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>

© Société Arithmétique de Bordeaux, 2013, tous droits réservés.

L’accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l’accord avec les conditions générales d’utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l’utilisation à fin strictement personnelle du copiste est constitutive d’une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.
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 $\text{Gal}(K) = \text{Gal}(K_s/K)$ for the absolute Galois group of $K$. For an $e$-tuple $\sigma = (\sigma_1, \ldots, \sigma_e) \in \text{Gal}(K)^e$ we denote by $[\sigma]_K = \langle \sigma_\nu^\tau \mid \nu = 1, \ldots, e \text{ and } \tau \in \text{Gal}(K) \rangle$ the closed normal subgroup of $\text{Gal}(K)$ that is generated by $\sigma$. For an algebraic extension $L/K$ we let $L[\sigma]_K = \{ a \in L \mid a^\tau = a, \ \forall \tau \in [\sigma]_K \}$ be the maximal Galois subextension of $L/K$ that is fixed by each $\sigma_\nu$, $\nu = 1, \ldots, e$. We note that the group $[\sigma]_K$, and hence the field $L[\sigma]_K$, depends on the base field $K$.

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

Other fields of this type that were studied intensively are the fields $K_{\text{tot},S}[\sigma]_K$, where $K$ is a number field, $S$ is a finite set of primes of $K$, and $K_{\text{tot},S}$ 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 $K_{\text{tot},S}[\sigma]_K$ was completely determined in \textit{loc. cit.} (for almost all $\sigma$), the question whether $K_{\text{tot},S}[\sigma]_K$ is Hilbertian or not remained open. Note that if $\sigma = (1, \ldots, 1)$, then $K_{\text{tot},S}[\sigma]_K = K_{\text{tot},S}$ is not Hilbertian, cf. [3]. Similarly, if $\sigma_1, \ldots, \sigma_e$ generate a decomposition subgroup of $\text{Gal}(K)$ above a prime $p$ of $K$, then $K_{\text{tot},S}[\sigma]_K = K_{\text{tot},S'}$, 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 $K_{\text{tot},S}[\sigma]_K$ affirmatively.

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

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 $\sigma$, the countable field $K_s[\sigma]_K$ is pseudo algebraically closed. Therefore, by Roquette, $K_s[\sigma]_K$ is Hilbertian if $[\sigma]_K$ is a free profinite group of infinite rank. Then Melnikov’s theorem is applied to reduce the proof of the freeness of $[\sigma]_K$ to realizing simple groups as quotients of $[\sigma]_K$.

However, if $L$ is not pseudo algebraically closed (e.g. $L = K_{\text{tot},S}$, whenever $S \neq \emptyset$), then also $L[\sigma]_K$ is never pseudo algebraically closed. Similarly, if $\text{Gal}(L)$ is not projective (again for example $L = K_{\text{tot},S}$ with $S \neq \emptyset$), then $\text{Gal}(L[\sigma]_K)$ 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 $L_K$ below). A combinatorial argument then shows that in the remaining case, $L[\sigma]_K$ 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 $L_K$** if the following holds:

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 $L_K$, 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 $i$. 
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 $\text{Gal}(M_i/K_1) \cong G$ 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 $K_1$. By 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 $M'_i = N'_i \cdot N'_{i+1} \cdots N'_{i+d-1}$ 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 $\text{Gal}(M_i/K_1) \cong G$ for all $i > 0$. □

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]. □

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 \( K \) 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 \( \mathcal{L}_K \). □

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 \( \mu_G \) 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 \( \mu_H \)-independent sets. Let \( \Sigma_i^* = \bigcup_{g \in S} g\Sigma_i \). Then \( \Sigma_1^*, \ldots, \Sigma_k^* \) are \( \mu_G \)-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

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

thus \( \Sigma_1^*, \ldots, \Sigma_k^* \) are \( \mu_G \)-independent. □

**Lemma 3.2.** Let \( (\Omega, \mu) \) be a measure space. For each \( i \geq 1 \) let \( A_i \subseteq B_i \) be measurable subsets of \( \Omega \). 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
\[ \left( \bigcup_{i=1}^{\infty} B_i \right) \setminus \left( \bigcup_{i=1}^{\infty} A_i \right) \subseteq \bigcup_{i=1}^{\infty} (B_i \setminus A_i), \]
and \( \mu(B_i \setminus A_i) = 0 \) for every \( i \geq 1 \) by assumption.

\[ \square \]

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 \( A \),
\[ \text{Ind}^G_{G_1}(A) = \{ f : G \to A \mid f(\sigma \tau) = f(\sigma)^\tau, \ \forall \sigma \in G \forall \tau \in G_1 \}, \]
forms a group under pointwise multiplication. Note that \( \text{Ind}^G_{G_1}(A) \cong A^{[G : G_1]} \).

The group \( G \) acts on \( \text{Ind}^G_{G_1}(A) \) 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
\[ A \rtimes_{G_1} G = \text{Ind}^G_{G_1}(A) \rtimes_{G_1} G, \]
cf. [4, Definition 13.7.2]. Let \( \pi : \text{Ind}^G_{G_1}(A) \to A \) 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 \( I = \text{Ind}^G_{G_1}(A) \). 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 \( A \rtimes_{G_1} G \) 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,
\[ a_i^{-1} = a_1 a_i^{-1} = \zeta(1)(\zeta(h_i))^{-1} = (\zeta \zeta^{-h_i})(1) \]
\[ = (\tau \tau^{-h_i})(1) = \pi(\tau \tau^{-h_i}) \in \pi(N \cap I). \]
We thus conclude that \( A = \pi(N \cap I) \), as claimed.

\[ \square \]

Following [5] we say that a tower of fields
\[ K \subseteq E' \subseteq E \subseteq N \subseteq \hat{N} \]
realizes a twisted wreath product $A \rtimes G_1$ if $\hat{N}/K$ is a Galois extension with Galois group isomorphic to $A \rtimes G_1$ and the tower of fields corresponds to the subgroup series

$$A \rtimes G_1 \supseteq \text{Ind}_{G_1}^G(\hat{A}) \rtimes G_1 \supseteq \text{Ind}_{G_1}^G(A) \supseteq \ker(\pi) \supseteq 1.$$ 

In particular we have the following commutative diagram:

$$\begin{array}{ccc}
\text{Gal}(\hat{N}/E) & \cong & \text{Ind}_{G_1}^G(\hat{A}) \\
\downarrow \text{res} & & \downarrow \pi \\
\text{Gal}(N/E) & \cong & A.
\end{array}$$

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.

$$\begin{array}{ccccc}
M & \longrightarrow & ME_1 & \longrightarrow & ME_1(\mathbf{x}) \longrightarrow & MN \\
\mid & & \mid & & \mid & \\
K_1 & \longrightarrow & E & \longrightarrow & E_1 \longrightarrow & E_1(\mathbf{x}) \longrightarrow & N
\end{array}$$

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 $\varphi$ of $N$ such that $b = \varphi(\mathbf{x})$ and $\varphi(y)$ are finite, $g(b) \neq 0$, the residue fields of $K_1(\mathbf{x})$, $E_1(\mathbf{x}, y)$ and $N$ are $K_1$, $E_1(\varphi(y))$ and $\hat{N}$, respectively, where $\hat{N}$ is a Galois extension of $K_1$ which is linearly disjoint from $M$ over $E$, and $\text{Gal}(\hat{N}/K_1) \cong \text{Gal}(N/K_1(\mathbf{x}))$.

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 $M(x)$ over $E(x)$, so $N \cap M(x) = E(x)$.

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

Since $K_1$ is Hilbertian, by [4, Lemma 13.1.1] (applied to the three separable extensions $E_1(x, y)$, $N$ and $MN$ of $K_1(x)$) there exists $b \in K_1^d$ with $g(b) \neq 0$ such that any extension $\varphi$ of $\varphi_b$ to $MN$ satisfies the following: $\varphi(y)$ is finite, the residue field of $E_1(x, y)$ is $E_1(\varphi(y))$, the residue fields $MN$ and $\hat{N}$ of $MN$ and $N$, respectively, are Galois over $K_1$, and $\varphi$ induces isomorphisms $\text{Gal}(N/K_1(\mathbf{x})) \cong \text{Gal}(\hat{N}/K_1)$ and $\text{Gal}(MN/K_1(\mathbf{x})) \cong \text{Gal}(MN/K_1)$.
By Galois correspondence, the latter isomorphism induces an isomorphism of the lattices of intermediate fields of $MN/K_1(x)$ and $MN/K_1$. Hence, $N \cap M(x) = E(x)$ implies that $N \cap M = E$, which means that $N$ 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 $K[x]$, and let $K_1'$ be a finite separable extension of $K_1$. Then for almost all $\sigma \in \text{Gal}(K_1)^e$ there exist infinitely many $a \in L[\sigma]_K$ such that $f(a,Y) \in L[\sigma]_K$ is irreducible over $K_1' \cdot L[\sigma]_K$.

**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 $G_1 = \text{Gal}(E/K_1)$. 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 $\text{Gal}(F/F') \cong G_1$. 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 $A = \text{Gal}(F/E(x))$ is a subgroup of $\text{Gal}(F/K_1(x))$, so $G_1 = \text{Gal}(F/F')$ acts on $A$ by conjugation.

\[
\begin{array}{ccc}
F' & \xrightarrow{G_1} & F \\
| & & | \\
K_1(x) & \xrightarrow{G_1} & E(x) \\
\end{array}
\]

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 $\text{Gal}(E'_i/K_1) \cong G_2$ such that the family $E, (E'_i)_{i>0}$ is linearly disjoint over $K_1$. Let $E_i = E E'_i$. Then $E_i/K$ is Galois and $\text{Gal}(E_i/K_1) \cong G := G_1 \times G_2$ for every $i$. 
Let $x = (x_1, \ldots, x_d)$ be a $d$-tuple of variables, and for each $i$ choose a basis $w_{i1}, \ldots, w_{id}$ of $E'_i/K_1$. By [5, Lemma 3.1], for each $i$ we have a tower

$$K_1(x) \subseteq E'_i(x) \subseteq E_i(x) \subseteq N_i \subseteq \hat{N}_i \subseteq \cdots$$

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

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

(a) the elements $\varphi_j(x_{ij}, Y) \in E'_{ij}$ are distinct for $j \geq 1$,

(b) the residue field tower of $(6.1)$, for $i = ij$, under $\varphi_j$,

$$K_1 \subseteq E'_{ij} \subseteq E_{ij} \subseteq M_{ij} \subseteq \hat{M}_{ij},$$

realizes the twisted wreath product $A \wr_{G_1} G$ and $M_{ij}$ is generated by a root of $f(a_{ij}, Y)$ over $E_{ij}$,

(c) the family $(\hat{M}_{ij})_{j=1}^\infty$ is linearly disjoint over $E$.

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

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

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

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

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

The equality $N = \text{Gal}(\hat{M}_i / \hat{M}_i \cap Q)$ gives

$$\text{Gal}(\hat{M}_i Q / M_i Q) \cong \text{Gal}(\hat{M}_i / (\hat{M}_i \cap Q) M_i) = N \cap \ker(\pi)$$

and

$$\text{Gal}(\hat{M}_i Q / E_i Q) \cong \text{Gal}(\hat{M}_i / (\hat{M}_i \cap Q) E_i) = N \cap I.$$  

Therefore,

$$\text{Gal}(M_i Q / E_i Q) \cong (N \cap I) / (N \cap \ker(\pi)) \cong \pi(N \cap I) = A.$$  

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 $\sigma \in \text{Gal}(K_1)^e$ lie in infinitely many $\Sigma^*_j$. Let $\Sigma^*_j$ be the set of those $\sigma \in \text{Gal}(E)^e$ such that

$$\sigma|_{\hat{M}_i} = (\zeta, (1, 1)) \in I \times (G_1 \times G_2) = \text{Gal}(\hat{M}_i / K_1)$$

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

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

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

$$\mu(\Sigma^*_j) = \frac{|G_1|^e}{|A|_{G_1} |G|^e} > 0$$

do 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 $\sigma \in \text{Gal}(K_1)^e$ lie in infinitely many $\sigma \in \Sigma^*_j$.  

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 $L[\sigma]_K$ is Hilbertian for almost all $\sigma \in \text{Gal}(K_1)^e$.

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 $L_0$ 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 $\Sigma'_{(K_2, K'_2, f)} \subseteq \text{Gal}(K_2)^e$ of full measure in $\text{Gal}(K_2)^e$ such that for every $\sigma \in \Sigma_{(K_2, K'_2, f)}$ there exist infinitely many $a \in L[\sigma]_K$ such that $f(a, Y)$ is irreducible over $K'_2 \cdot L[\sigma]_K$. Let

$$\Sigma_{(K_2, K'_2, f)} = \Sigma'_{(K_2, K'_2, f)} \cup (\text{Gal}(K_1)^e \setminus \text{Gal}(K_2)^e).$$

Then $\Sigma_{(K_2, K'_2, f)}$ has measure 1 in $\text{Gal}(K_1)^e$. 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 $\sigma \in \Sigma$ and let $P = L[\sigma]_K$. 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 $\sigma \in \text{Gal}(K_2)^e$. Since, in addition, $\sigma \in \Sigma_{(K_2, K'_2, f)}$, we get that $\sigma \in \Sigma'_{(K_2, K'_2, f)}$. 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.

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

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 $L[\sigma]_K$ is Hilbertian for almost all $\sigma \in \text{Gal}(K)^e$.

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

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

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

$$\Omega_{K_1} = \{\sigma \in \Omega : K_1 \subseteq L[\sigma]_K\}.$$
By Proposition 6.2, $\mu(\Sigma_{K_1}) = \mu(\Omega_{K_1})$ for each $K_1$. Let

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

If $\sigma \in \Delta$, then $L[\sigma]_K/K$ is small by Proposition 2.5, so $L[\sigma]_K$ 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. $\square$

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

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