Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Lior BARY-SOROKER et Arno FEHM

Random Galois extensions of Hilbertian fields

Tome 25, n° 1 (2013), p. 31-42.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_1_31_0>

Journal de Théorie des Nombres de Bordeaux **25** (2013), 31-42

Random Galois extensions of Hilbertian fields

par Lior BARY-SOROKER et Arno FEHM

Résumé. Soit L une extension galoisienne d'un corps K hilbertien et dénombrable. Bien que L ne soit pas nécessairement hilbertien, nous montrons qu'il existe beaucoup de grandes sous-extensions de L/K qui le sont.

Abstract. Let L be a Galois extension of a countable Hilbertian field K. Although L need not be Hilbertian, we prove that an abundance of large Galois subextensions of L/K are.

1. Introduction

Hilbert's irreducibility theorem states that if K is a number field and $f \in K[X,Y]$ is an irreducible polynomial that is monic and separable in Y, then there exist infinitely many $a \in K$ such that $f(a,Y) \in K[Y]$ is irreducible. Fields K with this property are consequently called **Hilbertian**, cf. [4], [9], [10].

Let K be a field with a separable closure K_s, let $e \geq 1$, and write $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ for the absolute Galois group of K. For an e-tuple $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$ we denote by

$$[\boldsymbol{\sigma}]_K = \langle \sigma_\nu^\tau \mid \nu = 1, \dots, e \text{ and } \tau \in \mathrm{Gal}(K) \rangle$$

the closed normal subgroup of $\mathrm{Gal}(K)$ that is generated by $\boldsymbol{\sigma}$. For an algebraic extension L/K we let

$$L[\boldsymbol{\sigma}]_K = \{a \in L \mid a^\tau = a, \ \forall \tau \in [\boldsymbol{\sigma}]_K\}$$

be the maximal Galois subextension of L/K that is fixed by each σ_ν, $\nu = 1, \dots, e$. We note that the group $[\boldsymbol{\sigma}]_K$, and hence the field $L[\boldsymbol{\sigma}]_K$, depends on the base field K.

Since $\mathrm{Gal}(K)^e$ is profinite, hence compact, it is equipped with a probability Haar measure. In [7] Jarden proves that if K is countable and Hilbertian, then $K_s[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. This provides a variety of large Hilbertian Galois extensions of K.

Other fields of this type that were studied intensively are the fields $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K$, where K is a number field, S is a finite set of primes of K, and $K_{\mathrm{tot},S}$ is the **field of totally S-adic numbers** over K – the maximal Galois extension of K in which all primes in S totally split; see for

Manuscrit reçu le 12 juin 2012.

example [6] and the references therein for recent developments. Although the absolute Galois group of $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K$ was completely determined in *loc. cit.* (for almost all $\boldsymbol{\sigma}$), the question whether $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K$ is Hilbertian or not remained open. Note that if $\boldsymbol{\sigma} = (1,\dots,1)$, then $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K = K_{\mathrm{tot},S}$ is not Hilbertian, cf. [3]. Similarly, if $\sigma_1,\dots,\sigma_e$ generate a decomposition subgroup of $\mathrm{Gal}(K)$ above a prime p of K, then $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K = K_{\mathrm{tot},S'}$, with $S' = S \cup \{p\}$, is not Hilbertian.

The main objective of this study is to prove the following general result, which, in particular, generalizes Jarden's result and resolves the above question for $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]_K$ affirmatively.

Theorem 1.1. *Let K be a countable Hilbertian field, let $e \geq 1$, and let L/K be a Galois extension. Then $L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Jarden's proof of the case $L = K_s$ is based on, among other results, Roquette's theorem [4, Corollary 27.3.3] and Melnikov's theorem [4, Theorem 25.7.5]: Jarden proves that for almost all $\boldsymbol{\sigma}$, the countable field $K_s[\boldsymbol{\sigma}]_K$ is pseudo algebraically closed. Therefore, by Roquette, $K_s[\boldsymbol{\sigma}]_K$ is Hilbertian if $[\boldsymbol{\sigma}]_K$ is a free profinite group of infinite rank. Then Melnikov's theorem is applied to reduce the proof of the freeness of $[\boldsymbol{\sigma}]_K$ to realizing simple groups as quotients of $[\boldsymbol{\sigma}]_K$.

However, if L is not pseudo algebraically closed (e.g. $L = K_{\mathrm{tot},S}$, whenever $S \neq \emptyset$), then also $L[\boldsymbol{\sigma}]_K$ is never pseudo algebraically closed. Similarly, if $\mathrm{Gal}(L)$ is not projective (again for example $L = K_{\mathrm{tot},S}$ with $S \neq \emptyset$), then $\mathrm{Gal}(L[\boldsymbol{\sigma}]_K)$ is never free. Thus, it seems that Jarden's proof cannot be extended to such fields L. Our proof utilizes Haran's twisted wreath product approach [5]. We can apply this approach whenever L/K has many linearly disjoint subextensions (in the sense of Condition $\mathcal{L}_K$ below). A combinatorial argument then shows that in the remaining case, $L[\boldsymbol{\sigma}]_K$ is a small extension of K, and therefore also Hilbertian.

2. Small extensions and linearly disjoint families

Let $K \subseteq K_1 \subseteq L$ be a tower of fields. We say that L/K_1 satisfies **Condition** $\mathcal{L}_K$ if the following holds:

($\mathcal{L}_K$) *There exists an infinite pairwise linearly disjoint family of finite proper subextensions of L/K_1 of the same degree and Galois over K.*

If a Galois extension satisfies Condition $\mathcal{L}_K$, then one can find linearly disjoint families of subextensions with additional properties:

Lemma 2.1. *Let $(M_i)_i$ be a pairwise linearly disjoint family of Galois extensions of K and let E/K be a finite Galois extension. Then M_i is linearly disjoint from E over K for all but finitely many i.*

Proof. This is clear since E/K has only finitely many subextensions, cf. [1, Lemma 2.5] and its proof. $\square$

Lemma 2.2. *Let $K \subseteq K_1 \subseteq L$ be fields such that L/K is Galois, K_1/K is finite and L/K_1 satisfies Condition $\mathcal{L}_K$. Let M_0/K_1 be a finite extension, and let $d \geq 1$. Then there exist a finite group G with $|G| \geq d$ and an infinite family $(M_i)_{i>0}$ of subextensions of L/K_1 which are Galois over K such that $\mathrm{Gal}(M_i/K_1) \cong G$ for every $i > 0$ and the family $(M_i)_{i\geq 0}$ is linearly disjoint over K_1.*

Proof. By assumption there exists an infinite pairwise linearly disjoint family $(N_i)_{i>0}$ of subextensions of L/K_1 which are Galois over K and of the same degree $n > 1$ over K_1. Iterating Lemma 2.1 gives an infinite subfamily $(N_i')_{i>0}$ of $(N_i)_{i>0}$ such that the family $M_0, (N_i')_{i>0}$ is linearly disjoint over K_1. If we let

$$M_i' = N_{id}' N_{id+1}' \cdots N_{id+d-1}'$$

be the compositum, then the family $M_0, (M_i')_{i>0}$ is linearly disjoint over K_1, and $[M_i' : K_1] = n^d > d$ for every i. Since up to isomorphism there are only finitely many finite groups of order n^d, there is a finite group G of order n^d and an infinite subfamily $(M_i)_{i>0}$ of $(M_i')_{i>0}$ such that $\mathrm{Gal}(M_i/K_1) \cong G$ for all $i > 0$. $\square$

Lemma 2.3. *Let $K \subseteq K_1 \subseteq K_2 \subseteq L$ be fields such that L/K is Galois, K_2/K is finite Galois and L/K_1 satisfies Condition $\mathcal{L}_K$. Then also L/K_2 satisfies Condition $\mathcal{L}_K$.*

Proof. By Lemma 2.2, applied to $M_0 = K_2$, there exists an infinite family $(M_i)_{i>0}$ of subextensions of L/K_1 which are Galois over K, of the same degree $n > 1$ over K_1 and such that the family $K_2, (M_i)_{i>0}$ is linearly disjoint over K_1. Let $M_i' = M_i K_2$. Then $[M_i' : K_2] = [M_i : K_1] = n$, M_i'/K is Galois, and the family $(M_i')_{i>0}$ is linearly disjoint over K_2, cf. [4, Lemma 2.5.11]. $\square$

Recall that a Galois extension L/K is **small** if for every $n \geq 1$ there exist only finitely many intermediate fields $K \subseteq M \subseteq L$ with $[M : K] = n$. Small extensions are related to Condition $\mathcal{L}_K$ by Proposition 2.5 below, for which we give a combinatorial argument using Ramsey's theorem, which we recall for the reader's convenience:

Proposition 2.4 ([8, Theorem 9.1])**.** *Let X be a countably infinite set and $n, k \in \mathbb{N}$. For every partition $X^{[n]} = \bigcup_{i=1}^k Y_i$ of the set of subsets of X of cardinality n into k pieces there exists an infinite subset $Y \subseteq X$ such that $Y^{[n]} \subseteq Y_i$ for some i.*

Proposition 2.5. *Let L/K be a Galois extension. If there exists no finite Galois subextension K_1 of L/K such that L/K_1 satisfies Condition $\mathcal{L}_K$, then L/K is small.*

Proof. Suppose that L/K is not small, so it has infinitely many subextensions of degree m over K, for some $m > 1$. Taking Galois closures we get that for some $1 < d \leq m!$ there exists an infinite family $\mathcal{F}$ of Galois subextensions of L/K of degree d: Indeed, only finitely many extensions of K can have the same Galois closure.

Choose d minimal with this property. For any two distinct Galois subextensions of L/K of degree d over K their intersection is a Galois subextension of L/K of degree less than d over K, and by minimality of d there are only finitely many of those. Proposition 2.4 thus gives a finite Galois subextension K_1 of L/K and an infinite subfamily $\mathcal{F}' \subseteq \mathcal{F}$ such that for any two distinct $M_1, M_2 \in \mathcal{F}'$, $M_1 \cap M_2 = K_1$. Since any two Galois extensions are linearly disjoint over their intersection, it follows that L/K_1 satisfies Condition $\mathcal{L}_K$. $\square$

The converse of Proposition 2.5 holds trivially. The following fact on small extensions will be used in the proof of Theorem 1.1.

Proposition 2.6 ([4, Proposition 16.11.1])**.** *If K is Hilbertian and L/K is a small Galois extension, then L is Hilbertian.*

3. Measure theory

For a profinite group G we denote by μ_G the probability Haar measure on G. We will make use of the following two very basic measure theoretic facts.

Lemma 3.1. *Let G be a profinite group, $H \leq G$ an open subgroup, $S \subseteq G$ a set of representatives of G/H, and $\Sigma_1, \ldots, \Sigma_k \subseteq H$ measurable μ_H-independent sets. Let $\Sigma_i^* = \bigcup_{g \in S} g\Sigma_i$. Then $\Sigma_1^*, \ldots, \Sigma_k^*$ are μ_G-independent.*

Proof. Let $n = [G : H]$. Then for any measurable $X \subseteq H$ we have $\mu_H(X) = n\mu_G(X)$. Since G is the disjoint union of the cosets gH, for $g \in S$, we have that

$$\mu_G(\Sigma_i^*) = \sum_{g \in S} \mu_G(g\Sigma_i) = n\mu_G(\Sigma_i) = \mu_H(\Sigma_i)$$

and

$$\mu_G\left(\bigcap_{i=1}^k \Sigma_i^*\right) = \sum_{g \in S} \mu_G\left(\bigcap_{i=1}^k g\Sigma_i\right) = n\mu_G\left(\bigcap_{i=1}^k \Sigma_i\right) =$$
$$= \mu_H\left(\bigcap_{i=1}^k \Sigma_i\right) = \prod_{i=1}^k \mu_H\left(\Sigma_i\right) = \prod_{i=1}^k \mu_G\left(\Sigma_i^*\right),$$

thus $\Sigma_1^*, \ldots, \Sigma_k^*$ are μ_G-independent. $\square$

Lemma 3.2. *Let (Ω, μ) be a measure space. For each $i \geq 1$ let $A_i \subseteq B_i$ be measurable subsets of Ω. If $\mu(A_i) = \mu(B_i)$ for every $i \geq 1$, then $\mu(\bigcup_{i=1}^\infty A_i) = \mu(\bigcup_{i=1}^\infty B_i)$.*

Proof. This is clear since

$$\left(\bigcup_{i=1}^{\infty} B_i\right) \smallsetminus \left(\bigcup_{i=1}^{\infty} A_i\right) \subseteq \bigcup_{i=1}^{\infty} (B_i \smallsetminus A_i),$$

and $\mu(B_i \smallsetminus A_i) = 0$ for every $i \geq 1$ by assumption. □

4. Twisted wreath products

Let A and $G_1 \leq G$ be finite groups together with a (right) action of G_1 on A. The set of G_1-invariant functions from G to A,

$$\mathrm{Ind}_{G_1}^{G}(A) = \{f \colon G \to A \mid f(\sigma\tau) = f(\sigma)^{\tau},\ \forall \sigma \in G\, \forall \tau \in G_1\},$$

forms a group under pointwise multiplication. Note that $\mathrm{Ind}_{G_1}^{G}(A) \cong A^{[G:G_1]}$. The group G acts on $\mathrm{Ind}_{G_1}^{G}(A)$ from the right by $f^{\sigma}(\tau) = f(\sigma\tau)$, for all $\sigma, \tau \in G$. The **twisted wreath product** is defined to be the semidirect product

$$A \wr_{G_1} G = \mathrm{Ind}_{G_1}^{G}(A) \rtimes G,$$

cf. [4, Definition 13.7.2]. Let $\pi \colon \mathrm{Ind}_{G_1}^{G}(A) \to A$ be the projection given by $\pi(f) = f(1)$.

Lemma 4.1. *Let $G = G_1 \times G_2$ be a direct product of finite groups, let A be a finite G_1-group, and let $I = \mathrm{Ind}_{G_1}^{G}(A)$. Assume that $|G_2| \geq |A|$. Then there exists $\zeta \in I$ such that for every $g_1 \in G_1$, the normal subgroup N of $A \wr_{G_1} G$ generated by $\tau = (\zeta, (g_1, 1))$ satisfies $\pi(N \cap I) = A$.*

Proof. Let $A = \{a_1, \ldots, a_n\}$ with $a_1 = 1$. By assumption, $|G_2| \geq n$, so we may choose distinct elements $h_1, \ldots, h_n \in G_2$ with $h_1 = 1$. For $(g, h) \in G$ we set

$$\zeta(g,h) = \begin{cases} a_i^{g}, & \text{if } h = h_i \text{ for some } i \\ 1, & \text{otherwise.} \end{cases}$$

Then $\zeta \in I$. Since G_1 and G_2 commute in G, for any $h \in G_2$ we have

$$\tau\tau^{-h} = \zeta g_1 (\zeta g_1)^{-h} = \zeta g_1 \cdot g_1^{-1} \zeta^{-h} = \zeta\zeta^{-h} \in N \cap I.$$

Hence,

$$\begin{aligned} a_i^{-1} = a_1 a_i^{-1} &= \zeta(1)\zeta(h_i)^{-1} = (\zeta\zeta^{-h_i})(1) \\ &= (\tau\tau^{-h_i})(1) = \pi(\tau\tau^{-h_i}) \in \pi(N \cap I). \end{aligned}$$

We thus conclude that $A = \pi(N \cap I)$, as claimed. □

Following [5] we say that a tower of fields

$$K \subseteq E' \subseteq E \subseteq N \subseteq \hat{N}$$

realizes a twisted wreath product $A \wr_{G_1} G$ if $\hat{N}/K$ is a Galois extension with Galois group isomorphic to $A \wr_{G_1} G$ and the tower of fields corresponds to the subgroup series

$$A \wr_{G_1} G \;\geq\; \mathrm{Ind}_{G_1}^G(A) \rtimes G_1 \;\geq\; \mathrm{Ind}_{G_1}^G(A) \;\geq\; \ker(\pi) \;\geq\; 1.$$

In particular we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(\hat{N}/E) \arrow[r, "\cong"] \arrow[d, "\mathrm{res}"] & \mathrm{Ind}_{G_1}^G(A) \arrow[d, "\pi"] \\
\mathrm{Gal}(N/E) \arrow[r, "\cong"] & A.
\end{tikzcd}$$

5. Hilbertian fields

We will use the following specialization result for Hilbertian fields:

Lemma 5.1. *Let K_1 be a Hilbertian field, let $\mathbf{x} = (x_1, \ldots, x_d)$ be a finite tuple of variables, let $0 \neq g(\mathbf{x}) \in K_1[\mathbf{x}]$, and consider field extensions M, E, E_1, N of K_1 as in the following diagram.*

$$\begin{tikzcd}
 & M \arrow[r, dash] \arrow[d, dash] & ME_1 \arrow[r, dash] \arrow[d, dash] & ME_1(\mathbf{x}) \arrow[r, dash] \arrow[d, dash] & MN \arrow[d, dash] \\
K_1 \arrow[r, dash] & E \arrow[r, dash] & E_1 \arrow[r, dash] & E_1(\mathbf{x}) \arrow[r, dash] & N
\end{tikzcd}$$

Assume that E, E_1, M are finite Galois extensions of K_1, $E = E_1 \cap M$, N is a finite Galois extension of $K_1(\mathbf{x})$ that is regular over E_1, and let $y \in N$. Then there exists an E_1-place φ of N such that $\boldsymbol{b} = \varphi(\mathbf{x})$ and $\varphi(y)$ are finite, $g(\boldsymbol{b}) \neq 0$, the residue fields of $K_1(\mathbf{x})$, $E_1(\mathbf{x}, y)$ and N are K_1, $E_1(\varphi(y))$ and $\bar{N}$, respectively, where $\bar{N}$ is a Galois extension of K_1 which is linearly disjoint from M over E, and $\mathrm{Gal}(\bar{N}/K_1) \cong \mathrm{Gal}(N/K_1(\mathbf{x}))$.

Proof. E_1 and M are linearly disjoint over E, and N and ME_1 are linearly disjoint over E_1. We thus get that M and N are linearly disjoint over E. Thus N is linearly disjoint from $M(\mathbf{x})$ over $E(\mathbf{x})$, so $N \cap M(\mathbf{x}) = E(\mathbf{x})$.

For every $\mathbf{b} \in K_1^d$ there exists a K_1-place $\varphi_{\mathbf{b}}$ of $K_1(\mathbf{x})$ with residue field K_1 and $\varphi_{\mathbf{b}}(\mathbf{x}) = \mathbf{b}$. It extends uniquely to $ME_1(\mathbf{x})$, and the residue fields of $M(\mathbf{x})$ and $E_1(\mathbf{x})$ are M and E_1, respectively.

Since K_1 is Hilbertian, by [4, Lemma 13.1.1] (applied to the three separable extensions $E_1(\mathbf{x}, y)$, N and MN of $K_1(\mathbf{x})$) there exists $\mathbf{b} \in K_1^d$ with $g(\mathbf{b}) \neq 0$ such that any extension φ of $\varphi_{\mathbf{b}}$ to MN satisfies the following: $\varphi(y)$ is finite, the residue field of $E_1(\mathbf{x}, y)$ is $E_1(\varphi(y))$, the residue fields $\overline{MN}$ and $\overline{N}$ of MN and N, respectively, are Galois over K_1, and φ induces isomorphisms $\mathrm{Gal}(N/K_1(\mathbf{x})) \cong \mathrm{Gal}(\overline{N}/K_1)$ and $\mathrm{Gal}(MN/K_1(\mathbf{x})) \cong \mathrm{Gal}(\overline{MN}/K_1)$.

By Galois correspondence, the latter isomorphism induces an isomorphism of the lattices of intermediate fields of $MN/K_1(\mathbf{x})$ and $\overline{MN}/K_1$. Hence, $N \cap M(\mathbf{x}) = E(\mathbf{x})$ implies that $\overline{N} \cap M = E$, which means that $\overline{N}$ and M are linearly disjoint over E. □

We will apply the following Hilbertianity criterion:

Proposition 5.2 ([5, Lemma 2.4])**.** *Let P be a field and let x be transcendental over P. Then P is Hilbertian if and only if for every absolutely irreducible $f \in P[X,Y]$, monic in Y, and every finite Galois extension P' of P such that $f(x,Y)$ is Galois over $P'(x)$, there are infinitely many $a \in P$ such that $f(a,Y) \in P[Y]$ is irreducible over P'.*

6. Proof of Theorem 1.1

Lemma 6.1. *Let $K \subseteq K_1 \subseteq L$ be fields such that K is Hilbertian, L/K is Galois, K_1/K is finite Galois, and L/K_1 satisfies Condition $\mathcal{L}_K$. Let $e \geq 1$, let $f \in K_1[X,Y]$ be an absolutely irreducible polynomial that is Galois over $K_s(X)$ and let K_1' be a finite separable extension of K_1. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ there exist infinitely many $a \in L[\boldsymbol{\sigma}]_K$ such that $f(a,Y)$ is irreducible over $K_1' \cdot L[\boldsymbol{\sigma}]_K$.*

Proof. Let E be a finite Galois extension of K such that $K_1' \subseteq E$ and f is Galois over $E(X)$ and put $G_1 = \mathrm{Gal}(E/K_1)$. Let x be transcendental over K and y such that $f(x,y) = 0$. Let $F' = K_1(x,y)$ and $F = E(x,y)$. Since $f(X,Y)$ is absolutely irreducible, F'/K_1 is regular, hence $\mathrm{Gal}(F/F') \cong G_1$. Since $f(X,Y)$ is Galois over $E(X)$, $F/K_1(x)$ is Galois (as the compositum of E and the splitting field of $f(x,Y)$ over $K_1(x)$). Then $A = \mathrm{Gal}(F/E(x))$ is a subgroup of $\mathrm{Gal}(F/K_1(x))$, so $G_1 = \mathrm{Gal}(F/F')$ acts on A by conjugation.

$$\begin{tikzcd}[arrows=dash]
F' \arrow[r, "G_1"] \arrow[d] & F \arrow[d, "A"] \\
K_1(x) \arrow[r, "G_1"] & E(x)
\end{tikzcd}$$

Since L/K_1 satisfies Condition $\mathcal{L}_K$, by Lemma 2.2, applied to $M_0 = E$, there exists a finite group G_2 with $d := |G_2| \geq |A|$ and a sequence $(E_i')_{i>0}$ of linearly disjoint subextensions of L/K_1 which are Galois over K with $\mathrm{Gal}(E_i'/K_1) \cong G_2$ such that the family $E, (E_i')_{i>0}$ is linearly disjoint over K_1. Let $E_i = EE_i'$. Then E_i/K is Galois and $\mathrm{Gal}(E_i/K_1) \cong G := G_1 \times G_2$ for every i.

Let $\mathbf{x} = (x_1, \dots, x_d)$ be a d-tuple of variables, and for each i choose a basis $w_{i1}, \dots, w_{id}$ of E_i'/K_1. By [5, Lemma 3.1], for each i we have a tower

$$K_1(\mathbf{x}) \subseteq E_i'(\mathbf{x}) \subseteq E_i(\mathbf{x}) \subseteq N_i \subseteq \hat{N}_i \tag{6.1}$$

that realizes the twisted wreath product $A \wr_{G_1} G$, such that $\hat{N}_i$ is regular over E_i and $N_i = E_i(\mathbf{x})(y_i)$, where $\mathrm{irr}(y_i, E_i(\mathbf{x})) = f(\sum_{\nu=1}^d w_{i\nu}x_\nu, Y)$.

We inductively construct an ascending sequence $(i_j)_{j=1}^\infty$ of positive integers and for each $j \geq 1$ an E_{i_j}-place φ_j of $\hat{N}_{i_j}$ such that

(a) the elements $a_j := \sum_{\nu=1}^d w_{i_j\nu}\varphi_j(x_\nu) \in E_{i_j}'$ are distinct for $j \geq 1$,
(b) the residue field tower of (6.1), for $i = i_j$, under φ_j,

$$K_1 \subseteq E_{i_j}' \subseteq E_{i_j} \subseteq M_{i_j} \subseteq \hat{M}_{i_j}, \tag{6.2}$$

realizes the twisted wreath product $A \wr_{G_1} G$ and M_{i_j} is generated by a root of $f(a_j, Y)$ over E_{i_j},
(c) the family $(\hat{M}_{i_j})_{j=1}^\infty$ is linearly disjoint over E.

Indeed, suppose that $i_1, \dots, i_{j-1}$ and $\varphi_1, \dots, \varphi_{j-1}$ are already constructed and let $M = \hat{M}_{i_1} \cdots \hat{M}_{i_{j-1}}$. By Lemma 2.1 there is $i_j > i_{j-1}$ such that E_{i_j}' is linearly disjoint from M over K_1. Thus, E_{i_j} is linearly disjoint from M over E. Since K is Hilbertian and K_1/K is finite, K_1 is Hilbertian. Applying Lemma 5.1 to M, E, E_{i_j}, $\hat{N}_{i_j}$, and y_{i_j}, gives an E_{i_j}-place φ_j of $\hat{N}_{i_j}$ such that (b) and (c) are satisfied. Choosing g suitably we may assume that $a_j = \varphi_j(\sum_{\nu=1}^d w_{i_j\nu}x_\nu) \notin \{a_1, \dots, a_{j-1}\}$, so also (a) is satisfied.

We now fix j and make the following identifications: $\mathrm{Gal}(\hat{M}_{i_j}/K_1) = A \wr_{G_1} G = I \rtimes (G_1 \times G_2)$, $\mathrm{Gal}(\hat{M}_{i_j}/E_{i_j}) = I$, $\mathrm{Gal}(M_{i_j}/E_{i_j}) = A$. The restriction map $\mathrm{Gal}(\hat{M}_{i_j}/E_{i_j}) \to \mathrm{Gal}(M_{i_j}/E_{i_j})$ is thus identified with $\pi : A \wr_{G_1} G \to A$, and $\mathrm{Gal}(\hat{M}_{i_j}/M_{i_j}) = \ker(\pi)$. Let $\zeta \in I := \mathrm{Ind}_{G_1}^G(A)$ be as in Lemma 4.1 and let Σ_j^* be the set of those $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ such that for every $\nu \in \{1, \dots, e\}$, $\sigma_\nu|_{\hat{M}_{i_j}} = (\zeta, (g_{\nu 1}, 1)) \in I \rtimes (G_1 \times G_2)$ for some $g_{\nu 1} \in G_1$. Then the normal subgroup N generated by $\boldsymbol{\sigma}|_{\hat{M}_{i_j}}$ in $\mathrm{Gal}(\hat{M}_{i_j}/K_1)$ satisfies $\pi(N \cap I) = A$.

Now fix $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_e) \in \Sigma_j^*$ and let $P = L[\boldsymbol{\sigma}]_K$ and $Q = K_s[\boldsymbol{\sigma}]_{K_1}$. Then

$$P = L \cap K_s[\boldsymbol{\sigma}]_K \subseteq K_s[\boldsymbol{\sigma}]_K \subseteq K_s[\boldsymbol{\sigma}]_{K_1} = Q.$$

Since E_{i_j}' is fixed by σ_ν, $\nu = 1, \dots, e$, and Galois over K, we have $E_{i_j}' \subseteq P \subseteq Q$. Thus $a_j \in P$ and $E_{i_j}Q = EQ$. Therefore, since M_{i_j} is generated by a root of $f(a_j, Y)$ over E_{i_j}, we get that $M_{i_j}Q$ is generated by a root of $f(a_j, Y)$ over EQ.

$$\begin{tikzcd}
Q \arrow[r, dash] \arrow[d, dash] & E_{i_j}Q \arrow[r, dash] \arrow[d, dash] & M_{i_j}Q \arrow[r, dash] \arrow[d, dash] & \hat{M}_{i_j}Q \arrow[d, dash] \\
\hat{M}_{i_j}\cap Q \arrow[r, dash] \arrow[rrr, dotted, dash, bend right=15, "N"'] & (\hat{M}_{i_j}\cap Q)E_{i_j} \arrow[r, dash] \arrow[d, dash] & (\hat{M}_{i_j}\cap Q)M_{i_j} \arrow[r, dash] \arrow[d, dash] & \hat{M}_{i_j} \\
& E_{i_j} \arrow[r, dash, "A"'] \arrow[urr, dotted, dash, "I"] & M_{i_j} \arrow[ur, dotted, dash, "\ker(\pi)"'] &
\end{tikzcd}$$

The equality $N = \mathrm{Gal}(\hat{M}_{i_j}/\hat{M}_{i_j}\cap Q)$ gives

$$\mathrm{Gal}(\hat{M}_{i_j}Q/M_{i_j}Q) \cong \mathrm{Gal}(\hat{M}_{i_j}/(\hat{M}_{i_j}\cap Q)M_{i_j}) = N \cap \ker(\pi)$$

and

$$\mathrm{Gal}(\hat{M}_{i_j}Q/E_{i_j}Q) \cong \mathrm{Gal}(\hat{M}_{i_j}/(\hat{M}_{i_j}\cap Q)E_{i_j}) = N \cap I.$$

Therefore,

$$\mathrm{Gal}(M_{i_j}Q/E_{i_j}Q) \cong (N\cap I)/(N\cap\ker(\pi)) \cong \pi(N\cap I) = A.$$

Since $|A| = \deg_Y f(X,Y) = \deg f(a_j,Y)$, we get that $f(a_j,Y)$ is irreducible over EQ. Finally, we have $K_1'P \subseteq EP \subseteq EQ$, therefore $f(a_j,Y)$ is irreducible over $K_1'P$.

It suffices to show that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ lie in infinitely many Σ_j^*. Let Σ_j be the set of those $\boldsymbol{\sigma} \in \mathrm{Gal}(E)^e$ such that

$$\sigma_\nu|_{\hat{M}_{i_j}} = (\zeta,(1,1)) \in I \rtimes (G_1\times G_2) = \mathrm{Gal}(\hat{M}_{i_j}/K_1)$$

for every $\nu \in \{1,\dots,e\}$. This is a coset of $\mathrm{Gal}(\hat{M}_{i_j})$. Since, by (c), the family $(\hat{M}_{i_j})_{j=1}^\infty$ is linearly disjoint over E, the sets $\mathrm{Gal}(\hat{M}_{i_j})$ are independent for $\mu_{\mathrm{Gal}(E)^e}$. Thus, by [4, Lemma 18.3.7], also the sets Σ_j are independent for $\mu_{\mathrm{Gal}(E)^e}$. Moreover, for every $g \in G_1 = \mathrm{Gal}(E/K_1)$ we can fix a $\hat{g} \in \mathrm{Gal}(K_1)$ such that $\hat{g}|_{\hat{M}_{i_j}} = (1,(g,1))$ for every j. Then

$$S = \{(\hat{g}_1,\dots,\hat{g}_e) : g_1,\dots,g_e \in G_1\}$$

is a set of representatives for the right cosets of $\mathrm{Gal}(E)^e$ in $\mathrm{Gal}(K_1)^e$, and $\Sigma_j^* = \bigcup_{g\in S}\Sigma_j g$ for every j. Therefore, Lemma 3.1 implies that the sets Σ_j^* are independent for $\mu = \mu_{\mathrm{Gal}(K_1)^e}$. Moreover,

$$\mu(\Sigma_j^*) = \frac{|G_1|^e}{|A \wr_{G_1} G|^e} > 0$$

does not depend on j, so $\sum_{j=1}^\infty \mu(\Sigma_j^*) = \infty$. It follows from the Borel-Cantelli lemma [4, Lemma 18.3.5] that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ lie in infinitely many $\boldsymbol{\sigma} \in \Sigma_j^*$. $\square$

Proposition 6.2. *Let $K \subseteq K_1 \subseteq L$ be fields such that K is countable Hilbertian, L/K is Galois, K_1/K is finite Galois and L/K_1 satisfies Condition $\mathcal{L}_K$. Let $e \geq 1$. Then $L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$.*

Proof. Let $\mathcal{F}$ be the set of all triples (K_2, K_2', f), where K_2 is a finite subextension of L/K_1 which is Galois over K, K_2'/K_2 is a finite separable extension (inside a fixed separable closure L_s of L), and $f(X,Y) \in K_2[X,Y]$ is an absolutely irreducible polynomial that is Galois over $K_s(X)$. Since K is countable, the family $\mathcal{F}$ is also countable. If $(K_2, K_2', f) \in \mathcal{F}$, then K_2 is Hilbertian ([4, Corollary 12.2.3]) and L/K_2 satisfies Condition $\mathcal{L}_K$ (Lemma 2.3), hence Lemma 6.1 gives a set $\Sigma'_{(K_2,K_2',f)} \subseteq \mathrm{Gal}(K_2)^e$ of full measure in $\mathrm{Gal}(K_2)^e$ such that for every $\boldsymbol{\sigma} \in \Sigma'_{(K_2,K_2',f)}$ there exist infinitely many $a \in L[\boldsymbol{\sigma}]_K$ such that $f(a,Y)$ is irreducible over $K_2' \cdot L[\boldsymbol{\sigma}]_K$. Let

$$\Sigma_{(K_2,K_2',f)} = \Sigma'_{(K_2,K_2',f)} \cup (\mathrm{Gal}(K_1)^e \smallsetminus \mathrm{Gal}(K_2)^e).$$

Then $\Sigma_{(K_2,K_2',f)}$ has measure 1 in $\mathrm{Gal}(K_1)^e$. We conclude that the measure of $\Sigma = \bigcap_{(K_2,K_2',f)\in\mathcal{F}} \Sigma_{(K_2,K_2',f)}$ is 1.

Fix a $\boldsymbol{\sigma} \in \Sigma$ and let $P = L[\boldsymbol{\sigma}]_K$. Let $f \in P[X,Y]$ be absolutely irreducible and monic in Y, and let P' be a finite Galois extension of P such that $f(X,Y)$ is Galois over $P'(X)$. In particular, f is Galois over $K_s(X)$. Choose a finite extension K_2/K_1 which is Galois over K such that $K_2 \subseteq P \subseteq L$ and $f \in K_2[X,Y]$. Let K_2' be a finite extension of K_2 such that $PK_2' = P'$. Then $\boldsymbol{\sigma} \in \mathrm{Gal}(K_2)^e$. Since, in addition, $\boldsymbol{\sigma} \in \Sigma_{(K_2,K_2',f)}$, we get that $\boldsymbol{\sigma} \in \Sigma'_{(K_2,K_2',f)}$. Thus there exist infinitely many $a \in P$ such that $f(a,Y)$ is irreducible over $PK_2' = P'$. So, by Proposition 5.2, P is Hilbertian. $\square$

Remark. The proof of Proposition 6.2 actually gives a stronger assertion: Under the assumptions of the proposition, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ the field $K_s[\boldsymbol{\sigma}]_{K_1}$ is Hilbertian over $L[\boldsymbol{\sigma}]_K$ in the sense of [2, Definition 7.2]. In particular, if L/K satisfies Condition $\mathcal{L}_K$ (this holds for example for $L = K_{\mathrm{tot},S}$ from the introduction), then $K_s[\boldsymbol{\sigma}]_K$ is Hilbertian over $L[\boldsymbol{\sigma}]_K$.

Proof of Theorem 1.1. Let K be a countable Hilbertian field, let $e \geq 1$, and let L/K be a Galois extension. We need to prove that $L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

Let $\mathcal{F}$ be the set of finite Galois subextensions K_1 of L/K for which L/K_1 satisfies Condition $\mathcal{L}_K$. Note that $\mathcal{F}$ is countable, since K is.

Let $\Omega = \mathrm{Gal}(K)^e$, let $\mu = \mu_\Omega$, and let

$$\Sigma = \{\boldsymbol{\sigma} \in \Omega : L[\boldsymbol{\sigma}]_K \text{ is Hilbertian}\}.$$

For $K_1 \in \mathcal{F}$ let $\Omega_{K_1} = \mathrm{Gal}(K_1)^e$ and $\Sigma_{K_1} = \Omega_{K_1} \cap \Sigma$. Note that

$$\Omega_{K_1} = \{\boldsymbol{\sigma} \in \Omega : K_1 \subseteq L[\boldsymbol{\sigma}]_K\}.$$

By Proposition 6.2, $\mu(\Sigma_{K_1}) = \mu(\Omega_{K_1})$ for each K_1. Let

$$\Delta \;:=\; \Omega \smallsetminus \bigcup_{K_1\in\mathcal{F}} \Omega_{K_1} \;=\; \{\boldsymbol{\sigma}\in\Omega : K_1 \not\subseteq L[\boldsymbol{\sigma}]_K \text{ for all } K_1\in\mathcal{F}\}\,.$$

If $\boldsymbol{\sigma}\in\Delta$, then $L[\boldsymbol{\sigma}]_K/K$ is small by Proposition 2.5, so $L[\boldsymbol{\sigma}]_K$ is Hilbertian by Proposition 2.6. Thus, $\Delta\subseteq\Sigma$. Since $\Omega = \Delta\cup\bigcup_{K_1\in\mathcal{F}}\Omega_{K_1}$, Lemma 3.2 implies that

$$\mu(\Sigma) = \mu\left((\Sigma\cap\Delta)\cup\bigcup_{K_1\in\mathcal{F}}\Sigma_{K_1}\right) = \mu\left(\Delta\cup\bigcup_{K_1\in\mathcal{F}}\Omega_{K_1}\right) = \mu(\Omega) = 1,$$

which concludes the proof of the theorem. □

Acknowledgements

The authors would like to express their sincere thanks to Moshe Jarden for pointing out a subtle gap in a previous version and for many useful suggestions and remarks. They also thank the referee for his or her numerous suggestions. This research was supported by the Lion Foundation Konstanz – Tel Aviv and the Alexander von Humboldt Foundation.

References

[1] Lior Bary-Soroker, *On the characterization of Hilbertian fields*. International Mathematics Research Notices, 2008.

[2] Lior Bary-Soroker, *On pseudo algebraically closed extensions of fields*. Journal of Algebra **322(6)** (2009), 2082–2105.

[3] Lior Bary-Soroker and Arno Fehm, *On fields of totally S-adic numbers*. http://arxiv.org/abs/1202.6200, 2012.

[4] M. Fried and M. Jarden, *Field Arithmetic*. Ergebnisse der Mathematik III **11**. Springer, 2008. 3rd edition, revised by M. Jarden.

[5] Dan Haran, *Hilbertian fields under separable algebraic extensions*. Invent. Math. **137(1)** (1999), 113–126.

[6] Dan Haran, Moshe Jarden, and Florian Pop, *The absolute Galois group of subfields of the field of totally S-adic numbers*. Functiones et Approximatio, Commentarii Mathematici, 2012.

[7] Moshe Jarden, *Large normal extension of Hilbertian fields*. Mathematische Zeitschrift **224** (1997), 555–565.

[8] Thomas J. Jech, *Set Theory*. Springer, 2002.

[9] Serge Lang, *Diophantine Geometry*. Interscience Publishers, 1962.

[10] Jean-Pierre Serre, *Topics in Galois Theory*. Jones and Bartlett Publishers, 1992.

Lior Bary-Soroker
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
Israel
E-mail: `barylior@post.tau.ac.il`

Arno Fehm
Universität Konstanz
Fachbereich Mathematik und Statistik
Fach D 203
78457 Konstanz
Germany
E-mail: `arno.fehm@uni-konstanz.de`