ON Σ-HILBERTIAN FIELDS

by

Michael D. Fried
Department of Mathematics, University of California, Irvine, Ca. 92717, USA
e-mail: mfried@math.uci.edu

and

Moshe Jarden
School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel. e-mail: jarden@math.tau.ac.il

For each nonnegative integer g, we construct a PAC field K which is g-Hilbertian but not Hilbertian.

directory: /works/paper66
31 January, 1997

Introduction

A field K is 0-Hilbertian if $K \neq \bigcup_{i=1}^n \varphi_i(K)$ for any collection of rational functions φ_i of degree at least 2, $i = 1, \ldots, m$. Corvaja and Zannier [CoZ] give an elementary construction for a 0-Hilbertian field that isn't Hilbertian. There is an obvious generalization of the notion of 0-Hilbertian to g-Hilbertian.

Guralnick-Thompson and Liebeck-Saxl have given a partial classification of monodromy groups of genus g covers of the projective line over $\mathbb{C}$. We use this to construct, for each nonnegative integer g, a PAC field K of characteristic 0 which is g-Hilbertian but not Hilbertian.

1. Σ-groups

Let Σ be a set of finite simple groups. A finite group G is said to be a **Σ-group**, if each composition factor of G belongs to Σ. An inverse limit of Σ-groups is a **pro-Σ-group**. Consider a short exact sequence of profinite groups:

$$1 \longrightarrow C \longrightarrow B \xrightarrow{\alpha} A \longrightarrow 1. \tag{1}$$

Then B is a pro-Σ-group if and only if both A and C are pro-Σ-groups. If $G = B_1 \times_A B_2$ is a fiber product of Σ-groups [FrJ, p. 288], then $\mathrm{Ker}(G \to B_2) \cong \mathrm{Ker}(B_1 \to A)$ is a Σ-group. Hence, G is a Σ-group.

For each cardinal number m there exists a unique (up to an isomorphism) free pro-Σ-group $\hat{F}_m(\Sigma)$ of rank m. This group has a subset X of cardinality m which converges to 1 such that each continuous map φ_0 of X into a pro-Σ group G uniquely extends to a homomorphism φ: $\hat{F}_m(\Sigma) \to G$. By Melnikov [Mel, Lemma 2.2], $\hat{F}_m(\Sigma)$ has the embedding property [FrJ, p. 353]. In particular,

(2) if m is infinite, then each finite embedding problem for $\hat{F}_m(\Sigma)$ where the kernel is a Σ-group is solvable.

If Σ is the set of all finite simple groups, then $\hat{F}_m(\Sigma)$ is the free profinite group $\hat{F}_m$ of rank m. In this case $\hat{F}_m$ is projective. This is also true in other cases:

Lemma 1: *Suppose each finite simple group in Σ is generated by m_0 elements. If $m \geq m_0$, then $\hat{F}_m(\Sigma)$ is projective if and only if the following holds:*

(3) *If a prime p divides the order of one of the groups in Σ, then $\mathbb{Z}/p\mathbb{Z} \in \Sigma$.*

Proof: Write $\hat{F}$ for $\hat{F}_m(\Sigma)$. Suppose first that Σ satisfies (3). In order to prove that $\hat{F}$ is projective, it suffices (and is necessary) to prove that for each prime p, each finite embedding problem for $\hat{F}$ with an abelian p-elementary kernel has a weak solution [FrJ, Lemma 20.8 or Rib, p. 211].

Indeed, assume that in the short exact sequence (1), $C \cong (\mathbb{Z}/p\mathbb{Z})^n$ for some positive integer n. Let $\varphi\colon \hat{F} \to A$ be an epimorphism. Choose $b_1, \ldots, b_k \in B$ such that $\langle \alpha(b_1), \ldots, \alpha(b_k) \rangle = A$ and $k \le m$ if m is finite. Let $B_0 = \langle b_1, \ldots, b_k \rangle$ and let α_0 be the restriction of α to B_0. Then $C_0 = \mathrm{Ker}(\alpha_0) = C \cap B_0$ is also an abelian p-elementary group. If p does not divide the order of A, then α_0 has a section [Hup, p. 122, Satz 17.5]. If p divides the order of A, then $\mathbb{Z}/p\mathbb{Z} \in \Sigma$ (by (3)). Therefore, both A and C_0 are Σ-groups. Hence, so is B_0. Since B_0 is generated by k elements and $k \le m$, it is a quotient of $\hat{F}_m(\Sigma)$. It follows that in each case there exists an epimorphism $\gamma\colon \hat{F} \to B_0$ such that $\alpha_0 \circ \gamma = \varphi$. This is a weak solution to the embedding problem. Conclude that $\hat{F}$ is projective.

Conversely, suppose that $\hat{F}$ is projective. Let S be a simple group in Σ and let p be a prime divisor of the order of S. We have to prove that $\mathbb{Z}/p\mathbb{Z} \in \Sigma$.

Indeed, since S is finite, $\mathrm{cd}_p(S) = \infty$ [Rib, p. 209, Cor. 205]*. In particular, by [Rib, p. 211], there exists a nonsplit short exact sequence $1 \longrightarrow C \longrightarrow G \xrightarrow{\alpha} S \longrightarrow 1$. where C is a finite elementary p-abelian group. Replace G by a subgroup of G if necessary, to assume that α is a Frattini cover [FrJ, p. 299].

Since $m \ge m_0$, this gives an epimorphism $\varphi\colon \hat{F} \to S$. As $\hat{F}$ is projective, there is a homomorphism $\gamma\colon \hat{F} \to G$ such that $\alpha \circ \gamma = \varphi$. Since α is Frattini, γ is surjective. Thus $\mathbb{Z}/p\mathbb{Z}$ is a composition factor of a Σ-group. Conclude that $\mathbb{Z}/p\mathbb{Z}$ is in Σ. ∎

Remark 2:

(a) If m_0 is the minimal integer such that all groups in Σ have rank m_0, then Lemma 1 is false with $m < m_0$. For example, it is false for $m = 1$. Indeed, suppose that Σ consists of the group A_5 only. Then $\hat{F}_1(\Sigma)$ is the trivial group, hence projective.

* This has a typo. Instead of "p does not divide $\#G$" it should say "p divides $\#G$".

But, $\mathbb{Z}/2\mathbb{Z}$ in not in Σ, although 2 divides the order of A_5.

(b) The classification of finite simple groups implies that any simple group S is generated by two elements [AsG, Thm. B]. That is, we may take $m_0 = 2$ in Lemma 1. We do not use the "if" part of Lemma 1 in the construction of a g-Hilbertian field which is not Hilbertian. In particular, the latter construction does not use the classification theorem for simple groups. ∎

2. Σ-Hilbertian fields

Let Σ be a set of finite simple groups and let t be a transcendental over K. We say K is **Σ-Hilbertian** if the following holds for each finite Galois extension $F/K(t)$ with $G(F/K(t))$ a Σ-group. There are infinitely many $a \in K$ such that each decomposition subgroup of $\mathcal{G}(F/K(t))$ over the specialization $t \to a$ coincides with the whole group.

In particular, if Σ is the set of all finite simple groups, then K is Σ-Hilbertian if and only if it is separably Hilbertian [FrJ, p. 147]. (Separable Hilbertian in characteristic 0 is the same as Hilbertian.) In many other cases this conclusion is false:

LEMMA 3: *Let Σ be a set of finite simple groups such that $\hat{F}_\omega(\Sigma)$ is projective. Let K_0 be a countable separably Hilbertian field. Suppose there exists a finite nonabelian simple group which does not belong to Σ. Then K_0 has a separable algebraic extension K which is PAC, Σ-Hilbertian, but not separably Hilbertian. Moreover, $G(K) \cong \hat{F}_\omega(\Sigma)$.*

Proof: Since $\hat{F}_\omega(\Sigma)$ has countable rank, K_0 has a separable algebraic extension K which is PAC such that $G(K) \cong \hat{F}_\omega(\Sigma)$ [FrJ, Thm. 20.22].

CLAIM A: *K is Σ-Hilbertian.* Indeed, let $F/K(t)$ be a finite Galois extension such that $\mathcal{G}(F/K(t))$ is a Σ-group. Let L be the algebraic closure of K in F. By (2), the embedding problem res: $\mathcal{G}(F/K(t)) \to \mathcal{G}(L/K)$ is solvable over K. Now continue with the proof of Claim A exactly as in the proof of [FrJ, Prop. 23.2] (for $E = K(t)$ and $H = \mathcal{G}(F/E)$) and obtain infinitely many $a \in K$ such that each decomposition group over the specialization $t \to a$ coincides with $\mathcal{G}(F/K(t))$.

CLAIM B: *K is not separably Hilbertian.* Let S be a finite simple nonabelian group which is not in Σ. Since K is PAC, $K(t)$ has a Galois extension F' with Galois group

S [FrV, Thm. 2, for characteristic 0, and Pop, Thm. 1 or HaJ, Thm. A in general]. If K were separably Hilbertian, we could specialize t to an element of K and realize S over K. Then S would be a quotient of $\hat{F}_\omega(\Sigma)$ and therefore would be a Σ-group. This would contradict the assumption we have made on S. ∎

Remark 4: The assumption that $\hat{F}_\omega(\Sigma)$ is projective is redundant. Suppose that $\hat{F}_\omega(\Sigma)$ is not projective. Let $\varphi\colon \tilde{F}_\omega(\Sigma) \to \hat{F}_\omega(\Sigma)$ be its universal Frattini cover. Then $\tilde{F}_\omega(\Sigma)$ is projective [FrJ, Prop. 20.33]. Since $\hat{F}_\omega(\Sigma)$ has the embedding property, so does $\tilde{F}_\omega(\Sigma)$ [FrJ, Prop. 23.9]. Moreover, $\mathrm{Ker}(\varphi)$ is contained in the Frattini subgroup of $\tilde{F}_\omega(\Sigma)$, which is nilpotent [FrJ, Lemma 20.2]. It follows that $\mathrm{Ker}(\varphi)$ itself is nilpotent. Suppose S is not a quotient of $\hat{F}_\omega(\Sigma)$ and S is a simple nonabelian group. Then S is not a quotient of $\tilde{F}_\omega(\Sigma)$. The proof of Lemma 3 remains therefore valid if we replace $\hat{F}_\omega(\Sigma)$ throughout by $\tilde{F}_\omega(\Sigma)$.

Indeed, in this case we may prove Claim B in another way: $\mathrm{Ker}(\varphi)$ is a nontrivial closed normal subgroup of $G(K)$ and it is pro-nilpotent. By [FrJ, Thm. 15.10], K is not separably Hilbertian. ∎

3. g-Hilbertian fields

Let K be a field and let g be a nonnegative integer. Call a separable rational map of absolutely irreducible curves, $\varphi\colon \Gamma \to \mathbb{A}^1$, over K **admissible** if it has degree at least 2. We say that K is **g-Hilbertian** if K is not the union of finitely many sets of the form $\varphi(\Gamma(K))$ with φ admissible and Γ of genus at most g. Each $a \in K$ belongs to a set of the form $\varphi(\Gamma(K))$ with φ admissible and Γ of genus at most g with a point $a' \in \varphi(\Gamma(K))$. Then $\varphi' = \varphi + a - a'$ is also admissible and $a' \in \varphi'(\Gamma(K))$. [FrJ, Lemma 12.1 or Ser, Cor. 3.2.4 for $\mathrm{char}(K) = 0$] shows that K is separably Hilbertian if and only if K is g-Hilbertian for each $g \geq 0$.

Observe that K is 0-Hilbertian if and only if K has the following property:

(4) $K \neq \bigcup_{i=1}^m \varphi_i(K)$ for each collection $\{\varphi \in K(t) \mid \deg(\varphi) \geq 2$ and φ_i separable $, i = 1, \ldots, t\}$.

Indeed, suppose that K satisfies Condition (4). Assume that $K = \bigcup_{i=1}^n \varphi_i(\Gamma_i(K))$, with $\varphi_i\colon \Gamma_i \to \mathbb{A}^1$ admissible and the genus of Γ_i is 0, $i = 1, \ldots, n$. Renumber $\varphi_1, \ldots, \varphi_n$, if necessary, to assume that $\Gamma_i(K)$ is infinite for $i = 1, \ldots, m$ and $\Gamma_i(K)$ is finite for $i = m+1, \ldots, n$. In particular, for each i between 1 and m, $\Gamma_i(K)$ contains a simple K-rational point. Hence, Γ_i is birationally equivalent to $\mathbb{A}^1$ over K, [Art, p. 304, Thm. 7] and φ_i can be considered as an element of $K(t)$. Moreover, $K \smallsetminus \bigcup_{i=1}^m \varphi_i(K)$ is a finite set, say $\{a_1, \ldots, a_r\}$. For each j between 1 and r let $\psi_j = t^2 + a_j$. Then $K = \bigcup_{i=1}^m \varphi_i(K) \cup \bigcup_{j=1}^r \psi_j(K)$. This contradicts Condition (4).

Corvaja and Zannier [CoZ, Thm. 1] give an example of an algebraic extension K of $\mathbb{Q}$ which is 0-Hilbertian but not Hilbertian.

The example of Theorem 6 generalizes that of Corvaja-Zannier and proves that for each g there are g-Hilbertian fields which are not Hilbertian.*

Let C be an algebraically closed field of characteristic p (which may be 0). Let G be a finite group. We say that G has **genus** g (in characteristic p) if there exists a finite separable extension $F/C(t)$, with F of genus g, such that $G \cong \mathcal{G}(\hat{F}/C(t))$. Here $\hat{F}$ is the Galois closure of $F/C(t)$. In particular, each cyclic group is a group of genus 0 in each characteristic.

Remark 5: Omission of Chevalley groups. A combination of works of Aschbacher, Frohardt, Guralnick, Liebeck, Magaard, Neubauer, Saxl, and Thompson, proves that for each g there are finite simple groups that are not composition factors of groups of genus g in characteristic 0. Indeed, there are only finitely many — depending on g — Chevalley groups defined over a field with more than 113 elements that occur as composition factors of groups of genus g in characteristic 0 [GuN, Thm. A].

We don't know, for $p > 0$ and a given g, if there is any finite simple group which does not occur as a composition factor of a group of genus at most g in characteristic p. This restricts the proof of Theorem 6 to characteristic 0. Thus, it is not clear if there exists a non-Hilbertian field K of characteristic p which is g-Hilbertian. ∎

THEOREM 6: *Let g be a nonnegative integer and let K_0 be a countable Hilbertian field of characteristic* 0. *Then, K_0 has an algebraic extension K which is PAC, g-Hilbertian, but not Hilbertian.*

* The [CoZ] example is a quotient field of a unique factorization domain R with infinitely many prime ideals. Our example does not have this property.

Proof: Denote the set of all finite simple groups that occur as composition factors of groups of genus at most g in characteristic 0 by Σ. Then Σ contains all groups $\mathbb{Z}/l\mathbb{Z}$, with l prime, but not all finite simple groups. For example, if $p > 113$ is a large prime, then Σ does not contain $\mathrm{PSL}(2, \mathbb{F}_p)$ (Remark 5).

By Lemma 1, $\hat{F}_\omega(\Sigma)$ is projective. Lemma 3 therefore gives an algebraic extension K of K_0 which is PAC, Σ-Hilbertian but not Hilbertian. Moreover, $G(K) \cong \hat{F}_\omega(\Sigma)$.

Claim: *K is g-Hilbertian.* For $i = 1, \ldots, m$ let Γ_i be an absolutely irreducible curve over K of genus at most g. Let $\varphi_i\colon \Gamma_i \to \mathbb{A}^1$ be a rational function of degree at least 2. Use primitive elements if necessary to assume that Γ_i is a plane curve defined by the equation $h_i(T, X) = 0$, where $h_i \in K[T, X]$ is an absolutely irreducible polynomial of degree at least 2 in X. Moreover, assume that φ_i is the projection on the first coordinate.

Now choose $x_i \in \widetilde{K(t)}$ such that $h_i(t, x_i) = 0$. Let $\hat{F}_i$ be the Galois closure of $K(t, x_i)/K(t)$, and let L_i be the algebraic closure of K in $\hat{F}_i$. Since $K(t, x_i)$ is linearly disjoint from $L_i(t)$ over $K(t)$, x_i has the same conjugates over $L_i(t)$ as over $K(t)$. Hence, $\hat{F}_i$ is the Galois closure of $L_i(t, x_i)/L_i(t)$ and therefore $\hat{F}_i\tilde{K}$ is the Galois closure of $\tilde{K}(t, x_i)/\tilde{K}(t)$. Moreover, $\mathcal{G}(\hat{F}_i/L_i(t)) \cong \mathcal{G}(\hat{F}_i\tilde{K}/\tilde{K}(t))$ and the genus of $\tilde{K}(t, x_i)$ is at most g. Hence, $\mathcal{G}(\hat{F}_i/L_i(t))$ is a group of genus at most g and therefore also a Σ-group. In addition, $\mathcal{G}(L_i/K)$ as a quotient of $\hat{F}_\omega(\Sigma)$ is also a Σ-group. Conclude from the short exact sequence

$$1 \longrightarrow \mathcal{G}(\hat{F}_i/L_i(t)) \longrightarrow \mathcal{G}(\hat{F}_i/K(t)) \longrightarrow \mathcal{G}(L_i/K) \longrightarrow 1$$

that $\mathcal{G}(\hat{F}_i/K(t))$ is a Σ-group.

Let $\hat{F} = \hat{F}_1 \cdots \hat{F}_m$. Take successive fiber products of $\mathcal{G}(\hat{F}_1/K(t)), \ldots, \mathcal{G}(\hat{F}_m/K(t))$ to obtain $\mathcal{G}(\hat{F}/K(t))$. By §1, $\mathcal{G}(\hat{F}/K(t))$ is a Σ-group. Since, K is Σ-Hilbertian, it is possible to specialize t in infinitely many ways to an element $a \in K$ such that $\mathcal{G}(\hat{F}/K(t))$ is preserved. For infinitely many of these a, each of the polynomials $h_i(a, X)$ is irreducible of degree at least 2. In particular, $h_i(a, b) \neq 0$ for all $b \in K$. So, $a \notin \bigcup_{i=1}^m \varphi_i(K)$ for infinitely many $a \in K$. This concludes the proof of the Claim and of the theorem. ∎

References

[Art] E. Artin, *Algebraic Numbers and Algebraic Functions,* Gordon and Breach, New York, 1967.

[AsC] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, Journal of Algebra **90** (1984), 446-460.

[CoZ] P. Corvaja and U. Zannier, *Values of rational functions on non-Hilbertian fields and a question of Weissauer,* Israel Journal of Mathematics

[Deu] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable,* Lecture Notes in Mathematics **314**, Springer, Berlin, 1973.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[FrV] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces,* Mathematische Annalen **290** (1991), 771–800.

[GuN] R. Guralnick and M. Neubauer, *Monodromy groups of branched coverings: The generic case,* Contemporary Mathematics **186** (1995), 325–352.

[HaJ] Dan Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Manuscript, Heidelberg, 1996

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

[Mel] O. V. Melnikov, *Normal subgroups of free profinite groups,* Math. USSR Izvestija **12** (1978), 1–20.

[Pop] F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996), 1–35.

[Rib] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.

[Ser] J.-P. Serre, *Topics in Galois Theory,* Jones and Barlett, Boston 1992.

29 May, 2007