BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 4, Number 1, 1981

DECIDABILITY AND UNDECIDABILITY THEOREMS FOR PAC-FIELDS

BY GREGORY CHERLIN, LOU VAN DEN DRIES AND ANGUS MACINTYRE[1]

A pseudo-algebraically closed field (PAC-field for short) is a field K such that every absolutely irreducible variety defined over K has K-rational points. In [Ax] Ax gave a decision method for the (elementary) theory of finite fields, the basis of which was his characterization of the infinite models of that theory as the perfect PAC-fields K with $G(K) \cong \hat{\mathbf{Z}}$. (Here and in the following we use the notations $G(K)$ for the absolute Galois group $\mathrm{Gal}(\widetilde{K}|K)$ of K, $\widetilde{K}$ = algebraic closure of K, $\hat{G}$ = profinite completion of the discrete group G.) In [J1] M. Jarden gave another natural source of PAC-fields: let $e \in \mathbf{N}$; then for almost all e-tuples $(\sigma_1, \ldots, \sigma_e) \in (\mathbf{Q})^e$—in the sense of the Haar measure on $G(\mathbf{Q})$—the fixed field $\mathrm{Fix}(\sigma_1, \ldots, \sigma_e) \subset \widetilde{\mathbf{Q}}$ is PAC, and e-free (where we call a field K e-free if $G(K) \cong \hat{F}_e$, F_e = free group on e generators). In 1975 Jarden and Kiehne classified e-free perfect PAC-fields up to elementary equivalence and derived the decidability of the theory of e-free perfect PAC-fields, cf. [J–K]. The next step was an extension of these results to a certain class of PAC-fields with infinitely generated absolute Galois group, cf. [J2]. We announce here solutions to the main questions provoked by this development.

THEOREM 1. *For each $e \in \mathbf{N}$, the theory of PAC-fields K with* $\mathrm{rk}(G(K)) \leqslant e$ *is decidable.* (*Where* $\mathrm{rk}(G)$ = *minimal number of* (*topological*) *generators of the profinite group* G.)

THEOREM 2. *The theory of PAC-fields is undecidable.*

While Theorem 2 puts a clear bound on decidability results for PAC-fields, Theorem 1 and its refinements extend the Jarden-Kiehne results considerably: for each $e \geqslant 1$ there are $2^{\aleph_0}$ pairwise nonisomorphic profinite groups G with $\mathrm{rk}(G) = e$ and $G = G(K)$ for some PAC-field K; $G = \hat{F}_e$ is the case treated by Jarden-Kiehne. In their proof a lemma on finite groups due to Gaschütz plays a crucial role. Our extension of the Jarden-Kiehne results has been made possible by finding a proof avoiding the Gaschütz lemma. Both theorems are deduced from (A) and (B) below.

Received by the editors August 14, 1980.
1980 *Mathematics Subject Classification*. Primary 03B25, 12L05; Secondary 20E18.
[1]The authors were partially supported by NSF grants.

(A) There exist "intelligible" *elementary invariants* classifying PAC-fields, which allow decision problems for those fields to be reduced to decision problems for projective profinite groups.

(B) The properties of the *projective cover* of a profinite group enable us to solve for each $e \in \mathbf{N}$ certain decision problems for projective profinite groups of rank $\leqslant e$ (leading to Theorem 1) and to code certain *undecidable* problems on graphs into decision problems for the class of all projective profinite groups (leading to Theorem 2).

OUTLINE OF (A). To avoid undue complications we assume all our fields to be of characteristic 0, and write $\mathrm{alg}(K)$ for the algebraic closure of $\mathbf{Q}$ within the field K. Let K be a PAC-field. Theorem 3.2 of **[J–K]** implies that $\mathrm{Th}(K)$ is determined by the isomorphism types of the field $\mathrm{alg}(K)$ and of the restriction map $G(K) \longrightarrow G(\mathrm{alg}(K))$ (considered as morphism in the category of profinite groups). Now the isomorphism type of $\mathrm{alg}(K)$ is determined by the set of polynomials in $\mathbf{Z}[X]$ with a root in K, so it is an elementary invariant. However, the isomorphism type of $G(K) \longrightarrow G(\mathrm{alg}(K))$ may change upon replacing K by a suitable elementary extension, so the isomorphism type of the map $G(K) \longrightarrow G(\mathrm{alg}(K))$ is in general not an elementary invariant. (It is, if $G(K)$ is finitely generated.) To overcome this obstacle we introduce a language to express the "coelementary" properties of profinite groups: associate to a profinite group G its inverse system $\mathrm{Inv}(G)$, consisting of the finite groups G/N and the natural maps $G/M \longrightarrow G/N$, M and N ranging over the open normal subgroups of G with $M \subset N$. Construe $\mathrm{Inv}(G)$ as a first-order structure, say with universe $\bigcup \{G/N \mid N$ an open normal subgroup of $G\}$, such that (continuous) epimorphisms $\phi\colon G \twoheadrightarrow H$ are in 1-1 correspondence with embeddings $\mathrm{Inv}(\phi)\colon \mathrm{Inv}(H) \rightarrowtail \mathrm{Inv}(G)$. Now, simply put $G \dashv \sigma$ ("G cosatisfies σ") iff $\mathrm{Inv}(G) \models \sigma$. Similarly, we define notions like cocardinality, coelementary equivalence, coultraproduct and cosaturatedness for profinite groups. (The last two require some care: an ultraproduct of "inverse systems of profinite groups" has to be "reduced" to become the inverse system associated to the coultraproduct of the corresponding profinite groups.) This comodel theory leads to the following properties:

(1) For each profinite group sentence σ we can construct a sentence $\mathrm{co}(\sigma)$ in the language of fields such that for each field K we have $G(K) \dashv \sigma$ iff $K \models \mathrm{co}(\sigma)$ (interpretability in fields).

(2) $G(\Pi K_i/D) =$ corresponding coultraproduct of the $G(K_i)$ (the K_i are fields).

(3) Nonprincipal coultraproducts of profinite groups are $\aleph_1$-cosaturated.

(4) If G_1 and G_2 are coelementarily equivalent cosaturated profinite groups of the same cocardinality, then every isomorphism of a coelementary

quotient of G_1 of smaller cocardinality onto a coelementary quotient of G_2 can be lifted to an isomorphism of G_1 onto G_2.

It is now routine to derive from these 4 properties that Th(K) for a PAC-field K is determined by the following two *elementary* invariants:

(I) The isomorphism type of alg(K).

(II) The coelementary equivalence type of $G(K)$ with distinguished quotient $G(\text{alg}(K))$.

Which of these invariants actually occur for PAC-fields K? Improving on **[Lu-v.d.D]**, one can show that $G(K)$ must be *projective* in the category of profinite groups, and that conversely for any projective profinite group P, any subfield F of $\tilde{\mathbf{Q}}$ and any epimorphism $\phi: P \twoheadrightarrow G(F)$, there exists a PAC-field K such that alg(K) $= F$ and the restriction map $G(K) \twoheadrightarrow G(F)$ is isomorphic to ϕ over $G(F)$.

OUTLINE OF (B). Using (A) and the fact that an f.g. profinite group G is determined by the class Im(G) of its finite homomorphic images, one routinely reduces the proof of Theorem 1 to the following decision problem: to decide, given $e \in \mathbf{N}$ and finite groups $F, F_1, \ldots, F_m$ whether there is a projective profinite group P with $\text{rk}(P) \leqslant e$, $F \in \text{Im}(P)$, $F_1, \ldots, F_m \notin \text{Im}(P)$. From the Proposition below it follows that such a decision method exists because one only has to consider for P the *projective cover* of F.

DEFINITION. A *minimal epi* is an epimorphism $\phi: G \longrightarrow H$ of profinite groups such that $\phi(G') \neq H$ for each proper closed subgroup G' of G. *A projective cover* of a profinite group G is a minimal epi $P \longrightarrow G$ with P projective.

PROPOSITION. *Each profinite group G has an up to isomorphism unique projective cover $P(G) \twoheadrightarrow G$. Moreover,* $\text{rk}(P(G)) = \text{rk}(G)$, *and* $\text{Im}(P(G)) =$ $\{F \mid F$ *is a finite group for which there exists a minimal epi* $F \longrightarrow K$ *for some* $K \in \text{Im}(G)\}$.

The proof of Theorem 2 is rather technical, but basically depends on the fact that for general G the structure Inv(G) is far from homogeneous. This failure of homogeneity can be lifted to projective profinite groups using projective covers.

Yu. L. Ersov informed us in May 1980 that he had obtained Theorem 2 and the basic properties of projective covers independently (abstract submitted to Doklady).

REFERENCES

[Ax] J. Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271.

[J1] M. Jarden, *Rational points on algebraic varieties over large number fields*, Bull. Amer. Math. Soc. **75** (1969), 603–606.

[J2] ———, *The elementary theory of ω-free Ax fields*, Invent. Math. **38** (1976), 187–206.

[J–K] M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank*, Invent. Math. **30** (1975), 275–294.

[Lu-v.d.D] A. Lubotzky and L. van den Dries, *Subgroup of free profinite groups and large subfields of* $\tilde{Q}$ (submitted).

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CONNECTICUT 06520

Current address (Gregory Cherlin): Department of Mathematics, Hebrew University, Jerusalem, Israel