Moshe JARDEN

PAC fields over number fields

PAC fields over number fields

par Moshe JARDEN

RÉSUMÉ. Soient K un corps de nombres et N une extension ga-
loisienne de $\mathbb{Q}$ qui n'est pas algébriquement close. Alors N n'est
pas PAC sur K.

ABSTRACT. We prove that if K is a number field and N is a
Galois extension of $\mathbb{Q}$ which is not algebraically closed, then N is
not PAC over K.

1. Introduction

A central concept in Field Arithmetic is "pseudo algebraically closed
(abbreviated **PAC**) field". Since our major result in this note concerns
number fields, we focus our attention on fields of characteristic 0. If K is a
countable Hilbertian field, then $\tilde{K}(\boldsymbol{\sigma})$ is PAC for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$
[1, Thm. 18.6.1]. Aharon Razon observed that the proof of that theorem
yields that the fields $\tilde{K}(\boldsymbol{\sigma})$ are even "PAC over K". Moreover, if K is the
quotient field of a countable Hilbertian ring R (e.g. $R = \mathbb{Z}$ and $K = \mathbb{Q}$),
then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $\tilde{K}(\boldsymbol{\sigma})$ is PAC over R [4, Prop. 3.1].

Here $\tilde{K}$ denotes the algebraic closure of K and $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/K)$
is its absolute Galois group. 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 $\tilde{K}(\boldsymbol{\sigma})$ is the fixed field in $\tilde{K}$ of $\sigma_1, \ldots, \sigma_e$.

Recall that a field M is said to be **PAC** if every nonempty absolutely
irreducible variety V over M has an M-rational point. One says that M
is **PAC over** a subring R if for every absolutely irreducible variety V
over M of dimension $r \geq 0$ and every dominating separable rational map
$\varphi \colon V \to \mathbb{A}^r_M$ there exists $\mathbf{a} \in V(M)$ 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 arith-
metical consequences. For example, $\tilde{O}(\boldsymbol{\sigma})$ (= the integral closure of O in
$\tilde{K}(\boldsymbol{\sigma})$) satisfies Rumely's local-global principle [5, special case of Cor. 1.9]:
If V is an absolutely irreducible variety over $\tilde{K}(\boldsymbol{\sigma})$ with $V(\tilde{O}) \neq \emptyset$, then V
has an $\tilde{O}(\boldsymbol{\sigma})$-rational point. Here $\tilde{O}$ is the integral closure of O in $\tilde{K}$.

For an arbitrary countable Hilbertian field K of characteristic 0 we further denote the maximal Galois extension of K in $\tilde{K}(\boldsymbol{\sigma})$ by $\tilde{K}[\boldsymbol{\sigma}]$. We know that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $\tilde{K}[\boldsymbol{\sigma}]$ is PAC [1, Thm. 18.9.3]. However, at the time we wrote [4], we did not know if $\tilde{K}[\boldsymbol{\sigma}]$ is PAC over K, so much the more we did not know if $\tilde{K}[\boldsymbol{\sigma}]$ is PAC over O when K is a number field. Thus, we did not know if $\tilde{O}[\boldsymbol{\sigma}]$ (= the integral closure of O in $\tilde{K}[\boldsymbol{\sigma}]$) satisfies Rumely's local global principle. We did not even know of any Galois extension of $\mathbb{Q}$ other than $\tilde{\mathbb{Q}}$ which is PAC over $\mathbb{Q}$. We could only give a few examples of distinguished Galois extensions of $\mathbb{Q}$ which are not PAC over $\mathbb{Q}$: The maximal solvable extension $\mathbb{Q}_{\mathrm{solv}}$ of $\mathbb{Q}$, the compositum $\mathbb{Q}_{\mathrm{symm}}$ of all symmetric extensions of $\mathbb{Q}$, and $\mathbb{Q}_{\mathrm{tr}}(\sqrt{-1})$ ($\mathbb{Q}_{\mathrm{tr}}$ is the maximal totally real extension of $\mathbb{Q}$). The proof of the second statement relies, among others, on Faltings' theorem about the finiteness of K-rational points of curves of genus at least 2. Note that $\mathbb{Q}_{\mathrm{symm}}$ is PAC [1, Thm. 18.10.3 combined with Cor. 11.2.5] and $\mathbb{Q}_{\mathrm{tr}}[\sqrt{-1}]$ is PAC [2, Remark 7.10(b)]. However, it is a major problem of Field Arithmetic whether $\mathbb{Q}_{\mathrm{solv}}$ is PAC [1, Prob. 11.5.8]. Thus, it is not known whether every absolutely irreducible equation $f(x, y) = 0$ with coefficients in $\mathbb{Q}$ can be solved by radicals.

The goal of the present note is to prove that the above examples are only special cases of a general result:

Main Theorem. *No number field K has a Galois extension N which is PAC over K except $\tilde{\mathbb{Q}}$.*

The proof of this theorem relies on a result of Razon about fields which are PAC over subfields, on Frobenius density theorem, and on Neukirch's recognition of p-adically closed fields among all algebraic extensions of $\mathbb{Q}$. The latter theorem has no analog for finitely generated extensions over $\mathbb{F}_p$ but it has one for finitely generated extensions of $\mathbb{Q}$ (a theorem of Efrat-Koenigsmann-Pop). However, at one point of our proof we use the basic fact that $\mathbb{Q}$ has no proper subfields. That property totally fails if we replace $\mathbb{Q}$ say by $\mathbb{Q}(t)$ with t indeterminate. Thus, any generalization of the main theorem to finitely generated fields or, more generally, to countable Hilbertian fields, should use completely other means.
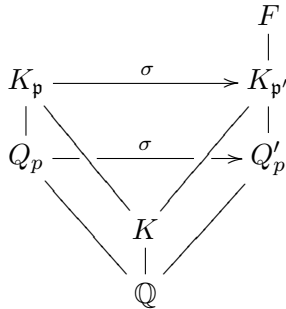
2. Galois extensions of number fields

Among all Hilbertian fields $\mathbb{Q}$ is the only one which is a prime field. This simple observation plays a crucial role in the proof of the main theorem (see Remark 2).

Lemma 1. *Let K be a finite Galois extension of $\mathbb{Q}$, $\mathfrak{p}$ an ultrametric prime of K, $K_{\mathfrak{p}}$ a Henselian closure of K at $\mathfrak{p}$, and F an algebraic extension of K such that $\mathrm{Gal}(K_{\mathfrak{p}}) \cong \mathrm{Gal}(F)$. Then $F = K_{\mathfrak{p}}^{\sigma}$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q})$. Thus, $F = K_{\mathfrak{p}'}$ for some prime $\mathfrak{p}'$ of K conjugate to $\mathfrak{p}$ over $\mathbb{Q}$.*

Proof. Let p be the prime number lying under $\mathfrak{p}$. Denote the closure of $\mathbb{Q}$ in $K_{\mathfrak{p}}$ under the $\mathfrak{p}$-adic topology by Q_p. Then Q_p is isomorphic to the field of all algebraic elements in $\mathbb{Q}_p$ (= the field of p-adic integers). By [7, Satz 1], F is Henselian and it contains an isomorphic copy Q_p' of Q_p such that $[F : Q_p'] = [K_{\mathfrak{p}} : Q_p]$. In particular, the prime $\mathfrak{p}'$ which F induces on K lies over p. Hence, KQ_p' is a Henselian closure of K at $\mathfrak{p}'$ which we denote by $K_{\mathfrak{p}'}$. Since $K/\mathbb{Q}$ is Galois, there is a $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\mathfrak{p}^{\sigma} = \mathfrak{p}'$. Moreover, σ extends to an element $\sigma \in \mathrm{Gal}(\mathbb{Q})$ with $K_{\mathfrak{p}}^{\sigma} = K_{\mathfrak{p}'}$.

$$
\begin{array}{ccc}
 & & F \\
 & & | \\
K_{\mathfrak{p}} & \xrightarrow{\ \sigma\ } & K_{\mathfrak{p}'} \\
| & & | \\
Q_p & \xrightarrow{\ \sigma\ } & Q_p' \\
 & K & \\
 & | & \\
 & \mathbb{Q} &
\end{array}
$$

Since Q_p (resp. Q_p') is the $\mathfrak{p}$-adic (resp. $\mathfrak{p}'$-adic) closure of $\mathbb{Q}$ in $K_{\mathfrak{p}}$ (resp. $K_{\mathfrak{p}'}$), we have $Q_p^{\sigma} = Q_p'$. Hence, $[K_{\mathfrak{p}} : Q_p] = [K_{\mathfrak{p}'} : Q_p']$. Therefore, $[F : K_{\mathfrak{p}'}] = 1$, so $F = K_{\mathfrak{p}'} = K_{\mathfrak{p}}^{\sigma}$. $\qquad\square$

Remark 2. *The arguments of Lemma 1 can not be generalized to finitely generated extensions of $\mathbb{Q}$ which are transcendental over $\mathbb{Q}$. For example, suppose $K = \mathbb{Q}(t)$ with t indeterminate. If K is a Galois extension a field K_0, then, by Lüroth, $K_0 = \mathbb{Q}(u)$ with u transcendental over $\mathbb{Q}$. As such, K_0 has infinitely many automorphisms τ, each of which extends to $\tilde{K}$ and, in the notation of Lemma 1, $\mathrm{Gal}(K_{\mathfrak{p}}^{\tau}) \cong \mathrm{Gal}(K_{\mathfrak{p}})$. However, the prime of K induced by the Henselian valuation of $K_{\mathfrak{p}}^{\tau}$ is in general not conjugate to $\mathfrak{p}|_{K_0}$ over K_0.*

Observation 3. *Let V be a vector space of dimension d over $\mathbb{F}_p$ and $V_1, \ldots, V_n$ subspaces of dimensions $d - 1$. Suppose $n < p$. Then, $\bigcup_{i=1}^{n} V_i$ is a proper subset of V. Indeed, $|\bigcup_{i=1}^{n} V_i| \leq \sum_{i=1}^{n} |V_i| = np^{d-1} < p^d = |V|$, as required.*

Let N/K be an algebraic extension of fields. We say that N is **Hilbertian over** K if each separable Hilbertian subset of N contains elements of K.

Lemma 4. *Let N be an algebraic extension of a field K. Suppose N is Hilbertian over K. Then, K has for each finite abelian group A a Galois extension K' with Galois group A such that $N \cap K' = K$.*

Proof. Let t be a transcendental element over K. By [1, Prop. 16.3.5], $K(t)$ has a Galois extension F with Galois group A such that F/K is regular. In particular, $FN/N(t)$ is Galois with Galois group A. By [1, Lemma 13.1.1], N has a Hilbertian subset H such that for each $a \in H$, the specialization $t \rightarrow a$ extends to an N-place φ of FN with residue field N' which a Galois extension of N having Galois group A. Moreover, omitting finitely many elements from H, we have that if $a \in K$, then the residue field K' of F at φ is a Galois extension of K, $\mathrm{Gal}(K'/K)$ is isomorphic to a subgroup of A and $NK' = N'$.

Since N is Hilbertian over K, we may choose $a \in K \cap H$. Then,

$$|A| = [N' : N] \leq [K' : K] \leq [F : K(t)] = |A|.$$

Consequently, $\mathrm{Gal}(K'/K) \cong A$ and K' is linearly disjoint from N over K, as desired. $\qquad\square$

Theorem 5. *Let N be a Galois extension of a number field K which is different from $\tilde{\mathbb{Q}}$. Then N is not PAC over K.*
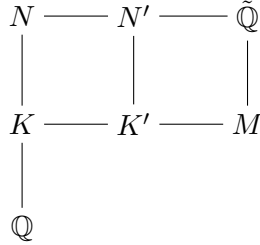
Proof. Assume N is PAC over K. First we replace K and N by fields satisfying additional conditions.

Since N is PAC, N is not real closed [1, Thm. 11.5.1]. Hence, as $N \neq \tilde{\mathbb{Q}}$, $[\tilde{\mathbb{Q}} : N] = \infty$ [6, p. 299, Cor. 3 and p. 452, Prop. 2.4], so $\mathbb{Q}$ has a finite Galois extension E containing K which is not contained in N. By Weissauer, NE is Hilbertian [1, Thm. 13.9.1]. Moreover, NE is Galois ever E, and by [1, Prop. 13.9.3], NE is Hilbertian over E. In addition, NE is PAC over E [4, Lemma 2.1]. Replacing N by NE and K by E, we may assume that, in addition to N being Galois and PAC over K, the extension $K/\mathbb{Q}$ is Galois and N is Hilbertian over K.
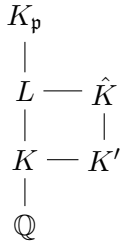
Let $n = [K : \mathbb{Q}]$ and choose a prime number $p > n$. Lemma 4 gives a cyclic extension K' of K of degree p which is linearly disjoint from N. Let $\hat{K}$ be the Galois closure of $K'/\mathbb{Q}$. Choose elements $\sigma_1, \ldots, \sigma_n$ of $\mathrm{Gal}(\hat{K}/\mathbb{Q})$ which lift the elements of $\mathrm{Gal}(K/\mathbb{Q})$. Finally let $K_i = (K')^{\sigma_i}$, $i = 1, \ldots, n$. Since $K/\mathbb{Q}$ is Galois, $K_1, \ldots, K_n$ are all of the conjugates of K' over $\mathbb{Q}$, so $\hat{K} = K_1 \cdots K_n$. Thus, $V = \mathrm{Gal}(\hat{K}/K)$ is a vector space over $\mathbb{F}_p$ of dimension d (which does not exceed n) and $V_i = \mathrm{Gal}(\hat{K}/K_i)$ is a subspace of V of dimension $d-1$. Observation 3 gives a $\sigma \in V \smallsetminus \bigcup_{i=1}^{n} V_i$. Denote the fixed field of σ in $\hat{K}$ by L. Then $K_i \nsubseteq L$, $i = 1, \ldots, n$.

Now choose a primitive element x for the extension K'/K. By the preceding paragraph, for each $\sigma \in \mathrm{Gal}(\hat{K}/\mathbb{Q})$, there is an i such that x^σ is a primitive element of K_i/K, so $x^\sigma \notin L$.

Again, by [5, Lemma 2.1], $N' = NK'$ is PAC over K'. Hence, there exists a field M such that $N' \cap M = K'$ and $N'M = \tilde{\mathbb{Q}}$ [8, Thm. 5], so $N \cap M = K$ and $NM = \tilde{\mathbb{Q}}$. In particular, the restriction map res: $\mathrm{Gal}(M) \to \mathrm{Gal}(N/K)$ is an isomorphism.

$$
\begin{array}{ccccc}
N & \text{---} & N' & \text{---} & \tilde{\mathbb{Q}} \\
| & & | & & | \\
K & \text{---} & K' & \text{---} & M \\
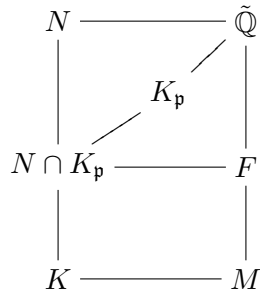| & & & & \\
\mathbb{Q} & & & &
\end{array}
$$

By the Frobenius density theorem, K has an ultrametric prime $\mathfrak{p}$ unramified in $\hat{K}$ such that each element of $\left(\frac{\hat{K}/K}{\mathfrak{p}}\right)$ generates $\mathrm{Gal}(\hat{K}/L)$ [3, p. 134, Thm. 5.2]. Hence, K has a Henselian closure $K_{\mathfrak{p}}$ at $\mathfrak{p}$ with $K_{\mathfrak{p}} \cap \hat{K} = L$. Therefore, no conjugate of x over $\mathbb{Q}$ belongs to $K_{\mathfrak{p}}$. Consequently, x belongs to no conjugate of $K_{\mathfrak{p}}$ over $\mathbb{Q}$.

$$
\begin{array}{ccc}
K_{\mathfrak{p}} & & \\
| & & \\
L & \text{---} & \hat{K} \\
| & & | \\
K & \text{---} & K' \\
| & & \\
\mathbb{Q} & &
\end{array}
$$

As an extension of N, the field $NK_{\mathfrak{p}}$ is PAC [1, Cor. 11.2.5]. On the other hand, as an extension of $K_{\mathfrak{p}}$, $NK_{\mathfrak{p}}$ is Henselian. Therefore, by Frey-Prestel, $NK_{\mathfrak{p}} = \tilde{\mathbb{Q}}$ [1, Cor. 11.5.5], so

$$\mathrm{Gal}(N/N \cap K_{\mathfrak{p}}) \cong \mathrm{Gal}(K_{\mathfrak{p}}).$$

Let $F = (N \cap K_{\mathfrak{p}})M$. Since res: $\mathrm{Gal}(M) \to \mathrm{Gal}(N/K)$ is an isomorphism, $\mathrm{Gal}(F) \cong \mathrm{Gal}(N/N \cap K_{\mathfrak{p}}) \cong \mathrm{Gal}(K_{\mathfrak{p}})$.

$$
\begin{array}{ccc}
N & \text{---------} & \tilde{\mathbb{Q}} \\
| & \quad K_{\mathfrak{p}} & | \\
N \cap K_{\mathfrak{p}} & \text{---------} & F \\
| & & | \\
K & \text{---------} & M
\end{array}
$$

It follows from Lemma 1 that there exists $\sigma \in \mathrm{Gal}(\mathbb{Q})$ with $F = K_{\mathfrak{p}}^{\sigma}$. In particular, $x \notin F$, contradicting that $x \in M$ and $M \subseteq F$. $\qquad\square$

Remark 6. *As already mentioned in the introduction, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ the field $\tilde{\mathbb{Q}}[\boldsymbol{\sigma}]$ is PAC [1, Thm. 18.9.3]. But, since $\tilde{\mathbb{Q}}[\boldsymbol{\sigma}]$ is Galois over $\mathbb{Q}$, it is not PAC over $\mathbb{Q}$ (Theorem 5), so much the more not PAC over $\mathbb{Z}$. However, the latter theorem does not rule out that $\tilde{\mathbb{Q}}[\boldsymbol{\sigma}]$ is PAC over its ring of integers $\tilde{\mathbb{Z}}[\boldsymbol{\sigma}]$. According to Lemma 7 below, the latter statement is equivalent to "$\tilde{\mathbb{Z}}[\boldsymbol{\sigma}]$ satisfies Rumely's local global theorem". We don't know whether these statements are true.*

Lemma 7 (Razon)**.** *The following statements on an algebraic extension M of $\mathbb{Q}$ are equivalent.*
- (a) *M is PAC over O_M.*
- (b) *O_M satisfies Rumely's local-global principle.*

Proof. The implication "(a)$\Longrightarrow$(b)" is a special case of [5, Cor. 1.9]. To prove (a) assuming (b), we consider an absolutely irreducible polynomial $f \in M[T, X]$ with $\frac{\partial f}{\partial X} \neq 0$ and a nonzero polynomial $g \in M[T]$. By [4, Lemma 1.3], it suffices to find $a \in O_M$ and $b \in M$ such that $f(a, b) = 0$ and $g(a) \neq 0$. Choose $a' \in \mathbb{Z}$ such that $g(a') \neq 0$ and $\frac{\partial f}{\partial X}(a', X) \neq 0$. Then choose $b' \in \tilde{\mathbb{Q}}$ with $f(a', b') = 0$. Next choose $c \in \mathbb{Z}$ with $b'c \in \tilde{\mathbb{Z}}$. For example, if $\sum_{i=0}^{n} c_i(b')^i = 0$ with $c_0, \ldots, c_n \in \mathbb{Z}$, then we may choose $c = c_n$. Now note that $(a', b'c)$ is a zero of the absolutely irreducible polynomial $f(T, c^{-1}X)$ with coefficients in M. By (a), there are $a \in O_M$ and $b'' \in M$ with $f(a, c^{-1}b'') = 0$. Then $b = c^{-1}b'' \in M$ satisfies $f(a, b) = 0$, as needed. $\qquad\square$

Problem 8. Prove or disprove the following statement: Let K be a finitely generated transcendental extension of $\mathbb{Q}$. Let N be a Galois extension of K different from $\tilde{K}$. Then N is not PAC over K.

Problem 9. The fact that $\mathbb{Q}_{\mathrm{solv}}$ is not PAC over $\mathbb{Q}$ implies the existence of an absolutely irreducible polynomial $f \in \mathbb{Q}_{\mathrm{solv}}[X, Y]$ such that for all $a \in \mathbb{Q}$ the equation $f(a, Y) = 0$ has no solvable root. Is it possible to choose f in $\mathbb{Q}[X, Y]$?

References

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

[2] W.-D. Geyer, M. Jarden, *PSC Galois extensions of Hilbertian fields.* Mathematische Nachrichten **236** (2002), 119–160.

[3] G. J. Janusz, *Algebraic Number Fields.* Academic Press, New York, 1973.

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

[5] M. JARDEN, A. RAZON, *Rumely's local global principle for algebraic PSC fields over rings.* Transactions of AMS **350** (1998), 55–85.

[6] S. LANG, *Introduction to Algebraic Geometry.* Interscience Publishers, New York, 1958.

[7] J. NEUKIRCH, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper.* Inventiones mathematicae **6** (1969), 296–314.

[8] A. RAZON, *Splitting of $\tilde{\mathbb{Q}}/\mathbb{Q}$.* Archiv der Mathematik **74** (2000), 263–265

Moshe JARDEN
Tel Aviv University
School of Mathematics
Ramat Aviv, Tel Aviv 69978, Israel
E-mail: jarden@post.tau.ac.il
URL: `http://www.math.tau.ac.il/~jarden/`