PSEUDO ALGEBRAICALLY CLOSED FIELDS OVER RATIONAL FUNCTION FIELDS

MOSHE JARDEN[1] AND SAHARON SHELAH

ABSTRACT. The following theorem is proved: Let T be an uncountable set of algebraically independent elements over a field K_0. Then $K = K_0(T)$ is a Hilbertian field but the set of $\sigma \in G(K)$ for which $\tilde{K}(\sigma)$ is PAC is nonmeasurable.

Introduction. A field M is said to be *pseudo algebraically closed* (= PAC) if every nonempty absolutely irreducible variety V defined over M has an M-rational point.

If M is an algebraic extension of a field K and every absolutely irreducible polynomial $f \in K[X, Y]$, separable in Y, has infinitely many M-rational zeros, then M is PAC. This is a combination of Ax's application of "descent" [**1**] and the generic hyperplane intersection method as in Frey [**3**]. If $\sigma_1, \ldots, \sigma_e$ are e-elements of the absolute Galois group $G(K)$ of K, then $\tilde{K}(\sigma)$ denotes the fixed field in $\tilde{K}$ of $\sigma_1, \ldots, \sigma_e$. Here $\tilde{K}$ is the algebraic closure of K. We denote by μ the normalized Haar measure of $G(K)^e$. It is proved in [**6**, Lemma 2.4] that if K is a Hilbertian field, if $f \in K[X, Y]$ is an absolutely irreducible polynomial and if $A(f) = \{\sigma \in G(K)^e \mid f$ has a $\tilde{K}(\sigma)$-zero$\}$, then $\mu(A(f)) = 1$. If in addition K is countable, then there are only countably many f's and therefore the intersection of all the $A(f)$'s is also a set of measure 1. Thus the set $S_e(K) = \{\sigma \in G(K)^e \mid \tilde{K}(\sigma)$ is PAC$\}$ has measure 1.

This basic result, which is called the *Nullstellensatz* in [**6**], has been the cornerstone for several model theoretic investigations of the fields $\tilde{K}(\sigma)$ (cf. [**9**, **7** and **4**]).

If K is uncountable, then the above argument is not valid any more. It is our aim in this note to show that indeed the *Nullstellensatz* itself is not true in this case. More precisely, we prove

THEOREM. *Let T be an uncountable set of algebraically independent elements over a field K_0. Then $K = K_0(T)$ is a Hilbertian field but $S_e(K)$ is a nonmeasurable subset of $G(K)^e$ for every positive integer e.*

1. The Haar measure of a profinite group. Let G be a profinite group and consider the boolean algebra of open-closed sets in G. They are finite unions of left cosets xN, where N are open normal subgroups. The σ-algebra generated by the open-closed sets is denoted by $\mathfrak{B}_0$. Every open subset of G is a union of open-closed sets. We

Received by the editors February 5, 1982 and, in revised form, May 27, 1982.

1980 *Mathematics Subject Classification*. Primary 12F20.

Key words and phrases. PAC fields, Hilbertian fields, Haar measure.

[1]Partially supported by the Fund for Basic Research administered by the Israel Academy of Sciences and Humanities.

denote by $\mathfrak{B}$ the σ-algebra generated by the open sets. This is the *Borel*-algebra of G. Attached to $\mathfrak{B}$ is the Haar measure μ of G. We make the convention that $\mu(G) = 1$ ensuring the uniqueness of μ. The σ-algebra generated by $\mathfrak{B}_0$ (resp. $\mathfrak{B}$) and the subsets of zero sets of $\mathfrak{B}_0$ (resp. $\mathfrak{B}$) is denoted by $\overline{\mathfrak{B}}_0$ (resp. $\overline{\mathfrak{B}}$). For every $B \in \overline{\mathfrak{B}}_0$ there exist $A, C \in \mathfrak{B}_0$ such that $A \subseteq B \subseteq C$ and $\mu(C - A) = 0$. The sets in $\overline{\mathfrak{B}}$ are the *measurable* sets of G.

LEMMA 1.1. *In the above notation we have* $\overline{\mathfrak{B}}_0 = \overline{\mathfrak{B}}$.

PROOF. It suffices to show that if U is an open set, then there exist $A, B \in \mathfrak{B}_0$ such that $A \subseteq U \subseteq B$ and $\mu(B - A) = 0$.

We write U as a union $U = \bigcup_{i \in I} x_i M_i$, where the M_i are open normal subgroups and $x_i \in G$, and let

$$\alpha = \sup\left\{ \mu\Big(\bigcup_{i \in I'} x_i M_i \Big) \,\Big|\, I' \text{ is a countable subset of } I \right\}.$$

For every positive integer n there exists a countable subset J_n of I such that $\alpha - \mu(\bigcup_{i \in J_n} x_i M_i) < 1/n$. Then for $J = \bigcup_{n=1}^{\infty} J_n$, the set $A = \bigcup_{j \in J} x_j M_j \subseteq U$ belongs to $\mathfrak{B}_0$ and satisfies $\mu(A) = \alpha$.

Consider the closed normal subgroup $N = \bigcap_{j \in J} M_j$ of G. The corresponding quotient group G/N has a countable basis for its topology. Denote by π: $G \to G/N$ the canonical homomorphism. Then the sets $\pi(x_i M) = x_i M_i N/N$ are open in G/N and their union is πU. By a theorem of Lindelöf, I has a countable subset K such that $\pi U = \bigcup_{k \in K} \pi(x_k M_k)$. In addition $\pi^{-1}\pi A = A$ and $\pi(U - A) = \pi U - \pi A$, as one may easily check. Hence

$$(1) \qquad U - A \subseteq \pi^{-1}\pi(U - A) = \bigcup_{k \in K} (x_k M_k N - A).$$

The right-hand side of (1), which we denote by B_0, belongs to $\mathfrak{B}_0$. If we prove that $\mu(B_0) = 0$, then $B = A \cup B_0$ is a set of $\mathfrak{B}_0$ that contains U and satisfies $\mu(B - A) = 0$. Of course, it suffices to prove that $\mu(x_k M_k N - A) = 0$ for every $k \in K$.

Assume that there exists a $k \in K$ such that $\mu(x_k M_k N - A) > 0$ and let $n_1, \ldots, n_r$ be representatives of N modulo $N \cap M_k$. Then $x_k M_k N - A = \bigcup_{\rho=1}^{r} (x_k M_k n_\rho - A)$ and therefore, there exists a $1 \leqslant \rho \leqslant r$ such that $\mu(x_k M_k n_\rho - A) > 0$. Note that $A n_\rho = A$, since $n_\rho \in M_j$ for every $j \in J$. Hence, $\mu(x_k M_k - A) = \mu((x_k M_k - A) n_\rho) = \mu(x_k M_k n_\rho - A) > 0$. It follows that

$$\mu\Big(\bigcup_{j \in J} x_j M_j \cup x_k M_k \Big) = \mu(A) + \mu(x_k M - A) > \alpha,$$

which contradicts the definition of α. □

LEMMA 1.2. *In the above notation let S be a subset of G. Suppose that for every $B \in \mathfrak{B}_0$ there exists an epimorphism r: $G \to H$ such that* (a) $B = r^{-1} r B$ *and* (b) $\mu_H(rS) = 1$. *Then $G - S$ contains no subset of a positive measure. If also $G - S$ has the above property, then S is not measurable.*

PROOF. Assume that $G - S$ contains a set $\bar{B} \in \bar{\mathfrak{B}}$. By Lemma 1.1 there exists a set $B \in \mathfrak{B}_0$ such that $B \subseteq \bar{B}$ and $\mu(\bar{B} - B) = 0$. Let $r\colon G \to H$ be an epimorphism such that (a) and (b) hold. Then $\mu_H(r(G - B)) = 1$ and $G - B = r^{-1}r(G - B)$. It follows that $\mu(G - B) = 1$, hence $\mu(\bar{B}) = 0$. □

2. Rational function fields of one variable. Let t be a transcendental element over an infinite field K and let $E = K(t)$. Then E is a Hilbertian field. If E is also countable, then, as noted in the introduction, $S_e(E) = \{\sigma \in G(K)^e \mid \tilde{E}(\sigma) \text{ is PAC}\}$ is a set of measure 1 for every $e \geqslant 1$. In the noncountable case we are able to prove only the following weaker result.

PROPOSITION 2.1. *If K is an uncountable field, then the complement of $S_e(E)$ in $G(E)^e$ contains no subsets of positive measure.*

The first step in the proof is a generalization of a basic result for polynomials in several variables. We use here both $\#A$ and $|A|$ to denote the cardinality of a set A.

LEMMA 2.2. *Let A be an infinite subset of a field K. If $F \subseteq K[X_1,\dots,X_n]$ is a set of nonzero polynomials and $|F| < |A|$, then $\#\{(a_1,\dots,a_n) \in A^n \mid f(a_1,\dots,a_n) \neq 0$ for every $f \in F\} = |A|$.*

PROOF. Our assertion is true for $n = 1$, since every polynomial $f \in F$ has only finitely many zeros. Suppose, by induction, that the assertion is true for $n - 1$, where $n \geqslant 2$. Then, since every $f \in F$ has a nonzero coefficient $g \in K[X_1,\dots,X_{n-1}]$, we have $\#\{(a_1,\dots,a_{n-1}) \in A^{n-1} \mid f(a_1,\dots,a_{n-1}, X_n) \neq 0$ for every $f \in F\} = |A|$. For every $(a_1,\dots,a_{n-1})$ in the above set there exists, by the case $n = 1$, an element $a_n \in A$ such that $f(a_1,\dots,a_n) \neq 0$ for every $f \in F$. Therefore, our assertion is also true for n. □

COROLLARY 2.3. *If $\{U_i \mid i \in I\}$ is a family of nonempty Zariski K-open sets in $\mathbf{A}^n$ and $|I| < |A|$, then $|A^n \cap \bigcap_{i\in I} U_i| = |A|$.*

PROOF. Every U_i is defined by finitely many polynomial inequalities. □

We define the *rank* of an infinite algebraic extension as the cardinality of the family of all finite subextensions. The *rank* of a finite algebraic extension is merely said to be *finite*.

A finite separable extension has only finitely many subextensions. Hence, if F is the compositum of m finite separable extensions of a field E and m is an infinite cardinal number, then $\operatorname{rank}(F/E) = m$.

LEMMA 2.4. *Let F be a separable extension of E with* $\operatorname{rank}(F/E) < |K|$ *and let $f \in E[X, Y]$ be an irreducible polynomial in $F[X, Y]$, separable in Y. Then there exists an $x \in E$ such that $f(x, y)$ is separable irreducible in $F[Y]$.*

PROOF. Let $\{E_i \mid i \in I\}$ be the family of all finite separable extensions of E which are contained in F. By assumption $|I| < |K|$. By a theorem of Inaba [**5**, §4], there exists for every $i \in I$ a nonempty Zariski K-open set $U_i \subseteq \mathbf{A}^2$ such that if $(a, b) \in U_i(K)$, then $f(a + bt, y)$ is separable irreducible in $E_i[Y]$. The intersection

$\bigcap_{i \in I} U_i(K)$ is, by Corollary 2.3, not empty. If (a, b) lies in this intersection and $x = a + bt$, then $f(x, Y)$ is separable irreducible over every E_i, hence also over F. □

LEMMA 2.5. *Let N be a Galois extension of E with* $\mathrm{rank}(N/E) < |K|$. *Then every $\sigma_1, \ldots, \sigma_e \in \mathcal{G}(N/E)$ can be extended to elements $\tau_1, \ldots, \tau_e \in G(E)$, respectively, such that $\tilde{E}(\tau)$ is a PAC field.*

PROOF. We well-order the absolutely irreducible polynomials of $K[X, Y]$ which are separable in Y in a transfinite sequence $\{f_\alpha \mid \alpha < m\}$, where $m = |K|$, such that each of the polynomials appears $\aleph_0$ times in the sequence. For every $\alpha < m$ we define a finite separable extension E_α of E in which f_α has a zero and such that the set of fields $\{N\} \cup \{E_\alpha \mid \alpha < m\}$ is linearly disjoint over E.

Indeed let $\beta < m$ and assume, by transfinite induction, that E_α has been defined for every $\alpha < \beta$. Let F be the compositum of N and all the fields E_α with $\alpha < \beta$. Then F is a separable extension of E with $\mathrm{rank}(F/E) < m$. By Lemma 2.4 there exists an $x \in E$ such that $f(x, y)$ is separable irreducible in $F[Y]$. If $y \in \tilde{E}$ satisfies $f(x, y) = 0$, then we may define $E_\beta = E(y)$ and E_β is linearly disjoint from F over E.

The compositum M of all the fields E_α is a separable algebraic extension of E which is linearly disjoint from N and which is PAC. The automorphisms $\sigma_1, \ldots, \sigma_e$ may be extended to automorphisms $\tau_1, \ldots, \tau_e \in G(M)$. Their fixed field $\tilde{K}(\tau)$ is an algebraic extension of M and hence is a PAC field itself. □

PROOF OF PROPOSITION 2.1. We follow the pattern of Lemma 1.2 and note first that every open-closed set of $G(E)^e$ is determined by a finite Galois extension of E. It follows that if B is a set belonging to the σ-algebra $\mathfrak{B}_0$ of $G(E)^e$ generated by the open-closed sets, then there exists a Galois extension N of E with $\mathrm{rank}(N/E) \leq \aleph_0$ such that $r^{-1}rB = B$, where $r\colon G(E)^e \to \mathcal{G}(N/E)^e$ is the restriction map.

By Lemma 2.5, $rS_e = \mathcal{G}(N/E)^e$. Hence, by Lemma 2.1, $G(E)^e - S_e(E)$ contains no sets of a positive measure.

3. Rational function fields of many variables. There is one case where we have enough information about the set $G(E)^e - S_e(E)$, which allows us to reach a decisive conclusion about the nonmeasurability of the set $S_e(E)$. This is the case where K itself is a rational function field of uncountably many variables over a field K_0.

LEMMA 3.1. *Let T be a nonempty set of algebraically independent elements over a field L and let $M = L(T)$. Then every e elements $\sigma_1, \ldots, \sigma_e$ of $G(L)$ can be extended to e elements $\rho_1, \ldots, \rho_e$ of $G(M)$ such that $\tilde{M}(\rho)$ is not a PAC field.*

PROOF. We single out an element $t \in T$ and denote $L' = L(T - \{t\})$. Then $\sigma_1, \ldots, \sigma_e$ can be extended to elements $\sigma_1', \ldots, \sigma_e'$ of $G(L')$. We may therefore assume without loss that T consists of one element t.

Consider first the case where one of the σ_i's is not the identity automorphism and note that L is algebraically closed in the field $F = L((t))$ of formal power series in t. Therefore, $\sigma_1, \ldots, \sigma_e$ may be extended to elements $\hat{\rho}_1, \ldots, \hat{\rho}_e$ of $G(F)$. The restrictions

$\rho_1, \ldots, \rho_e$ of $\hat{\rho}_1, \ldots, \hat{\rho}_e$ to $\tilde{M}$ are elements of $G(M)$ that extend $\sigma_1, \ldots, \sigma_e$ and $\tilde{M}(\rho)$ is not a PAC field. Indeed, $\tilde{M}(\rho) = \tilde{M} \cap \tilde{F}(\hat{\rho})$ and $\tilde{F}(\hat{\rho})$ is a Henselian field with respect to a real-valued valuation defined by the specialization $t \to 0$. Therefore, $\tilde{M}(\rho)$ itself is Henselian (cf. Ax [**2**, Proposition 12]) and it is not separably closed. Theorem 2 of Frey [**3**] implies that $\tilde{M}(\rho)$ is not a PAC field.

If $\sigma_1 = \cdots = \sigma_e = 1$, then noting that the separable closure M_s of M is not contained in $L_s((t))$, we may choose $\hat{\rho}_1, \ldots, \hat{\rho}_e$ in $G(L_s((t)))$ that do not fix M_s. Then we proceed as before. □

We are now in a position to prove our main result.

THEOREM 3.2. *Let T be an uncountable set of algebraically independent elements over a field K_0 and let $E = K_0(T)$. Then for every positive integer e, both $S_e(E)$ and $G(E)^e - S_e(E)$ contain no sets of positive measure. In particular $S_e(E)$ is nonmeasurable.*

PROOF. By Proposition 2.1 we have only to prove that $S_e(E)$ contains no sets of positive measure. Indeed, if $B \subseteq G(E)^e$ is open-closed, then there exists a finite subset T_0 of T and there exists a finite Galois extension F_0 of $K_0(T_0)$ such that B is the listing to $G(E)^e$ of a certain subset of $\mathcal{G}(F_0/K_0(T_0))^e$. It follows that if $B \in \mathfrak{B}_0$, then there exists a countable subset T_1 of T such that with $L = K_0(T_1)$ and r: $G(E)^e \to G(L)^e$ the restriction map, we have $B = r^{-1}rB$.

Note now that $E = L(T - T_1)$ and that $T - T_1$ is a nonempty set of algebraically independent elements over L. Hence, by Lemma 3.1, $r(G(E)^e - S_e(E)) = G(L)^e$. It follows by Lemma 1.2, that $S_e(E)$ contains no sets of positive measure. □

COROLLARY 3.3. *If F is a finite extension of E, then $S_e(F)$ is a nonmeasurable set.*

PROOF. If $S_e(F)$ were measurable, then either $S_e(F)$ or its complement would have a positive measure in $G(E)^e$, a contradiction. □

Note that there exist Hilbertian fields E_0 which are PAC (see [**8**, Theorem 3.3]). Every nonprincipal ultrapower E of E_0 is an uncountable Hilbertian PAC field. As already noted before every algebraic extension of E is again a PAC field. Hence, $S_e(E) = G(E)^e$ for every positive integer e. Thus Theorem 3.2 cannot be extended to arbitrarily uncountable Hilbertian fields.

The most interesting case which remains open is that of $E = \mathbf{C}(t)$.

PROBLEM. Are the sets $S_e((t))$ measurable?

Note that in case of a positive answer, we have $\mu(S_e(\mathbf{C}(t))) = 1$, by Proposition 2.1.

REFERENCES

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

2. ———, *A mathematical approach to some problems in number theory*, 1969 Number Theory Institute, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 161–190.

3. G. Frey, *Pseudo-algebraically closed fields with nonarchimedean real valuations*, J. Algebra **26** (1973), 202–207.

4. M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, Advances in Math. (to appear).

5. E. Inaba, *Über den Hilbertschen Irreduzibilitässatz*, Japan. J. Math. **19** (1944), 1–25.

6. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164 (1972)**, 67–97.

7. ______, *The elementary theory of ω-free ak-fields*, Invent. Math. **38** (1976), 187–206.

8. ______, *An analogue of Čebotarev density theorem for fields of finite corank*, J. Math. Kyoto Univ. **20** (1980), 141–147.

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

School of Mathematical Sciences, Tel-Aviv University, Ramat-Aviv, Tel-Aviv, Israel

Institute of Mathematics, The Hebrew University, Jerusalem, Isarel