J. S. Chahal
Nagoya Math. J.
Vol. 79 (1980) 141-144

SOLUTION OF THE CONGRUENCE SUBGROUP PROBLEM FOR SOLVABLE ALGEBRAIC GROUPS

JASBIR SINGH CHAHAL

1. Statement of the theorem

Let k be an algebraic number field of finite degree over the field $\boldsymbol{Q}$ of rational numbers. We denote by $\mathfrak{o}$ the ring of integers in k. In general, for a subring A, containing 1, of a universal domain Ω we denote by $GL(n, A)$ the subgroup of $GL(n, \Omega)$ consisting of matrices $x = (x_{ij})$ with $x_{ij} \in A$ and $\det x \in A^{\times}$, the group of units of A. Now, we consider an algebraic group G in $GL(n, \Omega)$ defined over k. For A as above, we put

$$G(A) = G \cap GL(n, A)$$

and for an integral ideal $\mathfrak{a} \neq 0$ in $\mathfrak{o}$, we put

$$G(\mathfrak{a}) = \{x \in G(\mathfrak{o}),\ x \equiv 1 \pmod{\mathfrak{a}}\}\,.$$

A subgroup Γ of $G(\mathfrak{o})$ is said to be a *congruence subgroup* for G if Γ contains $G(\mathfrak{a})$ for some $\mathfrak{a}$.

Obviously, a congruence subgroup has a finite index in $G(\mathfrak{o})$, but the converse is, in general, false (cf. [1]). The purpose of this paper is to establish the following

THEOREM. *Suppose $G \subseteq GL(n, \Omega)$ is a solvable algebraic group defined over a number field k. Then every subgroup Γ of $G(\mathfrak{o})$ with finite index is a congruence subgroup.*

The results and conjectures in [1] mainly concern simply connected simple Chevalley groups of rank > 1. To see what happens when the group is not simply connected, the author first studied the algebraic torus defined by the Pell's equation $x^2 - my^2 = 1$. This special case*) of our main theorem was treated by an elementary method the manuscript of

Received March 29, 1979.

*) See the remark at the end of the paper.

which was turned down by this Journal some months ago because a part of the results followed from a theorem of Chevalley (cf. [5]). The author wishes to thank the referee for drawing his attention to this work of Chevalley which lead him to generalize the results to the much wider case of arbitrary solvable groups.**)

2. Reduction of the proof

It is well known that an irreducible solvable algebraic group G defined over k is a semi-direct product $G = TU$, where T is a torus and U is an irreducible normal unipotent subgroup, both defined over k. In this section, we shall show that it is enough to prove our theorem when $G = T$ or $G = U$. Without loss of generality, we can assume that G is irreducible. It is clear that $G(\mathfrak{o}) \supseteq T(\mathfrak{o})U(\mathfrak{o})$. We know that the index $[G(\mathfrak{o}): T(\mathfrak{o})U(\mathfrak{o})]$ is finite (cf. Proposition 13 (δ) of [6]). Now, since $[G(\mathfrak{o}): \Gamma]$ is finite, so is $[T(\mathfrak{o})U(\mathfrak{o}): \Gamma \cap T(\mathfrak{o})U(\mathfrak{o})]$. Therefore, replacing Γ by $\Gamma \cap T(\mathfrak{o})U(\mathfrak{o})$, we can assume that $\Gamma \subseteq T(\mathfrak{o})U(\mathfrak{o})$. For each finite prime $\mathfrak{p}$ of k, denote by $\mathfrak{o}_\mathfrak{p}$ the ring of $\mathfrak{p}$-adic integers in the local field $k_\mathfrak{p}$. For the ideal $\mathfrak{p}^r$, $r \geq 0$, we put

$$G_\mathfrak{p}(\mathfrak{p}^r) = \{x \in G(\mathfrak{o}_\mathfrak{p}),\ x \equiv 1 \pmod{\mathfrak{p}^r}\}.$$

For almost all $\mathfrak{p}$, we have $G(\mathfrak{o}_\mathfrak{p}) = T(\mathfrak{o}_\mathfrak{p})U(\mathfrak{o}_\mathfrak{p})$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ be the primes for which we have the inequality

$$G(\mathfrak{o}_{\mathfrak{p}_j}) \supsetneq T(\mathfrak{o}_{\mathfrak{p}_j})U(\mathfrak{o}_{\mathfrak{p}_j}), \qquad 1 \leq j \leq s.$$

The group $T(\mathfrak{o}_\mathfrak{p})U(\mathfrak{o}_\mathfrak{p})$ is compact and open in $G(\mathfrak{o}_\mathfrak{p})$ and so are the groups $G_\mathfrak{p}(\mathfrak{p}^r)$ for all $r \geq 0$. For each $\mathfrak{p}$, there is an $r_\mathfrak{p}$ such that $r_\mathfrak{p} = 0$ if $\mathfrak{p} \neq \mathfrak{p}_j$ and $T(\mathfrak{o}_\mathfrak{p})U(\mathfrak{o}_\mathfrak{p}) \supseteq G_\mathfrak{p}(\mathfrak{p}^{r_\mathfrak{p}})$. Let $\mathfrak{c} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$. Then we have

$$T(\mathfrak{o}_\mathfrak{p})U(\mathfrak{o}_\mathfrak{p}) \supseteq G_\mathfrak{p}(\mathfrak{p}^{r_\mathfrak{p}}) \supseteq G(\mathfrak{p}^{r_\mathfrak{p}}) \supseteq G(\mathfrak{c}).$$

Let $x = tu \in G(\mathfrak{c})$ with $t \in T(k)$, $u \in U(k)$. Then $t \in T(\mathfrak{o}_\mathfrak{p})$, $u \in U(\mathfrak{o}_\mathfrak{p})$ for all $\mathfrak{p}$ and so $t \in T(\mathfrak{o})$, $u \in U(\mathfrak{o})$. Thus we have shown that

$$T(\mathfrak{o})U(\mathfrak{o}) \supseteq G(\mathfrak{c}).$$

Replacing Γ again by $\Gamma \cap G(\mathfrak{c})$, we can assume that $G(\mathfrak{c}) \supseteq \Gamma$. If we put $\Gamma_1 = \Gamma \cap T(\mathfrak{o})$ and $\Gamma_2 = \Gamma \cap U(\mathfrak{o})$, then the indices $[T(\mathfrak{o}): \Gamma_1]$ and

**) This paper is based on a part of the author's Ph.D. thesis, written at the Johns Hopkins University under the direction of Professor Takashi Ono.

$[U(\mathfrak{o}): \Gamma_2]$ are both finite. Assuming the theorem for $G = T$ and $G = U$, we have $\Gamma_1 \supseteq T(\mathfrak{b})$, $\Gamma_2 \supseteq U(\mathfrak{b})$ for some $\mathfrak{b}$ and hence $\Gamma \supseteq T(\mathfrak{b})U(\mathfrak{b})$. Let $\mathfrak{b} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_t^{e_t}$. By the topological argument as above, we have, for large a_i,

$$T_{\mathfrak{q}_i}(\mathfrak{q}_i^{e_i}) U_{\mathfrak{q}_i}(\mathfrak{q}_i^{e_i}) \supseteq G_{\mathfrak{q}_i}(\mathfrak{q}_i^{a_i}) .$$

We finally put $\mathfrak{a} = \mathfrak{q}_i^{a_i} \cdots \mathfrak{q}_t^{a_t}\mathfrak{c}$. It can be checked as before that if $x = tu \in G(\mathfrak{a})$, then $t \in T(\mathfrak{b})$, $u \in U(\mathfrak{b})$. Therefore, we have $\Gamma \supseteq G(\mathfrak{a})$, which completes the reduction of the proof.

3. The case of the unipotent group

If $\dim G = 1$, then $G \approx G_a$, the additive group and $G(\mathfrak{o})$ is isomorphic to $\mathfrak{o}$ up to finite index by Cor. 6.11 of [3]. If $[\mathfrak{o}: \Gamma] = g$, let $\mathfrak{a} = g\mathfrak{o}$, the ideal generated by g. Then $\Gamma \supseteq G(\mathfrak{a}) = \mathfrak{a}$. If now $\dim G = r$, we write $G = G_a U$ as semi-direct product with $\dim U = r - 1$. Repeating the argument of the last section for the semi-direct product $G = TU$, we complete the proof by induction on r.

4. The case of the algebraic tori

Let T be a torus defined over k. We begin with

PROPOSITION. *Let* $\mathfrak{O}$ (resp. $\mathfrak{o}$) *be the ring of integers of* K (resp. k) *where we assume that* K *is a finite galois extension of* k. *Let* Γ *be a subgroup of finite index in* $T(\mathfrak{o})$. *Then, there exists a subgroup* $\tilde{\Gamma}$ *of* $T(\mathfrak{O})$ *of finite index such that* $\tilde{\Gamma} \cap T(\mathfrak{o}) \subseteq \Gamma$.

Proof. By Theorem 4 of [6], $T(\mathfrak{O})$ is finitely generated and so we may assume that $T(\mathfrak{O})$ is free, since we are worried about Γ up to finite index only. Let $\mathfrak{g}$ be the galois group of K/k. Then we have for any natural number r, $(T(\mathfrak{O})^r)^{\mathfrak{g}} = (T(\mathfrak{O})^{\mathfrak{g}})^r$, where for a group H we denote by H^r the subgroup consisting of r-th powers and by $H^{\mathfrak{g}}$ the subgroup of fixed points under the action of a group $\mathfrak{g}$. In fact, the inclusion $(T(\mathfrak{O})^r)^{\mathfrak{g}} \subseteq (T(\mathfrak{O})^{\mathfrak{g}})^r$ is less trivial. Take an $x = y^r \in (T(\mathfrak{O})^r)^{\mathfrak{g}}$, with $y \in T(\mathfrak{O})$. Then, since $\sigma(y^r) = y^r$ for all $\sigma \in \mathfrak{g}$, we have $(y^{-1}\sigma(y))^r = 1$. Since, we assumed that $T(\mathfrak{O})$ is free, $\sigma(y) = y$ and so $x \in (T(\mathfrak{O})^{\mathfrak{g}})^r$, which proves our assertion. Now put $\tilde{\Gamma} = T(\mathfrak{O})^r$, where $r = [T(\mathfrak{o}): \Gamma]$. Then obviously $[T(\mathfrak{O}): \tilde{\Gamma}]$ is finite. Also, we have $\tilde{\Gamma} \cap T(\mathfrak{o}) = \tilde{\Gamma}^{\mathfrak{g}} = (T(\mathfrak{O})^r)^{\mathfrak{g}} = (T(\mathfrak{O})^{\mathfrak{g}})^r = T(\mathfrak{o})^r$, q.e.d.

Proof of the theorem for tori.

(i) If $T = G_m$, the multiplicative group, then $G(k) = k^\times$ and $G(\mathfrak{o}) = \mathfrak{o}^\times$. The proof now follows from a result of Chevalley (cf. Théorème 1, [5]).

(ii) If $T = (G_m)^d$, the trivial torus over k, and $\Gamma \subseteq G(\mathfrak{o}) = (\mathfrak{o}^\times)^d$, we put $\Gamma_i = \pi_i(\Gamma)$, where π_i is the i-th projection. If the index $[G(\mathfrak{o}): \Gamma]$ is finite, then so is $[\mathfrak{o}^\times: \Gamma_i]$ and by (i) we have $\Gamma_i \supseteq G_m(\mathfrak{a}_i)$ for some ideal $\mathfrak{a}_i$. Let $\mathfrak{a} = \mathfrak{a}_i \cdots \mathfrak{a}_d$. If $x = (x_1, \cdots, x_d) \equiv 1 \pmod{\mathfrak{a}}$, then $x_i \equiv 1 \pmod{\mathfrak{a}_i}$, which implies that $x_i \in \Gamma_i$ and $x \in \Gamma$, i.e. $\Gamma \supseteq G(\mathfrak{a})$.

(iii) Let T be split by a finite galois extension K/k. Let Γ be a subgroup of finite index in $T(\mathfrak{o})$. By the proposition, we can find a subgroup $\tilde{\Gamma}$ of $T(\mathfrak{O})$ such that it has finite index in $T(\mathfrak{O})$ and $\tilde{\Gamma} \cap T(\mathfrak{o}) \subseteq \Gamma$. By case (ii), we have $\tilde{\Gamma} \supseteq T(\mathfrak{A})$ for some ideal $\mathfrak{A}$ in $\mathfrak{O}$. Put $\mathfrak{a} = \mathfrak{A} \cap \mathfrak{o}$, then if $x \in T(\mathfrak{a})$, we have $x \in T(\mathfrak{A}) \cap T(\mathfrak{o}) \subseteq \tilde{\Gamma} \cap T(\mathfrak{o}) \subseteq \Gamma$, q.e.d.

Remark. In the case of the torus T defined by the Pell's equation $x^2 - my^2 = 1$, one obtains a more precise result than that obtained by merely applying the Chevalley's theorem. In fact, given Γ of finite index in $T(Z)$, one can choose a natural number N such that $[\Gamma: T(N)] = 1$ or 2 (cf. 4]).

References

[1] H. Bass, J. Milnor and J.-P. Serre, Solution of the congruence subgroup problem for $SL_n (n \geq 3)$ and $Sp_{2n} (n \geq 2)$, Pub. Math., I.H.E.S. (1967) n° 33, 59–137.

[2] A. Borel, Groupes linéaires algébriques, Ann. of Math., **64** (1956), 20–82.

[3] A. Borel and Harish-Chandra, Arithmetic subgroups of the algebraic groups, Ann. of Math., **75** (1962), 485–535.

[4] J. S. Chahal, A note on the Pell's equation (unpublished).

[5] C. Chevalley, Deux théorèmes d'arithmétique, J. of Math. Soc. of Japan, **3** (1951), 36–44.

[6] T. Ono, On some arithmetic properties of linear algebraic groups, Ann. of Math., **70** (1959), 266–290.

[7] T. Ono, Arithmetic of algebraic tori, Ann. of Math., **74** (1961), 101–139.

University of Wisconsin-Milwaukee
Department of Mathematical Sciences