TOPICS IN ALGEBRA
BANACH CENTER PUBLICATIONS, VOLUME 26, PART 2
PWN-POLISH SCIENTIFIC PUBLISHERS
WARSAW 1990

THE CONGRUENCE SUBGROUP PROBLEM FOR ALGEBRAIC GROUPS

A. RAPINCHUK

Institute of Mathematics of the Belorussian Academy of Sciences
Minsk, U.S.S.R.

1. The statement of the problem

Let Γ be a subgroup of $\mathrm{GL}_n(\mathbf{Z})$. What can be said about the normal structure of Γ? A large family of normal subgroups in Γ of finite index is formed by the so-called congruence subgroups $\Gamma(m) = \{g \in \Gamma \mid g \equiv e_n (\mathrm{mod}\, m)\}$. This family is large indeed since $\bigcap_m \Gamma(m) = (e_n)$, so the following question which is usually called the congruence subgroup problem looks quite natural:

> Does any normal subgroup in Γ of finite index contain a congruence subgroup $\Gamma(m)$?

This question is of interest not only for the theory of linear groups but also for other areas of mathematics. Indeed, the first counterexample to the congruence subgroup problem was constructed in 1880 by F. Klein who worked at that time in the theory of modular functions. He showed that there are subgroups of $\Gamma = \mathrm{SL}_2(\mathbf{Z})$ of finite index that contain no congruence subgroup. But the attempts to investigate the congruence subgroup problem for $\Gamma = \mathrm{SL}_3(\mathbf{Z})$ have been of no success for a long time. Only in 1965 did Bass–Lazard–Serre [3] and Mennicke [12] give a positive solution of this problem for $\mathrm{SL}_n(\mathbf{Z})$ ($n \geqslant 3$). Further investigations in this direction were held mainly for arithmetic subgroups of algebraic groups, and we are now going to give the necessary definitions.

Let $G \subset \mathrm{GL}_n$ be a linear algebraic group defined over an algebraic number field K, and let S be a finite subset of the set V^K of all valuations of K, which contains the set V_∞^K of archimedian valuations. Denote by $O(S)$ the ring of S-integers in K and by $G_{O(S)}$ the group of S-units of G. To any nonzero ideal $\mathfrak{a} \subset O(S)$ there corresponds the congruence subgroup

$$G_{O(S)}(\mathfrak{a}) = \{g \in G_{O(S)} \mid g \equiv e_n (\mathrm{mod}\, \mathfrak{a})\}.$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

One can easily see that $G_{O(S)}(\mathfrak{a})$ is a normal subgroup in $G_{O(S)}$ of finite index, and $\bigcap_{\mathfrak{a}} G_{O(S)}(\mathfrak{a}) = (e_n)$. In this situation the congruence subgroup problem can be stated in a similar way:

(1) Does any normal subgroup in $G_{O(S)}$ of finite index contain a congruence subgroup $G_{O(S)}(\mathfrak{a})$?

A more precise statement of the problem is: for which S and G the answer to the question (1) is "yes". In this case we have a complete description of all normal subgroups of finite index in $G_{O(S)}$. In the course of investigations it turned out that besides the statement of the problem in the form (1) one should also keep in mind its restatement in the form which is now called modern. This restatement is based on the concept of congruence kernel that we are going to define.

One can introduce two Hausdorff topologies τ_a and τ_c on the group G_K of K-rational points that are called the (S-) arithmetic topology and S-congruence topology, respectively. The complete system of neighbourhoods of unity for τ_a (resp. for τ_c) consists of all normal subgroups of finite index (resp. of all congruence subgroups) in $G_{O(S)}$. It is not hard to show that τ_a and τ_c satisfy all the properties that ensure the existence of the corresponding S-arithmetic and S-congruence completions $\hat{G}_K$ and $\bar{G}_K$ (see [8]). Since τ_a dominates τ_c, the identity map $(G_K, \tau_a) \to (G_K, \tau_c)$ is continuous, and therefore it can be extended to a continuous homomorphism $\pi\colon \hat{G}_K \to \bar{G}_K$ of the completions. By definition $\operatorname{Ker}\pi = C^S(G)$ is the *congruence kernel.*

PROPOSITION 1.1. *The projection π is surjective and $C^S(G)$ is a profinite group. $C^S(G)$ is trivial iff the congruence subgroup problem in the form* (1) *has an affirmative answer for $G_{O(S)}$.*

Thus the congruence kernel $C^S(G)$ measures the deviation from the positive solution of the congruence subgroup problem. That is why by modern statement of the problem we mean the problem of determination of $C^S(G)$. As the following proposition shows, the essential part of the congruence subgroup problem is the calculation of $C^S(G)$ for semisimple groups.

PROPOSITION 1.2 (Platonov [16], Platonov–Sharomet [18]). *Let G be an algebraic K-group, and let F be a maximal semisimple subgroup of G. Then $C^S(G) = C^S(F)$. In particular, if G is soluble then $C^S(G) = 1$.*

So in what follows the group G can and will be supposed to be semisimple. If the group $G_S = \prod_{v\in S} G_{K_v}$ (where K_v is the completion of K with respect to v) is compact then $G_{O(S)}$ is finite and the congruence subgroup problem for G trivially has a positive solution. More generally, if $G = \prod_{i=1}^{n} G^i$ is a decomposition of G into an almost direct product of K-simple components and G_S^i is compact for $i \leqslant m$, and noncompact for $i > m$, then $C^S(G) = C^S(H)$ where $H = \prod_{i>m} G^i$. Thus we obtain the reduction to the main case of a semisimple

group G that has no K-simple component G^i with G_S^i compact. Furthermore, it turns out that one can hope to obtain a positive solution of the congruence subgroup problem only for simply connected groups.

PROPOSITION 1.3 (Serre [29]). *Suppose that a semisimple K-group G is not simply connected and contains no K-simple component G^i with G_S^i compact. Then the congruence kernel $C^S(G)$ is infinite.*

Finally, since any semisimple simply connected group G is the direct product of its K-simple components, the latter being obtained by the ground field restriction construction from absolutely simple groups, we arrive at the reduction of the congruence subgroup problem to the case of absolutely simple simply connected groups.

As we have already remarked, the first positive result on the congruence subgroup problem for such groups is due to Bass–Lazard–Serre [3] and Mennicke [12] who studied the case of $\mathrm{SL}_n(\mathbf{Z})$ $(n \geqslant 3)$. Then Bass–Milnor–Serre [4] completed the consideration of SL_n $(n \geqslant 3)$ and Sp_{2n} $(n \geqslant 2)$ over an arbitrary algebraic number field K. It turned out that the congruence kernel $C^S(G)$ (where $G = \mathrm{SL}_n$ $(n \geqslant 3)$ or Sp_{2n} $(n \geqslant 2)$) can be described as follows:

$$C^S(G) = \begin{cases} 1 & \text{if } \exists v \in S \text{ such that } K_v \neq \mathbf{C}, \\ E(K) & \text{otherwise,} \end{cases} \tag{2}$$

where $E(K)$ is the group of all roots of unity in K. This result shows that one should distinguish at least three possibilities for $C^S(G)$ ($C^S(G)$ is trivial, finite or infinite) but not two ($C^S(G)$ is trivial or not). It is worth mentioning here that as proved by Mel'nikov [11] the congruence kernel for $\mathrm{SL}_2(\mathbf{Z})$ is a very large infinite group, namely, a free profinite group of countable rank. The second thing is that there is no purely algebraic solution of the congruence subgroup problem. Indeed, if $C^S(G)$ were always trivial one could hope to apply the structure theory of Dedekind rings etc. to prove it but it is not.

Developing further the methods of [4], Matsumoto [10] obtained the description of $C^S(G)$ in the form (2) for all universal Chevalley groups different from SL_2. In the case of $G = \mathrm{SL}_2$ Mennicke [13] first gave a positive solution of the congruence subgroup problem for $\mathrm{SL}_2(\mathbf{Z}[1/p])$ and then Serre [30] studied the general situation and showed that if $\mathrm{Card}\, S > 1$ then the answer is of the form (2). Analysing the obtained results Serre [30] stated the following congruence subgroup conjecture:

> Let G be a simple simply connected algebraic K-group. If $\mathrm{rang}_S G = \sum_{v \in S} \mathrm{rang}_{K_v} G \geqslant 2$ and $\mathrm{rang}_{K_v} G \geqslant 1$ for $v \in S \setminus V_\infty^K$ then $C^S(G)$ is finite.

Raghunathan [22], [23] proved this conjecture for K-isotropic groups. But until recently there was practically no progress for anisotropic groups. The aim of my report is to present the results on the congruence subgroup problem for anisotropic groups that were obtained in the last few years.

2. Congruence subgroup problem and metaplectic problem

In this section we show that to determine $C = C^S(G)$ one should actually solve two problems, namely, prove that C is central (i.e. contained in the centre of $\hat{G}_K$) and calculate the so-called metaplectic kernel $M(G, S)$. This scheme of solution of the congruence subgroup problem is classical and goes back to [4], [30].

Let us start with the exact sequence

$$1 \to C \to \hat{G}_K \to \bar{G}_K \to 1 \tag{1}$$

to which there corresponds the exact Hochschild–Serre cohomological sequence

$$H^1(\bar{G}_K) \xrightarrow{\varphi} H^1(\hat{G}_K) \to H^1(C)^{\bar{G}_K} \xrightarrow{\psi} H^2(\bar{G}_K)$$

where $H^i(*)$ denotes the ith group of continuous cohomologies with coefficients in $\mathbf{R}/\mathbf{Z}$. One can easily see that

$$\operatorname{Coker}\varphi = \overline{[G_K, G_K]}/[G_K, G_K]$$

where the bar denotes closure in G_K with respect to the S-arithmetic topology. According to the strong approximation theorem (see Platonov [15]), $\bar{G}_K$ can be identified with the group $G_{A(S)}$ of S-adeles. Then using the fact that the sequence (1) splits over G_K and is the "universal" sequence with this property one can show that $\operatorname{Im}\psi = M(G, S)$ where $M(G, S) = \operatorname{Ker}(H^2(G_{A(S)}) \to H^2(G_K))$ is the so-called *metaplectic kernel* (the group G_K is endowed with the discrete topology). Thus we have the following exact sequence:

$$1 \to \operatorname{Coker}\varphi \to H^1(C)^{\bar{G}_K} \to M(G, S) \to 1.$$

Unfortunately, the term $H^1(C)^{\bar{G}_K}$ in general carries information only on a portion of C. One can reconstruct the whole of C from $H^1(C)^{\bar{G}_K}$ only if C is central, i.e. contained in the centre of $\hat{G}_K$, because in this case $H^1(C)^{\bar{G}_K} = H^1(C)$ is the Pontryagin dual C^* for C.

THEOREM 2.1. *If C is central then it is finite. If, moreover,* $\operatorname{Coker}\varphi = 1$ *then* $C^* \simeq M(G, S)$.

Indeed, the metaplectic kernel $M(G, S)$ is always finite (see [22], [20]). On the other hand, $[G_K, G_K]$ has finite index in G_K (see [19]), in particular $\operatorname{Coker}\varphi$ is finite. It should be noted that the finiteness of C is actually equivalent to its centrality. More precisely, if C is finite and G_K is projectively simple, i.e. the factor group $G_K/Z(G_K)$ is an abstract simple group, then C is central. (For the discussion of the problem when G_K is really projectively simple see below.)

Having thus described the qualitative aspect of the problem of determination of C, one can hardly stand the temptation of trying to obtain the description of C similar to (2) of § 1 in the general case. The first step towards

this is to find out whether $\operatorname{Coker}\varphi = 1$ or not. At present we may claim that $\operatorname{Coker}\varphi$ is really trivial in most cases. Indeed, if G is K-isotropic then the Kneser–Tits conjecture is true for G_K (with a possible exception of E_6), therefore any normal subgroup of G_K either is contained in $Z(G_K)$ or coincides with G_K. In particular, $G_K = [G_K, G_K]$. Recently it turned out that for most K-anisotropic groups G_K has no noncentral normal subgroup either.

THEOREM 2.2 (Borovoi [5], Chernousov [6], [7]). *Let G be a simple simply connected K-anisotropic group of one of the following types: B_n ($n \geqslant 2$), C_n ($n \geqslant 2$), D_n ($n \geqslant 4$), E_7, E_8, F_4, G_2, or let G be a special unitary group SU_m associated to some quadratic extension L/K. Then G_K has no noncentral normal subgroup.*

The case of groups of type A_n is more complicated and here G_K is in general not projectively simple. Platonov [15a] conjectured that the problem of projective simplicity of G_K for any simple simply connected group G, including type A_n, can be solved in the following form:

(2) G_K is projectively simple iff G_{K_v} is projectively simple for all $v \in V^K \setminus V_\infty^K$.

There is also a refined version of conjecture (2) due to Margulis:

(3) If $T = \{v \in V^K \setminus V_\infty^K \mid G_{K_v}$ is compact$\}$ then for any noncentral normal subgroup $N \subset G_K$ there is an open normal subgroup $W \subset G_T = \prod_{v \in T} G_{K_v}$ such that $N = G_K \cap W$.

It should be remarked that if (3) is true for $N = [G_K, G_K]$ then under the assumptions of the congruence subgroup conjecture we have $\operatorname{Coker}\varphi = 1$ since in this case $S \cap T = \emptyset$.

If G is an anisotropic group of type ${}^1A_n$ then $G_K = \mathrm{SL}(1, D)$ where D is a finite-dimensional skew field over K. In this case the set T in (3) coincides with the set of all nonarchimedian v for which $D \otimes_K K_v$ is a skew field. As the next theorem shows, (3) is really true for $N = [G_K, G_K]$.

THEOREM 2.3 (Platonov–Rapinchuk [17], Raghunathan [24]). *Let G be an algebraic K-group associated to $\mathrm{SL}(1, D)$, and set $T = \{v \in V^K \setminus V_\infty^K \mid D \otimes_K K_v$ is a skew field$\}$. Then*

$$[G_K, G_K] = G_K \cap \prod_{v \in T} [G_{K_v}, G_{K_v}].$$

Thus, the triviality of $\operatorname{Coker}\varphi$ is not yet established only for some forms of types ${}^2A_n$ and E_6. So in most cases the calculation of C (if it is central) is reduced to calculation of $M(G, S)$.

The pioneer works of Moore [14] and Matsumoto [10] contain the determination of $M(G, S)$ for Chevalley groups in the form (2) of § 1. The case of quasi-split groups was considered by Deodhar. Prasad and Raghunathan [20], [21] (for classical groups see also Bak and Rehmann [1], [2]) managed to determine $M(G, S)$ for all K-isotropic groups.

THEOREM 2.4. *Let G be K-isotropic. Then*

$$M(G, S) = \begin{cases} 1 & \text{if } S \neq V_\infty^K, \\ \subset E(K) & \text{otherwise,} \end{cases}$$

where $E(K)$ is the group of all roots of unity in K.

The author [25]–[27] calculated $M(G, S)$ for a large series of K-anisotropic groups. These results look as follows:

Inner forms of type A_n. Here G is associated to $\mathrm{SL}(1, D)$. Let n be the index of D and $S_e = \{v \in V^K \setminus S \mid D \otimes_K K_v \simeq M_2(F_v)\}$ where F_v is a skew field over K_v, $s_e = [S_e]$ (the number s_e is finite if $n > 2$ and infinite if $n = 2$).

THEOREM 2.5. *Suppose that S contains a nonarchimedian v_0 such that $D \otimes_K K_{v_0} \simeq M_n(K_{v_0})$. Then $M(G, S)$ is a finite subgroup of $B(D, S) = (\mathbf{Z}/2\mathbf{Z})^{s_e}$. In the general case $M(G, S)$ is isomorphic to a finite subgroup of an extension of $B(D, S)$ by the group $E(K)$ of all roots of unity in K.*

COROLLARY. *If $S_e = \emptyset$, in particular if n is odd, then*

$$M(G, S) = \begin{cases} 1 & \text{if } \exists v_0 \in S \text{ such that } K_{v_0} \neq \mathbf{C} \text{ and } D \otimes_K K_{v_0} \simeq M_n(K_{v_0}), \\ \subset E(K) & \text{otherwise.} \end{cases}$$

In fact, the last statement is very similar to the classical result (2) of § 1.

Outer forms of type A_n. These are the algebraic groups associated to special unitary groups $\mathrm{SU}_m(D, f)$ where D is a finite-dimensional central division algebra over L endowed with an involution σ such that $L^\sigma = K$ and $[L:K] = 2$ (involution of the second kind), and f is a nondegenerate m-dimensional hermitian form with respect to σ.

THEOREM 2.6. *Let $m \geqslant 3$. If S contains a nonarchimedian valuation then $M(G, S)$ has exponent $\leqslant 2$. In the general case $M(G, S)$ is a finite group which is an extension of a group of exponent $\leqslant 2$ by a subgroup of $E(K)$.*

Other classical types. Using Theorem 2.5 and the geometric representation of groups of classical types we obtained the following.

THEOREM 2.7. *Let G be a simple simply connected K-group of one of the following types: B_n $(n \geqslant 2)$, C_n $(n \geqslant 2)$, D_n $(n \geqslant 5)$. Suppose that S contains a nonarchimedian valuation v_0 and the following conditions are satisfied:*

1) *If G is of type B_n then either $n \geqslant 3$, or $n = 2$ and G splits over K_{v_0}.*
2) *If G is of type C_n then G splits over K_{v_0}.*

Then $M(G, S)$ has exponent $\leqslant 2$. In the general case $M(G, S)$ is a finite group which is an extension of a group of exponent $\leqslant 2$ by a subgroup of $E(K)$.

Exceptional types.

THEOREM 2.8. *Let G be a simple K-group of one of the following types: E_8, F_4, G_2. Then $M(G, S)$ is trivial if S contains a nonarchimedian valuation and is a subgroup of $E(K)$ otherwise.*

For groups of type E_7 we obtained a result similar to Theorem 2.7. Thus it remains to study the metaplectic kernel for some groups of types ${}^2A_n$, D_4 and E_6.

3. Centrality of the congruence kernel for classical groups

The results of the previous section reduce the problem of determination of the congruence kernel to the problem whether it is central or not. In this section and the following one we are going to describe the results on centrality of $C^S(G)$.

First of all, the centrality of the congruence kernel can be established by manipulating with unipotent elements in the group G_K (if there are any). This idea goes back to the fundamental works of Bass–Milnor–Serre [4], Mennicke [12], [13], Matsumoto [10] and Serre [30]. The final result is due to Raghunathan [22], [23] who proved that the existence of unipotent elements in G_K together with the condition $\operatorname{rang}_S G \geqslant 2$ in fact guarantees the centrality of $C^S(G)$. For his methods the existence of unipotent elements is essential so they cannot be extended to the case of anisotropic groups. Until recently the only result on centrality of $C^S(G)$ which allows also anisotropic groups was Kneser's theorem [9] for the spinor groups of quadratic forms. It turned out, however, that Kneser's argument is of general nature and can be modified so as to work for other groups with nice geometric representation. First Raghunathan and Tomanov considered the case of groups of type C_n and then the author proved the following general

THEOREM 3.1. *Let G be a simple simply connected K-group of one of the following types: B_n $(n \geqslant 2)$, C_n $(n \geqslant 4)$, D_n $(n \geqslant 5)$, G_2 or let G be a special unitary group SU_m $(m \geqslant 4)$ of type ${}^2A_{m-1}$ associated to some quadratic extension L/K. Then if $\operatorname{rang}_S G \geqslant 2$ then $C^S(G)$ is central.*

The proof of Theorem 3.1 was actually independent of the type of G and its scheme for G of type G_2 was published in [28]. It is based on the following

PROPOSITION 3.1. *$C^S(G)$ is central if the group G_K is projectively simple and if there is a K-defined subgroup $H \subset G$ with the following properties:*

1) *The natural map $C^S(H) \to C^S(G)$ is surjective.*
2) *For some nontrivial K-defined automorphism $\sigma \in \operatorname{Aut} G$ the restriction $\sigma | H$ is trivial.*

If it is already known that G_K is projectively simple the main difficulty that arises in application of Proposition 3.1 is how to check condition 1). In all known cases this was carried out by means of the following

PROPOSITION 3.2. *Let G act K-rationally on some affine K-variety X, and let $x \in X_K$. Suppose that for any normal subgroup $N \subset G_{O(S)}$ of finite index the orbit Nx is open in $G_{O(S)}x$ in the (induced) S-congruence topology. Then for the stabilizer $G(x)$ of x the natural map $C^S(G(x)) \to C^S(G)$ is surjective. (Here by the S-congruence topology we mean the topology of the space of S-adeles $X_{A(S)}$).*

Propositions 3.1 and 3.2 have not been published explicitly but in fact they are not new. If we apply them to $\Gamma = \mathrm{SL}_n(\mathbf{Z})$ ($n \geqslant 3$) we get the proof of the centrality of the corresponding congruence kernel which is very close to the classical one (see [8]). Let us show this.

Put $G = \mathrm{SL}_n$ and take for H the subgroup

$$\begin{pmatrix} & & 0 \\ & * & \vdots \\ & & 0 \\ 0 & \dots\ 0 & 1 \end{pmatrix}$$

which is isomorphic to SL_{n-1}. Then condition (2) of Proposition 3.1 holds for the automorphism $\sigma = \mathrm{Int}\, g$ where $g = \mathrm{diag}(1, \dots, 1, -1)$. Thus, it remains to check (1). Fix a basis $e_1, \dots, e_n$ of the n-dimensional space. Denote by F the stabilizer of e_n with respect to the natural action of G. It is easily seen that H is a maximal semisimple subgroup in F. Consequently, $C(F) = C(H)$ by Proposition 1.2 and it suffices to prove that the map $C(F) \to C(G)$ is surjective. For this we use Proposition 3.2 Any normal subgroup $N \subset \Gamma$ of finite index contains the subgroup $E(m)$ for some m where $E(m)$ is generated as a normal subgroup of Γ by all elementary matrices contained in the congruence subgroup $\Gamma(m)$. Hence it is sufficient to prove that $E(m)e_n$ is open in Γe_n for all m. It is well known that the orbit Γe_n consists of all vectors $a = (a_1, \dots, a_n)$ whose coordinates are relatively prime. So the desired fact follows from

LEMMA 3.1. *If* g.c.d. $(a_1, \dots, a_n) = 1$ *and* $(a_1, \dots, a_n) \equiv (0, \dots, 0, 1) \pmod{m^2}$ *then* $a = (a_1, \dots, a_n) \in E(m)e_n$.

(In fact, $E(m)e_n$ consists precisely of those $a = (a_1, \dots, a_n) \in \Gamma e_n$ for which $a \equiv (0, \dots, 0, 1) \pmod{m}$, but this is a bit more difficult to prove, see [8]).

In the situation described in Theorem 3.1 the openness of Nx in $G_{O(S)}x$ can be established using the following fact.

LEMMA 3.2. *Under the assumptions of Proposition* 3.2, *let* $x, y \in X_K$ *and suppose there is* $u \in N$ *with*

$$G(u(x))_{O(S)}x \cap G(x)_{O(S)}y \neq \emptyset. \tag{1}$$

Then $y \in Nx$.

To end this section, let us give a sketch of proof of Theorem 3.1. For a group G of any type indicated in Theorem 3.1 one can take its natural geometric realization as the automorphism group of a quadratic, hermitian or shew-hermitian form f defined on a vector space W over a division algebra (for G_2 one should take the natural 7-dimensional representation). Fix a vector $x \in W$ nonisotropic with respect to f and consider the "sphere" passing through x: $X = \{y \in W | f(y) = f(x)\}$. Then for an arbitrary normal subgroup $N \subset G_{O(S)}$ of finite index we find an open subset $U \subset X_{A(S)}$ such that for any $y \in U \cap G_{O(S)}x$ there is $u \in N$ satisfying (1). This part of the proof is the most complicated. In fact we look for $u \in N$ such that local analogs of (1) are satisfied and then use local-global arguments based on the Hasse principle, strong approximation theorem for algebraic groups and new results on the strong approximation property for algebraic varieties (see [28]). It remains to note that the group $G(x)$ is stable under some nontrivial K-automorphism of G which is of order 2 for groups of classical types and of order 3 for G_2.

4. Centrality of the congruence kernel for exceptional groups

The geometric method yielding Theorem 3.1 seems inapplicable to most exceptional groups. The reason is the absense of convenient geometric realizations for these groups. Here the solution of the congruence subgroup problem was obtained by a new approach using the inner structure of the group.

THEOREM 4.1. *Let G be a simple simply connected K-anisotropic group of one of the following types: E_7, E_8, F_4. If $\operatorname{rang}_S G \geqslant 2$ then $C^S(G)$ is central.*

The groups of type E_6 are omitted in the theorem due to the fact that they do not split in general over a quadratic extension of K, unlike the groups of the indicated types.

PROPOSITION 4.1. *Let G be a simple K-group of one of the following types: B_n, C_n, E_7, E_8, F_4, G_2. Then there is a maximal K-torus $T \subset G$ which splits over a quadratic extension L/K.*

(It should be remarked here that the proof of Proposition 4.1 makes use of the Hasse principle for simply connected groups, which was known to be true for all groups except possibly for type E_8. But recently Chernousov showed that it does hold for the groups of type E_8 as well.)

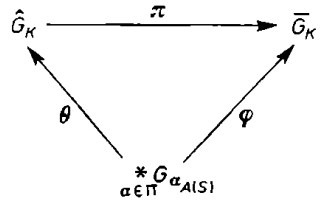
Let now G be a group as in Theorem 4.1. Choose a maximal K-torus $T \subset G$ satisfying the assertion of Proposition 4.1. If $R = R(T, G)$ denotes the corresponding root system then for every $\alpha \in R$ we have $\sigma(\alpha) = -\alpha$ where σ is a nonidentical automorphism of L/K. Thus the group G_α generated by one-dimensional unipotent subgroups U_α and $U_{-\alpha}$ is defined over K. The role that the groups G_α play in our situation is similar to the role that the ordinary root subgroups play for Chevalley groups. We shall try to explain the main idea of our proof of Theorem 4.1 using this analogy. More precisely, we shall

show that if G is a universal Chevalley group over K of rank $\geqslant 3$ and if it is already known that $C^S(H) = 1$ for any universal Chevalley group H over K of rank 2 then $C^S(G) = 1$.

Let T be a maximal K-split torus with root system $R = R(T, G)$. For any $\alpha \in R$ denote by G_α the corresponding root subgroup. As above we may identify the S-arithmetic completions $\bar{G}_K$ and $\bar{G}_{\alpha K}$ with the S-adelic groups $G_{A(S)}$ and $G_{\alpha A(S)}$. It is not hard to show that the groups $G_{\alpha A(S)}$ for simple roots α (the system of which will be denoted by Π) generate the group $G_{A(S)}$. Thus we have a surjective homomorphism

$$\varphi\colon \underset{\alpha\in\Pi}{*} G_{\alpha A(S)} \to G_{A(S)},$$

where $*$ denotes the free product. For any $\alpha \in R$ consider the closure C_α of $G_{\alpha K}$ in $\hat{G}_K$. Since G_α can always be imedded into a subgroup $H \subset G$ which is a universal Chevalley group of rank 2 and by our assumption $C^S(H) = 1$, the restriction $\pi | C_\alpha$ of the projection $\pi\colon \hat{G}_K \to \bar{G}_K$ induces an isomorphism θ_α: $C_\alpha \simeq G_{\alpha A(S)}$. If we take the inverse maps θ_α^{-1} and form their free product, we get a homomorphism $\theta\colon *_{\alpha\in\Pi} G_{\alpha A(S)} \to \hat{G}_K$ for which the diagram



is commutative.

If two roots $\alpha, \beta \in \Pi$ are connected in the Dynkin diagram of R then the group $G_{\alpha\beta}$ generated by G_α and G_β is a universal Chevalley group of rank 2. Our assumption implies that the restriction of π to the closure $C_{\alpha\beta}$ of $G_{\alpha\beta K}$ in $\hat{G}_K$ induces an isomorphism $\theta_{\alpha\beta}\colon C_{\alpha\beta} \simeq G_{\alpha\beta A(S)}$. In particular, for $v \neq w$ $(v, w \notin S)$ the groups $\theta_{\alpha\beta}^{-1}(G_{\alpha\beta K_v})$ and $\theta_{\alpha\beta}^{-1}(G_{\alpha\beta K_w})$ commute. Since $\theta_{\alpha\beta}^{-1} | G_{\alpha A(S)} = \theta_\alpha^{-1}$ and $\theta_{\alpha\beta}^{-1} | G_{\beta A(S)} = \theta_\beta^{-1}$ the groups $\theta_\alpha^{-1}(G_{\alpha K_v}) = \theta(G_{\alpha K_v})$ and $\theta_\beta^{-1}(G_{\beta K_w}) = \theta(G_{\beta K_w})$ also commute. The last fact is still true for orthogonal roots α and β. Indeed, if $\alpha \perp \beta$ then there is no root of the form $i\alpha + j\beta$ $(i, j \in \mathbf{Z}\setminus(0))$, whence the groups $G_{\alpha K}$ and $G_{\beta K}$ commute (see commutator relations in Chevalley groups, [31], § 6). Therefore the groups $C_\alpha = \theta(G_{\alpha A(S)})$ and $C_\beta = \theta(G_{\beta A(S)})$ also commute, and the desired fact is obvious.

Thus we have the following factorization for θ:

$$\underset{\alpha\in\Pi}{*} G_{\alpha A(S)} \to D \to \hat{G}_K \tag{1}$$

where D denotes the image of the natural homomorphism $*_{\alpha\in\Pi} G_{\alpha A(S)} \to \prod_{v\notin S}(*_{\alpha\in\Pi} G_{\alpha K_v})$. Then we use the following fundamental fact: for any field F the group G_F as an abstract group is generated by the groups $G_{\alpha F}$ $(\alpha \in \Pi)$ and can be defined by relations that exist between elements of the groups $G_{\alpha F}$ and

$G_{\beta F}$ for all pairs $\alpha, \beta \in \Pi$. In other words, the homomorphism δ: $*_{\alpha\in\Pi} G_{\alpha F} \to G_F$ is surjective and its kernel is generated as a normal subgroup by all the groups $N_{\alpha,\beta} = \mathrm{Ker}(G_{\alpha F} * G_{\beta F} \to G_{\alpha\beta F})$. Let us show that for any $v \notin S$, $\alpha, \beta \in \Pi$ the relations between the elements of $0(G_{\alpha K_v})$ and $0(G_{\beta K_v})$ are the same as those between the elements of $G_{\alpha K_v}$ and $G_{\beta K_v}$. If the roots α, β are not orthogonal then in the above notation we have the isomorphism $\theta_{\alpha\beta}$: $C_{\alpha\beta} \simeq G_{\alpha\beta A(S)}$. Consequently, $\mathrm{Ker}(0(G_{\alpha K_v}) * 0(G_{\beta K_v}) \to C_{\alpha\beta})$ and $\mathrm{Ker}(G_{\alpha K_v} * G_{\beta K_v} \to G_{\alpha\beta K_v})$ are naturally isomorphic. In the case of orthogonal roots α, β all relations between the elements of $G_{\alpha K_v}$ and $G_{\beta K_v}$ are consequences of the commutativity relations: $gh = hg$ for $g \in G_{\alpha K_v}$, $h \in G_{\beta K_v}$, these relations being satisfied by the elements of $0(G_{\alpha K_v})$ and $0(G_{\beta K_v})$.

The above argument together with the quoted fact from the theory of Chevalley groups shows that the sequence (1) can be expanded as follows:

$$\underset{\alpha\in\Pi}{*} G_{\alpha A(S)} \to D \to H \xrightarrow{\psi} \hat{G}_K$$

where H is the image of the natural homomorphism

$$\underset{\alpha\in\Pi}{*} G_{\alpha A(S)} \to \prod_{v\notin S} \left(\underset{\alpha\in\Pi}{*} G_{\alpha K_v} \right) \to \prod_{v\notin S} G_{K_v}.$$

It is easy to see that in fact H coincides with the group $G_{A(S)}$ and ψ provides a cross-section of π. Thus $\mathrm{Im}\,\psi \cap C^S(G) = 1$. The final step of the proof that we omit here is to establish that $\mathrm{Im}\,\psi \cap C^S(G)$ is dense in $C^S(G)$.

The proof of Theorem 4.1 uses a similar argument but is much more complicated. It is based on the fact that in the described situation any two groups G_α, G_β can be imbedded into a K-defined subgroup $H \subset G$ which belongs to one of the classical types and satisfies the condition $\mathrm{rang}_S H \geqslant 2$. Then $C^S(H)$ is central by Theorem 3.1 and one can argue as above substituting H for $G_{\alpha\beta}$. The details will be published elsewhere.

References

[1] A. Bak, *Le problème des sous-groupes de congruence et le problème métaplectique pour les groupes classiques de rang* > 1, C. R. Acad. Sci. Paris Sér. A–B, 292 (1981), A307–A310.

[2] A. Bak and U. Rehmann, *The congruence subgroup and metaplectic problems for* $\mathrm{SL}_{n\geqslant 2}$ *of division algebras*, J. Algebra 78 (1982), 475–547.

[3] H. Bass, M. Lazard et J.-P. Serre, *Sous-groupes d'indices finis dans* $\mathrm{SL}(n, \mathbf{Z})$, Bull. Amer. Math. Soc. 70 (1964), 385–392.

[4] H. Bass, J. Milnor and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geqslant 3)$ *and* Sp_{2n} $(n \geqslant 2)$, Inst. Hautes Études Sci. Publ. Math. 33 (1967), 54–137.

[5] M. V. Borovoi, *Abstract simplicity of some simple anisotropic algebraic groups over number fields*, Dokl. Akad. Nauk SSSR 283 (1985), 794–797 (in Russian).

[6] V. I. Chernousov, *On the structure of the groups of rational points of algebraic groups of type* D_l, Dokl. Akad. Nauk BSSR 31 (1987), 593–596 (in Russian).

[7] –, *On the projective simplicity of algebraic groups split by quadratic extension of a number field*, Dokl. Akad. Nauk SSSR 296 (1987), 1301–1305 (in Russian).

[8] J. E. Humphreys, *Arithmetic Groups*, Lecture Notes in Math. 789, Springer, Berlin 1980.
[9] M. Kneser, *Normalteiler ganzzahliger Spingruppen*, J. Reine Angew. Math. 311–312 (1979), 191–214.
[10] H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*, Ann. Sci. École Norm. Sup. (4), 2 (1969), 1–62.
[11] O. V. Mel'nikov, *Congruence kernel for the group* $SL_2(\mathbf{Z})$, Dokl. Akad. Nauk SSSR 228 (1976), 1034–1036 (in Russian).
[12] J. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. 81 (1965), 31–37.
[13] –, *On Ihara's modular group*, Invent. Math. 4 (1967), 202–228.
[14] C. Moore, *Group extensions of p-adic and adelic groups*, Inst. Hautes Études Sci. Publ. Math. 35 (1968), 5–70.
[15] V. P. Platonov, *Problem of strong approximation and Kneser–Tits conjecture for algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. 33 (1969), 1211–1219 (in Russian).
[15a] V. P. Platonov, *Arithmetic and structural problems for linear algebraic groups*, Proc. Intern. Congr. Math. Vancouver 1974, 471–476.
[16] –, *On the congruence subgroup problem for integral soluble groups*, Dokl. Akad. Nauk BSSR 15 (1971), 869–872 (in Russian).
[17] V. P. Platonov and A. S. Rapinchuk, *Multiplicative structure of skew fields over number fields and the Hasse norm principle*, Trudy Mat. Inst. Steklov. 165 (1984), 171–187 (in Russian).
[18] V. P. Platonov and A. A. Sharomet, *On the congruence subgroup problem for linear groups over arithmetic rings*, Dokl. Akad. Nauk BSSR 16 (1972), 393–396 (in Russian).
[19] G. Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. of Math. 105 (1977), 553–572.
[20] G. Prasad and M. S. Raghunathan, *On the congruence subgroup problem: Determination of the "Metaplectic kernel"*, Invent. Math. 71 (1983), 21–42.
[21] –, –, *Topological central extensions of semi-simple groups over local fields I, II*, Ann. of Math. 119 (1984), 143–201, 203–267.
[22] M. S. Raghunathan, *On the congruence subgroup problem*, Inst. Hautes Études Sci. Publ. Math. 46 (1976), 107–161.
[23] –, *On the congruence subgroup problem II*, Invent. Math. 85 (1986), 73–117.
[24] –, *On the group of norm 1 elements in a division algebra*, preprint IHES /M/84/15.
[25] A. S. Rapinchuk, *On the metaplectic kernel for anisotropic groups*, Dokl. Akad. Nauk BSSR 29 (1985), 1068–1071 (in Russian).
[26] –, *Metaplectic kernel for the group* $SL(1, D)$, Dokl. Akad. Nauk BSSR 30 (1986), 197–200 (in Russian).
[27] –, *Multiplicative arithmetic of division algebras over number fields and metaplectic problem*, Izv. Akad. Nauk SSSR Ser. Mat. 51 (1987), 1033–1064 (in Russian).
[28] –, *Congruence subgroup problem for algebraic groups and strong approximation for affine varieties*, Dokl. Akad. Nauk BSSR 32 (1988), 581–584 (in Russian).
[29] J.-P. Serre, *Groupes de Congruence*, in: Sém. Bourbaki (1966–1967), Benjamin, New York, 1968, exp. 330.
[30] –, *Le problème des groupes de congruence pour* SL_2, Ann. of Math. 92 (1970), 489–527.
[31] R. Steinberg, *Lectures on Chevalley Groups* (Notes prepared by J. Faulkner and R. Wilson), Yale Univ., 1967.

Added in proof (May 1990). 1. Results similar to Theorem 3.1 were obtained independently, but slightly later by G. Tomanov (see J. Reine Angew. Math. 402 (1989), 138–152).

2. Concerning the proof of Theorem 4.1 see A. S. Rapinchuk, *On the congruence subgroup problem for algebraic groups*, Dokl. Akad. Nauk SSSR 306 (1989), 1304–1307 (in Russian).

3. Another approach to the congruence subgroup problem in the general situation has been developed in A. S. Rapinchuk, *Combinatorial theory of arithmetic groups*, Preprint 20 (420) of the Institute of Mathematics of the Academy of Sciences of B.S.S.R.