MATHEMATICA, 62 (85), N° 1, 2020, pp. 61–72

RANDOM GALOIS EXTENSIONS OF HILBERTIAN RINGS

MOSHE JARDEN and AHAROM RAZON

Abstract. Let R be a countable Hilbertian ring with quotient field K and let L be a Galois extension of K. We generalize a result of Lior Bary-Soroker and Arno Fehm from fields to rings and prove that, for an abundance of large Galois extensions N of K within L, the integral closure of R in N is Hilbertian.

MSC 2010. 12E30
Key words. Hilbertian ring.

1. INTRODUCTION

Let R be an integral domain with quotient field K. Let $\mathbf{T} = (T_1, \dots, T_r)$ be an r-tuple of indeterminates and let X be an additional indeterminate. Given irreducible polynomials $f_1, \dots, f_m \in K(\mathbf{T})[X]$ that are separable in X, the set $H_K(f_1, \dots, f_m; g)$ of all $\mathbf{a} \in K^r$ such that $f_1(\mathbf{a}, X), \dots, f_m(\mathbf{a}, X)$ are defined and irreducible in $K[X]$ is a *separable Hilbert subset* of K^r. We say that R is a *Hilbertian ring* if $H \cap R^r \neq \emptyset$ for every positive integer r and every separable Hilbert subset H of K^r.

Let K be a field with a separable algebraic closure K_{sep}, let e be a positive integer and write $\mathrm{Gal}(K) = \mathrm{Gal}(K_{\mathrm{sep}}/K)$ for the absolute Galois group of K. For a Galois extension L/K and for an e-tuple $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$ we let

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

be the closed normal subgroup of $\mathrm{Gal}(K)$ that is generated by $\sigma_1, \dots, \sigma_e$. We also consider the maximal Galois subextension

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

of L/K that is fixed by each σ_ν, $\nu = 1, \dots, e$. Note that the group $[\boldsymbol{\sigma}]_K$ and the field $L[\boldsymbol{\sigma}]_K$ depend on the base field K.

Since $\mathrm{Gal}(K)^e$ is profinite, hence compact, it is equipped with a probability Haar measure [2, §18.5]. In [4], the first author proves that if K is a countable Hilbertian field, then $K_{\mathrm{sep}}[\boldsymbol{\sigma}]_K$ is Hilbertian for *almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, that is for all $\boldsymbol{\sigma}$ in $\mathrm{Gal}(K)^e$ but a set of measure zero. Bary-Soroker and Fehm generalize this result by replacing K_{sep} with an arbitrary Galois extension L of K. They prove that $L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ [1, Thm. 1.1]. The purpose of this work is to generalize their result to the level of rings:

DOI: 10.24193/mathcluj.2020.1.07

Theorem 1.1. *Let R be a countable Hilbertian ring with quotient field K and let $R_{\rm sep}$ be the integral closure of R in $K_{\rm sep}$. Let L be a Galois extension of K in $K_{\rm sep}$ and let e be a positive integer. Then $R_{\rm sep} \cap L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

2. PRELIMINARIES

We recall several concepts and results about linear disjointness of fields, measure theory, and twisted wreath products of groups.

2.1. LINEAR DISJOINTNESS

Let $K \subseteq K_1 \subseteq L$ be a tower of fields. We say that L/K_1 satisfies the K-*linearly disjoint condition* if there exists an infinite linearly disjoint sequence of finite proper extensions of K_1 within L of the same degree that are Galois over K.

This condition is related to the "$\mathcal{L}_K$-condition" introduced at the beginning of Section 2 of [1]. The following four lemmas are the counterparts of the lemmas that appear in that section.

Lemma 2.1. *Let $(M_i)_{i\geq 1}$ be a linearly disjoint sequence of extensions of a field 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. Assume towards contradiction that there there is an increasing sequence $i_1 < i_2 < i_3 < \cdots$ of positive integers such that E is not linearly disjoint from M_{i_j} over K for each $j \geq 1$. Since E/K is Galois, $E \cap M_{i_j}$ is a proper extension of K for each $j \geq 1$. Since K has only finitely many extensions in E, there are positive integers $j < k$ such that $E \cap M_{i_j} = E \cap M_{i_k}$. In particular, $M_{i_j} \cap M_{i_k}$ is a proper extension of K, contradicting the linear disjointness of M_{i_j} and M_{i_k} over K. □

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

Proof. By assumption, K_1 has a linearly disjoint sequence $M_1', M_2', M_3', \ldots$ of proper extensions within L of the same degree that are Galois over K. For each positive integer j we set $M_j'' = M_{(j-1)d+1}' \cdots M_{jd}'$. By the linear disjointness

$$[M_j'' : K_1] = [M_{(j-1)d+1}' : K_1] \cdots [M_{jd}' : K_1] = [M_1' : K_1]^d \geq 2^d > d.$$

As a compositum of Galois extensions over K, each of the fields M_j'' is Galois over K. In addition, the sequence $M_1'', M_2'', M_3'', \ldots$ is linearly disjoint over K_1. Since there are, up to isomorphism, only finitely many groups of order $[M_1' : K_1]^d$, we may replace the sequence $M_1'', M_2'', M_3'', \ldots$ by a subsequence to assume the existence of a finite group G of order greater than d such that $\mathrm{Gal}(M_j''/K_1) \cong G$ for each $j \geq 1$.

Finally, we may apply induction and Lemma 2.1 to extract an infinite subsequence $M_1, M_2, M_3, \ldots$ of $M_1'', M_2'', M_3'', \ldots$ such that $M_0, M_1, M_2, \ldots$ is linearly disjoint over K_1, as desired. □

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 the K-linearly disjoint condition. Then also L/K_2 satisfies the K-linearly disjoint condition.*

Proof. By assumption, K_1 has a linearly disjoint sequence $K_1', K_2', K_3', \ldots$ of proper extensions within L that are Galois over K of the same degree. We apply Lemma 2.1 to inductively construct an increasing sequence $i_1 < i_2 < i_3 < \cdots$ of positive integers such that $K_2K_{i_1}', K_2K_{i_2}', K_2K_{i_3}', \ldots$ are linearly disjoint proper extensions of K_2. Since all of these fields are contained in L and are Galois over K with the same degree, L/K_2 satisfies the K-linearly disjoint condition, as claimed. □

Recall that a Galois extension L/K is *small* if, for each positive integer n, K has only finitely many extensions of degree n within L, equivalently, if, for each positive integer n, K has only finitely many Galois extensions of degree n within L.

LEMMA 2.4. *Let L/K be a non-small Galois extension. Then K has a finite Galois extension K_1 within L such that L/K_1 satisfies the K-linearly disjoint condition.*

Proof. By definition, K is contained in infinitely many finite Galois extensions $M_1, M_2, M_3, \ldots$ of K within L of the same degree. Let K_1 be a maximal Galois extension of K which is contained in infinitely many of the M_i's. Replacing the above sequence by a subsequence, we may assume that $K_1 \subseteq M_i$ for all i.

We assume by induction that $i_1 < i_2 < \cdots < i_n$ are positive integers such that $M_{i_1}, M_{i_2}, \ldots, M_{i_n}$ are linearly disjoint over K_1. Let $M = M_{i_1}M_{i_2}\cdots M_{i_n}$. Since K_1 has only fintely many extensions within M, K_1 has an extension K_2 and there exist infinitely many $i > i_n$ with $M_i \cap M = K_2$. In particular, K_2 is Galois over K. The maximality property of K_1 implies that $K_2 = K_1$. Let i_{n+1} be the first integer greater than i_n such that $M_{n+1} \cap M = K_2 = K_1$. Then $M_{i_1}, \cdots, M_{i_n}, M_{i_{n+1}}$ are linearly disjoint over K_1.

It follows by induction that $M_{i_1}, M_{i_2}, M_{i_3}, \ldots$ is an infinite linearly disjoint sequence of extensions of K_1 of the same degree within L that are Galois over K. Thus, L/K_1 satisfies the K-linearly disjoint condition. □

Recall that a profinite group G is *small* if for each positive integer n, G has only finitely many open subgroups of the same degree [2, p. 329, Section 16.10]. Thus, a Galois extension L/K is small if and only if $\mathrm{Gal}(L/K)$ is small.

LEMMA 2.5 ([2], p. 332, Prop. 16.11.1). *Let L be a Galois extension of a Hilbertian field K. Suppose $\mathrm{Gal}(L/K)$ is small. Then for every positive integer r, each separable Hilbert subset H of L^r contains a separable Hilbert subset of K^r. In particular, L is Hilbertian.*

2.2. MEASURES

We cite two basic results about measure spaces.

For a profinite group G we denote the probability Haar measure on G by μ_G.

LEMMA 2.6 ([1, 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 $\Sigma_1, \dots, \Sigma_k \subseteq H$ measurable μ_H-independent sets. Let $\Sigma_i^* = \bigcup_{g\in S} g\Sigma_i$. Then $\Sigma_1^*, \dots, \Sigma_k^*$ are μ_G-independent.*

LEMMA 2.7 ([1, 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 $\mu(\bigcup_{i=1}^\infty A_i) = \mu(\bigcup_{i=1}^\infty B_i)$.*

2.3. 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,

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

forms a group under pointwise multiplication. 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

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

[2, p. 253, Def. 13.7.2]. Let $\pi\colon \mathrm{Ind}_{G_1}^G(A) \to A$ be the projection given by $\pi(f) = f(1)$.

LEMMA 2.8 ([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 $A\mathrm{wr}_{G_1} G$ generated by $\tau = (\zeta, (g_1, 1))$ satisfies $\pi(N \cap I) = A$.*

Following [3] we say that a tower of fields

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

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

$$A\mathrm{wr}_{G_1}G \geq \mathrm{Ind}_{G_1}^{G}(A) \rtimes G_1 \geq \mathrm{Ind}_{G_1}^{G}(A) \geq \mathrm{Ker}(\pi) \geq \mathbf{1}\,.$$

In particular, we have the following commutative diagram:

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

3. HILBERTIAN RINGS

We present results about Hilbertian rings needed in the proof of our main theorem. The first one is an adjusted version of [1, Lemma 5.1].

LEMMA 3.1. *Let K_1 be a Hilbertian field, let $\mathbf{x} = (x_1, \ldots, x_d)$ be a d-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:*

$$\begin{array}{ccccccccc} & & M & — & ME_1 & — & ME_1(\mathbf{x}) & — & MN \\ & & | & & | & & | & & | \\ K_1 & — & E & — & E_1 & — & E_1(\mathbf{x}) & — & N \end{array}$$

Assume that E, E_1, M are finite Galois extensions of K_1, $E = M \cap E_1$, N is a finite Galois extension of $K_1(\mathbf{x})$ that is regular over E_1 and let $y \in N$.

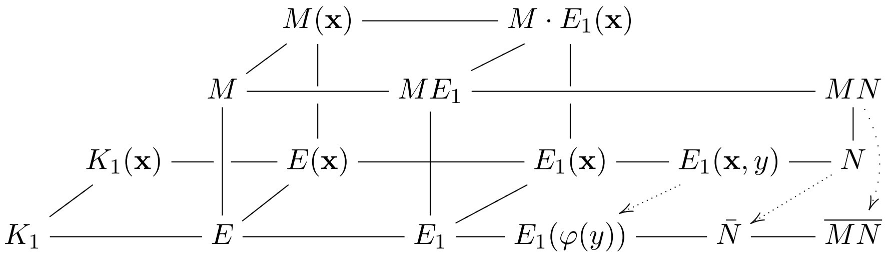
Then there exists a separable Hilbert subset H of K_1^d such that for each $\mathbf{b} \in H$ we have $g(\mathbf{b}) \neq 0$ and the specialization $\mathbf{x} \mapsto \mathbf{b}$ extends to an E_1-place φ of N such that $\varphi(y)$ is finite, the residue fields of $K_1(\mathbf{x})$, $E_1(\mathbf{x}, y)$ 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. Since $M \cap E_1 = E$, M and E_1 are linearly disjoint over E. Since N is regular over E_1, N is linearly disjoint from ME_1 over E_1. Hence, M and N are linearly disjoint over E. Therefore, $M(\mathbf{x})$ is linearly disjoint from N over $E(\mathbf{x})$, so $M(\mathbf{x}) \cap N = E(\mathbf{x})$.

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.

By [FrJ08, p. 231, Lemma 13.1.1], applied to the separable extensions $E_1(\mathbf{x}, y)$, N, and MN of $K_1(\mathbf{x})$, there exists a separable Hilbert subset H of K_1^d such that for each $\mathbf{b} \in H$ we have $g(\mathbf{b}) \neq 0$ and 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 $\bar{N}$ of MN and N, respectively, are Galois over K_1, and φ induces isomorphisms $\mathrm{Gal}(N/K_1(\mathbf{x})) \cong \mathrm{Gal}(\bar{N}/K_1)$ and $\mathrm{Gal}(MN/K_1(\mathbf{x})) \cong \mathrm{Gal}(\overline{MN}/K_1)$ such that the following diagram commutes:



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, $M(\mathbf{x}) \cap N = E(\mathbf{x})$ implies that $M \cap \bar{N} = E$, which means that M and $\bar{N}$ are linearly disjoint over E. ☐

LEMMA 3.2 ([5, Lemma 2.1]). *Let R be a Hilbertian ring with quotient field K and let L be a finite separable extension of K. Then the integral closure R_L of R in L is also Hilbertian.*

LEMMA 3.3 ([5, Lemma 1.2]). *Let R be an integral domain with quotient field K. Suppose that each separable Hilbert subset of K of the form $H_K(g)$ with irreducible $g \in K[X,Y]$, separable, monic and of degree at least 2 in Y, has an element in R. Then R is Hilbertian.*

The following result is a special case of [2, p. 235, Lemma 13.1.4].

LEMMA 3.4. *Let K be an infinite field and let $g \in K[X,Y]$ be an irreducible polynomial which is monic and separable in Y. Then there are a finite Galois extension L of K and an absolutely irreducible polynomial $f \in K[X,Y]$ which as a polynomial in Y is monic and Galois over $L(X)$ such that $K \cap H_L(f) \subseteq H_K(g)$.*

4. MAIN RESULT

The following lemma is the decisive step toward our main result. It generalizes [1, Lemma 6.1] to rings. Here we abuse our notation and for every field K and every positive integer e we use μ_K for the normalized Haar measure of $\mathrm{Gal}(K)^e$.

LEMMA 4.1. *Let R be a Hilbertian ring with quotient field K and let R_{sep} be the integral closure of R in K_{sep}. Let $K \subseteq K_1 \subseteq L \subseteq K_{\mathrm{sep}}$ be a tower of fields such that L/K is Galois, K_1/K is finite Galois and L/K_1 satisfies the K-linearly disjoint condition (Section 2). Let e be a positive integer, let $f \in K_1[X,Y]$ be an absolutely irreducible polynomial that is monic in Y and Galois over $K_{\mathrm{sep}}(X)$. Finally, let K_1' be a finite separable extension of K_1.*

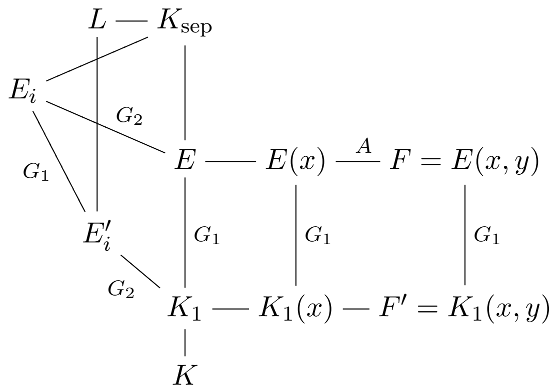
Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ *there exists* $a \in R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ *such that* $f(a, Y)$ *is irreducible over* $K_1' \cdot L[\boldsymbol{\sigma}]_K$*.*

Proof. We break up the proof into several parts.

Part A: *Diagram of fields.* Let E be a finite Galois extension of K such that $K_1' \subseteq E$ and f is Galois over $E(X)$ and set $G_1 = \mathrm{Gal}(E/K_1)$. It suffices to prove that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ there exists $a \in R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ such that $f(a, Y)$ is irreducible over $E \cdot L[\boldsymbol{\sigma}]_K$.

To this end we construct the following diagram of fields:

(1)



Let x be a transcendental element over K and let y be a root of $f(x, Y)$ in a separable algebraic closure of $K_1(x)$ that contains K_{sep}. Let $F' = K_1(x, y)$ and $F = E(x, y)$. Since $f(X, Y)$ is absolutely irreducible, F'/K_1 is regular, hence F' is linearly disjoint from E over K_1. Therefore, F' is linearly disjoint from $E(x)$ over $K_1(x)$, so $\mathrm{Gal}(F/F') \cong \mathrm{Gal}(E(x)/K_1(x)) \cong \mathrm{Gal}(E/K_1) = G_1$. Since $f(x, Y)$ is Galois over $E(x)$, the extension $F/E(x)$ is Galois. We set $A = \mathrm{Gal}(F/E(x))$. Then

$$|A| = [F : E(x)] = \deg(f(x, Y)) = \deg_Y f(X, Y). \tag{2}$$

Also, $K_1(x)$ is the fixed field of the subgroup $\langle A, G_1 \rangle$ of $\mathrm{Aut}(F)$. Therefore, $F/K_1(x)$ is a Galois extension with $\mathrm{Gal}(F/K_1(x)) = \langle A, G_1 \rangle$ and G_1 acts on A by conjugation.

Since L/K_1 satisfies the K-linearly disjoint condition, we get by Lemma 2.2, applied to $M_0 = E$, that there exists a finite group G_2 with $d := |G_2| > |A|$ and a sequence $(E_i')_{i \geq 1}$ of linearly disjoint extensions of K_1 within L which are Galois over K with $\mathrm{Gal}(E_i'/K_1) \cong G_2$ such that the sequence $E, E_1', E_2', E_3', \ldots$ is linearly disjoint over K_1. Let

$$E_i = EE_i'. \tag{3}$$

Then E_i/K is Galois and $\mathrm{Gal}(E_i/K_1) \cong G := G_1 \times G_2$ for every i.

Part B: *Twisted wreath product.* Let $\mathbf{x} = (x_1, \ldots, x_d)$ be a d-tuple of indeterminates and for each i choose a basis $w_{i1}, \ldots, w_{id}$ of E_i'/K_1 such that

$w_{i1},\dots,w_{id}$ are integral over R. By [3, Lemma 3.1], for each i we have a tower

$$K_1(\mathbf{x}) \subseteq E'_i(\mathbf{x}) \subseteq E_i(\mathbf{x}) \subseteq N_i = E_i(\mathbf{x},y_i) \subseteq \hat{N}_i \tag{4}$$

that realizes the twisted wreath product $A\mathrm{wr}_{G_1}G$, such that $\hat{N}_i$ is regular over E_i, where $\mathrm{irr}(y_i,E_i(\mathbf{x})) = f(\sum_{\nu=1}^d w_{i\nu}x_\nu, Y)$. In particular, $\mathrm{Gal}(\hat{N}_i/K_1(\mathbf{x})) = A\mathrm{wr}_{G_1}G$, $\mathrm{Gal}(\hat{N}_i/E_i(\mathbf{x})) = \mathrm{Ind}_{G_1}^G(A)$ and $\mathrm{Gal}(N_i/E_i(\mathbf{x})) = A$.

Part C: *Specialization of* (4). 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 for each positive integer k the following conditions hold.

(5a) For $j = 1,\dots,k$ and $\nu = 1,\dots,d$ we have $\varphi_j(x_\nu) \in R_{\mathrm{sep}} \cap K_1$, hence $a_j := \sum_{\nu=1}^d w_{i_j\nu}\varphi_j(x_\nu) \in R_{\mathrm{sep}} \cap E'_{i_j}$ and $\varphi_j(y_{i_j}) \in K_{\mathrm{sep}}$.

(5b) For $j = 1,\dots,k$ and for $i = i_j$, the residue field tower of (4) under φ_j,

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

realizes the twisted wreath product $A\mathrm{wr}_{G_1}G$. Moreover, $f(a_j,Y)$ is irreducible over E_{i_j} and M_{i_j} is generated over E_{i_j} by the root $\varphi_j(y_{i_j})$ of $f(a_j,Y)$. Thus, $[M_{i_j} : E_{i_j}] = \deg(f(a_j,Y)) = \deg_Y(f(X,Y)) =^{(2)} |A|$.

(5c) The sequence $\hat{M}_{i_1},\dots,\hat{M}_{i_k}$ is linearly disjoint over E.

Indeed, suppose that $i_1,\dots,i_{k-1}$ and $\varphi_1,\dots,\varphi_{k-1}$ with the appropriate properties have been constructed and let $M = \hat{M}_{i_1}\cdots\hat{M}_{i_{k-1}}$. By Lemma 2.1, there is $i_k > i_{k-1}$ such that E'_{i_k} is linearly disjoint from M over K_1. Hence, $E_{i_k} = EE'_{i_k}$ is linearly disjoint from M over E.

Let R_1 be the integral closure of R in K_1. Since R is Hilbertian and K_1/K is finite and separable, R_1 is Hilbertian (Lemma 3.2). Applying Lemma 3.1 to $M, E, E_{i_k}, \hat{N}_{i_k}, y_{i_k}$, we get a separable Hilbert subset H of K_1^d such that for each $\mathbf{b} \in H$, the specialization $\mathbf{x} \mapsto \mathbf{b}$ extends to an E_{i_k}-place φ_k of $\hat{N}_{i_k}$ such that (5b) and (5c) hold for $i_1,\cdots,i_{k-1},i_k$. Since R_1 is Hilbertian, there exists $\mathbf{b} \in H \cap R_1^d$, so also (5a) is satisfied for $i_1,\dots,i_{k-1},i_k$.

Part D: *A special element of* $\mathrm{Ind}_{G_1}^G(A)$. We set $I = \mathrm{Ind}_{G_1}^G(A)$, fix j and make the following identifications: $\mathrm{Gal}(\hat{M}_{i_j}/K_1) = A\mathrm{wr}_{G_1}G = I \rtimes (G_1 \times G_2)$, $\mathrm{Gal}(\hat{M}_{i_j}/E_{i_j}) = I$ and $\mathrm{Gal}(M_{i_j}/E_{i_j}) = A$. 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 $\pi\colon I \to A$ and $\mathrm{Gal}(\hat{M}_{i_j}/M_{i_j}) = \mathrm{Ker}(\pi)$.

Let $\zeta \in I$ be as in Lemma 2.8, let

$$\Sigma_j^* = \bigcap_{\nu=1}^e \{\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e \mid \exists g_{\nu 1} \in G_1\colon \sigma_\nu|_{\hat{M}_{i_j}} = (\zeta,(g_{\nu 1},1)) \in I \rtimes (G_1 \times G_2)\}, \tag{6}$$

and note that the intersected sets on the right hand side of (6) are μ_{K_1}-independent. Then, by that lemma, for each $\boldsymbol{\sigma} \in \Sigma_j^*$, the normal subgroup N

generated by $\sigma_1|_{\hat{M}_{i_j}}, \ldots, \sigma_e|_{\hat{M}_{i_j}}$ in $\mathrm{Gal}(\hat{M}_{i_j}/K_1)$ satisfies

$$\pi(N \cap I) = A. \tag{7}$$

Moreover, with $Q = K_{\mathrm{sep}}[\boldsymbol{\sigma}]_{K_1}$, we have $N = \mathrm{Gal}(\hat{M}_{i_j}/\hat{M}_{i_j} \cap Q)$.

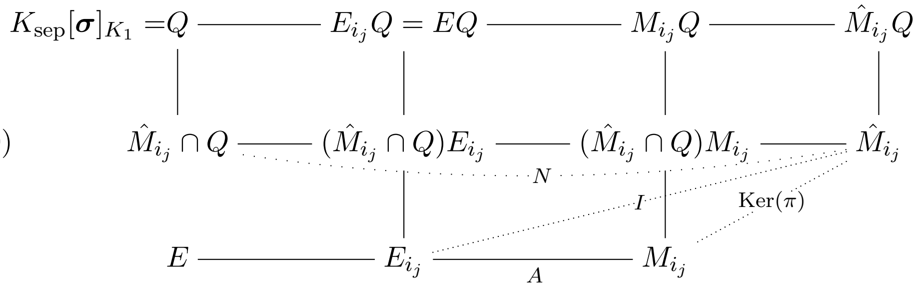
Part E: *We prove that for a fixed positive integer j and for each $\boldsymbol{\sigma} \in \Sigma_j^*$ the polynomial $f(a_j, Y)$ is irreducible over $E \cdot L[\boldsymbol{\sigma}]_K$.* Indeed, consider $\boldsymbol{\sigma} \in \Sigma_j^*$ and let $P = L[\boldsymbol{\sigma}]_K$. Then

$$P = L \cap K_{\mathrm{sep}}[\boldsymbol{\sigma}]_K \subseteq K_{\mathrm{sep}}[\boldsymbol{\sigma}]_K \subseteq K_{\mathrm{sep}}[\boldsymbol{\sigma}]_{K_1} = Q\,. \tag{8}$$

By Part A, E'_{i_j} is Galois over K. By (6), for $\nu = 1, \ldots, e$ we have $\sigma_\nu|_{\hat{M}_{i_j}} = (\zeta, (g_{\nu 1}, 1))$ with $\zeta \in I$ and $g_{\nu 1} \in G_1$. Hence, by the begining of Part D and by Diagram (1), σ_ν fixes E'_{i_j}. Therefore, $K \subseteq E'_{i_j} \subseteq L[\boldsymbol{\sigma}]_K = P$. It follows from (5a) that $a_j \in P$. Moreover,

$$E_{i_j}Q \overset{(3)}{=} EE'_{i_j}Q = EQ \overset{(8)}{\supseteq} EP. \tag{9}$$

Since by (5b) M_{i_j} is generated by a root of $f(a_j, Y)$ over E_{i_j}, (9) implies that $M_{i_j}Q$ is generated by a root of $f(a_j, Y)$ over EQ.

(10) 

Using Diagram (10), the equalities $N = \mathrm{Gal}(\hat{M}_{i_j}/\hat{M}_{i_j} \cap Q)$ and $\mathrm{Ker}(\pi) = \mathrm{Gal}(\hat{M}_{i_j}/M_{i_j})$ that appear in Part D imply that

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

and

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

Hence,

$$\mathrm{Gal}(M_{i_j}Q/E_{i_j}Q) \cong (N \cap I)/(N \cap \mathrm{Ker}(\pi)) \cong \pi(N \cap I) \overset{(7)}{=} A\,.$$

Therefore, $[M_{i_j}Q : E_{i_j}Q] = |A| =^{(2)} \deg_Y f(X, Y) = \deg f(a_j, Y)$. Since, by (5b) $M_{i_j}Q$ is generated over $E_{i_j}Q$ by a root of $f(a_j, Y)$, we get that $f(a_j, Y)$ is irreducible over $E_{i_j}Q$. It follows from (9) that $f(a_j, Y)$ is irreducible over $EP = E \cdot L[\boldsymbol{\sigma}]_K$, as claimed.

Part F: *We prove that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ lie in infinitely many Σ_j^*.* To this end we set

$$\Sigma_j = \bigcap_{\nu=1}^{e} \{\boldsymbol{\sigma} \in \mathrm{Gal}(E)^e \mid \sigma_\nu|_{\hat{M}_{i_j}} = (\zeta, (1,1)) \in I \rtimes (G_1 \times G_2) \overset{(5b)}{=} \mathrm{Gal}(\hat{M}_{i_j}/K_1)\}. \tag{11}$$

This is a coset of $\mathrm{Gal}(\hat{M}_{i_j})^e$ in $\mathrm{Gal}(E)^e$. Since, by (5c), the sequence $(\hat{M}_{i_j})_{j=1}^{\infty}$ is linearly disjoint over E, the sets $\mathrm{Gal}(\hat{M}_{i_j})^e$ are μ_E-independent [2, p. 378, Lemma 18.5.1]. Thus, by [2, p. 373, Lemma 18.3.7], also the sets Σ_j are μ_E-independent. In addition, since $\mathrm{Gal}(\hat{M}_{i_j}/K_1) \cong I \rtimes (G_1 \times G_2)$, we can choose for every positive integer j and for every $g \in G_1 =^{(1)} \mathrm{Gal}(E/K_1)$ an element $\hat{g}_j \in \mathrm{Gal}(K_1)$ such that $\hat{g}_j|_{\hat{M}_{i_j}} = (1, (g, 1))$. Then

$$S = \{\hat{\mathbf{g}}_j := (\hat{g}_{1,j}, \dots, \hat{g}_{e,j}) \in \mathrm{Gal}(K_1)^e \mid g_1, \dots, g_e \in G_1\}$$

is a set of representatives for the right cosets of $\mathrm{Gal}(E)^e$ in $\mathrm{Gal}(K_1)^e$. Moreover, since $(\zeta, (1,1))(1, (g,1)) = (\zeta, (g,1))$ for each $g \in G_1$, (6) and (11) imply that $\Sigma_j^* = \bigcup_{\hat{\mathbf{g}}_j \in S} \Sigma_j \hat{\mathbf{g}}_j$ for every j. Therefore, Lemma 2.6 implies that the sets Σ_j^* are μ_{K_1}-independent. Moreover, by (6),

$$\mu_{K_1}(\Sigma_j^*) = \frac{|G_1|^e}{|A\mathrm{wr}_{G_1} G|^e} > 0$$

does not depend on j, so $\sum_{j=1}^{\infty} \mu_{K_1}(\Sigma_j^*) = \infty$. It follows from the Borel-Cantelli lemma [2, p. 372, Lemma 18.3.5] that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ lie in infinitely many Σ_j^*, as claimed.

End of proof: By Part E, for each positive integer j and for every $\boldsymbol{\sigma} \in \Sigma_j^*$ the polynomial $f(a_j, Y)$ is irreducible over $E \cdot L[\boldsymbol{\sigma}]_K$. By Part F, almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ lie in infinitely many Σ_j^*. By (5a), a_j belong to $R_{\mathrm{sep}} \cap E'_{i_j}$, hence also to $R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$. Therefore, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_1)^e$ there exists $a \in R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ such that $f(a, Y)$ is irreducible over $E \cdot L[\boldsymbol{\sigma}]_K$, as claimed. □

The following proposition is a generalization of [1, Prop. 6.2] to rings.

PROPOSITION 4.2. *Let R be a countable Hilbertian ring with quotient field K and let R_{sep} be the integral closure of R in K_{sep}. Let $K \subseteq K_1 \subseteq L \subseteq K_{\mathrm{sep}}$ be a tower of fields such that L/K is Galois, K_1/K is finite Galois and L/K_1 satisfies the K-linearly disjoint condition. Let e be a positive integer. Then $R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ 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 extension of K_1 within L which is Galois over K, K_2'/K_2 is a finite separable extension, and $f(X,Y) \in K_2[X,Y]$ is an absolutely irreducible polynomial that is monic in Y and Galois over $K_{\mathrm{sep}}(X)$. Since K is countable, the set $\mathcal{F}$ is countable.

If $(K_2, K_2', f) \in \mathcal{F}$, then the integral closure R_2 of R in K_2 is Hilbertian (Lemma 3.2) and L/K_2 satisfies the K-linearly disjoint condition (Lemma 2.3). Hence, Lemma 4.1, applied to K_2 rather than to K_1, yields a subset $\Sigma'_{(K_2,K_2',f)}$ of $\mathrm{Gal}(K_2)^e$ with $\mu_{K_1}(\Sigma'_{(K_2,K_2',f)}) = \mu_{K_1}(\mathrm{Gal}(K_2)^e)$ such that for every $\boldsymbol{\sigma} \in \Sigma'_{(K_2,K_2',f)}$ there exists $a \in R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ 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 $\mu_{K_1}(\Sigma_{(K_2,K_2',f)}) = \mu_{K_1}(\mathrm{Gal}(K_1)^e)$. Since $\mathcal{F}$ is countable, it follows that the μ_{K_1}-measure of $\Sigma = \bigcap_{(K_2,K_2',f)\in\mathcal{F}} \Sigma_{(K_2,K_2',f)}$ is 1.

We consider $\boldsymbol{\sigma} \in \Sigma$ and let $P = L[\boldsymbol{\sigma}]_K$ and $R_P = R_{\mathrm{sep}} \cap P$. In order to prove that R_P is Hilbertian, it suffices, by Lemma 3.3, to consider an irreducible polynomial $g \in P[X, Y]$, separable, monic and of degree at least 2 in Y and to prove that $H_P(g)$ has an element in R_P.

By Lemma 3.4, there exist a finite Galois extension P' of P and an absolutely irreducible polynomial $f \in P[X, Y]$ which as a polynomial in Y is monic and Galois over $P'(X)$ such that

$$P \cap H_{P'}(f) \subseteq H_P(g). \tag{12}$$

In particular, f is Galois over $K_{\mathrm{sep}}(X)$. 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 exists $a \in R_P$ such that $f(a, Y)$ is irreducible over $PK_2' = P'$, so $a \in R_P \cap H_{P'}(f) \subseteq^{(12)} R_P \cap H_P(g)$, as desired. ☐

THEOREM 4.3. *Let R be a countable Hilbertian ring with quotient field K and let R_{sep} be the integral closure of R in K_{sep}. Let L be a Galois extension of K in K_{sep} and let e be a positive integer. Then $R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ is Hilbertian for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Proof. Let $\mathcal{F}$ be the set of all finite Galois extensions K_1 of K within L for which L/K_1 satisfies the K-linearly disjoint condition. Since K is countable, so is $\mathcal{F}$. Let

$$\Sigma = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K \text{ is Hilbertian}\}\,.$$

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

$$\mathrm{Gal}(K_1)^e = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid K_1 \subseteq L[\boldsymbol{\sigma}]_K\}\,. \tag{13}$$

By Proposition 4.2,

$$\mu_K(\Sigma_{K_1}) = \mu_K(\mathrm{Gal}(K_1)^e) \text{ for each } K_1 \in \mathcal{F}. \tag{14}$$

Let

$$\Delta = \mathrm{Gal}(K)^e \smallsetminus \bigcup_{K_1 \in \mathcal{F}} \mathrm{Gal}(K_1)^e$$
$$\overset{(13)}{=} \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid K_1 \not\subseteq L[\boldsymbol{\sigma}]_K \text{ for all } K_1 \in \mathcal{F}\}\,.$$

If $\boldsymbol{\sigma} \in \Delta$, then by Lemma 2.4, $L[\boldsymbol{\sigma}]_K/K$ is small. By Lemma 2.5, for every positive integer r, each separable Hilbert subset H of $L[\boldsymbol{\sigma}]_K^r$ contains a separable Hilbert subset H_K of K^r. Since R is Hilbertian, $R^r \cap H_K \neq \emptyset$. Therefore, $R_{\mathrm{sep}} \cap L[\boldsymbol{\sigma}]_K$ is Hilbertian. Thus, $\Delta \subseteq \Sigma$. Since $\mathrm{Gal}(K)^e = \Delta \cup \bigcup_{K_1 \in \mathcal{F}} \mathrm{Gal}(K_1)^e$, Lemma 2.7 implies that

$$\mu_K(\Sigma) = \mu_K\big((\Sigma \cap \Delta) \cup \bigcup_{K_1 \in \mathcal{F}} \Sigma_{K_1}\big) \overset{(14)}{=} \mu_K\big(\Delta \cup \bigcup_{K_1 \in \mathcal{F}} \mathrm{Gal}(K_1)^e\big)$$
$$= \mu_K(\mathrm{Gal}(K)^e) = 1\,,$$

which concludes the proof of the theorem. □

REFERENCES

[1] L. Bary-Soroker and A. Fehm, *Random Galois extensions of Hilbertian rings*, J. Théor. Nombres Bordeaux, **25** (2013), 31–42.

[2] M. Fried and M. Jarden, *Field arithmetic*, 3rd Edition, Ergebnisse der Mathematik, Vol. 11, Springer, Heidelberg, 2008.

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

[4] M. Jarden, *Large normal extension of Hilbertian fields,* Math. Z., **224** (1997), 555–565.

[5] M. Jarden and A. Razon, *Extensions of Hilbertian rings,* Glasg. Math. J., **62** (2018), 1–11.

Received September 8, 2018
Accepted November 4, 2018

Tel Aviv University
School of Mathematics
Tel Aviv, Israel
E-mail: jarden@post.tau.ac.il

Elta Industry
Ashdod, Israel
E-mail: razona@elta.co.il