ALMOST HILBERTIAN FIELDS[*]

by

Pierre Dèbes[1] and Dan Haran[2]

Abstract. This paper is devoted to some variants of the Hilbert specialization property. For example, the RG-hilbertian property (for a field K), which arose in connection with the Inverse Galois Problem, requires that the specialization property holds solely for extensions of $K(T)$ that are Galois and regular over K. We show that fields inductively obtained from a real hilbertian field by adjoining real p-th roots (p odd prime) are RG-hilbertian; some of these fields are not hilbertian. There are other variants of interest: the R-hilbertian property is obtained from the RG-hilbertian property by dropping the condition "Galois", the mordellian property is that every non-trivial extension of $K(T)$ has infinitely many non-trivial specializations, etc. We investigate the connections existing between these properties. In the case of PAC fields we obtain pure Galois-theoretic characterizations. We use them to show that "mordellian" does not imply "hilbertian" and that every PAC R-hilbertian field is hilbertian.

September 28, 1998

1991 MS Classification. Primary 12E25, 12F10; Secondary 12F12, 11xx.

[*] Research partially supported by the Minkowski Center for Geometry at Tel Aviv University.

[1] Supported by the University of California, Irvine (UCI).

[2] Supported by The Israel Science Foundation.

Introduction

Hilbert's irreducibility theorem is classically used in the Inverse Galois Problem in the following way. If a finite group G can be realized as the Galois group of an extension $E/\mathbb{Q}(T)$, then it can also be realized as the Galois group of an extension of $\mathbb{Q}$ by specializing T to some rational number $t \in \mathbb{Q}$: Hilbert's theorem indeed assures that the Galois group is preserved by specialization for infinitely many $t \in \mathbb{Q}$. A common approach to the Inverse Galois Problem is thus to work over $\mathbb{Q}(T)$, which provides a geometrical angle: finite extensions $E/\mathbb{Q}(T)$, if they are regular over $\mathbb{Q}$, *i.e.*, if $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$, exactly correspond to covers of $\mathbb{P}^1$ defined over $\mathbb{Q}$. In fact, most works in this area focus on this regular form of the Inverse Galois Problem: is each finite group the Galois group of a regular Galois extension of $\mathbb{Q}(T)$? But then, one does not need the full Hilbert specialization property to deduce the Inverse Galois problem: one only needs it for regular Galois extensions of $\mathbb{Q}(T)$. This weaker property is called the RG-hilbertian specialization property.

All this generalizes in a straightforward manner to arbitrary fields (instead of $\mathbb{Q}$) to give rise to the Inverse Galois Problem and its regular form over a field K, and to the notions of hilbertian and RG-hilbertian fields. The RG-hilbertian property has been introduced by Fried and Völklein. In their paper [FrVo] they give Galois-theoretic characterizations of hilbertian fields and RG-hilbertian fields that are Pseudo Algebraically Closed (PAC) and use them to produce an example of an RG-hilbertian but non-hilbertian PAC field, thereby showing that the RG-hilbertian property is indeed weaker than the full hilbertian property. These results along with the relevant definitions are recalled in §3.

In §1, we produce a new wide class of RG-hilbertian fields. These are all extensions inductively obtained from a real hilbertian field by adjoining real p-th roots (for some fixed prime $p \neq 2$); we call them real p-radical extensions. Furthermore, many such real p-radical extensions are not hilbertian and among them are some classical fields such as the real closure of $\mathbb{Q}$ under taking real p-th roots, the p-fermatian closure of $\mathbb{Q}$, etc. These new examples of RG-hilbertian non-hilbertian fields are contained in $\mathbb{R}$ and so, contrary to those from [FrVo], are not PAC; furthermore, they are relatively "small" in that their index over $\mathbb{Q}$ is p^∞ and the Galois group of their Galois closure is of order $(p-1)p^\infty$. This first part suggests that there are more RG-hilbertian fields than may have been expected first, and consequently more fields for which the Inverse Galois Problem should hold if one believes in the Regular Inverse Galois Problem.

In §3 we deal with another specialization property, close to the hilbertian property. We say a field K is *mordellian* if for every polynomial $P(T,Y) \in K[T,Y]$, absolutely irreducible and with $\deg_Y P \geq 2$, there exist infinitely many $t \in K$ such that $P(t,Y)$ has no root in K. If the same property holds but with the single polynomial $P(T,Y)$ replaced by any finite set of polynomials $P_1(T,Y), \ldots, P_n(T,Y)$ (and with t the same for all P_is), then the field K can classically be shown to be hilbertian (*e.g.* [FrJa, Lemma 12.1]). But it has been unknown whether this remains true with $n = 1$, that is, if mordellian fields are hilbertian. We show the answer is negative: the mordellian property is a new specialization property. In fact, we give a Galois characterization of mordellian PAC fields and combine it with [FrVo] to produce a mordellian non-hilbertian PAC field.

In §4 we introduce some further specialization properties in a more systematic manner. These are variations on the (RG)-hilbertian-mordellian definitions. For example an R-hilbertian field is a field for which the hilbertian specialization property holds but only for absolutely irreducible polynomials. Theorem 4.2 shows that R-hilbertian PAC fields are hilbertian. We do not know whether the same result holds if the PAC assumption is removed. In §5, we investigate more completely the relations existing between the variants of the hilbertian property we have introduced (Theorem 5.1). The paper ends with other related observations and open questions.

The somewhat more technical §2 contains several group-theoretic lemmas used in the paper.

We wish to thank Bruno Deschamps for valuable comments on a preliminary version of the paper.

Unless otherwise specified, the fields we consider are of characteristic 0.

1. RG-hilbertian fields

For each integer $n \neq 0$ let ζ_n be a primitive n-root of 1. Denote the nth root function $\mathbb{R} \to \mathbb{R}$ (if n is odd) and $\mathbb{R}^+ \to \mathbb{R}^+$ (if n is even) by $\sqrt[n]{-}$.

Given a prime $p \neq 2$, an extension K/k with $k \subseteq \mathbb{R}$ is called a *real p-radical extension* if there exists a sequence $(a_n)_{n>0}$ of real numbers $a_n \in \mathbb{R}$ such that:

$$\begin{cases} K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \sqrt[p]{a_3}, \ldots) \\ a_n \in k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \ldots, \sqrt[p]{a_{n-1}}) \text{ for each } n > 0. \end{cases}$$

Remark 1.1: Let K/k be a *tower* of real p-radical extensions, that is, K is the union of an increasing sequence of fields $K_1 = k, K_2, K_3, \dots$ such that K_{i+1}/K_i is a p-radical extension for each $i > 0$. Then K/k is itself a real p-radical extension.

Indeed, each extension K_{i+1}/K_i is of the form $K_{i+1} = K_i(\sqrt[p]{a_{in}}|\ n > 0)$ with $a_{in} \in K_i(\sqrt[p]{a_{ik}}|\ 0 < k < n)$ $(n > 0,\, i > 0)$. Choose an enumeration $(b_m)_{m>0}$ of the countable set $\{a_{ij}|\ i, j\}$. We may assume that each of the numbers in the sequence $(b_m)_{m>0}$ occurs infinitely many times — otherwise replace $b_1, b_2, b_3, \dots$ by

$$b_1, b_1, b_2, b_1, b_2, b_3, b_1, b_2, b_3, b_4, b_1, b_2, b_3, b_4, b_5, \dots$$

Next define by induction a sequence $(m_r)_{r>0}$ of integers (possibly finite) by letting m_{r+1} be the first integer larger than m_r such that $b_{m_{r+1}} \in k(\sqrt[p]{b_{m_1}}, \sqrt[p]{b_{m_2}}, \dots, \sqrt[p]{b_{m_r}})$. We are done if we prove that $\{a_{ij}|\ i, j > 0\} = \{b_{m_r}|\ r > 0\}$. Suppose that this is not the case and then let (i, j) be the smallest pair (in the lexicographical order) such that $a_{ij} \notin \{b_{m_r}|\ r > 0\}$. Then

$$a_{ij} \in K_i(\sqrt[p]{a_{i1}}, \sqrt[p]{a_{i2}}, \dots, \sqrt[p]{a_{i\,j-1}}) = k(\sqrt[p]{a_{\alpha\beta}}|\ (\alpha, \beta) < (i, j)).$$

Therefore there exists a finite subset S of $\{(\alpha, \beta)|\ (\alpha, \beta) < (i, j)\}$ such that $a_{ij} \in k(\sqrt[p]{a_{\alpha\beta}}|\ (\alpha, \beta) \in S)$. By assumption, $a_{\alpha\beta} \in \{b_{m_r}|\ r > 0\}$ for every $(\alpha, \beta) \in S$. Hence there is an integer r such that $\{a_{\alpha\beta}|\ (\alpha, \beta) \in S\} \subseteq \{b_{m_1}, b_{m_2}, \dots, b_{m_r}\}$. Now there is an integer $m > m_r$ such that $b_m = a_{ij}$. It then follows from

$$b_m = a_{ij} \in k(\sqrt[p]{a_{\alpha\beta}}|\ (\alpha, \beta) < (i, j)) \subseteq k(\sqrt[p]{b_{m_1}}, \sqrt[p]{b_{m_2}}, \dots, \sqrt[p]{b_{m_{r-1}}}),$$

that m is in the sequence $(m_r)_{r>0}$. Thus $a_{ij} \in \{b_{m_r}|\ r > 0\}$ — a contradiction. ∎

Examples 1.2: In this paper we will consider in particular the following examples:

(a) For each prime p define the field $K_{p,\infty}$ as the union of the field K_n $(n \geq 0)$ defined inductively by: $K_0 = \mathbb{Q}$ and for $n > 0$, K_{n+1} is the field generated over K_n by all elements $\sqrt[p]{b}$ where b runs over K_n. The field $K_{p,\infty}$ is the smallest extension of $\mathbb{Q}$ contained in $\mathbb{R}$ closed under taking real pth roots.

(b) For each prime p consider the field $\mathcal{F}_p$ defined similarly as in (a) but with K_{n+1} obtained from K_n by adjoining all elements $\sqrt[p]{1 + b^p}$ where

b runs over K_n. In [Ri], a field K is said to be p-fermatian if any sum $x^p + y^p$ is a p-th power in K. The field $\mathcal{F}_p$ is the real p-fermatian closure of $\mathbb{Q}$, *i.e.* the smallest extension of $\mathbb{Q}$ contained in $\mathbb{R}$ that is p-fermatian. The field $\mathcal{F}_2$ is more classically called the pythagorean closure of $\mathbb{Q}$.

The fields $K_{p,\infty}$, $\mathcal{F}_p$ are not hilbertian. In fact, for $P(T,Y) = Y^p - T$ [resp. $P(T,Y) = Y^p - (1+T^p)$], the polynomial $P(t,Y)$ has a root in K for each $t \in K_{p,\infty}$ [resp. for each $t \in \mathcal{F}_p$]. However Theorem 1.3 below will show that for $p \neq 2$, these fields are RG-hilbertian, as any real p-radical extension with $p \neq 2$. ▮

Below we say that the Inverse Galois Problem (IGP) [resp. the Regular Inverse Galois Problem (RIGP)] holds over a field K if every finite group G is the Galois group of a Galois extension E/K [resp. a Galois extension $E/K(T)$ with E/K regular (*i.e.* $E \cap \overline{K} = K$)]. Also recall from [FrVo, p. 478] that a field K is said to be *RG-hilbertian* if for each polynomial $P(T,Y) \in K[T,Y]$, absolutely irreducible, with $\deg_Y P \geq 1$ and such that the associated function field extension $K(T)[Y]/(P(T,Y))$ of $K(T)$ is Galois, there exist infinitely many $t \in K$ such that $P(t,Y)$ is irreducible in $K[Y]$.

THEOREM 1.3: *Let $k \subseteq \mathbb{R}$ be a field, $p \neq 2$ be a prime number and K/k be a real p-radical extension. Then K/k has the following properties.*

(a) *K/k is linearly disjoint from every Galois extension (finite or not) of k not containing ζ_p.*

(b) *If the IGP holds over k then the IGP holds over K.*

(c) *If k is hilbertian then K is RG-hilbertian. Consequently, if the RIGP holds over K, then the IGP holds over K.*

COROLLARY 1.4: *The fields $K_{p,\infty}$, $\mathcal{F}_p$ $(p \neq 2)$ are RG-hilbertian but they are not hilbertian. If the IGP holds over $\mathbb{Q}$ then it necessarily also holds over the fields $K_{p,\infty}$ and $\mathcal{F}_p$ $(p \neq 2)$.*

Remarks 1.5: (a) For each $\alpha \in \mathbb{R} \cap \overline{k}$, if K/k is a real p-radical extension, then $K(\alpha)/k(\alpha)$ is also a real p-radical extension. Furthermore, if the IGP holds over k, it also holds over $k(\alpha)$ and if k is hilbertian, so is $k(\alpha)$. So the conclusions of Theorem 1.3 also hold for every finite extension E of K contained in $\mathbb{R}$. On the other hand it is unclear whether the condition "$E \subseteq \mathbb{R}$" can be removed. For example, are the fields $K_{p,\infty}(\zeta_p)$, $\mathcal{F}_p(\zeta_p)$ RG-hilbertian? Are they hilbertian?

(b) Finding a p-radical extension $K/\mathbb{Q}$ such that the IGP does not hold over K would disprove the IGP over $\mathbb{Q}$ (from Theorem 1.3 (b)) and so the RIGP over $\mathbb{Q}$ but also the RIGP over K (from Theorem 1.3 (c)).

Also the field K could not be ample, for the RIGP is known to hold over ample fields ([Po], [DeDes]). ∎

Lemma 1.6: *Let F be a subfield of $\mathbb{R}$ and p be a prime number. Let N/F be a Galois extension (finite or not) not containing ζ_p. Then for each $b \in F$, the extensions $F(\sqrt[p]{b})/F$ and N/F are linearly disjoint and the field $N(\sqrt[p]{b})$ does not contain ζ_p.*

Proof: Let $b \in F$. Suppose $b \in F^p$, *i.e.* b has some pth root in F. Since $F \subseteq \mathbb{R}$, *a fortiori* the real p-root $\sqrt[p]{b}$ is in F and so the assertions of the lemma are trivial. Assume therefore that $b \notin F^p$. Then $X^p - b$ is irreducible over F [La, Corollary VIII.9.1], and hence $[F(\sqrt[p]{b}) : F] = p$. Since $[N \cap F(\sqrt[p]{b}) : F]$ divides this prime number, either $N \cap F(\sqrt[p]{b}) = F(\sqrt[p]{b})$ or $N \cap F(\sqrt[p]{b}) = F$.

In the first case $\sqrt[p]{b} \in N$; and, as N/F is Galois, also the root $\zeta_p \sqrt[p]{b}$ of $X^p - b$ is in N. Therefore $\zeta_p \in N$, a contradiction.

In the second case, N and $F(\sqrt[p]{b})$ are linearly disjoint over F. In particular, $[N(\sqrt[p]{b}) : N] = p$. But $[N(\zeta_p) : N]$ divides $p-1$ and is not 1, so it does not divide $p = [N(\sqrt[p]{b}) : N]$. Therefore $\zeta_p \notin N(\sqrt[p]{b})$. ∎

Proof of Theorem 1.3: (a) follows by induction from Lemma 1.6. By definition of real p-radical extension we have $K = \bigcup_{i=0}^{\infty} k_i$, where $k_0 = k$, and $k_i = k_{i-1}(\sqrt[p]{a_i})$, with $a_i \in k_{i-1}$, for each $i \geq 1$. It suffices to show that each k_i is linearly disjoint from any given Galois extension E of k not containing ζ_p.

Assume, by induction, that k_{i-1} is linearly disjoint from E over k and $\zeta_p \notin Ek_{i-1}$. By Lemma 1.6 (with $F = k_{i-1}$, $N = Ek_{i-1}$, and $b = a_i$), k_i is linearly disjoint from Ek_i over k_{i-1} and $\zeta_p \notin Ek_i$. Therefore [La, Proposition X.5.1], k_i is linearly disjoint from E over k.

(b) Let G be a finite group. It is a classical exercise to show that if the IGP holds over k, then there actually exists a Galois extension N/k of group G linearly disjoint from $k(\zeta_p)/k$ (and more generally, from any given finite extension of k). From (a), the extensions K/k and N/k are linearly disjoint. Thus we have $\mathcal{G}(NK/K) = G$. The group G being arbitrary, the IGP holds over K.

(c) For later reference, we prove a more general property than the RG-hilbertian property. Instead of a single polynomial $P(T,Y)$, consider n absolutely irreducible polynomials $P_1(T,Y), \ldots, P_n(T,Y) \in K[T,Y]$ such that

(*) $\deg_Y P_i \geq 2$ and the function field $K(T)[Y]/(P_i(T,Y))$ is a Galois extension of $K(T)$, for $i = 1, \ldots, n$.

We show that, under the assumption "k hilbertian", there exist infinitely many $t \in K$ such that each of the polynomials $P_1(t,Y),\dots,P_n(t,Y)$ is irreducible in $K[Y]$.

Let $K_0 \subseteq K$ be a finite extension of k such that (*) holds with K_0 replacing K. Denote the function field $K_0(T)[Y]/(P_i(T,Y))$ by $N_{i,T}$, $i = 1,\dots,n$. Consider the field $K_0(\zeta_p)$. It is a hilbertian field (as a finite extension of k) and each $P_i(T,Y)$ is irreducible over it (since $P_i(T,Y)$ is absolutely irreducible). Thus there exist infinitely many $t \in K_0$ such that $P_i(t,Y)$ is irreducible over $K_0(\zeta_p)$[3], $i = 1,\dots,n$. Conjoined with $\zeta_p \notin K_0$ (since $K_0 \subseteq K \subseteq \mathbb{R}$), that implies that the specialization $N_{i,t}$ of $N_{i,T}$ at t (which, since $N_{i,T}/K_0(T)$ is Galois, is the splitting field of $P_i(t,Y)$ over K_0) does not contain ζ_p, $i = 1,\dots,n$. The extension K/K_0 is a real p-radical extension. Thus part (a) of Theorem 1.3 applies to conclude that the extensions $N_{i,t}/K_0$ and K/K_0 are linearly disjoint; hence $P_i(t,Y)$ is irreducible in $K[Y]$, for $i = 1,\dots,n$. ∎

2. Some preliminary group-theoretic results

The following results will be used in the subsequent sections.

Lemma 2.1: *Let G be a finite group, let K be a normal subgroup of G and let B be a subgroup of G. Let C be a coset of K in G that satisfies $C \subseteq \bigcup_{\sigma\in G} B^\sigma$. Assume that $BK = G$. Then*

(a) *$|C \cap B^\sigma| = |K \cap B|$ for every $\sigma \in G$;*

(b) *C is the disjoint union $C = \dot{\bigcup}_{i=1}^n (C \cap B^{\sigma_i})$, where $B^{\sigma_1},\dots,B^{\sigma_n}$ are the distinct conjugates of B in G; and*

(c) *the number n of distinct conjugates of B in G is $(G:B)$.*

Proof: The condition $BK = G$ ensures that every conjugate of B in G is of the form B^k with $k \in K$. Moreover, it is of the form B^k, where k runs through a system Σ of representatives of the right cosets of $K \cap B$ in K. It then follows from $C \subseteq \bigcup_{\sigma\in G} B^\sigma$ that

$$C = \bigcup_{k\in K} (C \cap B^k) = \bigcup_{k\in\Sigma} (C \cap B^k). \tag{1}$$

If $g \in C$ and $k \in K$, then $g^k = k^{-1}gk = g(g^{-1}k^{-1}g)k \in gK = C$. Therefore

(d) C is invariant under conjugation by elements of K.

[3] Here we use the classical fact that Hilbert subsets of a finite extension E of a hilbertian field K contain infinitely many elements of the lower field K [FrJa, §11.2].

PROOF OF (a): Let $k \in K$. By (d), $C \cap B^k = (C \cap B)^k$, and hence $|C \cap B^k| = |C \cap B|$. In particular, by (1), we have $C \cap B \neq \emptyset$. Choose $g \in C \cap B$. Then $|C \cap B| = |gK \cap B| = |K \cap g^{-1}B| = |K \cap B|$.

PROOF OF (b): We have $|C| = |K| = (K : K \cap B) \cdot |K \cap B|$, hence by (a) , $|C| = \sum_{k \in \Sigma} |C \cap B^k|$. It follows from (1) that the sets $\{C \cap B^k\}_{k \in \Sigma}$ must be disjoint.

PROOF OF (c): Clearly $n \leq (G : B)$. By the proof of (b), the subgroups B^k, for $k \in \Sigma$, are distinct. Hence $n \geq |\Sigma| = (K : K \cap B) = (KB : B) = (G : B)$. ∎

Recall that a finite embedding problem $\rho\colon \Gamma \twoheadrightarrow A$, $\alpha\colon G \twoheadrightarrow A$ for a profinite group Γ is a diagram

$$\begin{tikzcd}
 & & & \Gamma \arrow[d, "\rho"] & \\
1 \arrow[r] & N \arrow[r] & G \arrow[r, "\alpha"] & A \arrow[r] & 1
\end{tikzcd}$$

in which the row is an exact sequence of finite groups and the map $\rho\colon \Gamma \to A$ is an epimorphism. A *(proper) solution* is a surjective homomorphism $\psi\colon \Gamma \to G$ such that $\alpha \circ \psi = \rho$; without the condition "ψ surjective", such a map ψ is said to be a *weak solution*. The embedding problem is said to be *split* if $\alpha\colon G \twoheadrightarrow A$ has a group-theoretic section.

LEMMA 2.2: *Let P be a projective profinite group, let $\hat{F}_2$ be the free profinite group on 2 generators, and let $\Gamma = P \star \hat{F}_2$ be the free profinite product of P and $\hat{F}_2$. Consider a finite embedding problem $\rho\colon \Gamma \twoheadrightarrow A$, $\alpha\colon G \twoheadrightarrow A$ for Γ, and let B be a proper subgroup of G. Then there exists a continuous homomorphism $\psi\colon \Gamma \to G$ such that $\alpha \circ \psi = \rho$ and $\psi(\Gamma) \not\subseteq B^\sigma$ for every $\sigma \in G$.*

Proof: As P is projective, there is a continuous homomorphism $\psi'\colon P \to G$ such that $\alpha \circ \psi' = \mathrm{res}_P\, \rho$. Let x_1, x_2 be free generators of $\hat{F}_2$ and let a_1, a_2 be their images in A by ρ. Let $C_1 = \alpha^{-1}(a_1)$ and $C_2 = \alpha^{-1}(a_2)$; these are cosets of the kernel K of α. Choose $g_1 \in C_1$ and $g_2 \in C_2$ (in a way to be specified below) and define $\psi''\colon \hat{F}_2 \to G$ by $\psi''(x_1) = g_1$ and $\psi''(x_2) = g_2$. Then $\alpha \circ \psi'' = \mathrm{res}_{\hat{F}_2}\, \rho$. The maps ψ' and ψ'' define a unique homomorphism $\psi\colon \Gamma \to G$ such that $\alpha \circ \psi = \rho$.

If $\alpha(B)$ is a proper subgroup of A, then, for every $\sigma \in G$,

$$\alpha(\psi(\Gamma)) = \rho(\Gamma) = A = A^{\alpha(\sigma)} \not\subseteq \alpha(B)^{\alpha(\sigma)} = \alpha(B^\sigma),$$

and hence $\psi(\Gamma) \not\subseteq B^\sigma$. Thus we are left with the case $\alpha(B) = A$, that is, $BK = G$.

By our choice $g_1, g_2 \in \psi(\Gamma)$. Therefore it suffices to show that we can choose $g_1 \in C_1$ and $g_2 \in C_2$ so that

$$\{g_1, g_2\} \not\subseteq B^\sigma \qquad \text{for each } \sigma \in G. \tag{2}$$

If either C_1 or C_2 are not contained in $\bigcup_{\sigma\in G} B^\sigma$, this is clear. Assume therefore that $C_1, C_2 \subseteq \bigcup_{\sigma\in G} B^\sigma$.

Let $B^{\sigma_1}, \ldots, B^{\sigma_n}$ be the distinct conjugates of B in G. By Lemma 2.1, $n \geq 2$ and so we may choose $g_1 \in C_1 \cap B^{\sigma_1}$ and $g_2 \in C_2 \cap B^{\sigma_2}$. By Lemma 2.1(b) we have

$$g_1 \notin \bigcup_{i\neq 1} B^{\sigma_i} \qquad \text{and} \qquad g_2 \notin \bigcup_{i\neq 2} B^{\sigma_i}.$$

Thus $\{g_1, g_2\} \not\subseteq B^{\sigma_i}$, for each $1 \leq i \leq n$. This gives (2). ▮

Lemma 2.3: *Let $H = H_n = G_0 \ltimes V$, where V is a vector space over $\mathbb{Z}/3\mathbb{Z}$ (written additively) of finite dimension $n \geq 3$, and $G_0 = \langle c \rangle$ of order 2 acts on V by $v^c = -v$, for all $v \in V$. Then*

(a) *If $\sigma \in H \smallsetminus V$, then $\sigma^2 = 1$ and $v^\sigma = -v$, for all $v \in V$.*
(b) *The centralizer of each $\sigma \in H \smallsetminus V$ in H is $\langle \sigma \rangle$.*
(c) *If $B \leq H$ and $\sigma \in B \smallsetminus V$, then $B = \langle \sigma \rangle \ltimes W$, where W is a subspace of V, and $\langle \sigma \rangle$ of order 2 acts on W by $w^\sigma = -w$. In particular, $B \cong H_m$ for some $m \leq n$.*
(d) $\operatorname{rank} H$ *(= the least number of generators of H) is $n+1$.*
(e) *The Frattini subgroup $\Phi(H)$ of H is trivial.*

Proof: Property (a) is immediate, and (b) follows from (a).

(c) Put $W = B \cap V$. By (a), $\langle \sigma, W \rangle = \langle \sigma \rangle \ltimes W$. Clearly, $\langle \sigma \rangle \ltimes W \subseteq B$. Conversely, let $b \in B$. If $b \in V$ then $b \in W$; if $b \notin V$, then $\sigma b \in V$, and hence $\sigma b \in W$. Therefore $b \in \langle \sigma \rangle \ltimes W$. Thus $B = \langle \sigma \rangle \ltimes W$.

(d) As $\operatorname{rank} V = \dim V = n$ and $\operatorname{rank} G_0 = 1$, we have $\operatorname{rank} H \leq n+1$. Suppose, by contrary, that $\sigma, \sigma_1, \ldots, \sigma_{n-1}$ generate H. Without loss of generality $\sigma \notin V$. We may assume that $\sigma_i \in V$, for $i = 1, \ldots, n-1$, otherwise replace σ_i by $\sigma\sigma_i$. Put $W = \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$. Then $H = \langle \sigma, W \rangle$ and $|W| = 3^{\dim W} < 3^n$. By (a), $H = \langle \sigma \rangle \ltimes W$, and hence $|H| < 2 \cdot 3^n$. But clearly $|H| = 2 \cdot 3^n$, a contradiction.

(e) If W is a subspace of V of dimension $n-1$, then $G_0 \ltimes W$ is a maximal subgroup of H; so is V. Therefore

$$\Phi(H) \subseteq V \cap \bigcap_{\substack{W \leq V \\ \dim W = n-1}} G_0 \ltimes W = \bigcap_{\substack{W \leq V \\ \dim W = n-1}} W = \{0\}. \qquad ▮$$

Lemma 2.4: *Let a finite group G act on a finite group A_0, and let $\alpha_0 \colon G \ltimes A_0 \to G$ be the canonical projection. Let $m \geq 1$ be an integer. Then there is a finite group A on which G acts, with the following property. Let $\Gamma = G \ltimes A$ and let $\alpha \colon \Gamma \to G$ be the canonical projection. If H is a subgroup of Γ such that $\alpha(H) = G$ and $(\Gamma : H) \leq m$, then there is an epimorphism $\theta \colon H \to G \ltimes A_0$ such that $\alpha_0 \circ \theta = \mathrm{res}_H\, \alpha$.*

Proof:

Part A: *It suffices to find A finitely generated (instead of finite).* Suppose that A is a finitely generated group that has all the required properties except for being finite. Then Γ is also finitely generated, and hence has only finitely many subgroups of index $\leq m|G \ltimes A_0|$. Therefore the intersection N of these subgroups is of finite index in Γ. Clearly, N is a characteristic subgroup of Γ and $N \leq A$. Let $A_1 = A/N$. It follows that A_1 is a finite group. We claim that it has the required property.

Let $\Gamma_1 = \Gamma/N = G \ltimes A_1$, let $\mu \colon \Gamma \to \Gamma_1$ be the quotient map, and let $\alpha_1 \colon \Gamma_1 \to G$ be the map induced from α, that is, $\alpha_1 \circ \mu = \alpha$.

Let H_1 be a subgroup of Γ_1 such that $\alpha_1(H_1) = G$ and $(\Gamma_1 : H_1) \leq m$. Let $H = \mu^{-1}(H_1) \leq \Gamma$. Then $\alpha(H) = G$ and $(\Gamma : H) \leq m$. Hence by assumption there is an epimorphism $\theta \colon H \to G \ltimes A_0$ such that $\alpha_0 \circ \theta = \mathrm{res}_H\, \alpha$.

Since $(\Gamma : H) \leq m$, we have $N \leq H$. Since $(H : \mathrm{Ker}\,\theta) = |G \ltimes A_0|$, we have $(\Gamma : \mathrm{Ker}\,\theta) \leq m|G \ltimes A_0|$, and hence $N \leq \mathrm{Ker}\,\theta$. Therefore θ induces an epimorphism $\theta_1 \colon H_1 \to G \ltimes A_0$ such that $\alpha_0 \circ \theta_1 = \mathrm{res}_{H_1}\, \alpha_1$.

$$\begin{tikzcd}
H \arrow[d] \arrow[dr, "\mu"] \arrow[drr, "\theta"] & & \\
\Gamma \arrow[dr, "\mu"] \arrow[drr, "\alpha"] & H_1 \arrow[r, "\theta_1"'] \arrow[d] & G \ltimes A_0 \arrow[d, "\alpha_0"] \\
& \Gamma_1 \arrow[r, "\alpha_1"'] & G
\end{tikzcd}$$

Thus we may relax the requirement that A be finite by A being finitely generated.

Part B: *Free products.* Let $e = |A_0|$. Let F be the free group on e generators and let $\Gamma = G \star F$ be the free product. Define an epimorphism $\alpha \colon \Gamma \to G$ by letting α be the identity on G and $\alpha(F) = 1$. Let $A = \mathrm{Ker}\,\alpha$; then $\Gamma = GA$ and $G \cap A = 1$, so $\Gamma = G \ltimes A$ and $\alpha \colon G \ltimes A \to G$ is the canonical projection.

Let H be a subgroup of Γ such that $\alpha(H) = G$ and $(\Gamma : H) \leq m$. By the Kurosh Subgroup Theorem [Mas, Theorems VII.5.1, VII.5.2]

$$H = \mathop{\star}_{i=1}^{m}(H \cap G^{\gamma_i}) \star \mathop{\star}_{j=1}^{n}(H \cap F^{\delta_j}) \star E$$

where $\gamma_1, \ldots, \gamma_m, \delta_1, \ldots, \delta_n \in \Gamma$ and E is a finitely generated free group [Mas, Theorem VII.5.3]. Thus H can be written as the free product $H = F_1 \star F_2$, where $F_1 = H \cap F^{\delta_1}$. Since $(F^{\delta_1} : F_1) \leq (\Gamma : H) \leq m < \infty$, the group F_1 is a finitely generated free group of rank

$$\operatorname{rank} F_1 = 1 + (F^{\delta_1} : F_1)(e-1) = e + [(F^{\delta_1} : F_1) - 1](e-1) \geq e$$

[FrJa, Proposition 15.25]. Therefore there exists an epimorphism $\theta_1 \colon F_1 \to A_0$.

Define $\theta \colon H \to G \ltimes A_0$ by letting θ be θ_1 on F_1 and $\mathrm{res}_{F_2}\, \alpha$ on F_2 (here we identify G with its preimage in $G \ltimes A_0$). As $F_1 \leq F^{\delta_1} \leq A$, and hence $\alpha(F_1) = 1$, we get that $\alpha_0 \circ \theta = \mathrm{res}_H\, \alpha$. In particular, $\alpha_0(\theta(H)) = G$; since $\theta(H) \supseteq \theta_1(F_1) = A_0$; thus θ is an epimorphism. ∎

3. Mordellian fields

We recall the following characterization of hilbertian fields (*e.g.* [FrJa, Lemma 12.1]):

LEMMA 3.1: *A field K is hilbertian if and only if for every finite set of absolutely irreducible polynomials $P_1(T,Y), \ldots, P_m(T,Y) \in K[T,Y]$, of degree ≥ 2 in Y, there exist infinitely many $t \in K$ such that none of the polynomials $P_1(t,Y), \ldots, P_m(t,Y) \in K[Y]$ has a root in K.*

It would be interesting to know whether one can take $m = 1$ in the above lemma. Formally, we define:

Definition 3.2: A field K is *mordellian*, if for every absolutely irreducible polynomial $P(T,Y) \in K[T,Y]$ with $\deg_Y P > 1$, there exist infinitely many $t \in K$ such that $P(t,Y) \in K[Y]$ has no root in K. ∎

Clearly, every hilbertian field is mordellian. Thus the question is, whether the converse is true[4]. In this section we show that this is not the case: we produce PAC mordellian fields that are not hilbertian. Recall a field K is P(seudo) A(lgebraically) C(losed) if every curve defined over K has at least one (in fact infinitely many) K-rational points [FrJa,

[4] See [FrJa, Exercise 12.1] for a related problem.

Chapter 10]. Moreover, we show that the mordellian property neither implies nor is implied by the RG-hilbertian property. To show this, we first develop a Galois theoretic characterization of mordellian fields.

Let K be a field, let $\bar{K}$ be its algebraic closure, and let F be a finite Galois extension of $E = K(T)$. Let $t \in K$. Extend $T \mapsto t$ to a place $\phi\colon F \to \bar{K}$; such an extension is unique up to composition with elements of the Galois group $\mathcal{G}(F/E)$ [La, Corollary VII.2.6]. Assume that ϕ is unramified in F; this is true for all but finitely many values of t. The decomposition group D_t of ϕ in F/E is a subgroup of $\mathcal{G}(F/E)$ and it is uniquely determined by t, up to conjugation in $\mathcal{G}(F/E)$. There is an epimorphism $\phi^*\colon G(K) \to D_t \subseteq \mathcal{G}(F/E)$ given by

$$\phi\big(\phi^*(\sigma)z\big) = \sigma\,\phi(z), \tag{1}$$

for all $\sigma \in G(K)$, $z \in F$ integral over $K[T]$. In fact, if F' is the residue field of F, then ϕ^* is the composition of $\mathrm{res}_{F'}\colon G(K) \to \mathcal{G}(F'/K)$ and the isomorphism $\mathcal{G}(F'/K) \to D_t$.

Remark 3.3: Embedding property. Let $E = K(T)$ and L be the algebraic closure of K in F.

(a) Replacing ϕ by $\phi \circ \sigma$ for a suitable $\sigma \in \mathcal{G}(F/E)$, if necessary, we may assume that ϕ is an L-place. It then follows from (1) with $z \in L$ that the following diagram commutes

$$\begin{tikzcd} & G(K) \arrow[dl, "\phi^*"'] \arrow[d, "\mathrm{res}_L"] \\ \mathcal{G}(F/E) \arrow[r, "\mathrm{res}_{F/L}"'] & \mathcal{G}(L/K)\ . \end{tikzcd} \tag{2}$$

(b) Conversely, let $\phi^*\colon G(K) \to \mathcal{G}(F/E)$ be a homomorphism such that (2) commutes. If K is PAC, the field-crossing argument (see [FrJa, Proposition 23.2]) says that there exist infinitely many L-places $\phi\colon F \to \bar{K}$ unramified over E such that $\phi(E) = K$ and (1) holds. In particular, $\phi^*(G(K))$ is the decomposition group of ϕ. Choose ϕ so that $t = \phi(T) \neq \infty$; then ϕ extends $T \mapsto t$. ∎

Now we can express the mordellian property in terms of decomposition groups.

Lemma 3.4: *A field K is mordellian if and only if the following property holds.*

(M1) *Let $F/K(T)$ be a finite Galois extension, let G be its Galois group, and let B be a proper subgroup of G. Then there exist infinitely many $t \in K$ such that $D_t \not\subseteq B^\sigma$ for every $\sigma \in G$.*

Proof: Let $P(T,Y) \in K[T,Y]$ be irreducible, monic in Y, and of degree ≥ 2 in Y. Let F be a finite Galois extension of $K(T)$ that contains the splitting field of $P(T,Y)$ over $K(T)$ and let G be its Galois group. Let y be a root of $P(T,Y)$ in F and let B be the (necessarily proper) subgroup of G that fixes y. Then $\{\sigma y | \sigma \in G\}$ are all the roots of $P(T,Y)$, and $\sigma B \sigma^{-1}$ is the fixed group of $K(T)(\sigma y)$, for each $\sigma \in G$.

Let $t \in K$ be such that $T \mapsto t$ is unramified in F. Extend $T \mapsto t$ to a place $\phi: F \to \bar{K}$ and let D_t be the decomposition group of ϕ in $F/K(T)$. Then $\{\phi(\sigma y) | \sigma \in G\}$ are the roots of $P(t,Y) \in \bar{K}$. We have $\phi(\sigma y) \in K$ iff D_t fixes σy iff $D_t \subseteq \sigma B \sigma^{-1}$.

Thus for all but finitely many $t \in K$ we have:

(3) $P(t,Y)$ has a root in K iff $D_t \subseteq B^\sigma$ for some $\sigma \in G$.

Therefore (M1) implies that K is mordellian. Conversely, let K be mordellian, and let F, G, and B be as in (M1). Let y be a primitive element for the fixed field of B over $K(T)$, integral over $K[T]$. Then the irreducible polynomial $P(T,Y)$ of y over $K(T)$ is in $K[T,Y]$, and so we can apply (3) to get that (M1) holds. ∎

Remark 3.5: In the setup of (M1) let L be the algebraic closure of K in F. We may assume in (M1) that the restriction map $\mathcal{G}(F/K(T)) \to \mathcal{G}(L/K)$ splits. Indeed, by [Ha, Lemma 2.2] there is a finite Galois extension $F'/K(T)$ such that $F \subseteq F'$ and, denoting by L' the algebraic closure of K in F', the map $\mathcal{G}(F'/K(T)) \to \mathcal{G}(L'/K)$ splits. Let G' be its Galois group and let $B' \leq G'$ be the pre-image of B under the restriction map $\mathrm{res}: G' \to G$. If $\phi': F' \to \bar{K}$ is a place and $\phi: F \to \bar{K}$ is its restriction to F, then $\phi^* = \mathrm{res} \circ \phi'^*$. Therefore, $\phi'^*(G(K)) \not\subseteq (B')^{\sigma'}$ for every $\sigma' \in G'$ implies $\phi^*(G(K)) \not\subseteq B^\sigma$ for every $\sigma \in G$. ∎

In the case of PAC fields, Lemma 3.4 leads to the following criterion.

Proposition 3.6: *Let K be a PAC field and let Γ be its absolute Galois group. Then K is mordellian if and only if the following condition holds:*

(M2) *Let $\alpha: G \to A$ be a split epimorphism of finite groups, let $\rho: \Gamma \to A$ be a continuous epimorphism, and let B be a proper subgroup of G. Then there exists a continuous homomorphism $\psi: \Gamma \to G$ such that $\alpha \circ \psi = \rho$ and $\psi(\Gamma)$ is contained in no conjugate of B in G.*

Proof: Suppose that (M2) holds. Let F, G, and B be as in (M1). Let L be the algebraic closure of K in F, let $A = \mathcal{G}(L/K)$, and let $\alpha: G \to A$ and $\rho: \Gamma \to A$ be the restriction maps to L. By Remark 3.5 we may assume that $\alpha: G \to A$ splits. Let ψ be as in (M2). By Remark 3.3(b) there are infinitely many $t \in K$ such that $D_t = \psi(\Gamma)$; for these t, $D_t \not\subseteq B^\sigma$ for every $\sigma \in G$. Thus (M1) holds.

Conversely, assume (M1). Let $\rho\colon\Gamma\to A$, $\alpha\colon G\to A$, and $B\le G$ be as in (M2). Let L be the fixed field of $\operatorname{Ker}\rho$; thus $A=\mathcal{G}(L/K)$ and ρ is the restriction map to L. We will use the following result recently proved in Inverse Galois Theory: if K is an ample field, split embedding problems over $K(T)$ have proper regular solutions ([Po, Main Theorem A] or [HJ, Theorem 6.4]). This result, applied here over the PAC (and so ample) field K, precisely asserts that there exists a Galois extension F of $K(T)$ that contains L and is regular over L, and an isomorphism $\theta\colon G\to\mathcal{G}(F/K(T))$ such that $\mathrm{res}_L\circ\theta=\alpha$. Without loss of generality $G=\mathcal{G}(F/K(T))$ and $\alpha=\mathrm{res}_L$.

By (M1) there is an element $t\in K$ such that $T\mapsto t$ is unramified in F and its extension $\phi\colon F\to\bar K$ defines a homomorphism $\phi^*\colon\Gamma\to G$ such that $\phi^*(\Gamma)=D_t\not\subseteq B^\sigma$ for every $\sigma\in G$. By Remark 3.3(a) we may assume that $\alpha\circ\phi^*=\rho$. ∎

Proposition 3.6 should be compared to the following result which provides a Galois theoretic characterization of the hilbertian and RG-hilbertian properties for PAC fields.

Proposition 3.7 ([FrVo, Theorems A and B]): *Let K be a PAC field. Then*

(a) *K is hilbertian if and only if all finite embedding problems over K are solvable.*

(b) *K is RG-hilbertian if and only if every finite group is a Galois group over K.*

We will now use Proposition 3.6 and Proposition 3.7 to prove the following.

Proposition 3.8: *There exist mordellian PAC fields K_1, K_2 that are not hilbertian and*

(a) *K_1 is not RG-hilbertian.*

(b) *K_2 is RG-hilbertian.*

Proof: Let $\hat F_2$ be the free profinite group on 2 generators. If P is a projective profinite group, then $\Gamma=P\star\hat F_2$ is projective. By [FrJa, Corollary 20.16] there is a PAC field K with absolute Galois group Γ. By Lemma 2.2, Γ satisfies the criterion (M2) of Proposition 3.6, and hence K is mordellian.

(a) In the above, take P to be finitely generated, *e.g.* $P=\hat{\mathbb{Z}}$. Then Γ is also finitely generated, and therefore not every finite group is a quotient of Γ. By Proposition 3.7, K is not RG-hilbertian. In particular, K is not hilbertian.

(b) Let $G_1, G_2, G_3, \dots$ be an enumeration of all finite groups. Let $G = \prod_{i=0}^{\infty} G_i$ and for each $i \geq 0$ let $\pi_i\colon G \to G_i$ be the canonical projection. Let $\rho\colon P \to G$ be the universal Frattini cover of G. Then P is projective [FrJa, Proposition 20.33]. Take Γ and K as above.

Let $\phi\colon \Gamma \to P$ be the epimorphism which is the identity on P and maps $\hat{F}_2$ onto 1. Every finite group G_i is a quotient of Γ (by $\pi_i \circ \rho \circ \phi$). By Proposition 3.7, K is RG-hilbertian; and to show that K is not hilbertian, it suffices to show that Γ is not ω-free, that is, that there is a finite embedding problem for Γ that has no solution.

Without loss of generality G_0 is of order 2, say, $G_0 = \langle c \rangle$. Let $H = H_n = G_0 \ltimes V$ as in Lemma 2.3, where $n \geq 3$, and let $\alpha\colon H \to G_0$ be the canonical projection. We claim that there is no epimorphism $\psi\colon \Gamma \to H$ such that $\alpha \circ \psi = \pi_0 \circ \rho \circ \phi\colon \Gamma \to G_0$.

Assume the contrary. Let $B = \psi(P)$. Then B is not contained in V, since $\alpha(B) = G_0$, while $\alpha(V) = 1$. By Lemma 2.3(c), $B \cong H_m$ for some $m \leq n$. By Lemma 2.3(e), the Frattini subgroup of B is trivial. Therefore ψ maps the Frattini subgroup of P into 1, and hence induces an epimorphism $\bar{\psi}\colon G \to B$ such that $\alpha \circ \bar{\psi} = \pi_0$.

Recall that c is the generator of the subgroup G_0 of G. Let $\sigma = \bar{\psi}(c)$. Since c centralizes G_i, for $i \geq 1$, σ centralizes $\bar{\psi}(G_i)$ in B. Furthermore, $\bar{\psi}(G_i) \leq V$, since $\pi_0(G_i) = 1$. By Lemma 2.3(b), $\bar{\psi}(G_i) = 1$. Hence $\bar{\psi}(G) = \langle \sigma \rangle$. It follows that $\psi(P) = \langle \sigma \rangle$.

Now let $D = \psi(\Gamma)$. Then $D = \langle \sigma, \sigma_1, \sigma_2 \rangle$, where σ_1, σ_2 are the images of the generators of $\hat{F}_2$ in G. By Lemma 2.3(d), $D \neq H$. ∎

4. R-hilbertianity and further specialization properties

The hilbertian property of a field K is that

(Data:)	For every polynomial $P(T,Y) \in K[T,Y]$ with $\deg_Y P \geq 2$ such that
(Assumption:)	$P(T,Y)$ is irreducible in $K(T)[Y]$, there exist infinitely many $t \in K$ such that
(Conclusion:)	$P(t,Y)$ is irreducible in $K[Y]$.

We consider variants of the hilbertian property where the assumption is modified to include the extra hypothesis (R) or/and (G) below and the conclusion about $P(t,Y)$ either remains the Hilbert conclusion or is weakened to be the Mordell conclusion below. Given a polynomial $P(T,Y) \in K[T,Y]$ irreducible in $K(T)[Y]$, the possible extra hypotheses (R) and (G) are:

(R) $P(T,Y)$ is absolutely irreducible,

(G) The function field $K(T)[Y]/(P(T,Y))$ is a Galois extension of $K(T)$.

and the possible conclusions (for $t \in K$) are:
(Hilbert) $P(t,Y)$ is irreducible in $K[Y]$,
(Mordell) $P(t,Y)$ has no root in $K[Y]$.

According to what the conclusion is, these new properties are called hilbertian or mordellian. We add the prefix R and/or G (or no prefix) according to the assumptions that are made on the polynomial $P(T,Y)$.

Examples 4.1: These definitions contain in particular the definitions of "RG-hilbertian" and "mordellian" given respectively in §1 and §3. But they give rise to new ones. For example, a field K is RG-*mordellian* if for every polynomial $P(T,Y) \in K[T,Y]$, absolutely irreducible, with $\deg_Y P \geq 2$ and such that the function field $K(T)[Y]/(P(T,Y))$ is a Galois extension of $K(T)$, there exist infinitely many $t \in K$ such that $P(t,Y)$ has no root in $K[Y]$.

There are some relations between all these specialization properties. Some are classical and some are proved in this paper. Theorem 5.1 (in next section) recapitulates these results. The current section is concerned with the R-hilbertian property. From above, a field K is R-hilbertian if for every polynomial $P(T,Y) \in K[T,Y]$, absolutely irreducible, with $\deg_Y P \geq 2$, there exist infinitely many $t \in K$ such that $P(t,Y)$ is irreducible in $K[Y]$.

Theorem 4.2: *Every PAC R-hilbertian field is hilbertian.*

Proof: Let K be a PAC R-hilbertian field. By Proposition 3.7(a) it suffices to show that every finite embedding problem for $G(K)$ is solvable. In fact, since PAC fields have a projective absolute Galois group, Jarden's Lemma [Mat, p. 231] allows us to restrict our attention to split embedding problems. So let L be a finite Galois extension of K and let its Galois group $G = \mathcal{G}(L/K)$ act on a finite group A_0. Let $\alpha_0 \colon G \ltimes A_0 \to G$ be the canonical projection, and let $\mathrm{res}_L \colon G(K) \to G$ be the restriction map. We have to find an epimorphism $\psi \colon G(K) \to G \ltimes A_0$ such that $\alpha_0 \circ \psi = \mathrm{res}_L$.

Put $m = |G|$ and let A and $\alpha \colon \Gamma = G \ltimes A \to G$ be as in Lemma 2.4. Using [Po, Main Theorem A] or [HJ, Theorem 6.4], as in the proof of Proposition 3.6, we may assume that there is a Galois extension F of $K(T)$ with Galois group Γ such that α is the restriction to L of $\mathcal{G}(F/K(T))$ and F/L is regular. Let E_1 be the fixed field of G in F. Then $E_1 \cap L = K$, and hence E_1 is regular over K. Therefore there is an absolutely irreducible polynomial $P(T,Y) \in K[T,Y]$, monic in Y, a root of which generates E_1 over $K(T)$.

Since K is R-hilbertian, there exist infinitely many $t \in K$ such that $P(t, Y) \in K[Y]$ is irreducible. Choose such an element t so that a place $\phi\colon F \to \bar{K}$ that extends $T \mapsto t$ is unramified over $K(T)$. By Remark 3.3(a) there is a homomorphism $\phi^*\colon G(K) \to \mathcal{G}(F/K(T))$ such that (2) (from §3) commutes. The image H of ϕ^* in $\mathcal{G}(F/K(T))$ is the decomposition group of ϕ. The residue field F' of F contains a root of $P(t, Y)$, and hence $|H| = [F' : K] \geq \deg P = |\Gamma|/|G|$. Therefore $(\Gamma : H) \leq |G|$. Furthermore, $\alpha(H) = \mathrm{res}_L\, G(K) = G$.

By Lemma 2.4 there is an epimorphism $\theta\colon H \to G \ltimes A_0$ such that $\alpha_0 \circ \theta = \mathrm{res}_H\, \alpha = \mathrm{res}_H\, \mathrm{res}_{F/L}$. Put $\psi = \theta \circ \phi^*$; then $\alpha_0 \circ \psi = \mathrm{res}_L$. ∎

5. Concluding remarks.

The next result recapitulates what we know about the relations existing between the various specializations properties that we have introduced.

Theorem 5.1: *All implications shown in the diagram below hold and none of the converses to (2), (3), (4), (5) and (6) holds.*

$$\begin{tikzcd}
& \begin{array}{c}\text{hilbertian}\\ \Leftrightarrow \text{G-hilbertian}\end{array} \arrow[d, Rightarrow, "(1)"'] & \\
& \text{R-hilbertian} \arrow[d, Rightarrow, "(2)"'] & \\
& \text{both mordellian and RG-hilbertian} \arrow[dl, Rightarrow, "(3)"'] \arrow[dr, Rightarrow, "(4)"'] & \\
\begin{array}{c}\text{mordellian}\\ \Leftrightarrow \text{R-mordellian}\end{array} \arrow[dr, Rightarrow, "(5)"'] & & \text{RG-hilbertian} \arrow[dl, Rightarrow, "(6)"'] \\
& \begin{array}{c}\text{G-mordellian}\\ \Leftrightarrow \text{RG-mordellian}\end{array} &
\end{tikzcd}$$

Thus, out of the 8 possible variants of the hilbertian property, there are at least 4 and at most 5 that are non-equivalent. We do not know whether the converse of (1) holds in general; from Theorem 4.2, that is the case for PAC fields.

Proof of Theorem 5.1: Some of the implications are classical. For example, "G-hilbertian ⇒ hilbertian" is proved in [FrJa, Lemma 11.12][5]. Equivalences "mordellian ⇔ R-mordellian" and "G-mordellian ⇔ RG-mordellian" readily follow from the fact that if a polynomial $P(T,Y)$ is irreducible in $K[T,Y]$ but is not absolutely irreducible, then the K-rational points (t,y) on the curve $P(t,y)=0$ are singular points; in particular there are only finitely many of them. Implications (1), (3), (4) and (5) are trivial and implications (2) and (6) hold because the Hilbert conclusion implies the Mordell conclusion.

From Corollary 1.4 the fields $K_{p,\infty}$, $\mathcal{F}_p$ $(p\neq 2)$ are RG-hilbertian, and hence, by (6), G-mordellian, but not hilbertian. In fact, these fields are not even mordellian (see Examples 1.2). It follows that neither the converse to (4) nor the converse to (5) hold. The field K_1 from Proposition 3.8 is mordellian but not RG-hilbertian. In particular, it is RG-mordellian. It follows that neither the converse to (3) nor the converse to (6) hold. Finally, the PAC field K_2 from Proposition 3.8 is both mordellian and RG-hilbertian, but not hilbertian. By Theorem 4.2 it is not even R-hilbertian. Therefore the converse to (2) does not hold. ∎

We end the paper with some related comments.

P-splitting fields. B. Deschamps [Des] introduces the following definition. Given a field K and an irreducible polynomial $P(T,Y)\in K[T,Y]$ with $\deg_Y P\geq 2$, a field K is said to be P-splitting (P-décomposant) if for all $t\in K$ the polynomial $P(t,Y)$ is totally split in $K[Y]$. A P-splitting field is not hilbertian and, in fact, most classical non-hilbertian fields are P-splitting for some polynomial $P(T,Y)$ (Examples 5.2 below). But there are non-hilbertian fields that are not P-splitting for any choice of P. In fact, we show below that "P-splitting for some P" is equivalent to "non G-mordellian" (Remark 5.3).

Examples 5.2: The fields $\mathbb{R}$, $\mathbb{Q}^{tr}$ (field of totally real algebraic numbers), $\mathcal{F}_2$ (pythagorean closure of $\mathbb{Q}$) are $P(T,Y)$-splitting for $P(T,Y)=Y^2-(1+T^2)$.

The fields $\mathbb{Q}_p$ and $\mathbb{Q}^{tp}$ (field of totally p-adic algebraic numbers) are $P(T,Y)$-splitting for $P(T,Y)=Y^p-Y-(pT/(T^2-p))$. More generally,

[5] With the slight adjustment that the extension $K(T,y)/K(T)$ in their proof should be required to be Galois.

let K be the quotient field of a henselian discrete valuation ring. Let $Q(Y) \in K[Y]$ be a monic polynomial with integral coefficients and such that the reduction $q(Y)$ of $Q(Y)$ is totally split and has no multiple roots in the residue field of K (*e.g.* $Q(Y) = Y^2 - Y$) and let π be an element of K of minimal positive valuation. Then K is $P(T,Y)$-splitting for $P(T,Y) = Q(Y) - (\pi T/(T^2 - \pi))$.

Indeed, it is straightforwardly checked that, for each $t \in K$, the element $t/(t^2 - \pi)$ is in the valuation ring of K. Thus for each $t \in K$, the reduction of $P(t,Y)$ equals $q(Y)$ and so is totally split in the residue field of K (with only simple roots). Apply Hensel's lemma to lift each of those roots to a root of $P(t,Y)$ in K.

Remark 5.3: We have: "P-splitting for some $P \Leftrightarrow$ non-G-mordellian". Indeed, suppose K is P-splitting for some polynomial $P(T,Y)$. Let N be the normal closure of the function field $K(T)[Y]/(P(T,Y))$. For all $t \in K$, the specialization of N at t is trivial. So if $Q(T,Y) \in K[T,Y]$ is the irreducible polynomial of a primitive element of the Galois extension $N/K(T)$, then $Q(t,Y)$ is totally split in $K[Y]$; thus the field K is not G-mordellian.

Conversely, suppose K is not G-mordellian. That is, there exists a polynomial $P(T,Y) = a_0(T)Y^d + a_1(T)Y^{d-1} + \cdots + a_d(T) \in K[T,Y]$ with $\deg_Y P \geq 2$, irreducible in $K(T)[Y]$, such that the function field $K(T)[Y]/(P(T,Y))$ is a Galois extension of $K(T)$ and $P(t,Y)$ has a root in K for all but finitely many $t \in K$. Because of the Galois assumption on $P(T,Y)$, we have that $P(t,Y)$ is in fact totally split in $K[Y]$ for all but finitely many $t \in K$. Let $\{t_1, \ldots, t_n\}$ be the finite set of possible exceptions and $p(T) = (T - t_1) \cdots (T - t_n)$. Set then $\widetilde{P}(T,Y) = a_0(T)Y^d + a_1(T)p(T)Y^{d-1} + \cdots + p(T)^d a_d(T)$. It is readily checked that $\widetilde{P}(t,Y)$ is totally split *for all* $t \in K$. Thus K is $\widetilde{P}$-splitting.

Finite extensions. Finite extensions of hilbertian fields are hilbertian (see *e.g.* [FrJa, §11.2]). On the other hand it is unclear whether the same is true for R-hilbertian [resp. RG-hilbertian, mordellian, G-mordellian] fields. However that is the case for PAC RG-hilbertian fields. This easily follows from the criterion of Lemma 3.7(b), since if the IGP holds over a field, then it holds over every finite extension (an easy exercise), and every finite extension of a PAC field is also PAC [FrJa, Corollary 10.7].

The similar question for transcendental extensions of finite type is not interesting: such extensions are automatically hilbertian [FrJa, Theorem 12.10].

Multi-polynomial variants. Other variants of the specialization property can be defined: allow the data to consist of any finite set of polynomials $P_1(T,Y),\dots,P_n(T,Y)$ satisfying the assumptions (instead of a single polynomial $P(T,Y)$) and require that the conclusion be satisfied for each of the specialized polynomials $P_1(t,Y),\dots,P_n(t,Y)$. We add the extra prefix "m" to the name of the property in question when we consider the "multi-polynomial variant" of it.

In fact, several polynomials are involved in the usual definition of "hilbertian". So according to our terminology, "hilbertian" is really "m-hilbertian". But as [FrJa, Lemma 11.12] shows, the two notions actually coincide. Also, the classical Lemma 3.1 shows that "mR-mordellian" implies "hilbertian". It immediately follows that "m-mordellian" and "mR-hilbertian" are equivalent to "hilbertian". On the other hand, "mRG-hilbertian" does not imply "hilbertian" (and does not even imply "mordellian"). Indeed the proof of Theorem 1.3 shows that each real p-radical extension of a hilbertian field contained in $\mathbb{R}$ is mRG-hilbertian. In particular, the fields $K_{p,\infty}$, $\mathcal{F}_p$ $(p \neq 2)$ are examples of mRG-hilbertian but non-mordellian (and so non-hilbertian) fields. Finally, using similar techniques as in §2 and §3, one can show the RG-hilbertian non-hilbertian fields produced in [FrVo] are not mRG-hilbertian. Thus "mRG-hilbertian" is strictly stronger than "RG-hilbertian".

References

[DeDes] P. Dèbes and B. Deschamps, *The Inverse Galois problem over large fields,* in *Geometric Galois Action,* London Math. Soc. Lecture Note Series, Cambridge University Press, (1997), 119–138.

[Des] B. Deschamps, *Corps pythagoriciens, corps P-réduisants,* Proceedings of the “1997 Journées arithmétiques” in Limoges, (to appear).

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

[FrVo] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field,* Annals of Math. **135**, (1992), 469–481.

[Ha] D. Haran, *Hilbertian Fields under Separable Algebraic Extensions,* a preprint.

[HaJa] D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Forum math. **10**, (1998), 329–351.

[Ku] A. G. Kurosh, *The Theory of Groups, Volume II,* Chelsea, New York, 1960.

[La] S. Lang, *Algebra, third edition,* Addison-Wesley, Reading, 1994.

[Mas] W. S. Massey, *Algebraic Topology: An introduction,* Springer, New York, 1984.

[Mat] B. H. Matzat, *Konstruktive Galoistheorie,* Lecture Notes in Mathematics **1284**, Springer, Berlin, 1987.

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

[Ri] P. Ribenboim, *Pythagorean and fermatian fields,* Istituto Nazionale di Alta Matematica, Symposia Mathematica **XV**, (1975), 469–481.

Pierre Dèbes, Univ. Lille, Mathématiques, 59655 Villeneuve d’Ascq Cedex, France.
E-mail address: Pierre.Debes@univ-lille1.fr

Dan Haran, School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel.
E-mail address: haran@math.tau.ac.il