Hilbertian fields and Galois representations

Lior Bary-Soroker   Arno Fehm   Gabor Wiese

November 25, 2013

Abstract

We prove a new Hilbertianity criterion for fields in towers whose steps are Galois with Galois group either abelian or a product of finite simple groups. We then apply this criterion to fields arising from Galois representations. In particular we settle a conjecture of Jarden on abelian varieties.

1   Introduction

A field K is called **Hilbertian** if for every irreducible polynomial $f(t, X) \in K[t, X]$ that is separable in X there exists $\tau \in K$ such that $f(\tau, X) \in K[X]$ is irreducible. This notion stems from Hilbert's irreducibility theorem, which, in modern terminology, asserts that number fields are Hilbertian. Hilbert's irreducibility theorem and Hilbertian fields play an important role in algebra and number theory, in particular in Galois theory and arithmetic geometry, cf. [9], [13], [15], [17], [18], [21].

In the light of this, an important question is under what conditions an extension of a Hilbertian field is Hilbertian. As central examples we mention Kuyk's theorem [9, Theorem 16.11.3], which asserts that an abelian extension of a Hilbertian field is Hilbertian, and Haran's diamond theorem [10], which is the most advanced result in this area.

In this work we introduce an invariant of profinite groups that we call **abelian-simple length** (see Section 2 for definition and basic properties) and prove a Hilbertianity criterion for extensions whose Galois groups have finite abelian-simple length:

Theorem 1.1. *Let L be an algebraic extension of a Hilbertian field K. Assume there exists a tower of field extensions*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$

such that $L \subseteq K_m$ and for each i the extension K_i/K_{i-1} is Galois with group either abelian or a (possibly infinite) product of finite simple groups. Then L is Hilbertian.

In the special case where $m = 1$ and K_1/K_0 is abelian we recover Kuyk's theorem. Already the case when $m = 2$ and both K_1/K_0 and K_2/K_1 are abelian is new. As a first

application of this criterion we then prove Hilbertianity of certain extensions arising from Galois representations:

Theorem 1.2. *Let K be a Hilbertian field, let L/K be an algebraic extension, let n be a fixed integer, and for each prime number ℓ let*

$$\rho_\ell \colon \operatorname{Gal}(K) \to \operatorname{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a Galois representation. Assume that L is fixed by $\bigcap_\ell \ker \rho_\ell$. Then L is Hilbertian.

This theorem is a strengthening of a recent result of Thornhill, who in [20] proves Theorem 1.2 under the extra assumptions that L is Galois over K and the image of ρ_ℓ is in $\operatorname{GL}_n(\mathbb{Z}_\ell)$.

Both Thornhill's and our research was motivated by a conjecture of Jarden. Namely, when applying Theorem 1.2 to the family of Galois representations $\rho_\ell \colon \operatorname{Gal}(K) \to \operatorname{GL}_{2\dim(A)}(\mathbb{Z}_\ell)$ coming from the action of the absolute Galois group $\operatorname{Gal}(K)$ on the Tate module $T_\ell(A)$ of an abelian variety A over K, Theorem 1.2 immediately implies the following result.

Theorem 1.3 (Jarden's conjecture). *Let K be a Hilbertian field and A an abelian variety over K. Then every field L between K and $K(A_{tor})$, the field generated by all torsion points of A, is Hilbertian.*

This conjecture was proven by Jarden in [11] for number fields K, and in [5] by Jarden, Petersen, and the second author for function fields K. Thornhill is able to deduce the special case where L is Galois over K, like above.

Jarden's proof in [11] uses Serre's open image theorem, while Thornhill's proof in [20] is based on a theorem of Larsen and Pink [14] on subgroups of GL_n over finite fields. Another key ingredient in both proofs is Haran's diamond theorem. The fact that L/K is Galois is crucial in Thornhill's approach, essentially since in this special case Theorem 1.1 is a straightforward consequence of Kuyk's theorem and the diamond theorem. We show in Section 4.3 that Theorem 1.2, and hence Theorem 1.3, follows rather simply from Theorem 1.1 and the theorem of Larsen and Pink. Our proof of Theorem 1.1, which takes up Sections 2 and 3 of this paper, utilizes the twisted wreath product approach that Haran developed to prove his diamond theorem.

Theorem 1.1 has many other applications, some of which are presented in Section 5. For example we show that if L is the compositum of all degree d extensions of $\mathbb{Q}$, for some fixed d, then every subfield of L is Hilbertian (Theorem 5.4). A similar application is given when L is the compositum of the fixed fields of all $\ker \bar{\rho}$, where $\bar{\rho}$ runs over all *finite* representations of $\operatorname{Gal}(\mathbb{Q})$ of fixed dimension d (Theorem 5.1). We also include one application to the theory of free profinite groups (Theorem 5.7).

2 Groups of finite abelian-simple length

2.1 Basic theory

Let G be a profinite group. 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 $i \geq 0$.

Lemma 2.1. *Let G be a profinite group with generalized derived series $G^{(i)}$, $i = 0, 1, 2, \ldots$. Then $G^{(i)} \trianglelefteq G$ for each $i \geq 0$, and if $G^{(i)} \neq 1$, then $G^{(i+1)} \neq G^{(i)}$.*

Proof. Since $G^{(i)}$ is characteristic in $G^{(i-1)}$ and since by induction $G^{(i-1)} \trianglelefteq G$, the first assertion follows. If $G^{(i)} \neq 1$, then $G^{(i)}$ has a nontrivial finite simple quotient. Hence $G^{(i+1)} = D(G^{(i)}) \neq G^{(i)}$, as claimed in the second assertion. $\square$

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 $l(G) < \infty$.

Lemma 2.2. *Let G be a finite group. Then $l(G) \leq \log_2(|G|) < \infty$.*

Proof. By Lemma 2.1, if $G^{(i)} \neq 1$, then $[G^{(i)} : G^{(i+1)}] \geq 2$. Hence $|G| = \prod_{i=1}^{l}[G^{(i-1)} : G^{(i)}] \geq 2^l$, where $l = l(G)$. $\square$

Example 2.3. If G is pro-solvable, then the generalized derived series coincides with the derived series of G. In particular, such G is solvable if and only if G is of finite abelian-simple length.

We will need the following well-known result.

Lemma 2.4. *Let $G = A \times \prod_{i \in I} S_i$ be a profinite group, where A is abelian and each S_i is a non-abelian finite simple group. If N is a closed normal subgroup of G, then $N = (N \cap A) \times \prod_{i \in J} S_i$ for some subset $J \subseteq I$. In particular, $G/N \cong (AN/N) \times \prod_{i \in I \smallsetminus J} S_i$.*

Proof. The proof of [9, Lemma 25.5.3] goes through almost literally. $\square$

For a profinite group G let us denote by $D_0(G)$ the intersection of all maximal open normal subgroups N of G such that G/N is not abelian. Then $D(G) = D_0(G) \cap G'$, where G' is the commutator subgroup of G.

Lemma 2.5. *Let G be a profinite group. Then $D(G)$ is the smallest closed normal subgroup of G such that $G/D(G)$ is isomorphic to a direct product of finite simple groups and abelian groups.*

Proof. By [9, Lemma 18.3.11], $G/D_0(G)$ is a product of finite non-abelian simple groups, and if N is a maximal closed normal subgroup of G containing $D_0(G)$, then G/N is non-abelian. It follows that $D_0(G)G' = G$, so $G/D(G) = (G/G') \times (G/D_0(G))$ is of the asserted form.

Conversely, assume that N is a closed normal subgroup of G with $G/N = \prod_{i \in I} S_i$, with S_i either abelian or finite simple. Let $\pi_j : \prod_{i \in I} S_i \to S_j$ be the projection map and $\pi : G \to G/N$ the quotient map. Then $N = \bigcap_{j \in I} \ker(\pi_j \circ \pi) \geq D(G)$, since $G/\ker(\pi_j \circ \pi) \cong S_j$. $\qquad\square$

Lemma 2.6. *Let G be a profinite group. Then G is of finite abelian-simple length if and only if there exists a subnormal series*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = 1$$

of closed subgroups of G with all factors G_{i-1}/G_i either abelian or a product of finite simple groups.

Proof. If G_i, $i = 0, \ldots, r$ is a subnormal series of G of length r of the asserted form, then $D(G) \leq G_1$ by Lemma 2.5. Thus, $G_i \cap D(G)$, $i = 1, \ldots, r$ is a subnormal series of $D(G)$ of length $r - 1$, so induction on r shows that $l(D(G)) < \infty$, and hence $l(G) < \infty$.

Conversely, if $l(G) < \infty$, then, by Lemma 2.5, $G^{(i)}$, $i = 0, \ldots, l(G)$ can easily be refined to a subnormal series of the asserted form. $\qquad\square$

Lemma 2.7.   1. *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, $l(H) \leq l(G)$.*

  2. *If N is a closed normal subgroup of a profinite group G, then $N^{(i)} \leq G^{(i)}$ for each i. In particular, $l(N) \leq l(G)$.*

  3. *If $\mathcal{N}$ is a downward directed family of closed normal subgroups of G with $\bigcap_{N \in \mathcal{N}} N = 1$, then $G^{(i)} = \varprojlim_{N \in \mathcal{N}} (G/N)^{(i)}$ for each i. In particular, $l(G) = \sup_{N \in \mathcal{N}} l(G/N)$.*

  4. *Let $\alpha \colon G \to K$ and $\beta \colon H \to K$ be epimorphisms of profinite groups, and let $G \times_K H$ be the corresponding fiber product. Then $(G \times_K H)^{(i)} \leq G^{(i)} \times_{K^{(i)}} H^{(i)}$ for each i. In particular, $l(G \times_K H) \leq \max(l(G), l(H))$.*

Proof. Recall that the Melnikov subgroup $M(G)$ of a profinite group G is defined as the intersection of all maximal open normal subgroups of G. Thus $D(\Gamma) = M(\Gamma) \cap \Gamma'$, for any profinite group Γ.

We start with Assertion 1. Since α is surjective, it follows that $\alpha(G') = H'$ and $\alpha(M(G)) = M(H)$ [9, Lemma 25.5.4]. Thus $\alpha(D(G)) \subseteq D(H)$. Since $H/\alpha(D(G))$ is a quotient of $G/D(G)$, Lemma 2.5 and Lemma 2.4 together give that $\alpha(D(G)) \supseteq D(H)$. So, $\alpha(D(G)) = D(H)$. By induction we are done.

To get Assertion 2 note that $N' \leq G'$ and that $M(N) \leq M(G)$ by [9, Lemma 25.5.1]. Therefore $D(N) \leq D(G)$. Since $D(N)$ is characteristic in N, we get that $D(N) \trianglelefteq D(G)$. Therefore, by induction, $N^{(i)} \leq G^{(i)}$ for every i.

Let us prove Assertion 3. Since $\mathcal{N}$ is directed and $\bigcap_{N \in \mathcal{N}} N = 1$, $G = \varprojlim_{N \in \mathcal{N}} G/N$. Assertion 1 implies that if $N \in \mathcal{N}$ and $\pi_N : G \to G/N$ is the quotient map, $\pi_N(G^{(i)}) = (G/N)^{(i)}$. Thus, $G^{(i)} = \varprojlim_{N \in \mathcal{N}} (G/N)^{(i)}$, cf. [16, Corollary 1.1.8a].

Finally we get to Assertion 4. Set $L = G \times_K H = \{(g, h) \colon \alpha(g) = \beta(h)\} \le G \times H$. Let $M = 1 \times \ker \beta$ and $N = \ker \alpha \times 1$. Then $NM = \ker \alpha \times \ker \beta \cong N \times M$, $L/M = G$, and $L/N = H$. Thus, if $\mathcal{U}$ denotes the set of closed normal subgroups U of L with L/U either abelian or finite simple, then

$$
D(L) \;=\; \bigcap_{U \in \mathcal{U}} U \;\le\; \Big(\bigcap_{\substack{U \in \mathcal{U} \\ M \le U}} U \Big) \cap \Big(\bigcap_{\substack{U \in \mathcal{U} \\ N \le U}} U \Big) \;=\; D(G) \times_{D(K)} D(H).
$$

The last equality holds since $\alpha(D(G)) = \beta(D(H)) = D(K)$ by Assertion 1. By induction, $L^{(i)} \le G^{(i)} \times_{K^{(i)}} H^{(i)}$. $\qquad\square$

Proposition 2.8. *If $\mathcal{N}$ is a family of closed normal subgroups of G with $\bigcap_{N \in \mathcal{N}} N = 1$, then $l(G) = \sup_{N \in \mathcal{N}} l(G/N)$.*

Proof. Let $\mathcal{N}'$ be the family of finite intersections of elements of $\mathcal{N}$. By Lemma 2.7.3, $l(G) = \sup_{N \in \mathcal{N}'} l(G/N)$. If $N_1, N_2 \in \mathcal{N}$, then $G/(N_1 \cap N_2) \cong (G/N_1) \times_{G/(N_1 N_2)} (G/N_2)$, so $\sup_{N \in \mathcal{N}'} l(G/N) = \sup_{N \in \mathcal{N}} l(G/N)$ by Lemma 2.7.4. $\qquad\square$

We already saw that the class of profinite groups of finite abelian-simple length is closed under taking quotients and normal subgroups. In fact, it is also closed under forming group extensions:

Proposition 2.9. *Let N be a closed normal subgroup of G. Then $l(G) \le l(N) + l(G/N)$.*

Proof. Let $m = l(G/N)$, $n = l(N)$, and let $\pi : G \to G/N$ be the quotient map. By Lemma 2.7.1, $\pi(G^{(m)}) = (G/N)^{(m)} = 1$, so $G^{(m)} \le N$. Since $G^{(m)}$ is normal in G and hence in N, Lemma 2.7.2 implies that $G^{(m+n)} = (G^{(m)})^{(n)} \le N^{(n)} = 1$. Hence, $l(G) \le m + n$. $\qquad\square$

2.2 Twisted wreath products

Let A and $G_0 \le G$ be finite groups together with a (right) action of G_0 on A. The set of G_0-invariant functions from G to A,

$$
\mathrm{Ind}_{G_0}^{G}(A) = \{f \colon G \to A \ | \ f(\sigma\tau) = f(\sigma)^{\tau}, \ \forall \sigma \in G, \tau \in G_0\},
$$

forms a group under pointwise multiplication, on which G acts from the right by $f^{\sigma}(\tau) = f(\sigma\tau)$, for all $\sigma, \tau \in G$. The **twisted wreath product** is defined to be the semidirect product

$$
A \wr_{G_0} G = \mathrm{Ind}_{G_0}^{G}(A) \rtimes G,
$$

cf. [9, Definition 13.7.2]. The following observation will be used several times.

Lemma 2.10. *Let A and $G_0 \leq G$ be finite groups together with an action of G_0 on A, and let A_0 be a normal subgroup of A that is G_0-invariant. Then G_0 acts on A/A_0 and*

$$1 \longrightarrow \mathrm{Ind}_{G_0}^G(A_0) \longrightarrow A \wr_{G_0} G \overset{\alpha}{\longrightarrow} (A/A_0) \wr_{G_0} G \longrightarrow 1,$$

is an exact sequence of finite groups. Here $\alpha(f, \sigma) = (\bar{f}, \sigma)$, where $\bar{f}(\tau) = f(\tau)A_0$, for $\tau \in G$.

Proof. G_0 acts on A/A_0 by $(aA_0)^\sigma = a^\sigma A_0$. To see that α is a homomorphism note that $\bar{f}^\sigma(\tau) = f(\sigma\tau)A_0 = f^\sigma(\tau)A_0 = \overline{f^\sigma}(\tau)$. It is trivial that α is surjective and that $\ker(\alpha) = \mathrm{Ind}_{G_0}^G(A_0)$. $\qquad\square$

The main objective of this section is to show that the abelian-simple length grows in wreath products:

Proposition 2.11. *Let $m \in \mathbb{N}$, let A be a nontrivial finite group, and let $G_0 \leq G$ be finite groups together with an action of G_0 on A. Assume that*

$$[G^{(m)} G_0 : G_0] > 2^m.$$

Then

$$(A \wr_{G_0} G)^{(m+1)} \cap \mathrm{Ind}_{G_0}^G(A) \neq 1.$$

Remark 2.12. We do not know whether the assumption $[G^{(m)} G_0 : G_0] > 2^m$ can be replaced by the weaker condition $G^{(m)} \not\subseteq G_0$. Our proof makes essential use of the stronger assumption only once (namely in the "Second Case" of Lemma 2.16).

2.3 Proof of Proposition 2.11

The rest of this section is devoted to proving Proposition 2.11. It is rather technical and the auxiliary statements will not be used anywhere else in this paper. First we deal with several special cases depending on A and on the action of G_0, and then deduce the proposition.

Direct product of non-abelian simple groups

Lemma 2.13. *Under the assumptions of Proposition 2.11, let S be a non-abelian finite simple group, and assume that $A \cong \prod_{j=1}^n S_j$ with $n \geq 1$ and $S_j \cong S$ for all j. Let $H = A \wr_{G_0} G$. Then $H^{(m+1)} = \mathrm{Ind}_{G_0}^G(A) \rtimes G^{(m+1)}$. In particular, $H^{(m+1)} \cap \mathrm{Ind}_{G_0}^G(A) \neq 1$.*

Proof. Let $L = \mathrm{Ind}_{G_0}^G(A)$. We prove by induction on i that $H^{(i)} = L \rtimes G^{(i)}$, for every $i = 0, \ldots, m+1$. For $i = 0$ the assertion is trivial.

Next assume that $i < m+1$ and $H^{(i)} = L \rtimes G^{(i)}$. It is clear that $H^{(i+1)} \leq L \rtimes G^{(i+1)}$, since the former is the intersection of all normal subgroups of $L \rtimes G^{(i)}$ whose quotient is either simple or abelian and the latter is the intersection of the subfamily of those normal subgroups that contain L. Therefore it suffices to show that if U is a normal subgroup of $L \rtimes G^{(i)}$ with $(L \rtimes G^{(i)})/U$ either simple or abelian, then $L \leq U$.

6

Assume the contrary, so $L \cap U$ is a proper normal subgroup of L. The quotient $L/(L \cap U) \cong LU/U$ is either simple or abelian, as a nontrivial normal subgroup of the simple resp. abelian group $(L \rtimes G^{(i)})/U$. Since L is a direct product of copies of A, hence of S, $L/(L \cap U)$ is not abelian. Lemma 2.4 implies that $L \cap U$ is the kernel of one of the projections $L \to A \to S_j$. More precisely, there exist $\sigma \in G$ and $1 \leq j \leq n$ such that if we denote by $\pi_j \colon A \to S_j$ the projection map, then $L \cap U = \{f \in \operatorname{Ind}_{G_0}^G(A) \mid \pi_j(f(\sigma)) = 1\}$.

The assumption $[G^{(m)}G_0 : G_0] > 2^m$ implies that $G^{(i)} \nsubseteq G_0$, since $i \leq m$. So since $G^{(i)}$ is normal in G, there exists $\tau \in G^{(i)} \smallsetminus (G_0)^{\sigma^{-1}}$. It follows that

$$
\begin{aligned}
L \cap U &= (L \cap U)^\tau = \{f \in \operatorname{Ind}_{G_0}^G(A) \mid \pi_j(f(\sigma)) = 1\}^\tau \\
&= \{f \in \operatorname{Ind}_{G_0}^G(A) \mid \pi_j(f(\tau^{-1}\sigma)) = 1\}.
\end{aligned}
$$

Since $\tau^{-1}\sigma G_0 \neq \sigma G_0$ by the choice of τ, there exists $f \in L$ such that $f(\tau^{-1}\sigma) \neq 1$ but $f(\sigma) = 1$. This implies that $f \in (L \cap U) \smallsetminus (L \cap U)^\tau = \emptyset$ – a contradiction. Thus $L \leq U$, as needed. $\qquad\square$

Nontrivial irreducible representation

We say that a representation V of G_0 is **nontrivial** if there exist $v \in V$ and $\sigma \in G_0$ such that $v^\sigma \neq v$.

Lemma 2.14. *Let $G_0 \leq G$ be finite groups, let p be a prime number and let A be a nontrivial finite irreducible $\mathbb{F}_p$-representation of G_0. Let $H = A \wr_{G_0} G$. Then $H' = \operatorname{Ind}_{G_0}^G(A) \rtimes G'$.*

Proof. Let A_0 be the subspace of A spanned by $\{a^\sigma - a \mid a \in A, \sigma \in G_0\}$. Since $(a^\sigma - a)^\tau = (a^\tau)^{\tau^{-1}\sigma\tau} - a^\tau \in A_0$ for all $\tau \in G_0$, we get that A_0 is G_0-invariant. Since the action of G_0 is nontrivial, $A_0 \neq 0$. The assumption that A is an irreducible representation then implies that $A_0 = A$.

For $a \in A$ and $\sigma \in G_0$, let $\tilde{f}_{a,\sigma} \in \operatorname{Ind}_{G_0}^G(A)$ be defined by $\tilde{f}_{a,\sigma}(\tau) = a^{\sigma\tau} - a^\tau$ if $\tau \in G_0$ and $\tilde{f}_{a,\sigma}(\tau) = 1$ if $\tau \in G \smallsetminus G_0$. Then $\tilde{F} = \{\tilde{f}_{a,\sigma} \mid a \in A, \sigma \in G_0\}$ generates the subgroup $\{f \mid f(\tau) = 1, \ \forall \tau \in G \smallsetminus G_0\}$ of $\operatorname{Ind}_{G_0}^G(A)$. Hence $\tilde{F}$ generates $\operatorname{Ind}_{G_0}^G(A)$ as a normal subgroup of $H = A \wr_{G_0} G$.

But $\tilde{f}_{a,\sigma} = [f_a, \sigma]$, where $f_a(\tau) = a^\tau$ if $\tau \in G_0$ and $f(\tau) = 1$ otherwise. So $\tilde{f}_{a,\sigma} \in H'$ and hence $\operatorname{Ind}_{G_0}^G(A) \leq H'$. So $\operatorname{Ind}_{G_0}^G(A) \rtimes G' \leq H'$. On the other hand, since $H/(\operatorname{Ind}_{G_0}^G(A) \rtimes G') \cong G/G'$ is abelian, $\operatorname{Ind}_{G_0}^G(A) \rtimes G' \geq H'$. Thus, $H' = \operatorname{Ind}_{G_0}^G(A) \rtimes G'$. $\qquad\square$

Trivial representation

Let p be a prime number and G a finite group acting on a finite set X. Then the group ring $\mathbb{F}_p[G]$ acts on the $\mathbb{F}_p$-vector space $V_0(G, X) = (\mathbb{F}_p)^X$ of functions from X to $\mathbb{F}_p$. For $i \geq 0$ we let $V_{i+1}(G, X)$ be the subspace of $V_i(G, X)$ generated by the elements $f^{1-g} = f - f^g$, where $f \in V_i(G, X)$ and $g \in G^{(i)}$.

Lemma 2.15. *Let G be a finite group acting on a finite set X, and let $m \in \mathbb{N}$. Assume there exists $x \in X$ such that $|G^{(m)}x| > 2^m$. Then $V_{m+1}(G, X) \neq 0$.*

Proof. For $f \in V_0(G, X)$ let $\mathrm{supp}(f) = \{y \in X : f(y) \neq 0\}$. Let $f_0 \in V_0(G, X)$ be defined by $f_0(x) = 1$ and $f_0(y) = 0$ for all $y \neq x$. We construct inductively a sequence $g_1, ..., g_{m+1} \in G^{(m)}$ such that for each $0 \leq k \leq m + 1$,

$$f_k := f_0^{(1-g_1)\cdots(1-g_k)} \in V_k(G, X)$$

satisfies $0 < |\mathrm{supp}(f_k)| \leq 2^k$. For $k = 0$, there is nothing to show. Let $0 < k \leq m$ and assume $g_1, \ldots, g_k$ are already constructed. Since $\emptyset \neq \mathrm{supp}(f_k) \subseteq G^{(m)}x$ and $|\mathrm{supp}(f_k)| \leq 2^k < |G^{(m)}x|$, there exists $g_{k+1} \in G^{(m)}$ with $\mathrm{supp}(f_k^{g_{k+1}}) \not\subseteq \mathrm{supp}(f_k)$, hence $f_{k+1} = f_k - f_k^{g_{k+1}} \neq 0$. Clearly, $|\mathrm{supp}(f_{k+1})| \leq 2|\mathrm{supp}(f_k)| \leq 2^{k+1}$, concluding the induction step. $\square$

Abelian group

Lemma 2.16. *Let p be a prime number. Let $n \geq 0$, let $k > 0$, let $G_0 \leq G$ be finite groups, and let G_0 act on $A = (\mathbb{F}_p)^k$. If $n > 0$, assume in addition that $[G^{(n-1)}G_0 : G_0] > 2^{n-1}$. Then $(A \wr_{G_0} G)^{(n)} \cap \mathrm{Ind}_{G_0}^G(A) \neq 1$.*

Proof. We prove the lemma by induction on n. For $n = 0$, the claim is obvious since $k > 0$. Therefore, assume that $n > 0$ and that the statement of the lemma holds for all smaller n (for arbitrary groups G_0, G and arbitrary $k > 0$).

Let V_0 be a maximal G_0-invariant proper subspace of A. Then $V = A/V_0 \neq 0$ is an irreducible $\mathbb{F}_p$-representation of G_0. By Lemma 2.10, $V \wr_{G_0} G$ is a quotient of $A \wr_{G_0} G$ and $\mathrm{Ind}_{G_0}^G(A)$ is the preimage of $\mathrm{Ind}_{G_0}^G(V)$. Thus, by Lemma 2.7.1 it suffices to show that $(V \wr_{G_0} G)^{(n)} \cap \mathrm{Ind}_{G_0}^G(V) \neq 1$.

To this end set $H = V \wr_{G_0} G$ and $L = \mathrm{Ind}_{G_0}^G(V)$. If N is a normal subgroup of H with H/N simple non-abelian, then $L/(N \cap L) = LN/N$ is an abelian normal subgroup of H/N, hence $L/(N \cap L) = 1$, so $L \leq N$. Therefore $D_0(H) = L \rtimes D_0(G)$ (cf. p. 3) and

$$D(H) = D_0(H) \cap H' = (L \rtimes D_0(G)) \cap H'. \tag{2.1}$$

We distinguish between two cases:

FIRST CASE: G_0 acts nontrivially on V.

By Lemma 2.14 we have $H' = L \rtimes G'$. Plugging this into (2.1) we get that $D(H) = L \rtimes D(G)$. Let $\tilde{G} = D(G)$ and $\tilde{G}_0 = \tilde{G} \cap G_0$. If $n > 1$, then

$$[\tilde{G}^{(n-2)}\tilde{G}_0 : \tilde{G}_0] = [\tilde{G}^{(n-2)} : \tilde{G}^{(n-2)} \cap \tilde{G}_0] = [G^{(n-1)} : G^{(n-1)} \cap G_0] > 2^{n-1} > 2^{n-2}.$$

Applying the induction hypothesis to $\tilde{G}_0 \leq \tilde{G}$ and V gives that $(V \wr_{\tilde{G}_0} \tilde{G})^{(n-1)} \cap \mathrm{Ind}_{\tilde{G}_0}^{\tilde{G}}(V) \neq 1$. The epimorphism $\pi : L \rtimes D(G) \to V \wr_{\tilde{G}_0} \tilde{G}, (f, \sigma) \mapsto (f|_{\tilde{G}}, \sigma)$, restricts by Lemma 2.7.1 to

an epimorphism $(V \wr_{G_0} G)^{(n)} = (L \rtimes D(G))^{(n-1)} \to (V \wr_{\tilde{G}_0} \tilde{G})^{(n-1)}$, and $\pi^{-1}(\mathrm{Ind}_{\tilde{G}_0}^{\tilde{G}}(V)) = \mathrm{Ind}_{G_0}^{G}(V)$. The claim follows.

SECOND CASE: G_0 acts trivially on V.

Since V is an irreducible $\mathbb{F}_p$-representation of G_0, $V \cong \mathbb{F}_p$. Note that $[f, \sigma] = f^\sigma - f$, for all $f \in \mathrm{Ind}_{G_0}^{G}(V)$ and $\sigma \in G$. Let $V_i = V_i(G, G/G_0)$. Since the action of G_0 on V is trivial we can identify $\mathrm{Ind}_{G_0}^{G}(V)$ with $V_0 = (\mathbb{F}_p)^{G/G_0}$. Hence, $[\mathrm{Ind}_{G_0}^{G}(V), G] = V_1$. Thus $H' \geq V_1 \rtimes G'$. Since $(V_0 \rtimes G)/(V_1 \rtimes G') \cong (V_0/V_1) \times (G/G')$ is abelian, we get that $H' = V_1 \rtimes G'$. Plugging this into (2.1) we get that $D(H) = V_1 \rtimes D(G)$. Inductively, if $H^{(i)} = V_i \rtimes G^{(i)}$, then as in the paragraph preceding (2.1), $D_0(H^{(i)}) = V_i \rtimes D_0(G^{(i)})$. Since $[f, \sigma] = f^{\sigma-1} \in V_{i+1}$ for all $f \in V_i$ and $\sigma \in G^{(i)}$, we have $(H^{(i)})' = V_{i+1} \rtimes (G^{(i)})'$ as above. So

$$H^{(i+1)} = D(H^{(i)}) = D_0(H^i) \cap (H^{(i)})' = V_{i+1} \rtimes G^{(i+1)}.$$

In particular, $H^{(n)} \cap \mathrm{Ind}_{G_0}^{G}(V) = V_n$. Finally, since we assume that $[G^{(n-1)}G_0 : G_0] > 2^{n-1}$, Lemma 2.15 gives that $V_n \neq 0$, proving the claim. $\qquad\square$

Proof of Proposition 2.11

Assume that $G_0 \leq G$ are finite groups, G_0 acts on the nontrivial finite group A, and $[G^{(m)}G_0 : G_0] > 2^m$. We claim that $(A \wr_{G_0} G)^{(m+1)} \cap \mathrm{Ind}_{G_0}^{G}(A) \neq 1$.

Let S be a simple quotient of A, and let A_0 be the intersection of all normal subgroups of A with $A/N \cong S$. Then A_0 is characteristic in A, hence G_0-invariant, and $\bar{A} = A/A_0$ is isomorphic to a nonempty direct product of copies of S (this is clear if S is abelian; see [16, Lemma 8.2.3] for the case where S is non-abelian). By Lemma 2.10, $\bar{A} \wr_{G_0} G$ is a quotient of $A \wr_{G_0} G$ and the preimage of $\mathrm{Ind}_{G_0}^{G}(\bar{A})$ is $\mathrm{Ind}_{G_0}^{G}(A)$. Thus, by Lemma 2.7.1, it suffices to show that $(\bar{A} \wr_{G_0} G)^{(m+1)} \cap \mathrm{Ind}_{G_0}^{G}(\bar{A}) \neq 1$.

If $\bar{A}$ is non-abelian, then the assertion follows from Lemma 2.13. If $\bar{A}$ is abelian, then the assertion follows from Lemma 2.16. $\qquad\square$

3   Hilbertianity criterion

We shall use the twisted wreath product approach of Haran, which we briefly recall for the reader's convenience.

We say that a tower of fields $K \subseteq E_0 \subseteq E \subseteq F \subseteq \hat{F}$ **realizes** a twisted wreath product $A \wr_{G_0} G$ if $\hat{F}/K$ is a Galois extension with Galois group isomorphic to $A \wr_{G_0} G$ and the tower of fields corresponds to the following subgroup series:

$$A \wr_{G_0} G \geq \mathrm{Ind}_{G_0}^{G}(A) \rtimes G_0 \geq \mathrm{Ind}_{G_0}^{G}(A) \geq \{f \in \mathrm{Ind}_{G_0}^{G}(A) \mid f(1) = 1\} \geq 1.$$

This definition coincides with [10, Remark 1.2].

Theorem 3.1 (Haran [10, Theorem 3.2 and the remark just before it])**.** *Let M be a separable algebraic extension of a Hilbertian field K. Suppose that for every α in M and every β in the separable closure M_s of M there exist*

1. *a finite Galois extension E of K that contains β; let $G = \mathrm{Gal}(E/K)$;*

2. *a field E_0 such that $K \subseteq E_0 \subseteq M \cap E$ and E_0 contains α; let $G_0 = \mathrm{Gal}(E/E_0)$;*

3. *a Galois extension N of K that contains both M and E,*

such that for every nontrivial finite group A and every action of G_0 on A there is no realization $K \subseteq E_0 \subseteq E \subseteq F \subseteq \hat{F}$ of $A \wr_{G_0} G$ with $\hat{F} \subseteq N$. Then M is Hilbertian.

We say that a separable algebraic extension M/K is **of finite abelian-simple length** if $\mathrm{Gal}(L/K)$ is, where L denotes the Galois closure of M/K.

Theorem 3.2. *Let M be a separable algebraic extension of a Hilbertian field K of finite abelian-simple length. Then M is Hilbertian.*
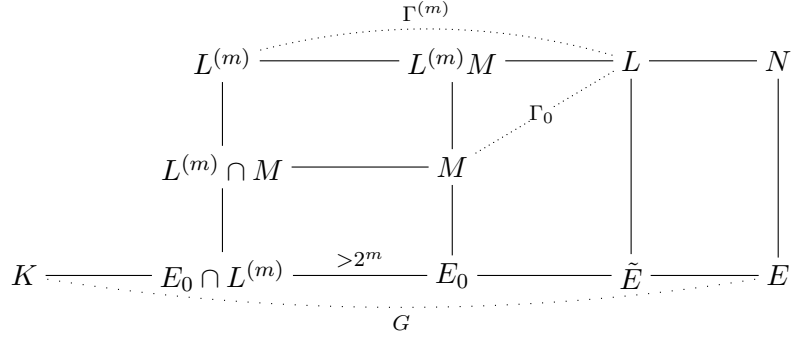
Proof. Let L be the Galois closure of M/K. Let $\Gamma = \mathrm{Gal}(L/K)$ and let $\Gamma^{(i)}$, $i = 0, 1, 2, \ldots$ be the generalized derived series of Γ. By assumption there exists a minimal $m \geq 0$ such that $\Gamma^{(m+1)} = 1$. Let $\Gamma_0 = \mathrm{Gal}(L/M)$ and for each i denote by $L^{(i)}$ the fixed field of $\Gamma^{(i)}$ in L.

If $[\Gamma_0 \Gamma^{(m)} : \Gamma_0] < \infty$, then, by Galois correspondence, M is a finite extension of $U = M \cap L^{(m)}$. Note that if $\hat{U}$ is the Galois closure of U/K, then $\hat{U} \subseteq L^{(m)}$ and thus $\mathrm{Gal}(\hat{U}/K)$ is a quotient of $\Gamma/\Gamma^{(m)}$. Thus $\mathrm{Gal}(\hat{U}/K)^{(m)}$ is a quotient of $(\Gamma/\Gamma^{(m)})^{(m)} = \Gamma^{(m)}/\Gamma^{(m)} = 1$ and therefore trivial (Lemma 2.7). Therefore induction on m implies that U is Hilbertian, and hence M is Hilbertian as a finite extension of U, see [9, Proposition 12.3.3].

Therefore we may assume that $[\Gamma_0 \Gamma^{(m)} : \Gamma_0] = \infty$, i.e. $[M : M \cap L^{(m)}] = \infty$. To prove that M is Hilbertian we apply Theorem 3.1. Let $\alpha \in M$ and $\beta \in M_s$. Since $M/M \cap L^{(m)}$ is infinite there exists a finite Galois extension E/K such that $\alpha, \beta \in E$ and $[E \cap M : E \cap M \cap L^{(m)}] > 2^m$.

Let $E_0 = E \cap M$, $G = \mathrm{Gal}(E/K)$, $G_0 = \mathrm{Gal}(E/E_0)$, and let $G^{(i)}$, $i = 0, 1, 2, \ldots$ be the generalized derived series of G. Note that $\alpha \in E_0$. We also let $N = EL$ and A a nontrivial group on which G_0 acts. By Theorem 3.1 it suffices to prove that there is no realization $K \subseteq E_0 \subseteq E \subseteq F \subseteq \hat{F}$ of $A \wr_{G_0} G$ with $\hat{F} \subseteq N$. Assume the contrary and identify $\mathrm{Gal}(\hat{F}/K)$ and $A \wr_{G_0} G$.

Let $\tilde{E} = E \cap L$, $\tilde{G} = \mathrm{Gal}(\tilde{E}/K)$, and let $\phi \colon \Gamma \to \tilde{G}$ and $\psi \colon G \to \tilde{G}$ be the corresponding restriction maps.

$$\Gamma^{(m)}$$

$$L^{(m)} \underline{\quad\quad} L^{(m)}M \underline{\quad\quad} L \underline{\quad\quad} N$$

$$\Gamma_0$$

$$L^{(m)} \cap M \underline{\quad\quad} M$$

$$K \underline{\quad\quad} E_0 \cap L^{(m)} \xrightarrow{>2^m} E_0 \underline{\quad\quad} \tilde{E} \underline{\quad\quad} E$$

$$G$$

By Lemma 2.7.1,

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

where $E^{(m)}$ is the fixed field of $G^{(m)}$ in E. Thus $E^{(m)} \cap \tilde{E} = L^{(m)} \cap \tilde{E}$. Since $E \cap M = \tilde{E} \cap M$ we have

$$E \cap M \cap E^{(m)} = \tilde{E} \cap M \cap E^{(m)} = M \cap E^{(m)} \cap \tilde{E} = M \cap L^{(m)} \cap \tilde{E} = \tilde{E} \cap M \cap L^{(m)} = E \cap M \cap L^{(m)}.$$

So

$$
\begin{aligned}
[G^{(m)}G_0 : G_0] &= [E \cap M : E \cap M \cap E^{(m)}] \\
&= [E \cap M : E \cap M \cap L^{(m)}] > 2^m.
\end{aligned}
$$

Proposition 2.11 gives that

$$(A \wr_{G_0} G)^{(m+1)} \cap \mathrm{Ind}_{G_0}^G(A) \neq 1.$$

Let $\tau \in (A \wr_{G_0} G)^{(m+1)} \cap \mathrm{Ind}_{G_0}^G(A)$ be nontrivial. Lift τ to $T \in \mathrm{Gal}(N/K)^{(m+1)}$ (Lemma 2.7). But $T|_L \in \mathrm{Gal}(L/K)^{(m+1)} = 1$ by the same lemma. Since $\tau \in \mathrm{Ind}_{G_0}^G(A) = \mathrm{Gal}(\hat{F}/E)$, it follows that $T|_E = 1$. But then $T = 1$, so $\tau = 1$. From this contradiction we get by Theorem 3.1 that M is Hilbertian. $\qquad\square$

Following [7] we call a field extension E/K an $\mathcal{H}$-**extension** if every intermediate field $K \subseteq M \subseteq E$ is Hilbertian.

Corollary 3.3. *Let K be Hilbertian and E/K a Galois extension of finite abelian-simple length. Then E/K is an $\mathcal{H}$-extension.*

Proof. Let $K \subseteq M \subseteq E$ be an intermediate field and let $\hat{M}$ be the Galois closure of M/K. Then $\mathrm{Gal}(E/K)$ surjects onto $\mathrm{Gal}(\hat{M}/K)$. Thus M/K is of finite abelian-simple length (Lemma 2.7), and by Theorem 3.2 it follows that M is Hilbertian. $\qquad\square$

Theorem 1.1 from the introduction is now an immediate consequence of Lemma 2.6 and Corollary 3.3.

4 Galois representations

4.1 Compact subgroups of GL_n

In this section we summarize a few well-known facts about compact subgroups of $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. For a finite extension F of $\mathbb{Q}_\ell$ we denote by $\mathcal{O}_F$ the integral closure of $\mathbb{Z}_\ell$ in F and by $\mathfrak{m}_F$ the maximal ideal of $\mathcal{O}_F$.

Lemma 4.1. *Every compact subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is contained in $\mathrm{GL}_n(F)$ for a finite extension F of $\mathbb{Q}_\ell$.*

Proof. See for example [19, p. 244]. $\qquad\qquad\square$

Lemma 4.2. *A compact subgroup of $\mathrm{GL}_n(F)$, where F is a finite extension of $\mathbb{Q}_\ell$, is conjugate to a subgroup of $\mathrm{GL}_n(\mathcal{O}_F)$.*

Proof. This can be proven exactly like the special case $F = \mathbb{Q}_\ell$ explained in [3, §6 Exercise 5a, p. 392]. $\qquad\qquad\square$

Lemma 4.3. *Every compact subgroup of $\mathrm{GL}_n(\mathcal{O}_F)$, where F is a finite extension of $\mathbb{Q}_\ell$, is a finitely generated profinite group.*

Proof. Let $m = [F : \mathbb{Q}_\ell]$. Then $\mathcal{O}_F$ is a free $\mathbb{Z}_\ell$-module of rank m. The regular representation of $\mathcal{O}_F$ as a $\mathbb{Z}_\ell$-module identifies the given compact subgroup of $\mathrm{GL}_n(\mathcal{O}_F)$ with a closed subgroup of $\mathrm{GL}_{mn}(\mathbb{Z}_\ell)$, and every such subgroup is finitely generated, see [9, Proposition 22.14.4]. $\qquad\qquad\square$

Lemma 4.4. *If F is a finite extension of $\mathbb{Q}_\ell$, then the kernel N of the residue map $\mathrm{GL}_n(\mathcal{O}_F) \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)$ is pro-ℓ.*

Proof. For the special case $F = \mathbb{Q}_\ell$, $\ell > 2$ see for example [4, Theorem 5.2]. For a direct proof of the general case observe that if $\mathfrak{m}_F = \lambda\mathcal{O}_F$, then $N = \varprojlim_k (I_n + \lambda\mathrm{Mat}_n(\mathcal{O}_F/\lambda^k))$, and $I_n + \lambda\mathrm{Mat}_n(\mathcal{O}_F/\lambda^k)$ is an ℓ-group. $\qquad\qquad\square$

4.2 A consequence of a theorem of Larsen and Pink

A straightforward application of the following theorem of Larsen-Pink allows us to conclude that a compact subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is an extension of a profinite group of finite abelian-simple length by a pro-ℓ group.

Theorem 4.5 (Larsen-Pink [14])**.** *For any n there exists a constant $J(n)$ depending only on n such that any finite subgroup Λ of GL_n over any field k possesses normal subgroups $\Lambda_3 \leq \Lambda_2 \leq \Lambda_1$ such that*

    1. $[\Lambda : \Lambda_1] \leq J(n)$.

2. *Either $\Lambda_1 = \Lambda_2$, or $\ell := \text{char}(k)$ is positive and Λ_1/Λ_2 is a direct product of finite simple groups of Lie type in characteristic ℓ.*

3. *Λ_2/Λ_3 is abelian of order not divisible by $\text{char}(k)$.*

4. *Either $\Lambda_3 = 1$, or $\ell := \text{char}(k)$ is positive and Λ_3 is an ℓ-group.*

Corollary 4.6. *For any n there exists $m = m(n)$ depending only on n such that every compact subgroup Λ of $\text{GL}_n(\mathcal{O}_F)$, where F is a finite extension of $\mathbb{Q}_\ell$, for some ℓ, admits a pro-ℓ normal subgroup N such that the abelian-simple length of Λ/N is at most m.*

Proof. Let $\Lambda_4 \leq \Lambda$ be the intersection of Λ with the kernel of the residue map $\text{GL}_n(\mathcal{O}_F) \to \text{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)$. Then Λ/Λ_4 is a subgroup of $\text{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)$ and Λ_4 is a pro-ℓ group by Lemma 4.4. Note that $\mathcal{O}_F/\mathfrak{m}_F$ is a finite field, so Λ/Λ_4 is a finite group.

Theorem 4.5 applied to Λ/Λ_4 gives normal subgroups $\Lambda_3 \leq \Lambda_2 \leq \Lambda_1$ of Λ that contain Λ_4 such that $[\Lambda : \Lambda_1] \leq J(n)$, Λ_1/Λ_2 is a product of finite simple groups, Λ_2/Λ_3 abelian, and Λ_3/Λ_4 is an ℓ-group.

Since Λ_4 is pro-ℓ we get that $N := \Lambda_3$ is also pro-ℓ. By Lemma 2.2, the abelian-simple length of Λ/Λ_1 is at most $\log_2(J(n))$. Thus by Proposition 2.9 the abelian-simple length of Λ/N is bounded by $m(n) := \log_2(J(n)) + 2$. $\qquad\square$

4.3 Proof of Theorem 1.2

The proof of the following proposition appears in [7, Proposition 2.4].

Proposition 4.7. *Let K_i, $i \in I$ be a family of $\mathcal{H}$-extensions of a Hilbertian field K which are Galois over K. Assume that there is an $\mathcal{H}$-extension E/K such that the fields K_iE, $i \in I$, are linearly disjoint over E. Then the compositum $\prod_{i \in I} K_i$ is an $\mathcal{H}$-extension of K.*

We now prove Theorem 1.2. Let K be Hilbertian, let $n \in \mathbb{N}$, let (ρ_ℓ) be a family of Galois representations of dimension n, and let L be an algebraic extension of K fixed by $\bigcap_\ell \ker \rho_\ell$. We want to prove that L is Hilbertian.

Since a purely inseparable extension of a Hilbertian field is Hilbertian, see [9, Proposition 12.3.3], we can assume without loss of generality that L/K is separable. Thus, if we denote by K_ℓ the fixed field of $\ker \rho_\ell$, L is contained in the compositum $\prod_\ell K_\ell$.

By Lemma 4.1 and Lemma 4.2, we can assume without loss of generality that for each ℓ, $\text{im}(\rho_\ell) \subseteq \text{GL}_n(\mathcal{O}_{F_\ell})$ for a finite extension F_ℓ of $\mathbb{Q}_\ell$. By Lemma 4.3, the Galois group $\text{Gal}(K_\ell/K) = \text{im}(\rho_\ell)$ is finitely generated, hence K_ℓ/K is an $\mathcal{H}$-extension, cf. [11, Lemma 4].

Applying Corollary 4.6 gives a constant $m = m(n)$ (depending only on n) and, for each ℓ, a Galois extension N_ℓ of K that is contained in K_ℓ such that $\text{Gal}(K_\ell/N_\ell)$ is pro-ℓ and the abelian-simple length of $\text{Gal}(N_\ell/K)$ is at most m. Let E be the compositum of all N_ℓ. By Proposition 2.8, the abelian-simple length of $\text{Gal}(E/K)$ is at most m. Thus E/K is an $\mathcal{H}$-extension by Corollary 3.3.

13

Since $\mathrm{Gal}(K_\ell E/E)$ embeds into $\mathrm{Gal}(K_\ell/N_\ell)$ via the restriction map, it is pro-ℓ. We thus get that the family $K_\ell E$ is linearly disjoint over E. By Proposition 4.7, the compositum $\prod_\ell K_\ell$ is an $\mathcal{H}$-extension of K, so L is Hilbertian, as claimed. $\qquad\square$

5 Further applications

5.1 Finite Galois representations

By a **finite n-dimensional representation** of $\mathrm{Gal}(K)$ we mean a continuous homomorphism $\rho : \mathrm{Gal}(K) \to \mathrm{GL}_n(k)$ with finite image, for some field k (equipped with the discrete topology). In Theorem 1.2, if instead of taking one n-dimensional ℓ-adic Galois representation for each prime number ℓ we take finite n-dimensional representations, we can actually handle all such representations simultaneously.

Theorem 5.1. *Let K be a Hilbertian field and let n be a fixed integer. Denote by Ω the family of all finite n-dimensional representations of $\mathrm{Gal}(K)$. Then every algebraic extension L of K fixed by $\bigcap_{\rho \in \Omega} \ker \rho$ is Hilbertian.*

Proof. As in the proof of Theorem 1.2 we can assume without loss of generality that L/K is separable. Let $\rho : \mathrm{Gal}(K) \to \mathrm{GL}_n(k)$ be an element of Ω, let K_ρ be the fixed field of $\ker(\rho)$, let $\Lambda = \mathrm{Gal}(K_\rho/K)$, and let $\ell = \mathrm{char}(k)$. By Theorem 4.5 there exist subgroups $\Lambda_3 \le \Lambda_2 \le \Lambda_1$ of Λ such that $[\Lambda : \Lambda_1] \le J(n)$, Λ_1/Λ_2 is a product of finite simple groups, Λ_2/Λ_3 abelian, and Λ_3 is an ℓ-group if $\ell > 0$, and trivial otherwise.

Since Λ_3 is unipotent (every element is annihilated by $X^{\ell^m} - 1 = (X-1)^{\ell^m}$ for some $m \in \mathbb{N}$), it is conjugate to a subgroup of the group of upper triangular matrices with diagonal $(1,\dots,1)$, and hence has derived length at most $n-1$, cf. [2, p. 87]. This implies that $l(\Lambda_3) \le n-1$. Putting everything together we get from Lemma 2.2 and Proposition 2.9 that $l(\Lambda) \le c := \log_2(J(n)) + 1 + n$.

Now let $M = \prod_{\rho \in \Omega} K_\rho$ be the compositum. Then $L \subseteq M$. Since $l(\mathrm{Gal}(K_\rho/K)) \le c$ for each $\rho \in \Omega$, by Proposition 2.8 we get $l(\mathrm{Gal}(M/K)) \le c < \infty$. Hence, by Corollary 3.3, L is Hilbertian. $\qquad\square$

Recall that if E/K is an elliptic curve then the action of $\mathrm{Gal}(K)$ on the p-torsion points $E[p]$ of E induces a Galois representation $\rho_{E,p} : \mathrm{Gal}(K) \to \mathrm{GL}_2(\mathbb{F}_p)$ and the fixed field $K_{\rho_{E,p}}$ of $\ker \rho$ is exactly the field one gets by adjoining the p-torsion points of E. Hence the following corollary follows from Theorem 5.1:

Corollary 5.2. *Let K be a Hilbertian field. Denote by K^{tor} the field obtained from K by adjoining for each prime number p all the p-torsions points $E[p]$ of all elliptic curves E/K. Then every subfield of K^{tor} that contains K is Hilbertian.*

Of course, a similar result holds true for all abelian varieties over K of a bounded dimension d.

5.2 Solvable extensions

A separable algebraic extension L/K is **solvable** if there exists a Galois extension N/K such that $L \subseteq N$ and $\mathrm{Gal}(N/K)$ is solvable. For example, if $K \subseteq K_1 \subseteq \cdots \subseteq K_n$ is a tower of abelian extensions, then K_n/K is solvable (note that the Galois group of the Galois closure of K_n/K has derived length at most n). On the other hand, the maximal pro-solvable extension $\mathbb{Q}^{sol}$ of $\mathbb{Q}$ is not solvable.

Let K be a Hilbertian field and L/K a solvable extension. If L/K is Galois, then L can be obtained from K by finitely many abelian steps. Thus an immediate application of Kuyk's theorem gives that if K is Hilbertian, then L is Hilbertian. To the best of our knowledge, the same result for non-Galois solvable extensions L/K was out of reach of the previously known Hilbertianity criteria.

Theorem 5.3. *Let K be a Hilbertian field and L/K a separable algebraic extension. Assume that L/K is solvable. Then L is Hilbertian.*

Proof. Let N/K be a solvable Galois extension with $L \subseteq N$. Then N/K is of finite derived length, thus of finite abelian-simple length. By Corollary 3.3, L is Hilbertian. $\qquad\square$

5.3 Extensions of bounded degree

Let K be a Hilbertian field, d a fixed integer, and $\{N_i \mid i \in I\}$ a family of finite extensions of K of *degree at most d*. Let $N = \prod_{i \in I} N_i$ be the compositum. If each N_i is Galois over K, then, using Haran's diamond theorem, it is rather easy to deduce that N is Hilbertian. It seems that the same statement in general, i.e. when the N_i/K are not necessarily Galois, is more difficult to achieve, and was unknown. However, it follows immediately from the following stronger result.

Theorem 5.4. *Let K be a Hilbertian field, let d be a fixed integer, and let N be the compositum of all extensions of K of degree at most d in some fixed algebraic closure of K. Then every intermediate field $K \subseteq L \subseteq N$ is Hilbertian.*

Proof. Since a purely inseparable extension of a Hilbertian field is Hilbertian [9, Proposition 12.3.3], we can assume without loss of generality that L is contained in the compositum N_0 of all separable extensions of K of degree at most d. Since a separable extension of degree at most d is contained in a Galois extension of degree at most $d!$, N_0 is contained in the compositum N_1 of all Galois extensions of K of degree at most $d!$. Since the abelian-simple length of a Galois extension of degree at most $d!$ is at most $\log_2(d!)$ (Lemma 2.2), by Proposition 2.8 the abelian-simple length of $\mathrm{Gal}(N_1/K)$ is at most $\log_2(d!)$. Thus by Corollary 3.3, L is Hilbertian. $\qquad\square$

5.4 Rational points on varieties

Let K be a Hilbertian field and let V be an affine K-variety of dimension n. By Theorem 5.4 there exists an $\mathcal{H}$-extension N/K such that $V(N)$ is Zariski-dense in V. Indeed, by the Noether normalization lemma there is a finite morphism $f : V \to \mathbb{A}_K^n$, and if the degree of f is d, then every point in $\mathbb{A}_K^n(K)$ is the image of a point of $V(\bar{K})$ of degree at most d, so if N denotes the compositum of all extensions of K of degree at most d, then $\mathbb{A}_K^n(K) \subseteq f(V(N))$ and $V(N)$ is Zariski-dense in V. Actually, if K is countable, one can find one $\mathcal{H}$-extension that works for all K-varieties V simultaneously: Recall that a field K is called **pseudo algebraically closed** if for every absolutely irreducible K-variety V, the set of K-rational points $V(K)$ is Zariski-dense in V, cf. [9, Chapter 11].

Theorem 5.5. *Every countable Hilbertian field K has a Galois extension M/K such that M is pseudo algebraically closed and every intermediate field $K \subseteq L \subseteq M$ is Hilbertian.*

Proof. By [9, Theorem 18.10.3] there exists a Galois extension M of K which is pseudo algebraically closed, and $\mathrm{Gal}(M/K) \cong \prod_{n=1}^{\infty} S_n$, where S_n is the symmetric group of degree n. Since each S_n has abelian-simple length at most 3, so has $\prod_{n=1}^{\infty} S_n$ by Proposition 2.8. By Corollary 3.3, every L as in the theorem is Hilbertian. $\qquad\square$

A conjecture of Frey and Jarden in [8] states that every abelian variety over $\mathbb{Q}$ acquires infinite rank over $\mathbb{Q}^{\mathrm{ab}}$, the maximal abelian extension of $\mathbb{Q}$. We cannot prove this but instead show that there is some other $\mathcal{H}$-extension with this property:

Corollary 5.6. *There exists an algebraic extension M of $\mathbb{Q}$ such that every subfield of M is Hilbertian and every nonzero abelian variety $A/\mathbb{Q}$ acquires infinite rank over M.*

Proof. By [6], every nonzero abelian variety over a pseudo algebraically closed field of characteristic zero has infinite rank. $\qquad\square$

5.5 Free profinite groups

Using the theory of pseudo algebraically closed fields we get the following freeness criterion for subgroups of the free profinite group of countable rank $\hat{F}_\omega$, cf. [9, Chapter 17].

Theorem 5.7. *Let $N \leq M \leq \hat{F}_\omega$ be closed subgroups such that N is normal in $\hat{F}_\omega$ and $\hat{F}_\omega/N$ is of finite abelian-simple length. Then $M \cong \hat{F}_\omega$.*

Proof. Recall that a countable pseudo algebraically closed field K is Hilbertian if and only if $\mathrm{Gal}(K) \cong \hat{F}_\omega$, see [12, Proposition 5.10.1 and Theorem 5.10.3]. Let K be such a countable Hilbertian pseudo algebraically closed field of characteristic 0, cf. [12, Example 5.10.7, 2nd paragraph].

Now view $N \leq M$ as subgroups of $\mathrm{Gal}(K) \cong \hat{F}_\omega$ and let E (respectively L) be the fixed field of N (respectively M) in an algebraic closure of K. Then $\mathrm{Gal}(E/K) = \hat{F}_\omega/N$ is of finite

abelian-simple length and $L \subseteq E$. Thus L is Hilbertian by Corollary 3.3, pseudo algebraically closed by [9, Corollary 11.2.5], and countable. Hence, $M = \mathrm{Gal}(L) \cong \hat{F}_\omega$, as claimed. $\square$

We conclude by pointing out without a complete proof that a more general statement holds in the category of pro-$\mathcal{C}$ groups, where $\mathcal{C}$ is an arbitrary Melnikov formation, cf. [9, Section 17.3]. The following result can be deduced from Theorem 5.7 along the lines of [1, second paragraph of proof of Theorem 3.1].

Corollary 5.8. *Let $\mathcal{C}$ be a Melnikov formation, let $F = \hat{F}_\omega(\mathcal{C})$ be the free pro-$\mathcal{C}$ group of countable rank and let $N \leq M \leq F$ be closed subgroups. Assume that N is normal in F, F/N is of finite abelian-simple length, and M is pro-$\mathcal{C}$. Then $M \cong \hat{F}_\omega(\mathcal{C})$.*

Acknowledgements

References

[1] Lior Bary-Soroker. Diamond theorem for a finitely generated free profinite group. *Mathematische Annalen*, 336(4):949–961, 2006.

[2] Armand Borel. *Linear Algebraic Groups.* Springer, second edition, 1991.

[3] Nicolas Bourbaki. *Lie groups and Lie algebras.* Springer, 1989.

[4] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups.* Cambridge University Press, second edition, 1999.

[5] Arno Fehm, Moshe Jarden, and Sebastian Petersen. Kuykian Fields. Forum Math. 24(5):1013–1022, 2012.

[6] Arno Fehm and Sebastian Petersen. On the rank of abelian varieties over ample fields. *International Journal of Number Theory*, 6(3):579–586, 2010.

[7] Arno Fehm and Sebastian Petersen. Division fields of commutative algebraic groups. Israel J. Math. 195(1):123–134, 2013.

[8] Gerhard Frey and Moshe Jarden. Approximation theory and the rank of abelian varieties over large algebraic fields. *Proceedings of the London Mathematical Society*, 28:112–128, 1974.

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

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

[11] Moshe Jarden. Diamonds in torsion of abelian varieties. J. Inst. Math. Jussieu 9(3):477–480, 2010.

[12] Moshe Jarden. *Algebraic patching*. Springer, 2011.

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

[14] Michael J. Larsen and Richard Pink. Finite subgroups of algebraic groups. *J. Amer. Math. Soc.*, 24(4):1105–1158, 2011.

[15] G. Malle and B. H. Matzat. *Inverse Galois Theory*. Springer, 1999.

[16] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, 2000.

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

[18] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Vieweg, 1997.

[19] Christopher Skinner. A note on the p-adic Galois representations attached to Hilbert modular forms. *Documenta Math.*, 14:241–258, 2009.

[20] Christopher Thornhill. Abelian varieties and Galois extensions of hilbertian fields. *J. Inst. Math. Jussieu*, 12(2):237–247, 2013.

[21] Helmut Völklein. *Groups as Galois groups. An introduction*. Cambridge University Press, 1996.

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, RAMAT AVIV, TEL AVIV 69978, ISRAEL

E-mail address: `barylior@post.tau.ac.il`

UNIVERSITÄT KONSTANZ, FACHBEREICH MATHEMATIK UND STATISTIK, FACH D 203, 78457 KONSTANZ, GERMANY

E-mail address: `arno.fehm@uni-konstanz.de`

UNIVERSITÉ DU LUXEMBOURG, FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION, 6, RUE RICHARD COUDENHOVE-KALERGI, L-1359 LUXEMBOURG, LUXEMBOURG

E-mail address: `gabor.wiese@uni.lu`