

Extensions of Hilbertian Rings

by

Moshe Jarden, Tel Aviv University, jarden@post.tau.ac.il

and

Aharon Razon, Elta, razona@elta.co.il

Abstract: We generalize known results about Hilbertian fields to Hilbertian rings. For example, let R be a Hilbertian ring (e.g. R is the ring of integers of a number field) with quotient field K and let A be an abelian variety over K . Then, for every extension M of K in $K(A_{\text{tor}}(K_{\text{sep}}))$, the integral closure R_M of R in M is Hilbertian.

MR Classification: 12E30

2 October 2018

Introduction

Some of the most important results in the theory of Hilbertian fields are of the form: if K is a Hilbertian field and M/K is an extension satisfying certain properties, then M is Hilbertian as well. This article proves integral analogues of some of these theorems: if R is a Hilbertian domain with quotient field K and M/K is an algebraic extension of fields satisfying some condition that is known to preserve Hilbertianity (of fields), then the integral closure of R in M is also Hilbertian.

Given irreducible polynomials $f_1, \dots, f_m \in \mathbb{Q}(T_1, \dots, T_r)[X]$ and a non-zero polynomial $g \in \mathbb{Q}[T_1, \dots, T_r]$, Hilbert's irreducibility theorem yields an r -tuple $\mathbf{a} \in \mathbb{Q}^r$ such that $f_i(\mathbf{a}, X)$ is defined and irreducible in $\mathbb{Q}[X]$ for $i = 1, \dots, m$ and $g(\mathbf{a}) \neq 0$. The set $H_{\mathbb{Q}}(f_1, \dots, f_m; g)$ of all \mathbf{a} with that property is said to be a **Hilbert subset** of \mathbb{Q}^r . It contains $\mathbf{a} \in \mathbb{Q}^r$ such that $\text{Gal}(f_i(\mathbf{a}, X), \mathbb{Q}) \cong \text{Gal}(f_i(\mathbf{T}, X), \mathbb{Q}(\mathbf{T}))$ for $i = 1, \dots, m$ [FrJ08, p. 294, Prop. 16.1.5]. The importance of the latter property lies in the fact that it is the main (albeit not the only) tool to realize finite groups over \mathbb{Q} .

The above definition applies to an arbitrary field K . A **separable Hilbert set** of K is then a Hilbert subset $H_K(f_1, \dots, f_m; g)$ of K^r for some positive integer r with the additional property that each $f_i(\mathbf{T}, X)$ is in $K(\mathbf{T})[X]$ and is separable in X . If each of these sets is non-empty, then K is **Hilbertian**. It turns out that every global field is Hilbertian. Moreover, every finitely generated transcendental extension of an arbitrary field is Hilbertian [FrJ08, p. 242, Thm. 13.4.2]. Furthermore, every finite extension of a Hilbertian field is Hilbertian [FrJ08, p. 227, Prop. 12.3.5].

Generalizing prior results of Willem Kuyk [Kuy70] and Reiner Weissauer [Wei82], Dan Haran proved a “diamond theorem” in [Har99]: Given Galois extensions N_1 and N_2 of a Hilbertian field K , every extension M of K in $N_1 N_2$ that is neither contained in N_1 nor in N_2 is Hilbertian.

The first author conjectured in [Jar10] that if K is a Hilbertian field and A is an abelian variety over K , then, every extension M of K in $K(A_{\text{tor}})$ is Hilbertian. He proved the conjecture for number fields. The proof uses Haran's diamond theorem and a theorem of Serre that in that time was known only for number fields. Arno Fehm and Sebastian Petersen referred to the conjecture as the **Kuykian Conjecture** and proved it when K is an infinite finitely generated extension of its prime field [FeP12].

Haran's proof of the Diamond Theorem relies on a technical result [Har99, Thm. 3.2]. That result is exploited by Lior Bary-Soroker, Arno Fehm, and Gabor Wiese in [BFW16] to prove far reaching generalization of the results mentioned so far:

Proposition A ([BFW16, Thm. 1.1]): *Let M be a separable algebraic extension of a Hilbertian field K . Suppose that there exist a tower of field extensions $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ such that for each $1 \leq i \leq n$ the extension K_i/K_{i-1} is Galois with Galois group that is either abelian or a direct product of finite simple groups and $M \subseteq K_n$. (We call $K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ a **finite abelian-***

simple tower.) Then, M is Hilbertian.

Using a deep result of Michael Larsen and Richard Pink [LaP97], Bary-Soroker, Fehm, and Wiese also prove that for every field K and every abelian variety A over K , the extension $K(A_{\text{tor}})/K$ admits a finite abelian-simple tower. Thus, the Kuykian Conjecture (renamed in [BFW16] **Jarden Conjecture**) turns out to be a special case of Proposition A.

The present work originates in an arithmetic proof of the Hilbert irreducibility theorem which proves for a global field K that every Hilbert subset of K^r contains points in O_K^r , where O_K is the ring of integers of K [FrJ08, p. 241, Thm. 13.3.5]. Thus, O_K may be called a **Hilbertian ring**.

The first thing we do is to slightly modify the proof of [Har99, Thm. 3.2] to Hilbertian rings (Proposition 1.4). Then, we use the modified criterion to generalize Haran's diamond theorem:

Theorem B (Theorem 2.2): *Let R be a Hilbertian ring with quotient field K , let N_1 and N_2 be Galois extensions of K and M an extension of K in N_1N_2 such that $M \not\subseteq N_1$ and $M \not\subseteq N_2$. Then, the integral closure R_M of R in M is Hilbertian.*

Our second main result generalizes Proposition A:

Theorem C (Theorem 3.5): *Let R be a Hilbertian ring with quotient field K and let M be a separable algebraic extension of K of finite abelian-simple length (Definition 3.1). Then, the integral closure R_M of R in M is Hilbertian.*

Theorem C has two interesting corollaries. For the first one, we denote the compositum of all Galois extensions with symmetric Galois groups of a field K by K_{sym} .

Corollary D (Corollary 3.6): *Let R be a Hilbertian ring with quotient field K . Let M be an extension of K in K_{sym} . Then, the ring R_M is Hilbertian.*

The second one refers to the torsion subgroup A_{tor} of an abelian variety A .

Corollary E (Theorem 4.5): *Let R be a Hilbertian ring with quotient field K . Let A be an abelian variety over K and let M be an extension of K in $K(A_{\text{tor}}(K_{\text{sep}}))$. Then, the ring R_M is Hilbertian.*

The authors thank the referee for useful comments.

1 Hilbertian Rings

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 and a nonzero polynomial $g \in K[\mathbf{T}]$, 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 $K[X]$ and $g(\mathbf{a}) \neq 0$ is a **separable Hilbert subset** of K^r . In the special case, where $g = 1$, we write $H_K(f_1, \dots, f_m)$ rather than $H_K(f_1, \dots, f_m; 1)$.

{HILDOM}

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 . In this case, K is a Hilbertian field.

Recall that a profinite group G is **small** if for every positive integer n the group G has only finitely many subgroups of index n . In particular, if G is finitely generated, then G is small [FrJ08, page 328, Lemma 16.10.2].

Let M/K be a separable algebraic extension of fields and let N be the Galois hull of M/K . In particular, $\text{Gal}(N/K)$ is small if M/K is finite.

We need the following improvement of [FrJ08, p. 332, Prop. 16.1.1]:

Lemma 1.1. *Let N be a Galois extension of a field K with small Galois group $\text{Gal}(N/K)$. Let M be an extension of K in N . Then, every separable Hilbert subset H of M^r contains a separable Hilbert subset of K^r .*

{ABHf}

In particular, if K is Hilbertian, then so is M . Moreover, if K is the quotient field of a Hilbertian domain R , then the integral closure R_M of R in M is also Hilbertian.

Proof: By definition, $H = H_M(f_1, \dots, f_k; g)$, where $f_i \in M(T_1, \dots, T_r)[X]$ is irreducible and separable, $i = 1, \dots, k$, and $g \in M[T_1, \dots, T_r]$ with $g \neq 0$. Let $n = \max(\deg_X(f_1), \dots, \deg_X(f_k))$. We choose a finite extension L of K in M that contains all of the coefficients of f_1, \dots, f_k, g , and set $d = [L : K]$. Then, we denote the compositum of all extensions of K in M of degree at most dn by L' . Then, $L \subseteq L'$, and by our assumption on N , we have $[L' : K] < \infty$. Hence, by [FrJ08, p. 224, Cor. 12.2.3], $H_{L'}(f_1, \dots, f_k; g)$ contains a separable Hilbert subset H_K of K^r .

Let $\mathbf{a} \in H_K$ and consider an i between 1 and k . Then, $g(\mathbf{a}) \neq 0$ and $f_i(\mathbf{a}, X)$ is irreducible over L' . Let b be a zero of $f_i(\mathbf{a}, X)$ in K_{sep} . Then, $L(b)$ is linearly disjoint from L' over L . In addition, $[M \cap L(b) : K] \leq [L(b) : K] \leq dn$. Hence, $M \cap L(b) \leq L' \cap L(b) = L$. It follows that $f_i(\mathbf{a}, X)$ is irreducible over M . Consequently, $\mathbf{a} \in H$.

If K is the quotient field of a Hilbertian domain R , then H_K contains a point \mathbf{a} that lies in R^n , so also in R_M^n . Therefore, R_M is Hilbertian. \square

The following result is a generalization of [FrJ08, p. 236, Prop. 13.2.2].

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

{HILa}

Proof: By [FrJ08, p. 222, Lemma 12.1.6], it suffices to consider a separable irreducible polynomial $f \in K[T_1, \dots, T_r, X]$ in X and to prove that $H_K(f) \cap R^r \neq \emptyset$. The case $r = 1$ is covered by the assumption of the lemma. Suppose $r \geq 2$ and the statement holds for $r - 1$. The assumption of the lemma implies that R is infinite. Let $K_0 = K(T_1, \dots, T_{r-2})$, $t = T_{r-1}$, and regard f as a polynomial in $K_0(t)[T_r, X]$. By [FrJ08, p. 236, Prop. 13.2.1], there exists a non-empty Zariski-open subset U of $\mathbb{A}_{K_0}^2$ such that $\{a + bt \mid (a, b) \in U(K_0)\} \subseteq H_{K_0(t)}(f)$. Since R is infinite, we can choose a, b such that $(a, b) \in U(R)$. Hence, $f(T_1, \dots, T_{r-1}, a + bT_{r-1}, X)$ is irreducible and separable in $K(T_1, \dots, T_{r-1})[X]$. The induction hypothesis gives $a_1, \dots, a_{r-1} \in R$ such that $f(a_1, \dots, a_{r-1}, a + ba_{r-1}, X)$ is irreducible and separable in $K[X]$. Let $a_r = a + ba_{r-1}$. Then, $a_r \in R$ and $f(a_1, \dots, a_r, X)$ is irreducible in $K[X]$. \square

Proposition 1.4 below is the basic result used in the proof of our two main theorems 2.2 and 3.5. We start the proof of that proposition with a generalization of [Har99, Thm. 3.2]. The proof of that generalization uses the notion of “twisted wreath product” that we now recall from [FrJ08, p. 253, Def. 13.7.2].

Let G be a group and G' a subgroup. Suppose that G' acts on a group A from the right. We consider the group

$$\text{Ind}_{G'}^G(A) = \{f: G \rightarrow A \mid f(\sigma\sigma') = f(\sigma)^{\sigma'} \text{ for all } \sigma \in G \text{ and } \sigma' \in G'\}$$

and let G acts on $\text{Ind}_{G'}^G(A)$ by the rule $f^\sigma(\tau) = f(\sigma\tau)$. The **twisted wreath product** of A and G with respect to G' is defined as the semi-direct product

$$\text{Aw}_{G'}G = G \rtimes \text{Ind}_{G'}^G(A).$$

We say that a tower of fields $K \subseteq E' \subseteq E \subseteq F \subseteq \hat{F}$ **realizes** a twisted wreath product $\text{Aw}_{G'}G$ if \hat{F}/K is a Galois extension with Galois group isomorphic to $\text{Aw}_{G'}G$ and the tower yields a commutative diagram of groups,

$$\begin{array}{ccccccc} \text{Gal}(\hat{F}/F) & \longrightarrow & \text{Gal}(\hat{F}/E) & \longrightarrow & \text{Gal}(\hat{F}/E') & \longrightarrow & \text{Gal}(\hat{F}/K) \\ \parallel & & \parallel & & \parallel & & \parallel \\ J & \longrightarrow & \text{Ind}_{G'}^G(A) & \longrightarrow & G' \times \text{Ind}_{G'}^G(A) & \longrightarrow & \text{Aw}_{G'}G, \end{array}$$

where

(1) $J = \{f \in \text{Ind}_{G'}^G(A) \mid f(1) = 1\}$ is a normal subgroup of $\text{Ind}_{G'}^G(A)$

and each of the maps in the first and the second rows is the inclusion map. See [FrJ08, p. 255, Remark 13.7.6], where a more elaborate diagram is referred to.

The following result is a special case of [FrJ08, p. 235, Lemma 13.1.4].

Lemma 1.3. *Let K be an infinite field and let $f \in K[T, X]$ be an irreducible polynomial which is monic and separable in X . Then, there are a finite Galois extension L of K and an absolutely irreducible polynomial $g \in K[T, X]$ which as a polynomial in X is monic, separable, and Galois over $L(T)$ such that $K \cap H_L(g) \subseteq H_K(f)$.*

{jnor}

{HILb}

We denote the maximal separable algebraic extension of a field K by K_{sep} .

Proposition 1.4. *Let R be a Hilbertian ring with quotient field K and let M be a separable algebraic extension of K . Suppose that for every $\alpha \in M$ and every $\beta \in K_{\text{sep}}$ there exist:*

{HILc}

- (a) a finite Galois extension L of K that contains α and β ; let $G = \text{Gal}(L/K)$;
- (b) a field K' that contains α such that $K \subseteq K' \subseteq M \cap L$; let $G' = \text{Gal}(L/K')$; and
- (c) a Galois extension N of K that contains both M and L ,

such that for every finite non-trivial group A_0 and every action of G' on A_0 there is no realization K, K', L, F_0, \hat{F}_0 of $A_0 \text{wr}_{G'} G$ with $\hat{F}_0 \subseteq N$.

Then, the integral closure R_M of R in M is Hilbertian.

Proof: We break the proof into four parts.

Part A: *Preliminaries* We apply the criterion for Hilbertianity of Lemma 1.2 combined with Lemma 1.3. So let $f \in M[T, X]$ be an absolutely irreducible polynomial, monic and separable in X , and let M'/M be a finite Galois extension such that $f(T, X)$ is Galois over $M'(T)$. We have to prove that there exists $a \in R_M$ such that $f(a, X) \in M[X]$ is irreducible over M' . Let $A = \text{Gal}(f, M'(T)) = \text{Gal}(f, K_{\text{sep}}(T))$. Without loss we may assume that $\deg_X(f) \geq 2$.

There is $\alpha \in M$ such that $f \in K(\alpha)[T, X]$ and there is $\beta \in K_{\text{sep}}$ such that $M' \subseteq M(\beta)$ and $f(T, X)$ is Galois over $K(\beta)(T)$ with $\text{Gal}(f(T, X), K(\beta)(T)) = A$. For these α, β let K', L , and N be as in (a), (b), and (c). Then, $f \in K'[T, X]$ and $f(T, X)$ is Galois over $L(T)$ with $\text{Gal}(f(T, X), L(T)) = A$.

Let R' be the integral closure of R in K' . Then, $R' \subseteq R_M$ and $M' \subseteq N$, so it suffices to find $a \in R'$ such that $f(a, X)$ is irreducible over N .

Part B: *Specialization of the wreath product.* We choose $c_1, \dots, c_n \in R'$ that form a basis of K' over K .

Let $\mathbf{t} = (t_1, \dots, t_n)$ be an n -tuple of algebraically independent elements over K' . By [FrJ08, p. 258, Lemma 13.8.1], $G' = \text{Gal}(L/K')$ acts on A and there are fields P and \hat{P} such that

{hi12a}

(2a) $K(\mathbf{t}), K'(\mathbf{t}), L(\mathbf{t}), P, \hat{P}$ realize $\text{Awr}_{G'} G$ and \hat{P} is regular over L .

{hi12b}

(2b) $P = L(\mathbf{t}, x)$, where $\text{irr}(x, L(\mathbf{t})) = f(\sum_{i=1}^n c_i t_i, X)$.

Since R is Hilbertian, [FrJ08, p. 231, Lemma 13.1.1] gives an n -tuple $\mathbf{b} = (b_1, \dots, b_n) \in R^n$ such that the specialization $\mathbf{t} \mapsto \mathbf{b}$ yields an L -place of \hat{P} onto a Galois extension \hat{F} of K with Galois group isomorphic to $\text{Gal}(\hat{P}/K(\mathbf{t}))$. That is, there are fields F and \hat{F} such that

{hi12}

(3a) K, K', L, F, \hat{F} realize $\text{Awr}_{G'} G$.

{hi13b}

(3b) $F = L(y)$, where $\text{irr}(y, L) = f(\sum_{i=1}^n c_i b_i, X)$.

We set $a = \sum_{i=1}^n c_i b_i$ and observe that $a \in R'$, so $f(a, X) \in K'[X]$.

Part C: $L = N \cap F$ Indeed, by (1), F/L is a Galois extension, so $F_0 = N \cap F$ is a Galois extension of L . Let $A_0 = \text{Gal}(F_0/L)$. By [FrJ08, p. 257, Remark 13.7.6(c)], there is a Galois extension \hat{F}_0 of K such that G' acts on A_0 and $\{hi14\}$
 (4) K, K', L, F_0, \hat{F}_0 realize $A_0 \text{wr}_{G'} G$.

Moreover, \hat{F}_0 is the Galois closure of F_0 over K . Since $F_0 \subseteq N$ and N/K is Galois, we have $\hat{F}_0 \subseteq N$. By assumption, this is possible only if $A_0 = 1$, that is, if $L = N \cap F$.

Part D: *Conclusion* By Part B, $f(a, y) = 0$ and $F = L(y)$. By Part C,

$$[N(y) : N] = [NF : N] = [F : L] = [L(y) : L].$$

Thus, $f(a, X) = \text{irr}(y, N)$. In particular, $f(a, X)$ is irreducible over N . \square

2 Haran's diamond theorem

Our first application of Proposition 1.4 generalizes Haran's diamond theorem [Har99, Thm. 4.1] from fields to integral domains.

The following result is [Har99, Lemma 1.4(a)].

Lemma 2.1. *Let $\pi: \text{Awr}_{G'}G \rightarrow G$ be a twisted wreath product with $A \neq \mathbf{1}$. Let $H_1 \triangleleft \text{Awr}_{G'}G$ and $h_2 \in \text{Awr}_{G'}G$ and let $G_1 = \pi(H_1)$. Suppose that $\pi(h_2) \notin G'$ and $(G_1G' : G') > 2$. Then, there exists $h_1 \in \text{Ker}(\pi) \cap H_1$ such that $[h_1, h_2] \neq 1$.*

{HAR1.4}

Theorem 2.2 (Haran's Diamond theorem for rings). *Let R be a Hilbertian ring with quotient field K . Let M_1 and M_2 be Galois extensions of K and let M be an extension of K in M_1M_2 . Suppose that $M \not\subseteq M_1$ and $M \not\subseteq M_2$. Then, the integral closure R_M of R in M is Hilbertian.*

{HARb}

Proof: By Lemma 1.1, we may assume that $[M : K] = \infty$. Part A of the proof strengthens this assumption.

Part A: We may assume that $[M : (M_1 \cap M)] = \infty$ Otherwise,

$$[M : (M_1 \cap M)] < \infty.$$

Then, K has a finite Galois extension M'_2 with $M \subseteq (M_1 \cap M)M'_2$. Hence, $M \subseteq M_1M'_2$ and $[M : M \cap M'_2] = \infty$. Replace M_1 by M'_2 and M_2 by M_1 to restore our assumption.

Part B: *Construction of N and L* Following Proposition 1.4, we consider $\alpha \in M$ and $\beta \in K_{\text{sep}}$. Let L be a finite Galois extension of K that contains $K(\alpha, \beta)$ and let $N = LM_1M_2$. Then, N/K is Galois and both $\text{Gal}(N/M_1)$ and $\text{Gal}(N/M_2)$ are normal in $\text{Gal}(N/K)$.

Let $G = \text{Gal}(L/K)$ and let $\varphi: \text{Gal}(N/K) \rightarrow G$ be the restriction map. Let $G_1 = \varphi(\text{Gal}(N/M_1))$ and $G_2 = \varphi(\text{Gal}(N/M_2))$. Then,

$$G_1, G_2 \triangleleft G. \tag{1} \text{ {har1}}$$

Now we set $K' = M \cap L$ and $G' = \varphi(\text{Gal}(N/M))$. Then, $\alpha \in K'$ and $G' = \text{Gal}(L/K')$.

Since $M \not\subseteq M_i$, we may choose L sufficiently large such that $K' \not\subseteq M_i$ for $i = 1, 2$, hence

$$G_1, G_2 \not\subseteq G'. \tag{2} \text{ {har2}}$$

Similarly, since $[M : K] = \infty$, we may choose L sufficiently large such that

$$(G : G') > 2. \tag{3} \text{ {har3}}$$

Finally, by Part A, we may choose L sufficiently large such that

$$(G_1G' : G') > 2. \tag{4} \text{ {har4}}$$

Part C: *Realization* We consider a non-trivial group A on which G' acts and set $H = \text{Awr}_{G'}G$. By Proposition 1.4, it suffices to prove that a realization K, K', L, F, \hat{F} of H with $\hat{F} \subseteq N$ does not exist.

Assume toward contradiction that such a realization exists. We identify H with $\text{Gal}(\hat{F}/K)$ such that the restriction map $\text{res}_{\hat{F}/L}: \text{Gal}(\hat{F}/K) \rightarrow \text{Gal}(L/K)$ coincides with the projection $\pi: H \rightarrow G$. Then, $\pi \circ \text{res}_{N/\hat{F}} = \text{res}_{N/L}$.

For $i = 1, 2$ let $H_i = \text{res}_{N/\hat{F}}(\text{Gal}(N/M_i))$. Then, $H_i \triangleleft H$ and $\pi(H_i) = \text{res}_{N/L}(\text{Gal}(N/M_i)) = G_i$.

Claim: *There are $h_1 \in H_1 \cap \text{Ker}(\pi)$ and $h_2 \in H_2$ such that $[h_1, h_2] \neq 1$* Indeed, by (2), there exists $g_2 \in G_2 \setminus G'$. Choose $h_2 \in H_2$ such that $\pi(h_2) = g_2$, so $\pi(h_2) \notin G'$. Hence, our claim follows from (4) and Lemma 2.1.

For $i = 1, 2$ we choose $\gamma_i \in \text{Gal}(N/M_i)$ with $\text{res}_{N/\hat{F}}(\gamma_i) = h_i$. Then, by the claim,

$$\text{res}_{N/L}(\gamma_1) = \pi(h_1) = 1 \text{ and } [\gamma_1, \gamma_2] \neq 1. \quad (5) \quad \{\text{comm1}\}$$

However, since $\text{Gal}(M_1M_2/M_1 \cap M_2) \cong \text{Gal}(M_1M_2/M_1) \times \text{Gal}(M_1M_2/M_2)$, the subgroups $\text{Gal}(M_1M_2/M_1)$ and $\text{Gal}(M_1M_2/M_2)$ commute. Hence,

$$\text{res}_{N/M_1M_2}[\gamma_1, \gamma_2] = [\text{res}_{N/M_1M_2}(\gamma_1), \text{res}_{N/M_1M_2}(\gamma_2)] = 1. \quad (6) \quad \{\text{one1}\}$$

Furthermore, by (5),

$$\text{res}_{N/L}[\gamma_1, \gamma_2] = [\text{res}_{N/L}(\gamma_1), \text{res}_{N/L}(\gamma_2)] = [1, \text{res}_{N/L}(\gamma_2)] = 1. \quad (7) \quad \{\text{one2}\}$$

Since $N = (M_1M_2)L$, it follows from (6) and (7) that $[\gamma_1, \gamma_2] = 1$, a contradiction to (5). \square

An immediate corollary of Theorem 2.2 generalizes a well known result of Reiner Weissauer (see [Wei82, Satz 9.7] or [FrJ08, p. 262, Thm. 13.9.1]).

{WEIs}

Corollary 2.3. *Let R be a Hilbertian ring with quotient field K and let M' be a separable algebraic extension of K . Suppose that M' is a finite extension of a field M and there exists a Galois extension N of K that contains M but does not contain M' . Then, the ring of integers $R_{M'}$ of R in M' is Hilbertian.*

Proof: The case where M' is a finite extension of K is covered by Lemma 1.1, so assume that $[M' : K] = \infty$. Hence, K has a finite Galois extension L such that $M' \subseteq NL$. In particular, $M' \not\subseteq L$. By assumption, $M' \not\subseteq N$. Hence, by Theorem 2.2, $R_{M'}$ is Hilbertian, as claimed. \square

3 Abelian-Simple Towers

We strengthen a theorem of Lior Bary-Sorker, Arno Fehm, and Gabor Wiese saying that a Galois extension N of a Hilbertian field K obtained by finitely many subextensions, each of which is either abelian or a compositum of simple non-abelian extensions is Hilbertian.

{HILd}

Definition 3.1. Let G be a profinite group. Following [BFW16], we define the **generalized derived subgroup** $D(G)$ of G as the intersection of all open normal subgroups N of G with G/N either abelian or simple. The **generalized derived series** of G ,

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots,$$

is defined inductively by $G^{(0)} = G$ and $G^{(i+1)} = D(G^{(i)})$ for $i \geq 0$.

We define the **abelian-simple length** of a profinite group G , denoted by $l(G)$, to be the smallest integer l for which $G^{(l)} = 1$. If $G^{(i)} \neq 1$ for all i , we set $l(G) = \infty$. We say that G is **of finite abelian-simple length** if $l(G) < \infty$. \square

The following result is a special case of [BFW16, Prop. 2.8].

{SUPa}

Lemma 3.2. *Let $(K_i/K)_{i \in I}$ be a family of Galois extensions, let $N = \prod_{i \in I} K_i$, and let m be a positive integer. If for each $i \in I$ the abelian-simple length of $\text{Gal}(K_i/K)$ is less than or equal to m , then so is the abelian-simple length of $\text{Gal}(N/K)$.*

We quote two results from [BFW16].

Lemma 3.3. *[BFW16, Lemma 2.7(i)] If $\alpha: G \rightarrow H$ is an epimorphism of profinite groups, then $\alpha(G^{(i)})$, $i = 0, 1, 2, \dots$, is the generalized derived series of H . In particular, $l(H) \leq l(G)$.*

{HILe}

Lemma 3.4. *[BFW16, Prop. 2.11] Let m be a positive integer, let A be a non-trivial finite group, and let $G' \leq G$ be finite groups together with an action of G' on A . Assume that $(G^{(m)}G' : G') > 2^m$. Then,*

{HILf}

$$(\text{Awr}_{G'}G)^{(m+1)} \cap \text{Ind}_{G'}^G(A) \neq \mathbf{1}.$$

We say that a separable algebraic extension M/K is **of finite abelian-simple length** if $l(\text{Gal}(\hat{M}/K)) < \infty$, where \hat{M} denotes the Galois closure of M/K . The following result strengthens [BFW16, Thm. 3.2].

{HILg}

Theorem 3.5. *Let R be a Hilbertian ring with quotient field K and let M be a separable algebraic extension of K of finite abelian-simple length. Then, the integral closure R_M of R in M is Hilbertian.*

Proof: Our proof closely follows the proof of [BFW16, Thm. 3.2] which proves that M is Hilbertian.

Let $\varphi: \Gamma \rightarrow \bar{G}$ and $\psi: G \rightarrow \bar{G}$ be the restriction maps. By Lemma 3.3,

$$\begin{aligned}\bar{G}^{(m)} &= \varphi(\Gamma^{(m)}) = \text{Gal}(\bar{E}/L^{(m)} \cap \bar{E}), \\ \bar{G}^{(m)} &= \psi(G^{(m)}) = \text{Gal}(\bar{E}/E^{(m)} \cap \bar{E}),\end{aligned}$$

where $E^{(m)}$ is the fixed field of $G^{(m)}$ in E .

$$\begin{array}{ccccc} & & \varphi & & \\ & & \curvearrowright & & \\ \Gamma^{(m)} & & & \xrightarrow{\psi} & \bar{G}^{(m)} \\ \parallel & & \parallel & & \parallel \\ \text{Gal}(L/L^{(m)}) & & \text{Gal}(E/L^{(m)} \cap E) & \xrightarrow{\text{res}} & \text{Gal}(\bar{E}/L^{(m)} \cap \bar{E}) \end{array}$$

Thus,

$$E^{(m)} \cap \bar{E} = L^{(m)} \cap \bar{E}. \quad (4) \quad \{\text{hil6}\}$$

Since $E \cap M = E \cap L \cap M = \bar{E} \cap M$, we have

$$\begin{aligned}E \cap M \cap E^{(m)} &= \bar{E} \cap M \cap E^{(m)} = M \cap E^{(m)} \cap \bar{E} \\ &\stackrel{(4)}{=} M \cap L^{(m)} \cap \bar{E} = \bar{E} \cap M \cap L^{(m)} = E \cap M \cap L^{(m)}.\end{aligned}$$

Hence,

$$(G^{(m)}G' : G') = [E' : E' \cap E^{(m)}] = [E' : E \cap P] \stackrel{(2)}{>} 2^m.$$

Lemma 3.4 yields

$$(\text{Awr}_{G'}G)^{(m+1)} \cap \text{Ind}_{G'}^G(A) \neq \mathbf{1},$$

so there exists a non-trivial element

$$\tau \in (\text{Awr}_{G'}G)^{(m+1)} \cap \text{Ind}_{G'}^G(A).$$

Since $\text{Gal}(\hat{F}/K) = \text{Awr}_{G'}G$, the map $\text{res}_{N/\hat{F}}: \text{Gal}(N/K) \rightarrow \text{Gal}(\hat{F}/K)$ maps $\text{Gal}(N/K)^{(m+1)}$ onto $(\text{Awr}_{G'}G)^{(m+1)}$ (Lemma 3.3). Hence, we may lift τ to an element $\tilde{\tau} \in \text{Gal}(N/K)^{(m+1)}$. Again, by Lemma 3.3, $\tilde{\tau}|_L \in \text{Gal}(L/K)^{(m+1)} = \Gamma^{(m+1)} \stackrel{(1)}{=} \mathbf{1}$. Since $\tau \in \text{Ind}_{G'}^G(A) = \text{Gal}(\hat{F}/E)$, it follows that $\tilde{\tau}|_E = 1$. Then, since $LE = N$, we have $\tilde{\tau} = 1$, so $\tau = 1$. We conclude from this contradiction that R_M is Hilbertian. \square

Let R be an integral domain with quotient field K and let N be an extension of K . Recall that [FeP12] calls N an \mathcal{H} -**extension** of K if every field M between K and N is Hilbertian. We say that N is an \mathcal{HR} -**extension** of R if for every field M between K and N the integral closure R_M of R in M is Hilbertian. \{APPa\}

Corollary 3.6. *Let R be a Hilbertian ring with quotient field K . Then, K_{symm}/R is an \mathcal{HR} -extension.*

Proof: One observes that the abelian-simple length of each S_n is at most 3. Hence, by Lemma 3.2, the abelian-simple length of K_{symm}/K is at most 3. Therefore, by Theorem 3.5, K_{symm}/R is an \mathcal{HR} -extension. \square

4 Abelian Varieties

Let R be a Hilbertian ring with quotient field K and let A be an abelian variety over K . Let $A_{\text{tor}}(K_{\text{sep}})$ be the group of all points in $A(K_{\text{sep}})$ of finite order. We use both main results of this work to prove that $K(A_{\text{tor}}(K_{\text{sep}}))/R$ is an \mathcal{HR} -extension.

We start by a ring version of [FeP12, Lemma 2.2].

Lemma 4.1. *Let R be a Hilbertian ring with quotient field K and let K_1, \dots, K_n be \mathcal{HR} -extensions of R that are Galois over K . Then, $\prod_{i=1}^n K_i$ is an \mathcal{HR} -extension of R .*

{FePb}

Proof: Induction on n reduces the lemma to the case $n = 2$. Let M be an extension of K in $K_1 K_2$. If M is contained either in K_1 or in K_2 , then R_M is Hilbertian, by assumption. Otherwise, R_M is Hilbertian, by Theorem 2.2. \square

The following result is a special case of [BFW16, Cor. 4.6].

Lemma 4.2. *For every positive integer n there exists m with the following property: For every l , every closed subgroup Λ of $\text{GL}_n(\mathbb{Z}_l)$ has a closed pro- l normal subgroup N such that the abelian-simple length of Λ/N is at most m .*

{ABSi}

We also need Lemma 2.3 of [FeP12].

Lemma 4.3. *Let $(L_i)_{i \in I}$ be a linearly disjoint family of extensions of a field L . Then, $\bigcap_{\substack{J \subseteq I \\ \text{finite}}} \prod_{i \in I \setminus J} L_i = L$.*

{DIVi}

Lemma 4.4. *Let R be a Hilbertian ring with quotient field K . Let $(K_i)_{i \in I}$ be a family of Galois \mathcal{HR} -extensions of R . Suppose that there exists an \mathcal{HR} -extension L of R such that $(K_i L)_{i \in I}$ is a linearly disjoint family of field extensions of L . Then, the field $\prod_{i \in I} K_i$ is an \mathcal{HR} -extension of R .*

{FEPa}

Proof: If $M \subseteq \prod_{i \in I \setminus J} K_i$ for every finite subset J of I , then $M \subseteq L$, by Lemma 4.3. Hence, R_M is a Hilbertian ring in this case.

Otherwise, I has a finite subset J such that $M \not\subseteq \prod_{i \in I \setminus J} K_i$. If $M \subseteq \prod_{i \in J} K_i$, then R_M is Hilbertian, by Lemma 4.1. Otherwise, $M \not\subseteq \prod_{i \in J} K_i$. Hence, R_M is Hilbertian, by Theorem 2.2. \square

The following result is the ring version of a special case of [BFW16, Cor. 4.3].

Corollary 4.5. *Let R be a Hilbertian ring with quotient field K . Let A be an abelian variety over K . Then, $K(A_{\text{tor}}(K_{\text{sep}}))$ is an \mathcal{HR} -extension of R .*

{HILi}

Proof: We set $g = \dim(A)$ and let l range over the set of prime numbers. For each l , let $A_{l^\infty}(K_{\text{sep}})$ be the group of all points of $A(K_{\text{sep}})$ whose order is a power of l . It is well known that $\text{Gal}(K(A_{l^\infty}(K_{\text{sep}}))/K)$ is a closed subgroup of $\text{GL}_{2g}(\mathbb{Z}_l)$. Therefore, by Lemma 4.2, $\text{Gal}(K(A_{l^\infty}(K_{\text{sep}}))/K)$ has a closed normal pro- l subgroup Λ_l such that the abelian-simple length of

$$\text{Gal}(K(A_{l^\infty}(K_{\text{sep}}))/K)/\Lambda_l$$

is bounded by a positive integer m that depends on g but not on l . Let E_l be the fixed field of Λ_l in $K(A_{l^\infty}(K_{\text{sep}}))$. Then, E_l is a Galois extension of K and $\text{Gal}(K(A_{l^\infty}(K_{\text{sep}}))/E_l) \cong \Lambda_l$ is a pro- l -group and the abelian-simple length of $\text{Gal}(E_l/K)$ is bounded by a positive integer m that depends on g but is independent of l .

Let $E = \prod_{l \in \mathbb{L}} E_l$. By the preceding paragraph and Lemma 3.2, the abelian-simple length of $\text{Gal}(E/K)$ is less than or equal to m .

Moreover, for each l , the group $\text{Gal}(E(A_{l^\infty}(K_{\text{sep}})))$ is isomorphic to a normal closed subgroup of $\text{Gal}(K(A_{l^\infty}(K_{\text{sep}}))/E_l)$, hence is itself pro- l . Therefore, the fields $E(A_{l^\infty}(K_{\text{sep}}))$, with l ranging over all prime numbers, are linearly disjoint over E .

Since $K(A_{\text{tor}}(K_{\text{sep}})) = \prod_l K(A_{l^\infty}(K_{\text{sep}}))$, it follows from the last two paragraphs and from Lemma 4.4 that $K(A_{\text{tor}}(K_{\text{sep}}))$ is an \mathcal{HR} -extension of R . \square

References

- [BFW16] L. Bary-Soroker, A. Fehm, and G. Wiese, *Hilbertian fields and Galois representations*, Journal für die reine und angewandte Mathematik **712** (2016), 123–139.
- [FeP12] A. Fehm and S. Petersen, *Division fields of commutative algebraic groups*, Israel Journal of Mathematics **195** (2013), 123–134.
- [FrJ08] M. Fried and M. Jarden, *Field Arithmetic (3rd Edition)*, Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.
- [Har99] D. Haran, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137** (1999), no. 1, 113–126.
- [Jar10] M. Jarden, *Diamonds in torsion of Abelian varieties*, Journal of the Institute of Mathematics Jussieu **9** (2010), 477–480.
- [Kuy70] W. Kuyk, *Extensions de corps hilbertiens*, Journal of Algebra **14** (1970), 112–124.
- [LaP97] M. Larsen and R. Pink, *Finite subgroups of algebraic groups*, Journal of the American Mathematical Society **24** (2011), 1105–1158.
- [Wei82] R. Weissauer, *Der Hilbertsche Irreduzibilitätssatz*, Journal für die reine und angewandte Mathematik **334** (1982), 203–220.