A. S. RAPINCHUK

Congruence subgroup problem for algebraic groups: old and new

Astérisque, tome 209 (1992), p. 73-84
<http://www.numdam.org/item?id=AST_1992__209__73_0>

CONGRUENCE SUBGROUP PROBLEM FOR ALGEBRAIC GROUPS: OLD AND NEW

A. S. RAPINCHUK*

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

$$G_{\mathcal{O}(S)}(\mathfrak{a}) = \{g \in G_{\mathcal{O}(S)} \mid g \equiv E_n \pmod{\mathfrak{a}}\},$$

which is a normal subgroup of finite index in $G_{\mathcal{O}(S)}$. The initial statement of the Congruence Subgroup Problem was:

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

In fact, it was found by F. Klein as far back as 1880 that for the group $\mathrm{SL}_2(\mathbb{Z})$ the answer to question (1) is "no". So a more accurate statement of the problem should be: for which G and S does (1) have an affirmative answer? However, till the mid sixties there were no nontrivial examples of groups for which this is actually true. Only in 1965 did Bass-Lazard-Serre [1] and Mennicke [10] give a positive solution to the congruence subgroup problem for $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. In the course of further investigations, it appeared convenient

* The author wishes to thank the Department of Mathematics in Geneva for editing and retyping the manuscript.

to introduce the object measuring deviation from the positive solution of (1) and then to view the congruence subgroup problem as the problem of its computation. This object (called the congruence kernel) was defined by Serre [27] as follows.

Let us introduce on the group G_K of K-rational points two Hausdorff topologies, τ_a and τ_c, called S-arithmetic topology and S-congruence topology, respectively. The complete system of neighbourhoods of unity for τ_a (resp., τ_c) consists of all normal subgroups of finite index (resp., all congruence subgroups) in $G_{\mathcal{O}(S)}$. It is easy to show that these topologies satisfy all the properties that ensure the existence of the corresponding S-arithmetic and S-congruence completions $\widehat{G}$ and $\overline{G}$. Since τ_a is stronger than τ_c, the identity map

$$(G_K, \tau_a) \longrightarrow (G_K, \tau_c)$$

is continuous. Therefore it can be extended to a continuous homomorphism $\pi\colon \widehat{G} \longrightarrow \overline{G}$ of the completions. By definition, $C^S(G) = \operatorname{Ker}\pi$ is the *congruence kernel.*

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

Thus, in general, the congruence kernel $C^S(G)$ measures deviation from a positive answer to the congruence subgroup problem. So, by the modern statement of the problem we mean the problem of determination of $C^S(G)$. It is well-known (see for example [23]) that this problem can be reduced to the main case of an (absolutely) simple, simply connected algebraic group G. Here we shall be exclusively concerned with that case. As we have already remarked, the first positive result on the congruence subgroup problem for such groups is due to Bass-Lazard-Serre [1] and Mennicke [10], who studied the case of $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. Then Bass-Milnor-Serre [2] completed the investigation of SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$ over an arbitrary number field K, after obtaining a description of $C^S(G)$ in the following form:

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

where $E(K)$ is the group of all roots of unity in K. By further developing the methods of [2], Matsumoto [9] extended (2) to all universal Chevalley groups different from SL_2 (the case of twisted Chevalley groups was considered by Deodhar [4]). In the case $G = \mathrm{SL}_2$, first Mennicke [11] gave a positive solution to the congruence subgroup problem for the group $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$, and then Serre

[27] studied the general situation and showed that, provided $\operatorname{Card} S > 1$, the answer is of the form (2). On analysing the obtained results, Serre [27] formulated the following congruence subgroup conjecture, which gives sufficient conditions for $C^S(G)$ to be finite or infinite, in terms of the so-called S-rank:

$$\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G,$$

where $\operatorname{rang}_P G$ denotes the rank of the group G over the field P, i.e., the dimension of a maximal P-split subtorus in G.

CONJECTURE 1. *Let G be simple and simply connected. Then in case $\operatorname{rang}_S G \geq 2$ and G is K_v-isotropic for all $v \in S \setminus V_\infty^K$, the congruence kernel $C^S(G)$ should be finite. In case $\operatorname{rang}_S G = 1$, it should be infinite.*

The case of finite $C^S(G)$ is the most interesting and important for applications. In that case, we shall say that the group $\Gamma = G_{\mathcal{O}(S)}$ has the *congruence subgroup property* (CSP). In this paper we are going to describe the class of groups for which (CSP) is known to hold and outline some new methods of attacking the congruence subgroup problem, which, as we hope, will enable us to enlarge this class considerably.

Let us first describe the general scheme for calculating the congruence kernel $C = C^S(G)$. It follows from our definitions that C can be determined from the exact sequence:

$$1 \longrightarrow C \longrightarrow \widehat{G} \xrightarrow{\pi} \overline{G} \longrightarrow 1 \tag{3}$$

Let us consider the initial segment of the Hochschild-Serre spectral sequence corresponding to (3):

$$H^1(\overline{G}) \xrightarrow{\varphi} H^1(\widehat{G}) \longrightarrow H^1(C)^{\overline{G}} \xrightarrow{\psi} H^2(\overline{G}), \tag{4}$$

where $H^i(*)$ denotes the i-th continuous cohomology group with coefficients in the one-dimensional torus $\mathbb{R}/\mathbb{Z}$. The term $H^1(C)^{\overline{G}}$ in (4) is connected with C as follows:

$$H^1(C)^{\overline{G}} = \operatorname{Hom}(C/[C, \hat{G}]\, , \mathbb{R}/\mathbb{Z}).$$

So one can reconstruct C from $H^1(C)^{\overline{G}}$ only under the assumption that C is central, i.e., lies in the centre of $\widehat{G}$. Indeed, in this case $H^1(C)^{\overline{G}}$ coincides with the Pontryagin dual C^* of C. Suppose now that C is central. Then we have the following exact sequence:

$$1 \longrightarrow \operatorname{Coker} \varphi \longrightarrow C^* \longrightarrow \operatorname{Im} \psi \longrightarrow 1.$$

Ignoring the trivial case $\mathrm{rang}_S\, G = 0$, in which $G_{\mathcal{O}(S)}$ is finite and consequently $C^S(G) = 1$, we immediately obtain from the strong approximation theorem that the group $\overline{G}$ can be identified with the group $G_{A(S)}$ of S-adeles. Then, using the fact that the sequence (3) splits over the group G_K and is the "universal" sequence with this property, one can show that $\mathrm{Im}\,\psi$ coincides with the so-called *metaplectic kernel*

$$M(G,S) = \mathrm{Ker}\big(H^2(G_{A(S)}) \longrightarrow H^2(G_K)\big),$$

where G_K is endowed with the discrete topology. On the other hand

$$\mathrm{Coker}\,\varphi \cong \overline{[G_K, G_K]}/\,[G_K, G_K]\,,$$

where the bar denotes closure in G_K for the S-arithmetic topology. Taking into account that $M(G,S)$ is always finite (see [17]) and that $[G_K, G_K]$ has finite index in G_K (see [8]), we arrive at the following

PROPOSITION 2. *If C is central then it is finite. If, moreover,* $\mathrm{Coker}\,\varphi = 1$ *then $C^* \simeq M(G,S)$.*

In fact, at present it is known that $\mathrm{Coker}\,\varphi$ is indeed trivial for most cases. This depends on the validity for G_K of the following conjecture, which describes the normal structure. (This conjecture was formulated by Platonov [13] in the form of a local-to-global principle for projective simplicity and then by Margulis [8] in the final form).

CONJECTURE 2. *Let $V_f^K = V^K \setminus V_\infty^K$ be the set of nonarchimedean valuations, and let $T = \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic}\}$. 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 $N = W \cap G_K$. In other words, any noncentral normal subgroup is open (equivalently, closed) in the T-adic topology.*

If Conjecture 2 is true for G_K then we say that G_K has a *standard description of normal subgroups*. In the situation of Conjecture 1 we have $S \cap T = \varnothing$, and so the triviality of $\mathrm{Coker}\,\varphi$ is equivalent to saying that Conjecture 2 holds for $N = [G_K, G_K]$. But the latter statement is actually true for all groups, with the possible exception of some anisotropic forms of types ${}^2A_n$, ${}^{3,6}D_4$ and E_6 (see [14]). Thus, in most cases, the calculation of C (provided it is central) reduces to that of $M(G,S)$.

The first computations of the metaplectic kernel had been carried out by Moore [12] and Matsumoto [9]. They obtained the description of $M(G,S)$