Consider case 1. If all roots have the same length there are no small semisimple elements in $G(\overline{K})$. Thus every non-central coefficient d_k of the monomial f has a non-central and non-small semisimple part s_k or non-trivial unipotent part u_k. Hence we obtain from Lemma 1 $\Lambda((G(\overline{K}), V) = \emptyset$. Now our statement follows from (3.1).

Consider case 2. Suppose d_k is a non-central and non-small element. Then either s_k is a non-central and non-small element or $u_k \neq 1$. Thus one of the conditions of Lemma 1 holds and therefore $d_k \notin \Lambda(G\overline{K}), V(\alpha_0))$. Let d_k be a small element. If d_k is almost unipotent then again by Lemma 1 $d_k \notin \Lambda(G(\overline{K}), V(\alpha_0))$. Suppose d_k is a small semisimple element. Let $V(\beta)$ be an irreducible $G(\overline{K})$-module corresponding to the highest weight β where β is a short root of R (say, $\beta = \omega_1$ if $R = B_l, C_l$, $\beta = \omega_4$ if $R = F_4$ and $\beta = \omega_1$ if $R = G_2$; see, [3]). There exists an element $t \in T$ which is conjugate to d_k in $G(\overline{K})$ and such that $[t, x_{-\beta}] \neq 1$. Using the same arguments as in the proof of Lemma 1 we obtain $d_k \notin \Lambda(G(\overline{K}), V(\beta))$. If the identity $f \equiv 1$ holds in the group $G(\overline{K})$ then according to (3.1) $\Lambda(G(\overline{K}), V) \neq \emptyset$ for every irreducible $G(\overline{K})$-module. Thus we need to have both small semisimple and small almost unipotent elements among the coefficients of f to have the identity $f \equiv 1$.

Consider case 3. In this case we have no small semisimple elements (see 2,I-IV). Further, if u is a small almost unipotent element belonging to the first class we have (as above) $u \notin \Lambda(G(\overline{K}), V(\alpha_0))$. If u is a small unipotent element belonging to the second class then the Zariski closure of its conjugacy class contains a short root element, [8], and hence $u \notin \Lambda(G(\overline{K}), V(\beta))$. Using the same arguments as above we conclude that we need to have both sorts of almost unipotent elements among the coefficients of f to obtain the identity $f \equiv 1$ in the group $G(\overline{K})$.

4. Identities with small constants. Proof of Theorem 3

Let Δ be a simple root system for R and $\Delta' \subset \Delta$. Further, let P be the parabolic subgroup of $G(\overline{K})$ corresponding to the set Δ', let L be the semisimple part of the Levi factor (here L is the semisimple group corresponding to the root system generated by Δ') and let W' be the Weyl group of L. If $S = \{w_j\}$ is a set of the representatives of double cosets $W'wW'$ in W then ([4],2.8.1)

$$G(\overline{K}) = \bigcup\nolimits_{w_j \in S} P\dot{w}_j P$$

where $\dot{w_j}$ is a preimage of an element w_j of the Weyl group W in the group N (recall that N is the normalizer of T). Thus every element $\tau \in G(\overline{K})$ can be written in the form

$$\tau = \gamma_1 \dot{w} t \gamma_2 \tag{4.1}$$

for some $\gamma_1, \gamma_2 \in LR_u(P)$, $t \in T$ and $\dot{w} \in N$ (here $R_u(P)$ is the unipotent radical of P). Now let $\sigma \in G(\overline{K})$ be an element satisfying the following condition:

$$LR_u(P) \subset C_{G(\overline{K})}(\sigma). \tag{4.2}$$

The inclusion (4.2) implies that the pair $(\sigma, \tau\sigma\tau^{-1})$ is conjugate to the pair $(\sigma, \dot{w}t\sigma t^{-1}\dot{w}^{-1})$. Using the trick which is taken from [13] we prove the following

Lemma 2. *Let $R = B_l, C_l, F_4, G_2$ and let $\sigma = x_{\alpha_0}(v)$, $v \neq 0$, where α_0 is the maximal root with respect to Δ. Further, let τ be a small semisimple element of $G(\overline{K})$ if char$k \neq 2$ and $R = B_l, C_l, F_4$ or if char$k \neq 3$ and $R = G_2$, or let τ be a short root element of $G(\overline{K})$ in cases when char$k = 2$ and $R = B_l, C_l, F_4$ or char$k = 3$ and $R = G_2$. Then the pair $(\sigma, \tau\sigma\tau^{-1})$ cannot be conjugate to a pair $(x_{\alpha_0}(v), x_{-\alpha_0(v')})$ for some v'.*

Proof. Using the notation of N.Bourbaki, [3], we have $\alpha_0 = \epsilon_1 + \epsilon_2$ if $R = B_l, F_4$, $\alpha_0 = 2\epsilon_1$ if $R = C_l$ and $\alpha_0 = 3\alpha_1 + 2\alpha_2$ if $R = G_2$. Put $\Delta' = \Delta \setminus \{\alpha_1\}$ if $R = C_l, F_4$ and $\Delta' = \Delta \setminus \{\alpha_2\}$ if $R = B_l, G_2$. Then the normalizer $N_{G(\overline{K})}(X_{\alpha_0})$ of the root subgroup $X_{\alpha_0} = \langle x_{\alpha_0}(r) \,|, r \in \overline{K} \rangle$ contains the parabolic subgroup P. Indeed, in the cases described the elements of the Levi factor L commute with the elements of X_{α_0}. Since P is a maximal closed proper subgroup of $G(\overline{K})$, then $N_{G(\overline{K})}(X_{\alpha_0}) = P$. Moreover, (4.2) also holds for σ, L and $R_u(P)$.

Let τ be written in the form (4.1). Then the pair $(\sigma, \tau\sigma\tau^{-1})$ is conjugate to a pair $(x_{\alpha_0}(v), x_\beta(v''))$ where $\beta = w(\alpha_0)$, $v'' \in \overline{K}$. If $\beta \neq -\alpha_0$ then the pair $(x_{\alpha_0}(v), x_\beta(v''))$

cannot be conjugate by an element of the group $G(\overline{K})$ to a pair $(x_{\alpha_0}(v), x_{-\alpha_0}(v'))$. Indeed, conjugation by an element of the group $G(\overline{K})$ of a pair of root elements which transforms it into another pair of root elements which preserve the configuration between roots. Thus the pair $(\sigma, \tau\sigma\tau^{-1})$ can be conjugate to a pair $(x_{\alpha_0}(v), x_{-\alpha_0}(v'))$ if and only if

$$w(\alpha_0) = -\alpha_0. \tag{4.3}$$

The equality (4.3) implies $w = w_{\alpha_0}w'$ where w_{α_0} is the corresponding reflection and $w' \in W'$. Conjugating τ by γ_1^{-1} we obtain an element $\delta = \dot{w}_{\alpha_0}\dot{w}'t\gamma$ for some $\gamma \in LR_u(P)$. We may assume $\dot{w}' \in L$ and rewrite the element δ in the form

$$\delta = \dot{w}_{\alpha_0}tlu \tag{4.4}$$

where $l \in L$, $u \in R_u(P)$. Since $\overline{K}$ is an algebraically closed field $t = t_1t_2$ where $t_1 \in \langle X_{\pm\alpha_0}\rangle$, $t_2 \in L$. The element $\dot{w}_{\alpha_0}t_1$ is also a preimage of w_{α_0} in the group N. Thus we may replace $\dot{w}_{\alpha_0}t_1$ for $\dot{w}_{\alpha_0}$. Further, we may replace t_2l for l and replace (4.4) for

$$\delta = \dot{w}_{\alpha_0}lu. \tag{4.5}$$

Moreover, we may assume

$$\dot{w}_{\alpha_0}l = l\dot{w}_{\alpha_0} \tag{4.6}$$

because the elements of the group $\langle X_{\pm\alpha_0}\rangle$ commute with group L and the element $\dot{w}_{\alpha_0}$ can be chosen from the group $\langle X_{\pm\alpha_0}\rangle$. Further, if we consider $\dot{w}_{\alpha_0}$ as an element of the group $\langle X_{\pm\alpha_0}\rangle \approx SL_2(\overline{K})$ or $PSL_2(\overline{K})$ we can see

$$\dot{w}^2_{\alpha_0} = h_{\alpha_0}(-1) \tag{4.7}$$

where $h_{\alpha_0}(-1)$ is the corresponding semisimple root element (see, [10]). From (4.5), (4.6), (4.7) we obtain

$$\delta^2 = \dot{w}_{\alpha_0} lu\dot{w}_{\alpha_0} lu = \dot{w}^2_{\alpha_0}\dot{w}^{-1}_{\alpha_0} lu\dot{w}_{\alpha_0} lu = h_{\alpha_0}(-1)l^2l^{-1}\dot{w}^{-1}_{\alpha_0} u\dot{w}_{\alpha_0} lu. \tag{4.8}$$

Put $u_1 = l^{-1}\dot{w}^{-1}_{\alpha_0} u\dot{w}_{\alpha_0} l$. We have

$$u_1 \in R^-_u(P) \tag{4.9}$$

where $R^-_u(P) = \dot{w}_0 R_u(P)\dot{w}_0^{-1}$. Indeed, if $\alpha \in R^+$ and the root α does not belong to the root subsystem generated by Δ' then $w_{\alpha_0}(\alpha) \in R^-$ and the root $w_{\alpha_0}(\alpha)$ does not belong the root system generated by Δ'. This follows from the definition of α_0 and Δ'. Hence $\dot{w}^{-1}_{\alpha_0} u\dot{w}_{\alpha_0} \in R^-_u(P)$. Since the group $R^-_u(P)$ is normalized by elements of the group L we obtain (4.9).

Further, (4.8) can be written in the form

$$\delta^2 = h_{\alpha_0}(-1)l^2u_1u. \tag{4.10}$$

Assume $\delta^2 = z \in Z(G(\overline{K}))$. Then (4.10) implies

$$zh_{\alpha_0}(-1)l^{-2} = u_1u. \tag{4.11}$$

The right side of (4.11) belongs to the Gauss cell of $G(\overline{K})$ because of the choice of u and (4.9). Hence it can be considered as the Gauss decomposition of the element $zh_{\alpha_0}(-1)l^{-2}$. Since $u \in R_u(P)$ and $u_1 \in R_u^-(P)$ the decomposition (4.11) can take place if and only if $u = u_1 = zh_{\alpha_0}(-1)l^{-2} = 1$ (this follows from the uniqueness of the Gauss decomposition). Thus if

$$\delta^2 = z \in Z(G(\overline{K})) \tag{4.12}$$

then

$$\delta = \dot{w}_{\alpha_0} l. \tag{4.13}$$

Let $R = B_l, C_l, F_4$. Then a small semisimple element s satisfies the condition $s^2 \in Z(G(\overline{K}))$ (see,2.I-IV). If $char k = 2$ then the element u_0 is an involution. Hence the condition (4.12) holds for $\delta \in C_\tau$ where C_τ is the conjugacy class of τ in $G(\overline{K})$. Let $char k \neq 2$ and let $\tau = s$ be a small semisimple element. Then $\dot{w}_{\alpha_0}$ is a semisimple element of $G(\overline{K})$. This implies with (4.6) that the element l is also semisimple. Thus

$$x_1 \dot{w}_{\alpha_0} x_1^{-1} = h_{\alpha_0}(t)\,,\ x_2\ l x_2^{-1} = h_1$$

for some $x_1 \in \langle X_{\pm\alpha_0}\rangle, x_2 \in L, t \in \overline{K}, h_1 \in T \cap L$. Using (4.6) and (4.13) we obtain

$$\delta_1 = x_1 x_2 \delta x_2^{-1} x_1^{-1} = h_{\alpha_0}(t) h_1 \in T.$$

From (4.7) we have $t = \pm i$. But $\delta_1 = h_{\alpha_0}(\pm i) h_1 \notin C_{G(\overline{K})}(X_{\alpha_0})$. This is a contradiction with the choice of s. Thus we have proved that if τ is a small semisimple element then the pair $(\sigma, \tau\sigma\tau^{-1})$ cannot be conjugate to a pair $(x_{\alpha_0}(v), x_{-\alpha_0}(v'))$. Let $char k = 2$ and let $\tau = u_0$. Then δ is a product of two commuting involutions $\dot{w}_{\alpha_0}$ and l (see (4.6), (4.7)) Since $char k = 2$ both of these involutions are unipotent. Further, $\dot{w}_{\alpha_0} \in \langle X_{\pm\alpha_0}\rangle$, $l \in L$, and $\langle X_{\pm\alpha_0}\rangle$, L are commuting subgroups of $G(\overline{K})$). Therefore $\dot{w}_{\alpha_0} \in \overline{C}_\delta = \overline{C}_\tau$ where $\overline{C}_\delta, \overline{C}_\tau$ are Zariski closure of conjugacy classes in $G(\overline{K})$ of δ, τ. On the other hand, $\dot{w}_{\alpha_0}$ is a long root element here. Thus we have the contradiction with the choice of τ.

Consider the case $R = G_2$. Let $char k \neq 3$ and let τ be a small semisimple element. The group $C_{G(\overline{K})}(\tau)$ is generated by T and all long root subgroups of $G(\overline{K})$ ([4, Theorem 3.5.3]).Hence

$$dim C_{G(\overline{K})}(\tau) = dim C_{G(\overline{K})}(\delta) = 8 \tag{4.14}$$

Since $\sigma = x_{\alpha_0}(v)$

$$dim C_{G(\overline{K})}(\sigma) = 8 \tag{4.15}$$

([4],13.1.). From (4.14), (4.15)

$$dim(C_{G(\overline{K})}(\sigma) \cap C_{G(\overline{K})}(\delta)) \geq 8 + 8 - 14 = 2. \tag{4.16}$$

Let $x \in C_{G(\overline{K})}(\sigma) \cap C_{G(\overline{K})}(\delta)$. Then the element x commutes with $\sigma = x_{\alpha_0}(v)$ and with $\delta\sigma\delta^{-1} = x_{-\alpha_0}(v')$ (recall that our assumption that the pair $(\sigma, \tau\sigma\tau^{-1})$ is conjugate to a pair $(x_{\alpha_0}(v), x_{-\alpha_0}(v'))$ implies that the element τ is conjugate to an element δ of the form (4.5)). There exists a non-central semisimple element ϵ of the group $\langle X_{\pm\alpha_0}\rangle$

which belongs to the subgroup $\langle \sigma, \delta\sigma\delta^{-1}\rangle$. Since $x \in C_{G(\overline{K})}(\epsilon)$ then $x = \epsilon' g$ where ϵ' is a semisimple element of the group $\langle X_{\pm\alpha_0}\rangle$ commuting with ϵ and $g \in L = \langle X_{\pm\alpha_1}\rangle$ ([4, 3.5.3]). Since x commutes with $x_{\alpha_0}(v), x_{-\alpha_0}(v')$ then $\epsilon' = h_{\alpha_0}(\pm 1)$. We have

(4.17)

$$x = h_{\alpha_0}(\pm 1)g = \delta x \delta^{-1} = \dot{w}_{\alpha_0} l u x u^{-1} l^{-1} \dot{w}_{\alpha_0}^{-1} = \dot{w}_{\alpha_0} l x [x^{-1}, u] l^{-1} \dot{w}_{\alpha_0}^{-1}.$$

Put $y' = [x^{-1}, u]$. Since $x = h_{\alpha_0}(\pm 1)g, u \in R_u(P)$ then $y' \in R_u(P)$ and therefore $y = l y' l^{-1} \in R_u(P)$. From (4.17)

(4.18)

$$x = \dot{w}_{\alpha_0} l x l^{-1} y \dot{w}_{\alpha_0}^{-1} = \dot{w}_{\alpha_0} l h_{\alpha_0}(\pm 1) g l^{-1} y \dot{w}_{\alpha_0}^{-1} = h_{\alpha_0}(\pm 1) l g l^{-1} \dot{w}_{\alpha_0} y \dot{w}_{\alpha_0}^{-1}.$$

Since $y \in R_u(P)$ then $\dot{w}_{\alpha_0} y \dot{w}_{\alpha_0}^{-1} \in R_u^-$ and therefore (4.18) implies $y = 1$. Hence $y' = [x^{-1}, u] = 1$. This implies

(4.19) $$u \in X_{\alpha_0}$$

if the element g is a non-central semisimple element of L (the existence of $x = h_{\alpha_0}(\pm 1)g$ with such g follows from (4.16)) Further, the equality (4.18) implies

(4.20) $$lgl^{-1} = g.$$

Since every element $x \in C_{G(\overline{K})}(\sigma) \cap C_{G(\overline{K})}(\delta)$ can be written in the form $x = h_{\alpha_0}(\pm 1)g$ where $g \in L$ then (4.20) implies

(4.21) $$dim(C_{G(\overline{K})}(\sigma) \cap C_{G(\overline{K})}(\delta)) \leq dim C_L(l).$$

If $l \notin Z(L)$ then $dim C_L(l) = 1$ and in this case the inequality (4.21) contradicts (4.16). Hence

$$l = h_{\alpha_1}(\pm 1). \tag{4.22}$$

Now using (4.19) and (4.22) we obtain

$$\delta = \dot{w}_{\alpha_0} h_{\alpha_1}(\pm 1) u_{\alpha_0}$$

where $u_{\alpha_0} \in X_{\alpha_0}$. Hence $\delta^2 \in \langle X_{\pm\alpha_0} \rangle$. This is in contradiction with the choice of δ.

Let $R = G_2, char k = 3, \tau = u_0$. We have $dim C_{G(\overline{K})}(u_0) = 8$ ([8, 10.4,10.15]). Thus we may use here the same arguments as above to prove that the assumption of conjugation of pairs $(\sigma, \delta\sigma\delta^{-1})$ and $(x_{\alpha_0}(v), x_{-\alpha_0}(v'))$ leads to the inclusion $\delta^2 \in \langle X_{\pm\alpha_0} \rangle$ which contradicts to the choice of u_0 (recall that the element δ we take from the conjugacy class of u_0 and the element u_0 is a short root element of $G(\overline{K})$). □

Now we can prove the existence identities a.b.c.d. of Theorem 3.

According to Lemma 2 we may assume

$$\tau X_{\alpha_0} \tau^{-1} = X_\beta, \beta \neq -\alpha_0,$$

where τ is a small semisimple element or $\tau = u_0$. Thus

$$[x, \tau x \tau^{-1}] \in X_{\alpha_0 + \beta}$$

for every $x \in X_{\alpha_0}$ (if $\alpha_0 + \beta$ is not a root we put $X_{\alpha_0+\beta} = 1$). Since $X_{\alpha_0+\beta}$ is an abelian group

$$(4.23) \qquad [\,[y_1, \tau y_1 \tau^{-1}]\,,\,[y_2, \tau y_2 \tau^{-1}]\,] = 1$$

for every $y_1, y_2 \in X_{\alpha_0}$. Now the identities a. and c. follow from (4.23). Indeed, we can substitute $y_1 = u, y_2 = u', \tau = s$ or u_0 and since (4.23) holds for every such u, u', s from given conjugacy classes we obtain a. and c.

Now consider the case $R = C_l$. Then $\alpha_0 + \beta$ is not a root and hence

$$(4.24) \qquad [x, \tau x \tau^{-1}] = 1$$

for every $x \in X_{\alpha_0}$. If we substitute $x = u, \tau = s$ or u_0 we obtain b. and d. for the case $R = C_l$.

Let $R = B_l$. If $\alpha_0 + \beta$ is not a root the proof for b. and d. is the same as for the case C_l. Suppose $\alpha_0 + \beta$ is a root. Let $char k \neq 2$. We may assume $G(\overline{K}) = SO(V)$ where $dim V = 2l + 1$. If $\alpha_0 + \beta$ is a root then $q = u\tau u\tau^{-1}$ is a regular unipotent element in the group $\langle X_{\pm\alpha_0}, \tau X_{\pm\alpha_0}\tau^{-1}\rangle$. This group is isomorphic to $SL_3(\overline{K})$ and the codimension of the subspace V^q of q-fixed vectors is equal to 4. On the other hand τ is a small semisimple element of order 2 which has eigenvalues :(-1,...,-1, 1). Hence $codim V^q = 2$. This is a contradiction. If $char k = 2$ then we can consider the group $G(\overline{K})$ as the group $Sp(V), dim V = 2l$. Again if $u, \tau u \tau^{-1}$ do not commute then the element q defined above is a regular unipotent element of the group $SL_3(\overline{K})$ and the codimension of subspace V^q is equal to 4. On the other hand, the codimension of subspace V^τ where $\tau = u_0$ is equal to 1. Since u_0 is an involution the codimension of V^q should be 2. This is a contradiction. Thus we have b. and d. for the case B_l.

Theorem 3 has been proved.

5. Freedom in conjugacy classes. Proof of Theorem 1

Let $\omega(x_1, \ldots, x_n)$ be a non-empty reduced word on n letters.One can define a map

$$f_\omega : G^n \longrightarrow G \tag{5.1}$$

defined by the formula

$$f_\omega((g_1, \ldots, g_n)) = \omega(g_1, \ldots, g_n).$$

This map is a dominant morphism of algebraic varieties, [1]. Thus the preimage $X_\omega = f^{-1}(1)$ of the identity is a proper closed subset. A.Borel, [1], has shown that the set

$$G^n(K) \setminus \bigcup_{\omega \in \Omega} X_\omega(K)$$

is dense in G if the transcendence degree $tr.degK/k$ is big enough.

Here we use the same approach to prove Theorem 1. Namely, let $c_1, \ldots, c_n$ be a fixed set of representatives of the conjugacy classes $C_1, \ldots, C_n$. For every non empty reduced word ω on n letters we can define the map

$$f_{\tilde{\omega}} : G^n \longrightarrow G \tag{5.2}$$

by the formula

$$f_{\widetilde{\omega}}((g_1, \dots, g_n)) = \omega(g_1 c_1 g_1^{-1}, \dots, g_n c_n g_n^{-1}).$$

Obviously, the map $f_{\widetilde{\omega}}$ is a morphism of algebraic varieties which is defined over the field K . Note that the set $f_{\widetilde{\omega}}(G(K))$ does not depend of the choice on representatives $c_1, \dots, c_n$.

Assume that $f_{\widetilde{\omega}}(G(K)) = 1$. This means that the identity $f_{\widetilde{\omega}} \equiv 1$ with constants holds in the group $G(K)$. The constants here are powers of elements $c_1, \dots, c_n$. We will say that the word ω is *appropriate* for given set of conjugacy classes if for every power of a letter x_i^n which occurs in ω the element c_i^n is not the identity. Now if we consider the word ω which is appropriate for $C_1, \dots, C_n$ then $\widetilde{\omega}(x_1, \dots, x_n) = \omega(x_1 c_1 x_1^{-1}, \dots, x_n c_n x_n^{-1})$ is a generalized monomial (Definition 4; recall that the group G is of adjoint type). Further, if we assume that K is an infinite field and one of the conditions of Theorem 1. holds then coefficients of the generalized monomial $\widetilde{\omega}$ satisfy one of the conditions Theorem 2. (This follows directly from the definitions.) In this case the identity $f_{\widetilde{\omega}} \equiv 1$ cannot hold in the group $G(K)$ and therefore the preimage $X_{\widetilde{\omega}}(K) = f_{\widetilde{\omega}}^{-1}(1)$ is a proper closed subset of $G^n(K)$.

Let Ω be the set of all appropriate non-empty reduced words on n letters. We consider the set

$$X(K) = G^n(K) \setminus (\bigcup_{\omega \in \Omega} X_{\widetilde{\omega}}(K)).$$

Since conjugacy classes $C_1, \ldots, C_n$ are defined over the field k we can choose elements $c_1, \ldots, c_n$ from the group $G(k)$. Thus we may assume that all maps (5.2) are defined over the field k. Hence we may assume that every set $X_{\tilde{\omega}}$ is defined over k. Now we use the fact that the group G is a unirational variety over the field k , [2, 18.2]. According to the definition of the number $d(G)$ we have the dominant rational map

$$\varphi : A_k^{d(G)} \longrightarrow G_k$$

defined over k where $A_k^{d(G)}$ is $d(G)$-dimensional affine k-space. Thus we have the dominant rational map

$$\varphi^n : A_k^{nd(G)} \longrightarrow G_k^n$$

defined over k. Since $tr.degK/k \geq nd(G)$ there exists a Zariski dense subset $Y(K)$ in $A_k^{nd(G)}(K)$ such that there are no algebraic relations over k between coordinates of the elements of $Y(K)$ (indeed, say, elements of the form $(x_1^{m_1}, \ldots, x_s^{m_s})$, where $s = nd(G)$, m_i are positive integers and $x_1, \ldots, x_s$ are algebraically independent elements over the field k, are already dense in $A_k^{nd(G)}(K)$). Obviously, the image of the set $Y(K)$ with respect to φ^n is in $X(K)$. Thus the set $X(K)$ is dense in G^n. Now let

$$\psi : G^n(K) \longrightarrow C_1 \times \ldots \times C_n$$

be the map given by the formula

$$\psi(g_1, \ldots, g_n) = (g_1 c_1 g_1^{-1}, \ldots, g_n c_n g_n^{-1}).$$

Put $M = \psi(X(K))$. Then the set M is dense in $C_1 \times \ldots \times C_n$. Moreover, the definition of the set $X(K)$ implies that there are no non-trivial relations among elements $g'_1, \ldots, g'_n$ of the group $G(K)$ such that $(g'_1, \ldots, g'_n) \in M$ (except, of course, those relations which follow from the relations of the form $x^m = 1$ in cases of elements of finite orders). Thus the set M satisfies the conditions of Theorem 1.

Now Theorem 1. has been proved.

6. Freedom over $\overline{Q}$. Proof of Theorems 4 and 5.

In the case when the trancendence degree $tr.degK/k$ is small the method used in the proof of Theorem 1 does not work. Indeed, it may happen that the set

$$\bigcup_{\omega\in\Omega} X_{\widetilde{\omega}}(K)$$

coincides with $G^n(K)$. As an example we may consider the case $K = \overline{F}_p$. (In this case every sequence $g_1, \ldots, g_n \in G(\overline{F}_p)$ satisfies a relation.)

We prove here Theorem 4. using a different approach.

Consider the group $SL_2(\overline{Q})$ and conjugacy classes $\widetilde{C_1}, \widetilde{C_2}$ which are preimages of classes C_1, C_2. Let $g_1 = diag(\epsilon, \epsilon^{-1}), g_2 = diag(\delta, \delta^{-1})$ be diagonal matrices belonging to classes $\widetilde{C_1}, \widetilde{C_2}$ respectively. The eigenvalues ϵ, δ here are a m_1 and m_2-th root of 1 for some m_1, m_2. Let Π be the set of all prime divisors of the field $Q(\epsilon, \delta)$. Further, we define the set

(6.1)

$$S = \{P \in \Pi \mid P|(\epsilon^r - \epsilon^{-r}) \text{ or } P|(\delta^s - \delta^{-s}) \text{ for some } 0 < r < m_1, 0 < s < m_2\}$$

(here $(\epsilon^r - \epsilon^{-r})$, $(\delta^s - \delta^{-s})$ are principal divisors).

Let Ω be the set of appropriate words on 2 letters (see definition above,in 5) for conjugacy classes C_1, C_2 and let $\omega(x_1, x_2) \in \Omega$. Consider the equation

$$\omega(g_1, xg_2x^{-1}) = 1 \tag{6.2}$$

where x is a general matrix

$$\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$$

from the group $GL_2(\overline{Q})$. If we conjugate both sides of the equation (6.2) with an appropriate powers of g_1 and xg_2x^{-1} we obtain

$$\begin{pmatrix} \epsilon^{r_1} & 0 \\ 0 & \epsilon^{-r_1} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_1} & 0 \\ 0 & \delta^{-s_1} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}^{-1} \cdots \tag{6.3}$$

$$\cdots \begin{pmatrix} \epsilon^{r_n} & 0 \\ 0 & \epsilon^{-r_n} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_n} & 0 \\ 0 & \delta^{-s_n} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

If we change the matrix x^{-1} in (6.3) for the matrix

$$x' = \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} \tag{6.4}$$

we obtain the following equation

$$\begin{pmatrix} \epsilon^{r_1} & 0 \\ 0 & \epsilon^{-r_1} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_1} & 0 \\ 0 & \delta^{-s_1} \end{pmatrix} \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} \dots \tag{6.5}$$

$$\dots \begin{pmatrix} \epsilon^{r_n} & 0 \\ 0 & \epsilon^{-r_n} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_n} & 0 \\ 0 & \delta^{-s_n} \end{pmatrix} \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} =$$

$$= \begin{pmatrix} (detx)^n & 0 \\ 0 & (detx)^n \end{pmatrix}.$$

On the other hand we can look at the left side of (6.5) as an expression with indeterminates t_{ij}:

$$\begin{pmatrix} \epsilon^{r_1} & 0 \\ 0 & \epsilon^{-r_1} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_1} & 0 \\ 0 & \delta^{-s_1} \end{pmatrix} \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} \dots \tag{6.6}$$

$$\dots \begin{pmatrix} \epsilon^{r_n} & 0 \\ 0 & \epsilon^{-r_n} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} \delta^{s_n} & 0 \\ 0 & \delta^{-s_n} \end{pmatrix} \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} =$$

$$\dots = \begin{pmatrix} \theta_{11}(t_{11}, t_{12}, t_{21}, t_{22}) & \theta_{12}(t_{11}, t_{12}, t_{21}, t_{22}) \\ \theta_{21}(t_{11}, t_{12}, t_{21}, t_{22}) & \theta_{22}(t_{11}, t_{12}, t_{21}, t_{22}) \end{pmatrix}.$$

where $\theta_{ij}(t_{11}, t_{12}, t_{21}, t_{22})$ are polynomials in $t_{11}, t_{12}, t_{21}, t_{22}$ with coefficients from the ring $Z[\epsilon, \delta]$.

Now we need the following

Lemma 3. $\theta_{12}(1,1,1,1) = -\epsilon^{r_1}\pi, \theta_{21}(1,1,1,1) = \epsilon^{-r_1}\pi$ *where*

$$\pi = (\textstyle\prod_{i=2}^{n}(\epsilon^{r_i} - \epsilon^{-r_i}))(\prod_{i=1}^{n}(\delta^{s_i} - \delta^{-s_i})).$$

Proof. We can substitute $t_{11} = a_{11}, t_{12} = a_{12}, t_{21} = a_{21}, t_{22} = a_{22}$ for every a_{ij} belonging to any ring which contains $Z[\epsilon,\delta]$. Thus we obtain the values of polynomials θ_{ij} at the points $t_{ij} = a_{ij}$. In particular, if we substitute $t_{11} = 1, t_{12} = 1, t_{21} = 1, t_{22}) = 1$ we obtain the values $\theta_{ij}(1,1,1,1)$.

We have

$$\begin{pmatrix} \epsilon^{r_i} & 0 \\ 0 & \epsilon^{-r_i} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \delta^{s_i} & 0 \\ 0 & \delta^{s_i} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \tag{6.7}$$

$$= \begin{pmatrix} \epsilon^{r_i}(\delta^{s_i} - \delta^{-s_i}) & -\epsilon^{r_i}(\delta^{s_i} - \delta^{-s_i}) \\ \epsilon^{-r_i}(\delta^{s_i} - \delta^{-s_i}) & -\epsilon^{-r_i}(\delta^{s_i} - \delta^{-s_i}) \end{pmatrix}.$$

Further,

(6.8)

$$\begin{pmatrix} \epsilon^{k}a & -\epsilon^{k}a \\ \epsilon^{-k} & -\epsilon^{-k}a \end{pmatrix} \begin{pmatrix} \epsilon^{l}b & -\epsilon^{l}b \\ \epsilon^{-l}b & -\epsilon^{-l}b \end{pmatrix} = \begin{pmatrix} \epsilon^{k}(\epsilon^{l} - \epsilon^{-l})ab & -\epsilon^{k}(\epsilon^{l} - \epsilon^{-l})ab \\ \epsilon^{-k}(\epsilon^{l} - \epsilon^{-l})ab & -\epsilon^{-k}(\epsilon^{l} - \epsilon^{-l})ab \end{pmatrix}.$$

Now our assertion obviously follows from (6.7) and (6.8). □

Let A be the subset of matricies from $GL_2(\overline{Q})$ satisfying the following conditions:

1'.if $a \in A$ then all entries a_{ij} of a are algebraic integers;

2'. there exists a prime divisor p_a of the field $Q[\epsilon, \delta, a_{11}, a_{12}, a_{21}, a_{22}]$ such that $p_a|(a_{ij}-1)$ for every i, j and p_a is prime to every divisor P from the set $S($ (6.1)).

Let $a \in A$. Then if we input a in the left side of (6.3) instead of x we obtain the matrix

$$(6.9) \qquad \begin{pmatrix} \frac{\theta_{11}(a_{11},a_{12},a_{21},a_{22})}{(deta)^n} & \frac{\theta_{12}(a_{11},a_{12},a_{21},a_{22})}{(deta)^n} \\ \frac{\theta_{21}(a_{11},a_{12},a_{21},a_{22})}{(deta)^n} & \frac{\theta_{22}(a_{11},a_{12},a_{21},a_{22})}{(deta)^n} \end{pmatrix}$$

If the matrix a satisfies the equation (6.3) then according (6.5) for elements of the matrix (6.9) we have

$$(6.10) \qquad \theta_{12}(a_{11}, a_{12}, a_{21}, a_{22}) = \theta_{21}(a_{11}, a_{12}, a_{21}, a_{22}) = 0.$$

But (6.10) cannot hold if $a \in A$. Indeed, the conditions (6.10) and 2' imply that the divisor p_a divides $(\theta_{12}(1,1,1,1))$ and $(\theta_{21}(1,1,1,1))$. Lemma 3 ,in its turn, implies that the prime divisors of the field $Q[\epsilon, \delta, a_{11}, a_{12}, a_{21}, a_{22}])$ dividing $(\theta_{12}(1,1,1,1))$, $(\theta_{21}(1,1,1,1))$ are only those which divide divisors from the set S. This contradicts the conditions of 2' that p_a is prime to every P from the set S.

Thus every matrix $a \in A$ cannot satisfy the equation (6.3), that is , cannot satisfy the equation (6.2) for every appropriate non-empty reduced word ω on two letters. This implies that the group , $\subset PSL_2(\overline{Q})$ generated by the images $\overline{g_1}$, $\overline{ag_2a^{-1}}$ of elements g_1 and ag_2a^{-1} is isomorphic to the free-product $\langle\overline{g_1}\rangle * \langle\overline{ag_2a^{-1}}\rangle$.

It is easy to see that the set A is Zariski dense in $GL_2(\overline{Q})$. Hence the set of pairs $(\sigma g_1\sigma^{-1}, \sigma ag_2a^{-1}\sigma^{-1})$ where $\sigma \in GL_2(\overline{Q})$ and $a \in A$ is dense in $\widetilde{C} \times \widetilde{C}$. Therefore, the set M of pairs (g_1', g_2') from $C_1 \times C_2$ such that the group generated by g_1', g_2' is isomorphic to the free-product $\langle g_1' \rangle * \langle g_2' \rangle$ is dense in $C_1 \times C_2$.

Theorem 4 has been proved.

Now we prove Theorem 5.

First of all we show the existence of such a set M. In the case $n = 2$ this follows from Theorem 4 (we can put $C_1 = C_2 = C$). If elements of C are not involutions then for every $n > 2$ one can find in the group $, = \langle g_1 \rangle * \langle g_2 \rangle$ where $g_1, g_2 \in C$ the subgroup

$$,' = \langle g_1 \rangle * \langle \tau_1 g_2 \tau_1^{-1} \rangle * \ldots * \langle \tau_{n-1} g_2 \tau_{n-1}^{-1} \rangle$$

where $\tau_1, \ldots, \tau_{n-1} \in ,$. This follows from the Kurosch theorem on subgroups of free products (see ,[7] or [6, 17.2]). Thus we have a non-empty set M containing the sequence $(g_1, \tau_1 g_2 \tau_1^{-1}, \ldots, \tau_{n-1} g_2 \tau_{n-1}^{-1})$. If elements of C are involutions we may take an element $g \in C \cap PSL_2(Z)$ and using the isomorphism $PSL_2(Z) \approx \langle g \rangle * \langle \sigma \rangle$ where $\sigma \in PSL_2(Z)$ is an element of the order 3 and again using the Kurosch theorem we obtain a non-empty set M satisfying the condition of Theorem 5.

Now we prove that the set $M \subset C^n$ such that

$$\langle g_1, \ldots, g_n \rangle \approx \langle g_1 \rangle * \ldots * \langle g_n \rangle$$

for every sequence $(g_1, \dots, g_n) \in M$ is dense in C^n. For $n = 2$ this follows from Theorem 4. Thus we may assume $n > 2$. Let , $= \langle g_1, \dots, g_n \rangle$ where $(g_1, \dots, g_n) \in M$. Then

$$\langle w_1 g_1 w_1^{-1}, \dots, w_n g_n w_n^{-1} \rangle \approx \langle w_1 g_1 w_1^{-1} \rangle * \dots * \langle w_n g_n w_n^{-1} \rangle$$

for every $w_1, \dots, w_n \in$, . This follows from the Kurosch theorem. Hence

$$(w_1 g_1 w_1^{-1}, \dots, w_n g_n w_n^{-1}) \in M \tag{6.11}$$

for every $w_1, \dots, w_n \in$, . Since $n > 2$ the group , is dense in $PSL_2(\overline{Q})$. (This is also true for $n = 2$ except in the case when the elements of C are involutions.) This implies that the set of sequences of the form (6.11) is dense in C^n. Therefore the set M is also dense in C^n.

Theorem 5 has been proved.

We now prove the corollaries.

Proof. Let T be a maximal torus of the group G and let $g \in C \cap T$. Let $d = p^l$ be the order of g. Since G is the group of adjoint type and since d is a primary number one can find a root $\alpha : T \longrightarrow \overline{Q^*}$ such that $\alpha(g^r) \neq 1$ for every $0 < r < d$. Let $G_\alpha = \langle X_\alpha, X_{-\alpha} \rangle$ where $X_\alpha, X_{-\alpha}$ are the corresponding root subgroups of G. Then the image $\overline{g}$ of g in the factor group $G_\alpha T / Z(G_\alpha) T \approx PSL_2(\overline{Q})$ has also the order d. Now we can apply Theorem 4 and 5. □

Acknowledgement. This paper was written by the author during his stay at the Isaac Newton Instiute and his participating in the programm "Representations of Algebraic Groups and Related Finite Groups". The author is grateful to the Institute for the support.

References

[1] A.Borel, *On free subgroups of semisimple groups*, L'Enseignement Mathematique, II-Ser. 29 (1983),151-164.

[2] A.Borel, *Linear algebraic groups.* (Springer-Verlag, New York, 1991.)

[3] N.Bourbaki, Groupes et algèbres de Lie, ch.IV - VI. (Hermann, Paris, 1968.)

[4] R.W.Carter, Finite Groups of Lie type. Conjugacy Classes and Complex Characters. (John Wiley and Sons, New York et al., 1985)

[5] I.Z.Golubchik and A.V.Mikhalev, Generalized group identities in linear groups, in: Modules and algebraic groups. Zapiski Nauchnukh Seminarov Leningrad.Otdel. Mat. Inst. Steklov(LOMI), 114(1982), 96-119; English translation in: J.Sovjet Math.,27(1984).

[6] M.Hall, The theory of groups. (The Macmillan Company, New York, 1959.)

[7] A.Kurosch, The theory of groups. (Chelsea Publishing Co, New York, 1955)

[8] N.Spaltenstein, Classes Unipotentes et Sous-groups de Borel, Lecture Notes in Mathematics 946 (1982)(Springer-Verlag, Berlin-Heidelberg-New York)

[9] T.A.Springer and R.Steinberg, Conjugacy classes, in: A.Borel et al:Seminar on algebraic groups and related finite groups. Lecture Note in Mathematics 131. (Springer-Verlag, Berlin-Heidelberg-New York, 1970.)

[10] R.Steinberg, Lectures on Chevalley groups. (Yale University, 1967.)

[11] J.Tits, Free subgroups in Linear Groups, J.Algebra, 20(1972), 250 -270.

[12] G.M.Tomanov, Generalized group identities in linear groups, Mat.Sbornik, 123(1984),35-49; English translation in: Math.USSR.Sb, 51(1985), 33-46.

[13] N.A.Vavilov, On the geometry of long root subgroups in Chevalley groups, Vestnik Leningr.Univ., Math.,1(1988), 8-11.