Glasgow Math. J. **62** (2020) 1–11. © Glasgow Mathematical Journal Trust 2018.
doi:10.1017/S0017089518000496.

EXTENSIONS OF HILBERTIAN RINGS

MOSHE JARDEN
School of Mathematics, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel
e-mail: jarden@post.tau.ac.il

and AHARON RAZON
Elta Industry, Ashdod, Israel
e-mail: razona@elta.co.il

(Received 30 May 2018; revised 3 October 2018; accepted 3 October 2018;
first published online 5 November 2018)

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 $K(A_{\mathrm{tor}}(K_{\mathrm{sep}}))$, the integral closure R_M of R in M is Hilbertian.

Mathematics Subject Classification. 12E30.

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 $f_1, \ldots, f_m \in \mathbb{Q}(T_1, \ldots, T_r)[X]$ and a non-zero polynomial $g \in \mathbb{Q}[T_1, \ldots, T_r]$, 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 $i = 1, \ldots, m$ and $g(\mathbf{a}) \neq 0$. The set $H_{\mathbb{Q}}(f_1, \ldots, f_m; g)$ 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 $\mathrm{Gal}(f_i(\mathbf{a}, X), \mathbb{Q}) \cong \mathrm{Gal}(f_i(\mathbf{T}, X), \mathbb{Q}(\mathbf{T}))$ for $i = 1, \ldots, m$ [**3**, p. 294, Proposition 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 $H_K(f_1, \ldots, f_m; g)$ 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 [**3**, p. 242, Theorem 13.4.2]. Furthermore, every finite extension of a Hilbertian field is Hilbertian [**3**, p. 227, Proposition 12.3.5].

Generalizing prior results of Willem Kuyk [**6**] and Reiner Weissauer [**8**], Dan Haran proved a 'diamond theorem' in [**4**]: Given Galois extensions N_1 and N_2 of a Hilbertian field K, every extension M of K in N_1N_2 that is neither contained in N_1 nor in N_2 is Hilbertian.

The first author conjectured in [**5**] that if K is a Hilbertian field and A is an abelian variety over K, then, every extension M of K in $K(A_{\mathrm{tor}})$ 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 [**2**].

Haran's proof of the Diamond Theorem relies on a technical result [**4**, Theorem 3.2]. That result is exploited by Lior Bary-Soroker, Arno Fehm and Gabor Wiese in [**1**] to prove far reaching generalization of the results mentioned so far:

PROPOSITION A. ([**1**, Theorem 1.1]): *Let M be a separable algebraic extension of a Hilbertian field K. Suppose that there exist a tower of field extensions $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ such that for each $1 \le i \le n$ 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 $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ a* **finite abelian-simple tower.***) Then, M is Hilbertian.*

Using a deep result of Michael Larsen and Richard Pink [**7**], Bary-Soroker, Fehm and Wiese also prove that for every field K and every abelian variety A over K, the extension $K(A_{\mathrm{tor}})/K$ admits a finite abelian-simple tower. Thus, the Kuykian Conjecture (renamed in [**1**] **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 [**3**, p. 241, Theorem 13.3.5]. Thus, O_K may be called a **Hilbertian ring**.

The first thing we do is to slightly modify the proof of [**4**, Theorem 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 1.3 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_{symm}.

COROLLARY D. (Corollary 3.6): *Let R be a Hilbertian ring with quotient field K. Let M be an extension of K in K_{symm}. 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 $K(A_{\mathrm{tor}}(K_{\mathrm{sep}}))$. 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 $\mathbf{T} = (T_1, \ldots, T_r)$ be an r-tuple of indeterminates and let X be an additional indeterminate.

https://doi.org/10.1017/S0017089518000496 Published online by Cambridge University Press

Given irreducible polynomials $f_1, \ldots, f_m \in K(\mathbf{T})[X]$ that are separable in X and a non-zero polynomial $g \in K[\mathbf{T}]$, the set $H_K(f_1, \ldots, f_m; g)$ of all $\mathbf{a} \in K^r$ such that $f_1(\mathbf{a}, X), \ldots, f_m(\mathbf{a}, X)$ 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 $H_K(f_1, \ldots, f_m)$ rather than $H_K(f_1, \ldots, f_m; 1)$.

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 [**3**, 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, $\mathrm{Gal}(N/K)$ is small if M/K is finite.

We need the following improvement of [**3**, p. 332, Proposition 16.1.1]:

LEMMA 1.1. *Let N be a Galois extension of a field K with small Galois group* $\mathrm{Gal}(N/K)$. *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.*

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, $H = H_M(f_1, \ldots, f_k; g)$, where $f_i \in M(T_1, \ldots, T_r)[X]$ is irreducible and separable, $i = 1, \ldots, k$, and $g \in M[T_1, \ldots, T_r]$ with $g \neq 0$. Let $n = \max(\deg_X(f_1), \ldots, \deg_X(f_k))$. We choose a finite extension L of K in M that contains all of the coefficients of $f_1, \ldots, f_k, g$, 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 [**3**, p. 224, Corollary 12.2.3], $H_{L'}(f_1, \ldots, f_k; g)$ 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, $M \cap L(b) \subseteq L' \cap L(b) = L$. 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^r_M. Therefore, R_M is Hilbertian. □

The following result is a generalization of [**3**, p. 236, Proposition 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.*

Proof. By [**3**, p. 222, Lemma 12.1.6], it suffices to consider a separable irreducible polynomial $f \in K[T_1, \ldots, T_r, X]$ 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 $K_0 = K(T_1, \ldots, T_{r-2})$, $t = T_{r-1}$, and regard f as a polynomial in $K_0(t)[T_r, X]$. By [**3**, p. 236, Proposition 13.2.1], there exists a non-empty Zariski-open subset U of $\mathbb{A}^2_{K_0}$ 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, $f(T_1, \ldots, T_{r-1}, a + bT_{r-1}, X)$ is irreducible and separable

https://doi.org/10.1017/S0017089518000496 Published online by Cambridge University Press

in $K(T_1, \ldots, T_{r-1})[X]$. The induction hypothesis gives $a_1, \ldots, a_{r-1} \in R$ such that $f(a_1, \ldots, a_{r-1}, a + ba_{r-1}, X)$ is irreducible and separable in $K[X]$. Let $a_r = a + ba_{r-1}$. Then, $a_r \in R$ and $f(a_1, \ldots, a_r, X)$ 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 [**4**, Theorem 3.2]. The proof of that generalization uses the notion of 'twisted wreath product' that we now recall from [**3**, p. 253, Definition 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

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

and let G acts on $\mathrm{Ind}_{G'}^{G}(A)$ 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

$$A\mathrm{wr}_{G'}G = G \ltimes \mathrm{Ind}_{G'}^{G}(A).$$

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

$$\begin{tikzcd}
\mathrm{Gal}(\hat{F}/F) \arrow[r] \arrow[d, equal] & \mathrm{Gal}(\hat{F}/E) \arrow[r] \arrow[d, equal] & \mathrm{Gal}(\hat{F}/E') \arrow[r] \arrow[d, equal] & \mathrm{Gal}(\hat{F}/K) \arrow[d, equal] \\
J \arrow[r] & \mathrm{Ind}_{G'}^{G}(A) \arrow[r] & G' \ltimes \mathrm{Ind}_{G'}^{G}(A) \arrow[r] & A\mathrm{wr}_{G'}G,
\end{tikzcd}$$

where
(1) $J = \{f \in \mathrm{Ind}_{G'}^{G}(A) \mid f(1) = 1\}$ is a normal subgroup of $\mathrm{Ind}_{G'}^{G}(A)$
and each of the maps in the first and the second rows is the inclusion map. See [**3**, p. 255, Remark 13.7.6], where a more elaborate diagram is referred to.

The following result is a special case of [**3**, 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 $K \cap H_L(g) \subseteq H_K(f)$.*

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 $\beta \in K_{\mathrm{sep}}$, there exist*

(a) *a finite Galois extension L of K that contains α and β; let $G = \mathrm{Gal}(L/K)$;*
(b) *a field K' that contains α such that $K \subseteq K' \subseteq M \cap L$; let $G' = \mathrm{Gal}(L/K')$; 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 $A_0\mathrm{wr}_{G'}G$ with $\hat{F}_0 \subseteq N$.

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

https://doi.org/10.1017/S0017089518000496 Published online by Cambridge University Press

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

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 $c_1, \ldots, c_n \in R'$ that form a basis of K' over K.

Let $\mathbf{t} = (t_1, \ldots, t_n)$ be an n-tuple of algebraically independent elements over K'. By [**3**, p. 258, Lemma 13.8.1], $G' = \mathrm{Gal}(L/K')$ acts on A and there are fields P and $\hat{P}$ such that

(2a) $K(\mathbf{t}), K'(\mathbf{t}), L(\mathbf{t}), P, \hat{P}$ realize $A\mathrm{wr}_{G'}G$ and $\hat{P}$ is regular over L;
(2b) $P = L(\mathbf{t}, x)$, where $\mathrm{irr}(x, L(\mathbf{t})) = f(\sum_{i=1}^n c_i t_i, X)$.

Since R is Hilbertian [**3**, p. 231, Lemma 13.1.1], gives an n-tuple $\mathbf{b} = (b_1, \ldots, b_n) \in R^n$ 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 $\mathrm{Gal}(\hat{P}/K(\mathbf{t}))$. That is, there are fields F and $\hat{F}$ such that

(3a) $K, K', L, F, \hat{F}$ realize $A\mathrm{wr}_{G'}G$.
(3b) $F = L(y)$, where $\mathrm{irr}(y, L) = f(\sum_{i=1}^n c_i b_i, X)$.
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 $A_0 = \mathrm{Gal}(F_0/L)$. By [**3**, 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
(4) $K, K', L, F_0, \hat{F}_0$ realize $A_0\mathrm{wr}_{G'}G$.
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, $f(a, X) = \mathrm{irr}(y, N)$. In particular, $f(a, X)$ is irreducible over N. □

2. Haran's diamond theorem. Our first application of Proposition 1.4 generalizes Haran's diamond theorem [**4**, Theorem 4.1] from fields to integral domains.

The following result is [**4**, Lemma 1.4(a)].

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

https://doi.org/10.1017/S0017089518000496 Published online by Cambridge University Press

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.*

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 $\beta \in K_{\mathrm{sep}}$. 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 $\mathrm{Gal}(N/M_1)$ and $\mathrm{Gal}(N/M_2)$ are normal in $\mathrm{Gal}(N/K)$.

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

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

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

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

$$G_1, G_2 \not\leq G'. \tag{2}$$

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

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

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

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

Part C: *Realization.* We consider a non-trivial group A on which G' acts and set $H = A\mathrm{wr}_{G'}G$. 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 towards contradiction that such a realization exists. We identify H with $\mathrm{Gal}(\hat{F}/K)$ such that the restriction map $\mathrm{res}_{\hat{F}/L}\colon \mathrm{Gal}(\hat{F}/K) \to \mathrm{Gal}(L/K)$ coincides with the projection $\pi\colon H \to G$. Then, $\pi \circ \mathrm{res}_{N/\hat{F}} = \mathrm{res}_{N/L}$.

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

Claim: There are $h_1 \in H_1 \cap \mathrm{Ker}(\pi)$ and $h_2 \in H_2$ such that $[h_1, h_2] \neq 1$ Indeed, by (2), there exists $g_2 \in G_2 \smallsetminus G'$. 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 $\gamma_i \in \mathrm{Gal}(N/M_i)$ with $\mathrm{res}_{N/\hat{F}}(\gamma_i) = h_i$. Then, by the claim,

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

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

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

Furthermore, by (5),

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

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

An immediate corollary of Theorem 2.2 generalizes a well-known result of Reiner Weissauer (see [**8**, Satz 9.7] or [**3**, p. 262, Theorem 13.9.1]).

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. □

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.

Definition 3.1. Let G be a profinite group. Following [**1**], 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,

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

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 $l(G) < \infty$. □

The following result is a special case of [**1**, Proposition 2.8].

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* $\mathrm{Gal}(K_i/K)$ *is less than or equal to m, then so is the abelian-simple length of* $\mathrm{Gal}(N/K)$.

We quote two results from [**1**].

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

LEMMA 3.4 ([**1**, Proposition 2.11]). *Let m be a positive integer, let A be a non-trivial finite group, and let $G' \le G$ be finite groups together with an action of G' on A. Assume that $(G^{(m)}G' : G') > 2^m$. Then,*

$$(A\mathrm{wr}_{G'}G)^{(m+1)} \cap \mathrm{Ind}_{G'}^{G}(A) \neq \mathbf{1}\,.$$

We say that a separable algebraic extension M/K is **of finite abelian-simple length** if $l(\mathrm{Gal}(\hat{M}/K)) < \infty$, where $\hat{M}$ denotes the Galois closure of M/K. The following result strengthens [**1**, Theorem 3.2].

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 [**1**, Theorem 3.2] which proves that M is Hilbertian.

Let L be the Galois closure of M/K. Let $\Gamma = \mathrm{Gal}(L/K)$ and let $\Gamma^{(i)}$, $i = 0, 1, 2, \ldots,$ be the generalized derived series of Γ. By assumption, there exists a minimal $m \ge 0$ such that

$$\Gamma^{(m+1)} = \mathbf{1}. \tag{1}$$

Let $\Gamma' = \mathrm{Gal}(L/M)$ and for each i denote by $L^{(i)}$ the fixed field of $\Gamma^{(i)}$ in L.

Let $P = M \cap L^{(m)}$. If $(\Gamma'\Gamma^{(m)} : \Gamma') < \infty$, then by the Galois correspondence, M is a finite extension of P. Note that if $\hat{P}$ is the Galois closure of P/K, then $\hat{P} \subseteq L^{(m)}$ and thus $\mathrm{Gal}(\hat{P}/K)$ is a quotient of $\Gamma/\Gamma^{(m)}$. Thus, $\mathrm{Gal}(\hat{P}/K)^{(m)}$ is a quotient of

$$(\Gamma/\Gamma^{(m)})^{(m)} = \Gamma^{(m)}/\Gamma^{(m)} = \mathbf{1}$$

and therefore trivial (Lemma 3.3). Hence, induction on m implies that the integral closure R_P of R in P is Hilbertian. Since M is a finite extension of P, it follows from Lemma 1.1 that R_M is Hilbertian.

Therefore, we may assume that $(\Gamma'\Gamma^{(m)} : \Gamma') = \infty$, that is, $[M : P] = \infty$. To prove that R_M is Hilbertian, we apply Proposition 1.4.

Let $\alpha \in M$ and $\beta \in K_{\mathrm{sep}}$. Since M/P is infinite, there exists a finite Galois extension E/K such that $\alpha, \beta \in E$ and

$$[E' : E \cap P] > 2^m, \tag{2}$$

where $E' = E \cap M$.

Let $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/E')$, and let $G^{(i)}$, $i = 0, 1, 2, \ldots,$ be the generalized derived series of G (Definition 3.1). Note that $\alpha \in E'$. In addition, we set $N = EL$ and consider a non-trivial group A on which G' acts. By Proposition 1.4, it suffices to prove that there are no fields $F, \hat{F}$ such that
(3) $\hat{F} \subseteq N$ and $K \subseteq E' \subseteq E \subseteq F \subseteq \hat{F}$ is a realization of $A\mathrm{wr}_{G'}G$.

Assume towards contradiction that there exist fields F and $\hat{F}$ that satisfy (3) and identify $\mathrm{Gal}(\hat{F}/K)$ with $A\mathrm{wr}_{G'}G$ and $\mathrm{Gal}(\hat{F}/E)$ with $\mathrm{Ind}_{G'}^{G}(A)$.

Let $\bar{E} = L \cap E$, $\bar{G} = \mathrm{Gal}(\bar{E}/K)$, and consider the following diagram:

$$
\begin{tikzcd}
 & L^{(m)} \arrow[r, dash] \arrow[d, dash] \arrow[rr, dotted, dash, bend left, "\Gamma^{(m)}"] & L^{(m)}M \arrow[r, dash] \arrow[d, dash] & L \arrow[r, dash] \arrow[dd, dash] & N \arrow[d, dash] \\
 & L^{(m)} \cap M \arrow[r, dash] \arrow[d, dash] & M \arrow[d, dash] \arrow[ur, dotted, dash, "\Gamma'"] & & \hat{F} \arrow[d, dash, "\mathrm{Ind}_{G'}^{G}(A)"] \\
K \arrow[r, dash] \arrow[uurrr, dotted, dash, bend left=60, "\Gamma"] \arrow[rrr, dotted, dash, bend right, "\bar{G}"'] \arrow[rrrr, dotted, dash, bend right=40, "G"'] & L^{(m)} \cap E' \arrow[r, dash, "2^m <"] & E' \arrow[r, dash] & \bar{E} \arrow[r, dash] & E
\end{tikzcd}
$$

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

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

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

$$
\begin{tikzcd}
\Gamma^{(m)} \arrow[rr, bend left, "\varphi"] \arrow[d, equal] & G^{(m)} \arrow[r, "\psi"] \arrow[d, equal] & \bar{G}^{(m)} \arrow[d, equal] \\
\mathrm{Gal}(L/L^{(m)}) & \mathrm{Gal}(E/L^{(m)} \cap E) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(\bar{E}/L^{(m)} \cap \bar{E})
\end{tikzcd}
$$

Thus,

$$
E^{(m)} \cap \bar{E} = L^{(m)} \cap \bar{E}. \tag{4}
$$

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

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

Hence,

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

Lemma 3.4 yields

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

so there exists a non-trivial element

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

https://doi.org/10.1017/S0017089518000496 Published online by Cambridge University Press

Since $\mathrm{Gal}(\hat{F}/K) = A\mathrm{wr}_{G'}G$, the map $\mathrm{res}_{N/\hat{F}}\colon \mathrm{Gal}(N/K) \to \mathrm{Gal}(\hat{F}/K)$ maps $\mathrm{Gal}(N/K)^{(m+1)}$ onto $(A\mathrm{wr}_{G'}G)^{(m+1)}$ (Lemma 3.3). Hence, we may lift τ to an element $\tilde{\tau} \in \mathrm{Gal}(N/K)^{(m+1)}$. Again, by Lemma 3.3, $\tilde{\tau}|_L \in \mathrm{Gal}(L/K)^{(m+1)} = \Gamma^{(m+1)} \overset{(1)}{=} \mathbf{1}$. Since $\tau \in \mathrm{Ind}_{G'}^{G}(A) = \mathrm{Gal}(\hat{F}/E)$, 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. □

Let R be an integral domain with quotient field K and let N be an extension of K. Recall that [**2**] 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.

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. □

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

We start by a ring version of [**2**, Lemma 2.2].

LEMMA 4.1. *Let R be a Hilbertian ring with quotient field K and let $K_1, \ldots, K_n$ 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.*

Proof. Induction on n reduces the lemma to the case $n = 2$. Let M be an extension of K in K_1K_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. □

The following result is a special case of [**1**, Corollary 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 $\mathrm{GL}_n(\mathbb{Z}_l)$ has a closed pro-l normal subgroup N such that the abelian-simple length of Λ/N is at most m.*

We also need Lemma 2.3 of [**2**].

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

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 $(K_iL)_{i\in I}$ 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.*

Proof. If $M \subseteq \prod_{i\in I\smallsetminus J} K_i$ 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 $M \not\subseteq \prod_{i\in I\smallsetminus J} K_i$. 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. □

The following result is the ring version of a special case of [**1**, Corollary 4.3].

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

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

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

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 $K(A_{l^\infty}(K_{\mathrm{sep}}))$. Then, E_l is a Galois extension of K and $\mathrm{Gal}(K(A_{l^\infty}(K_{\mathrm{sep}}))/E_l) \cong \Lambda_l$ is a pro-l-group and the abelian-simple length of $\mathrm{Gal}(E_l/K)$ 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 $\mathrm{Gal}(E/K)$ is less than or equal to m.

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

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

REFERENCES

1. L. Bary-Soroker, A. Fehm and G. Wiese, Hilbertian fields and Galois representations, *J. für die reine und Angew. Math.* **712** (2016), 123–139.

2. A. Fehm and S. Petersen, Division fields of commutative algebraic groups, *Isr. J. Math.* **195** (2013), 123–134.

3. M. Fried and M. Jarden, *Field arithmetic* (3rd edn.), Ergebnisse der Mathematik (3), vol. 11 (Springer, Heidelberg, 2008).

4. D. Haran, Hilbertian fields under separable algebraic extensions, *Invent. Math.* **137** (1) (1999), 113–126.

5. M. Jarden, Diamonds in torsion of Abelian varieties, *J. Inst. Math. Jussieu* **9** (2010), 477–480.

6. W. Kuyk, Extensions de corps hilbertiens, *J. Algebra* **14** (1970), 112–124.

7. M. Larsen and R. Pink, Finite subgroups of algebraic groups, *J. Am. Math. Soc.* **24** (2011), 1105–1158.

8. R. Weissauer, Der Hilbertsche Irreduzibilitätssatz, *J. für die reine und Angew. Math.* **334** (1982), 203–220.