BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 1, Number 6, November 1979

THE SOLUBILITY OF CERTAIN DECISION PROBLEMS IN ARITHMETIC AND ALGEBRA

BY FRITZ J. GRUNEWALD AND DANIEL SEGAL

Introduction. In contrast to the negative solution of Hilbert's 10th problem, we show that a certain type of Diophantine question connected with algebraic groups is effectively decidable. Applications include the solution of the conjugacy problem in all arithmetic groups and the solution of the isomorphism problem for finitely generated nilpotent groups.

Results. We have constructed some rather general algorithms, which can (in theory) be applied in diverse situations. Let us describe them.

A. ARITHMETIC GROUPS. Let G be an algebraic subgroup of GL_n, defined by an explicitly given finite set of polynomial equations over $\mathbf{Q}$ in the matrix entries; suppose Γ is an explicitly given arithmetic subgroup in G: by this we mean (i) Γ is a subgroup of finite index in $G_{\mathbf{Z}}$, (ii) an upper bound for this index is given, and (iii) we have an effective procedure to decide for each $g \in G_{\mathbf{Z}}$ whether or not $g \in \Gamma$.

Algorithm A1 finds finitely many matrices $\gamma_1, \ldots, \gamma_s \in \Gamma$ and a finite set R of relations satisfied by them such that $\Gamma = \langle \gamma_1, \ldots, \gamma_s | R \rangle$ is a presentation of Γ.

Suppose now that we are also given rational functions over $\mathbf{Q}$, in the matrix entries, which define a rational representation $\rho : G \longrightarrow GL_m$, for some m.

Algorithm A2 determines for any two vectors a and b in $\mathbf{Q}^m$ whether there exists $\gamma \in \Gamma$ such that $a\rho(\gamma) = b$; if so, it also finds such a matrix γ.

The algorithms proceed by constructing "fundamental sets" for $G_{\mathbf{Z}}$ in $G_{\mathbf{R}}$ (and for $H_{\mathbf{Z}}$ in $H_{\mathbf{R}}$, where H is the stabilizer of a in G in Algorithm A2), after the manner of Borel and Harish-Chandra, [BH] and [Bo]. Of course these constructions have to be made effective, which involves a certain amount of technical difficulty. There is then a fairly standard way to complete A1. The basic idea for A2, somewhat oversimplified, is as follows. One first decides whether there exists $x \in G_{\mathbf{R}}$ with $a\rho(x) = b$, and if so, computes a sequence of rational approximations to such a matrix x; this is possible by Tarski's decision method for elementary algebra over $\mathbf{R}$ [T]. Then one constructs a "fundamental set" Ω with the following properties: (i) $\Omega H_{\mathbf{Z}} = H_{\mathbf{R}}$, (ii) $\Omega \subseteq Sc_1 \cup \cdots \cup USc_k$

Received by the editors June 6, 1979.

AMS (MOS) subject classifications (1970). Primary 10C30, 10N05; Secondary 20F18.

where $c_1, \ldots, c_k$ are finitely many known matrices in $GL_n(\mathbf{Z})$ and S satisfies (iii) $S \cdot GL_n(\mathbf{Z}) = GL_n(\mathbf{R})$ and (iv) $S^{-1}S \cap GL_n(\mathbf{Z}) = \{g_1, \ldots, g_l\}$ where $g_1, \ldots, g_l$ are finitely many known matrices. A matrix $\lambda \in GL_n(\mathbf{Z})$ such that $x\lambda \in S$ is effectively computable; and it is then easy to see that there exists $\gamma \in G_{\mathbf{Z}}$ with $a\rho(\gamma) = b$ if and only if there exist $i \leqslant k$ and $j \leqslant l$ such that $\lambda g_j c_i \in G$ and $a\rho(c_i^{-1}g_j^{-1}\lambda^{-1}) = b$. This is of course easy to decide.

Applying A2 in special cases enables one to solve various more or less classical decision problems. For example we deduce

THEOREM 1. *Every arithmetic group has soluble conjugacy problem.*

In fact, for Γ as above and any positive integer r, one can decide whether two r-tuples of $n \times n$ matrices over $\mathbf{Q}$ are simultaneously conjugate under Γ. The work of M. A. Tayzlin [Ta] implies then, that the isomorphism problem for finitely generated commutative semigroups has a positive solution. Theorem 1 is already known in certain cases (GL_n and SL_n over rings of algebraic integers, etc.), see [G], [Sal].

B. FORMS. The group $GL_n(\mathbf{Z})$ operates by substitution on the space of forms of a fixed degree in n·variables over $\mathbf{Q}$, and a classical problem is to decide whether two forms are equivalent under this operation. With certain exceptions, the solution is also classical, at least implicitly; see [J], [P], [Si], and [C, §13.12]. With Algorithm A2, this can be generalized.

THEOREM 2. *Let k be an algebraic number field and let $f_1, \ldots, f_r$ and $g_1, \ldots, g_r$ be forms in n variables over k. Let Γ be an explicitly given arithmitic group of degree n over k. Then it is effectively decidable whether there exists $\gamma \in \Gamma$ transforming f_i to g_i for $i = 1, \ldots, r$.*

Here the field k is supposed effectively given in some way; and an "arithmetic group over k" is what one gets on replacing $\mathbf{Q}$ by k and $\mathbf{Z}$ by the ring of integers of k in the definition of §A above.

C. $\mathbf{Z}$-ALGEBRAS. A fairly straightforward application of Algorithms A2 and A1 to an algebraic problem is given by

THEOREM 3. *Let A and B be (not necessarily associative) rings whose additive groups are finitely generated. Assume that A and B are specified in terms of $\mathbf{Z}$-bases and the corresponding structure constants. Then it is effectively decidable whether A and B are isomorphic rings.*

D. NILPOTENT GROUPS. A more elaborate application of the algorithms, indeed our original motivation for the whole enterprise, is to the *isomorphism problem* for nilpotent groups. Let G be a torsion-free finitely generated nilpotent group. There is a well-known canonical embedding $\theta_G\colon G \longrightarrow \mathrm{Tr}_1(n, \mathbf{Z})$, for a suitable $n = n(G)$, with the following "naturalness" property: if H is another such group of the same nilpotency class and if $n(H) = n(G) = n$ say, then to every isomorphism $\varphi\colon G \longrightarrow H$ there corresponds a matrix $\varphi^* \in GL_n(\mathbf{Z})$ making the following diagram commute:

$$\begin{tikzcd}
G \arrow[r, "\theta_G"] \arrow[d, "\varphi"'] & \mathrm{Tr}_1(n, \mathbf{Z}) \arrow[r, hook] & GL_n(\mathbf{Z}) \arrow[d, "\varphi^{**}"] \\
H \arrow[r, "\theta_H"'] & \mathrm{Tr}_1(n, \mathbf{Z}) \arrow[r, hook] & GL_n(\mathbf{Z})
\end{tikzcd}$$

where φ^{**} denotes conjugation by φ^*. (See [**H**, Chapter 7].) It follows that $G \cong H$ if and only if $G\theta_G$ and $H\theta_H$ are conjugate in $GL_n(\mathbf{Z})$; and this is a question which can be decided by Algorithm A2, also using ideas from [**GS2**, §4] and [**GS1**]. It also follows–taking $H = G$–that Aut G can be identified in a natural way with $N_{GL_n(\mathrm{Z})}(G\theta_G)/C_{GL_n(\mathrm{Z})}(G\theta_G)$; this is a quotient of two arithmetic groups to which A1 may be applied.

These observations explain the idea behind the following algorithms.

Algorithm D1. Let $G = \langle X|R\rangle$ be a given finite presentation of a group G, which is also given to be nilpotent. The algorithm finds a finite presentation for Aut G, each generator being specified by its action on X.

Algorithm D2. Let $G_i = \langle X_i|R_i\rangle$ be given finite presentations of groups G_i, $i = 1, 2$, which are also given to be nilpotent. The algorithm determines whether $G_1 \cong G_2$, and if so produces an explicit isomorphism.

Thus we have

THEOREM 4. *The isomorphism problem for nilpotent groups is soluble.*

This answers a question which has been open for some time, see e.g. [**K** p. 392, Problem 9]. It is interesting to note that, in contrast, the "epimorphism problem" for finitely generated nilpotent groups is undecidable: this has recently been proved by Remeslennikov.

Final remarks. 1. It should be made clear that the present results are of theoretical rather than practical significance. While the algorithms which reduce the problems of §§B–D to Algorithms A1 and A2 can be made reasonably efficient, the algorithms of §A would be hopeless to carry out in practice. This is because their extreme generality forces them to rely on general, and mainly nonconstructive, existence theorems. The interesting and important task of inventing usable versions of these algorithms to deal with particular cases still remains; existing work along these lines includes [**Be**], [**G**], [**Hu**], [**Sw**] and other papers.

2. V. N. Remeslennikov informs us that R. A. Sarkisjan in Moscow has

independently obtained results similar to those of §§A and D above [Sa2]. His results however only hold modulo a certain conjecture—the validity of the "Hasse principle" for all semisimple simply connected linear algebraic groups—which is apparently still unproved in the case of the algebraic group of type $E8$. Our methods are quite independent of this, indeed they are elementary in the sense that no use is made of the classification or structure theory of semisimple algebraic groups.

REFERENCES

[Be] H. Behr, *Uber die endliche Definierbarkeit verallgemeinerter Einheitengruppen,* J. Reine Angew. Math. 211 (1962), 123–135.

[Bo] A. Borel, *Introduction aux groupes arithmètiques,* Hermann, Paris, 1969.

[BH] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups,* Ann. of Math. (2) 75 (1962), 485–535.

[C] J. W. S. Cassells, *Rational quadratic forms,* Academic Press, London, 1978.

[G] F. J. Grunewald, *Solution of the conjugacy problem in certain arithmetic groups,* Word Problems II (S. I. Adian, W. W. Boone and G. Higman, eds.), North-Holland, Amsterdam, 1979.

[GS1] F. J. Grunewald and D. Segal *A note on arithmetic groups,* Bull. London Math. Soc. 10 (1978), 297–302.

[GS2] ———, *Conjugacy of subgroups in arithmetic groups* (to appear).

[H] P. Hall, *Nilpotent groups,* Queen Mary College, London, 1969.

[Hu] A. Hurwitz, *Die unimodularen Substitutionen in einem algebraischen Zahlkörper,* Nachr. Gesellschaft Wiss. Göttingen, 1895.

[J] C. Jordan, *Mémoire sur l'èquivalence des formes,* J. École Polytech. 48 (1880), 112–150.

[K] M. I. Kargapolov, *Some questions in the theory of soluble groups,* Proc. 2nd Internat. Conf. Theory of Groups, Lecture Notes in Math., vol. 372, Springer-Verlag, Berlin and New York, 1973, pp. 389–394.

[P] H. Poincaré, *Sur les formes cubiques ternaires et quaternaires,* J. École Polytech. 51 (1882), 45–91.

[Sa1] R. A. Sarkisjan, *On the conjugacy problem,* Mat. Zametkie N1 and N6, 1979. (Russian)

[Sa2] ———, *Symposium on Group Theory in Tscherkasse,* Uspehi Mat. Nauk (to appear)

[Si] C. L. Siegel, *Zur Reduktionstheorie Quadratischer Formen,* Math. Soc. Japan, Tokyo, 1959.

[SW] R. G. Swan, *Generators and relations for certain special linear groups,* Advances in Math. 6 (1971), 1–77.

[T] A. Tarski, *A Decision method for elementary algebra and geometry,* 2nd. ed., University of California, 1951.

[Ta] M. A. Tayzlin, *On the isomorphism problem for commutative semigroups,* Mat. Sb. 93, No. 1, 1979.

FAKULTÄT FÜR MATHEMATIK,UNIVERSITÄT BIELEFELD, POSTFACH 8640, 4800 BIELEFELD 1, WEST GERMANY

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MANCHESTER INSTITUTE OF SCIENCE AND TECHNOLOGY, P. O. BOX 88, MANCHESTER M60 1QD, ENGLAND