PAC FIELDS OVER FINITELY GENERATED FIELDS*

by

LIOR BARY-SOROKER AND MOSHE JARDEN

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

barylior@post.tau.ac.il *and* *jarden@post.tau.ac.il*

MR Classification: 12E30

Directory: \Jarden\Diary\BSJ

10 June, 2006

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

Introduction

A central concept in Field Arithmetic is "pseudo algebraically closed (abbreviated **PAC**) field". If K is a countable Hilbertian field, then $K_s(\boldsymbol{\sigma})$ is PAC for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ [FrJ, Thm. 18.6.1]. Moreover, if K is the quotient field of a countable Hilbertian ring R (e.g. $R = \mathbb{Z}$), then $K_s(\boldsymbol{\sigma})$ is PAC over R [JaR, Prop. 3.1], hence also over K.

Here K_s is a fixed separable closure of K and $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ is the absolute Galois group of K. This group is equipped with a Haar measure and the close "almost all" means "for all but a set of measure zero". If $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, then $K_s(\boldsymbol{\sigma})$ denotes the fixed field in K_s of $\sigma_1, \ldots, \sigma_e$.

Recall that a field M is said to be **PAC** if every nonempty absolutely irreducible variety V defined over M has an M-rational point. One says that M is **PAC over** a subring R if for every absolutely irreducible variety V defined over M of dimension $r \geq 0$ and every dominating separable rational map φ: $V \to \mathbb{A}^r_M$ there exists an $\mathbf{a} \in V(M)$ with $\varphi(\mathbf{a}) \in R^r$.

When K is a number field, the stronger property of the fields $\tilde{K}(\boldsymbol{\sigma})$ (namely, being PAC over the ring of integers O of K) has far reaching arithmetical consequences (here $\tilde{K}$ is the algebraic closure of K). For example, $\tilde{O}(\boldsymbol{\sigma})$ (= the integral closure of O in $\tilde{K}(\boldsymbol{\sigma})$) satisfies Rumely's local-global principle [JaR2, special case of Cor. 1.9]: If V is an absolutely irreducible variety defined over $\tilde{K}(\boldsymbol{\sigma})$ with $V(\tilde{O}) \neq \emptyset$, then V has an $\tilde{O}(\boldsymbol{\sigma})$-rational point. Here $\tilde{K}$ denotes the algebraic closure of K and $\tilde{K}(\boldsymbol{\sigma})$ is, as before, the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{K}$.

The article [JaR1] gives several distinguished Galois extensions of $\mathbb{Q}$ which are not PAC over any number field and notes that no Galois extension of a number field K (except $\tilde{K}$) is known to be PAC over K. This lack of knowledge has come to an end in [Jar], where Neukirch's characterization of the p-adically closed fields among all algebraic extensions of $\mathbb{Q}$ is used in order to prove the following theorem:

Theorem A: *No number field K has a PAC Galois extension M (except $\tilde{K}$) such that M is PAC over K.*

The goal of the present note is to generalize Theorem A to arbitrary finitely generated fields:

Theorem B: *Let K be a finitely generated field (over its prime field). Then no Galois extension of K (except K_s) is pseudo algebraically closed over K.*

The proof of Theorem B is based on Lemma 2 of [JaR1] which combines Faltings' theorem in characteristic 0 and the Grauert-Manin theorem in positive characteristic. The latter theorems are much deeper that the result of Neukirch use in the proof of Theorem A.

1. Accessible Fields

The proof of Theorem B actually gives a stronger theorem: No accessible extension (see definition prior to Theorem 4) of a finitely generated field K except K_s is PAC over K. Technical tools in the proof are the "field crossing argument" and "ring covers":

An extension S/R of integral domains with an extension F/E of quotient fields is said to be a **cover of rings** if $S = R[z]$ and $\mathrm{discr}(\mathrm{irr}(z, E)) \in R^\times$ [FrJ, Definition 6.1.3]. We say that S/R is a **Galois cover of rings** if S/R is a cover of rings and F/E is a Galois extension of fields. Every epimorphism φ_0 of R onto a field $\bar{E}$ extends to an epimorphism φ of S onto a Galois extension $\bar{F}$ of $\bar{E}$ and φ induces an isomorphism of the **decomposition group** $D_\varphi = \{\sigma \in \mathrm{Gal}(F/E) \mid \sigma(\mathrm{Ker}(\varphi)) = \mathrm{Ker}(\varphi)\}$ onto $\mathrm{Gal}(\bar{F}/\bar{E})$ [FrJ, Lemma 6.1.4]. In particular, $\mathrm{Gal}(F/E) \cong \mathrm{Gal}(\bar{F}/\bar{E})$ if and only if $[F : E] = [\bar{F} : \bar{E}]$.

As in the proof of [FrJ, Lemma 24.1.1], the field crossing argument is the basic ingredient of the construction included in the proof of the following lemma.

LEMMA 1: *Let K be a field, M an extension of K, n a positive integer, N a Galois extension of M with Galois group A of order at most n, and t an indeterminate. Then there exist fields $D, F_0, F, \hat{F}$ as in diagram (1) such that the following holds:*

(a) *F_0 is regular over K, F and D are regular over M, and $\hat{F}$ is regular over N.*

(b) *$FD = DN = \hat{F}$.*

(c) *$F_0/K(t)$, $F/M(t)$, and $\hat{F}/N(t)$ are Galois extensions with Galois groups isomorphic to S_n.*

(1)
$$\begin{tikzcd}[arrows=dash]
F_0 \arrow[r] \arrow[d, "S_n"'] & F \arrow[r, "A"] \arrow[d, "S_n"'] & \hat{F} \arrow[d, "S_n"] \\
K(t) \arrow[r] \arrow[d] & M(t) \arrow[r] \arrow[d] \arrow[ur, "D"] & N(t) \arrow[d] \\
K \arrow[r] & M \arrow[r, "A"] & N
\end{tikzcd}$$

Proof: The field $K(t)$ has a Galois extension F_0 with Galois group S_n such that F_0 is regular over K [FrJ, Example 16.2.5 and Proposition 16.2.8]. In particular, F_0 is linearly disjoint from N and M over K. Set $F = F_0M$ and $\hat{F} = FN$. By [FrJ, Cor. 2.6.8], both

F/M and $\hat{F}/N$ are regular extensions. Moreover, both $F/M(t)$ and $\hat{F}/N(t)$ are Galois extensions with Galois groups isomorphic to S_n and $\hat{F}/F$ is a Galois extension. We identify $\mathrm{Gal}(\hat{F}/F)$ with A via restriction. Finally, $\hat{F}/M(t)$ is a Galois extension and $\mathrm{Gal}(\hat{F}/M(t)) = \mathrm{Gal}(\hat{F}/F)) \times \mathrm{Gal}(\hat{F}/N(t))$.

Multiplication from the right embeds A into S_m, where $m = |A|$. Since $m \le n$, there exists an embedding $\alpha\colon A \to \mathrm{Gal}(\hat{F}/N(t))$. Consider the diagonal subgroup $\Delta = \{(\sigma, \alpha(\sigma)) \in \mathrm{Gal}(\hat{F}/M(t)) \mid \sigma \in A\}$ of $\mathrm{Gal}(\hat{F}/M(t))$. Then $\Delta \cap \mathrm{Gal}(\hat{F}/F) = \Delta \cap \mathrm{Gal}(\hat{F}/N(t) = 1$. By Galois theory, $FD = DN(t) = \hat{F}$, so $DN = \hat{F}$. Restriction to N maps $\mathrm{Gal}(\hat{F}/D)$ onto $\mathrm{Gal}(N/M)$, hence $D \cap N = M$. Since $\hat{F}$ is regular over N, it follows that D is regular over M. ∎

The main ingredient in the proof of Lemma 3 is the following result of Faltings' theorem in characteristic 0 and the Grauert-Manin theorem in positive characteristic.

Lemma 2 ([JaR1, Prop. 5.4]): *Let K be an infinite finitely generated field, $f \in K[T, Y]$ an absolutely irreducible polynomial which is separable in Y, $g \in K[T, Y]$ an irreducible polynomial which is separable in Y, and $0 \ne r \in K[T]$. Then there exist a purely inseparable extension K' of K, a nonconstant rational function $q \in K'(T)$, and a finite subset B of K' such that $f(q(T), Y)$ is absolutely irreducible, $g(q(a), Y)$ is irreducible in $K'[Y]$, and $r(q(a)) \ne 0$ for each $a \in K' \smallsetminus B$.*

Lemma 3: *Let K be an infinite finitely generated field, M a separable PAC extension of K, n a positive integer, and N a Galois extension of M of degree at most n with Galois group A. Then there exist finite extensions $K' \subseteq L$ of K such that with $M' = K'M$ and $N' = K'N$ the following holds:*

(a) *$N' = LM'$ and $\mathrm{Gal}(N'/M') \cong A$.*

(b) *L/K' is a Galois extension and $\mathrm{Gal}(L/K') \cong S_n$.*

$$\begin{tikzcd}
L \arrow[rr, dash] \arrow[d, dash, "S_n"'] & & N' \arrow[dd, dash] \\
K' \arrow[r, dash] \arrow[d, dash] & M' \arrow[ur, dash, "A"] \arrow[d, dash] & \\
K \arrow[r, dash] & M \arrow[r, dash] & N
\end{tikzcd}$$

Proof: We break the proof into three parts.

PART A: *Transcendental extensions.* First we apply Lemma 1 to construct Diagram (1). Then we choose $x \in F_0$ integral over $K[t]$ with $F_0 = K(t, x)$ and let $g \in K[T, X]$ be a monic polynomial in X such that $g(t, X) = \mathrm{irr}(x, K(t))$. In particular, $r_1(t) = \mathrm{discr}(g(t, X)) \in K[t]$ and $r_1(t) \neq 0$. Finally we choose $z \in D$ integral over $M[t]$ with $D = M(t, z)$ and let $f \in K[T, X]$ be a monic polynomial such that $f(t, X) = \mathrm{irr}(z, M(t))$. Then $r_2(t) = \mathrm{discr}(f(t, X)) \in M[t]$ and $r_2(t) \neq 0$. Since D is regular over M, the polynomial $f(T, X)$ is absolutely irreducible [FrJ, Cor. 10.2.2(b)]. Let $r(t) = r_1(t)r_2(t)$.

Replacing K by a finite extension in M, we may assume that K contains all of the coefficients of $f(t, X)$, $g(t, X)$, and $r(t)$. Set $R_0 = K[t, r(t)^{-1}]$, $R = R_0M = M[t, r(t)^{-1}]$, $S_0 = R_0[x]$, $S = S_0M = R[x]$, and $V = R[z]$. Then S_0/R_0, S/R, and V/R are ring covers and $F_0/K(t)$, $F/M(t)$, and $D/M(t)$ are the corresponding field covers.

$$\begin{tikzcd}
S_0 \arrow[r, dash] \arrow[d, dash] & S \arrow[d, dash] & V \\
R_0 \arrow[r, dash] \arrow[d, dash] & R \arrow[d, dash] \arrow[ur, dash] & \\
K \arrow[r, dash] & M \arrow[r, dash] & N
\end{tikzcd}$$

PART B: *Specialization.* Lemma 2 gives a finite purely inseparable extension K' of K, a nonconstant rational function $q \in K'(T)$, and a finite subset B of K' such that $f(q(T), X)$ is absolutely irreducible and $g(q(a), X)$ is irreducible in $K'[X]$ and $r(q(a)) \neq 0$ for each $a \in K' \smallsetminus B$.

We put $'$ on rings and fields to denote their composition with K'. For example $M' = K'M$. Since $\hat{F}/K$ is separable and K'/K is purely inseparable, these extensions are linearly disjoint. In follows that (a), (b), and (c) of Lemma 1 holds for the tagged rings and fields. In particular, S_0'/R_0' and S'/R' are Galois covers of rings and $\mathrm{Gal}(N'/M') \cong A$. By [JaR, Cor. 2.5], M' is PAC over K', hence there exists $(a, c) \in K' \times M'$ such that $a \notin B$ and $f(b, c) = 0$ with $b = q(a)$. By the choice of B, $g(b, X)$ is irreducible in $K'[X]$ and $r(b) \neq 0$.

The tag notation also gives $R_0' = K'[t, r(t)^{-1}]$ and $V' = M'[t, z, r(t)^{-1}]$. Since V' is integral over R' we may extend the specialization $(t, z) \to (b, c)$ to an M'-epimorphism ψ: $V' \to M'$ satisfying $\psi(R_0') = K'$.

Part C: *Finite extensions of K'.* Let $\hat{S}'$ be the integral closure of R' in $\hat{F}'$. Then $S' = \hat{S}' \cap F'$. By [FrJ, Lemma 2.5.10], $\hat{S}' = V' \otimes_{M'} N'$. Furthermore, D' is linearly disjoint from F' over $F' \cap D'$, hence by the same lemma, $\hat{S}' = S'V'$.

$$\begin{tikzcd}
S_0' = R_0'[x] \arrow[r, dash] \arrow[d, dash] & S' \arrow[r, dash] \arrow[d, dash] & \hat{S}' \arrow[d, dash] \\
R_0' = K'[t, r(t)^{-1}] \arrow[r, dash] \arrow[d, dash] & R' = M'[t, r(t)^{-1}] \arrow[r, dash] \arrow[d, dash] \arrow[ur, dash, "V'=R'[z]" description] & R'N' \arrow[d, dash] \\
K' \arrow[r, dash] & M' \arrow[r, dash] & N'
\end{tikzcd}$$

Setting $\psi(vn) = \psi(v)n$ for each $v' \in V'$ and $n \in N'$ extends ψ to an N'-epimorphism ψ: $\hat{S}' \to N'$. In particular, $M' \subseteq \psi(S')$, hence $N' = \psi(\hat{S}') = \psi(S'V') = \psi(S')M' = \psi(S')$.

Let $L = K'(\psi(x))$. Then $\psi(S_0') = \psi(R_0'[x]) = K'(\psi(x)) = L$. Since $\psi(x)$ is a root of $g(b, X)$ and $g(b, X)$ is irreducible over K', we have

$$[L : K'] = \deg(g(b, X)) = \deg(g(t, X)) = [F_0 : K(t)] = n!.$$

Hence, $\mathrm{Gal}(L/K') \cong \mathrm{Gal}(F_0/K(t)) \cong S_n$. Finally, $N' = \psi(S') = \psi(S_0'M') = \psi(S_0')M' = LM'$, as desired. ∎

We say that a separable algebraic extension M of a field K is **accessible** if there exists a sequence of fields

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq M$$

such that K_{i+1}/K_i is Galois for each i and $\bigcup_{i=0}^{\infty} K_i = M$. In particular, every Galois extension of K is accessible. If L/K is a finite Galois extension, then the sequence $\mathrm{Gal}(L/L \cap K_i)$, $i = 0, 1, 2, \ldots$, of subgroups of $\mathrm{Gal}(L/K)$ is finite, so there is a positive integer m such that

$$\mathrm{Gal}(L/L \cap M) = \mathrm{Gal}(L/L \cap K_m) \triangleleft \mathrm{Gal}(L/L \cap K_{m-1}) \triangleleft \cdots \triangleleft \mathrm{Gal}(L/L \cap K_1) \triangleleft \mathrm{Gal}(L/K).$$

In other words, $\mathrm{Gal}(L/L \cap M)$ is a **subnormal subgroup** of $\mathrm{Gal}(L/K)$.

THEOREM 4: *Let K be a finitely generated field, M_0 an accessible extension of K, and M a separable algebraic extension of M. If M is PAC over K and $M \neq K_s$, then, as a supernatural number, $[M : M_0] = \prod_p p^\infty$.*

Proof: By [JaR1, Remark 1.2(b)], K is an infinite field. Choose a proper finite Galois extension N of M with Galois group A and let $n \geq \max(5, |A|)$. Let K' and L be fields satisfying Conditions (a) and (b) of Lemma 3. Set $M_0' = K'M_0$, $M' = K'M$, $L_0 = L \cap M_0'$, and $L_1 = L \cap M'$. Then M_0' is an accessible extension of K', hence $\mathrm{Gal}(L/L_0)$ is a subnormal subgroup of $\mathrm{Gal}(L/K') \cong S_n$. Since $n \geq 5$, the sequence $1 \triangleleft A_n \triangleleft S_n$ is the only composition series of S_n [Hup, p. 173, Thm. 5.1]. Therefore $\mathrm{Gal}(L/L_0)$ is either 1 or A_n or S_n. By Condition (a) of Lemma 3,

$$\mathrm{Gal}(L/L_0) \geq \mathrm{Gal}(L/L_1) \cong \mathrm{Gal}(N'/M') \cong A \neq 1.$$

Therefore, $A_n \leq \mathrm{Gal}(L/L_0)$, so $\frac{(n-1)!}{2}$ divides $[L_1 : L_0] = [L_1 M_0' : M_0']$.

$$\begin{tikzcd}
 & L \arrow[rrr, dash] \arrow[d, dash, "A"'] & & & N' \arrow[dl, dash, "A"'] \arrow[ddd, dash] \\
 & L_1 \arrow[r, dash] \arrow[d, dash] & L_1 M_0' \arrow[r, dash] \arrow[d, dash] & M' \arrow[dd, dash] & \\
K' \arrow[r, dash] \arrow[d, dash] & L_0 \arrow[r, dash] & M_0' \arrow[d, dash] & & \\
K \arrow[rr, dash] & & M_0 \arrow[r, dash] & M \arrow[r, dash] & N
\end{tikzcd}$$

Since n is arbitrary large and $L_1 M_0' \subseteq M'$, we have $[M' : M_0'] = \prod_p p^\infty$. Since K' is a finite extension, $[M : M_0] = \prod_p p^\infty$. ∎

The main result of this note is a special case of Theorem 4:

COROLLARY 5: *Let K be a finitely generated field and let N be a PAC extension of K, $N \neq K_s$. Then N is not an accessible extension of K. In particular N is not Galois over K.*

Corollary 6: *Let K be an infinite finitely generated field and let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the extension $K_s(\boldsymbol{\sigma})$ of K is inaccessible.*

Proof: By [JaR1, Prop. 3.1], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_s(\boldsymbol{\sigma})$ is PAC over K. Hence, by Theorem 4, $K_s(\boldsymbol{\sigma})$ is inaccessible over K. ∎

Conjecture 7: *Let K be a finitely generated field and M an algebraic extension of K. If M is PAC over K, then $\mathrm{Gal}(M)$ is finitely generated.*

References

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[Hup] B. Huppert, *Endliche Gruppen I,* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer, Berlin, 1967.

[JaR1] M. Jarden and A. Razon, *Pseudo algebraically closed fields over rings,* Israel Journal of Mathematics **86** (1994), 25–59.

[JaR2] M. Jarden and A. Razon, *Rumely's local global principle for algebraic PSC fields over rings,* Transactions of AMS **350** (1998), 55-85.

[Jar] M. Jarden, *PAC fields over number fields,* Journal de Theorie des Nombres de Bordeaux