HILBERTIAN FIELDS UNDER SEPARABLE ALGEBRAIC EXTENSIONS

by

Dan Haran*

School of Mathematical Sciences, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: haran@math.tau.ac.il

July 7, 1998

* Research supported by The Israel Science Foundation and the Minkowski Center for Geometry at Tel Aviv University.

Introduction

A field K is said to be Hilbertian if for every irreducible polynomial $f \in K[X]$ there exist infinitely many $a \in K$ such that $f(a, X)$ is irreducible in $K[X]$. The name derives from the classical Hilbert Irreducibility Theorem [Hi] which states that $\mathbb{Q}$ possesses this property.

Hilbertian fields are essential in the investigation of the Inverse Galois Problem. It is therefore mostly desirable to know of an ambient field whether it is Hilbertian.

The question, when a separable algebraic extension M of a given Hilbertian field K is Hilbertian, has been addressed by Kuyk [Ku], Uchida [U], Weissauer [W], Jarden-Lubotzky [JL], and in [HJ] and [J1]. The hitherto accumulated knowledge has been summarized as follows in [JL]. In the following cases an extension M of a Hilbertian field K is Hilbertian:

(F1) M/K is a finite separable extension.

(F2) M/K is Galois and $\mathcal{G}(M/K)$ is finitely generated.

(F3) M is a proper finite separable extension of a Galois extension of K.

(F4) M/K is abelian.

(F5) M is the compositum of two Galois extensions of K, neither of which contains the other.

(F6) M is contained in a pronilpotent extension of K and $[M : K]$ is divisible by at least two primes.

(F7) M/K is separable and $[M : K] = \prod_p \alpha(p)$, with all $\alpha(p)$ finite.

In the present paper we exhibit a quite general sufficient condition for an algebraic separable extension M of a Hilbertian field K to be Hilbertian. The precise criterion (Theorem 3.2) is somewhat technical; it roughly states that certain embedding problems over K should have no solution contained in some Galois extension of K containing M.

The criterion is general in the sense that it can be used to prove all the above mentioned cases (F1) – (F7). But, furthermore, it provides a new large class of extensions that are Hilbertian. Our main result is:

THEOREM 4.1: *Let K be a Hilbertian field and let M_1, M_2 be two Galois extensions of K. Let M be an intermediate field of M_1M_2/K such that $M \not\subseteq M_1$ and $M \not\subseteq M_2$.*

Then M is Hilbertian.

The method also provides some insight into the Twinning principle of [JL], but this will be dealt with elsewhere.

The starting point of this investigation was M. Fried's proof of Weissauer's Theorem [FJ, Lemma 12.13 and Proposition 12.14], that looked like a disguised group theoretical method, similar to that of [HJ]. It took some time, however, to realize that the group theoretical construction behind it was not the usual wreath product, but the so-called twisted wreath product discussed in Section 1.

ACKNOWLEDGEMENT: The author thanks M. Jarden for helpful discussions and suggestions concerning the presentation of the paper.

1. Twisted wreath products

Let G and A be finite groups and let G' be a subgroup of G. Assume that G' acts on A (from the right). Let

$$\text{(1)} \qquad \mathrm{Ind}_{G'}^{G}(A) = \{f\colon G \to A \mid f(\sigma\rho) = f(\sigma)^{\rho}, \quad \text{for all } \sigma \in G,\ \rho \in G'\}$$

with the standard multiplication rule $(fg)(\sigma) = f(\sigma)g(\sigma)$. (We do not require that A be commutative.) Then G acts on $\mathrm{Ind}_{G'}^{G}(A)$ by the formula

$$\text{(2)} \qquad (f^{\tau})(\sigma) = f(\tau\sigma) \qquad \tau, \sigma \in G.$$

Definition 1.1: Let $A \,\mathrm{wr}_{G'}\, G$ be the semidirect product $G \ltimes \mathrm{Ind}_{G'}^{G}(A)$. Explicitly, each element of $A \,\mathrm{wr}_{G'}\, G$ is a pair (σ, f) with $\sigma \in G$ and $f \in \mathrm{Ind}_{G'}^{G}(A)$, and the product and the inverse in $A \,\mathrm{wr}_{G'}\, G$ are given by

$$\text{(3)} \qquad (\sigma, f)(\tau, g) = (\sigma\tau, f^{\tau}g) \qquad \text{and} \qquad (\sigma, f)^{-1} = (\sigma^{-1}, f^{-\sigma^{-1}}).$$

Let $\mathrm{pr}\colon A \,\mathrm{wr}_{G'}\, G \to G$ be the projection $(\sigma, f) \mapsto \sigma$.

We call both $\mathrm{pr}\colon A \,\mathrm{wr}_{G'}\, G \to G$ and $A \,\mathrm{wr}_{G'}\, G$ the **(twisted) wreath product** of A and G with respect to G' (see [Hp, p. 99]). ∎

Embed A in $\mathrm{Ind}_{G'}^{G}(A)$ by identifying each $a \in A$ with the function $f_a\colon G \to A$ given by $f_a(\rho) = \begin{cases} a^{\rho} & \rho \in G' \\ 1 & \rho \in G \smallsetminus G' \end{cases}$. Then $A = \{f \in \mathrm{Ind}_{G'}^{G}(A) \mid f(G \smallsetminus G') = 1\}$. If $\sigma \in G$, then $A^{\sigma} = \{f \in \mathrm{Ind}_{G'}^{G}(A) \mid f(G \smallsetminus \sigma^{-1}G') = 1\}$. In particular, if $G'\sigma = G'\tau$, then $A^{\sigma} = A^{\tau}$. Let Σ be a set of representatives of the right cosets of G' in G. It follows that $\mathrm{Ind}_{G'}^{G}(A)$ (as a group) is the direct product $\mathrm{Ind}_{G'}^{G}(A) = \prod_{\sigma\in\Sigma} A^{\sigma}$, which is isomorphic to the product of $(G : G')$ copies of A.

In another words, $\mathrm{Ind}_{G'}^{G}(A) = \prod_{\sigma\in\Sigma} \mathrm{Ind}_{G'}^{G}(A)/N^{\sigma}$, where

$$\text{(4)} \qquad N^{\sigma} = \{f \in \mathrm{Ind}_{G'}^{G}(A) \mid f(\sigma^{-1}) = 1\} = \prod_{\substack{\tau\in\Sigma \\ G'\sigma \neq G'\tau}} A^{\tau}$$

Here N^{σ} is the kernel of the epimorphism $\mathrm{Ind}_{G'}^{G}(A) \to A$ given by $f \mapsto f(\sigma^{-1})$. (Observe that $N = N^{1}$ is G'-invariant.)

Remark 1.2: Interpretation of generalized wreath products in Galois theory.

First a piece of notation: Let K'/K be a separable algebraic extension and let F/K' be a Galois extension. Fix a separable closure K_s of K that contains F. For an K-embedding $\sigma\colon K' \to K_s$ we denote by F^σ the field $F^{\hat\sigma}$, where $\hat\sigma \in G(K) = \mathrm{Aut}(K_s/K)$ extends σ. This is well defined. Furthermore, let $\mathcal{E}(K'/K)$ be the collection of K-embeddings $K' \to K_s$.

(i) Let $A \,\mathrm{wr}_{G'}\, G = G \ltimes \mathrm{Ind}_{G'}^{G}(A)$ and let N be as in (4).

Let $\hat F/K$ be a finite Galois extension such that $\mathcal{G}(\hat F/K) \cong A \,\mathrm{wr}_{G'}\, G$. Let L, K', F, $\hat K$, be the fixed fields of the subgroups $\mathrm{Ind}_{G'}^{G}(A)$, $G'\,\mathrm{Ind}_{G'}^{G}(A)$, N, G, respectively. It then follows from Galois theory that

(a) $K \subseteq K' \subseteq L \subseteq F \subseteq \hat F$,

(b) L/K, F/K' and $\hat F/K$ are finite Galois extensions,

(c) $\{F^\sigma\}$, for $\sigma \in \mathcal{E}(K'/K)$, are linearly disjoint over L and $\hat F = \prod_{\sigma\in\mathcal{E}(K'/K)} F^\sigma$.

(d) There is a field $\hat K$ such that $\hat K \cap L = K$ and $L\hat K = \hat F$.

(e) There is a field F' such that $L \cap F' = K'$ and $F = LF'$.

Notice that condition (e) follows from conditions (a)–(d) with $F' = F \cap (K'\hat K)$, the fixed field of G' in F.

$$
\begin{tikzcd}
 & F^\sigma \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[r, dash, "A"'] \arrow[d, dash, "G'"] & F \arrow[r, dash, "N"'] \arrow[d, dash, "G'"] & \hat F \arrow[d, dash, "G'"] \\
K' \arrow[r, dash, "A"'] \arrow[d, dash] & F' \arrow[r, dash] & K'\hat K \arrow[d, dash] \\
K \arrow[rr, dash] & & \hat K
\end{tikzcd}
$$

(ii) Conversely, consider a tower (a) of fields that satisfies conditions (b), (c), (d), for some field $\hat K$. Put $F' = F \cap (K'\hat K)$, $G = \mathcal{G}(\hat F/\hat K) \cong \mathcal{G}(L/K)$, $G' = \mathcal{G}(\hat F/K'\hat K)) \cong \mathcal{G}(F/F') \cong \mathcal{G}(L/K')$, and $A = \mathcal{G}(F/L) \cong \mathcal{G}(F'/K')$. Then $G' \le \mathcal{G}(F/K')$ acts on $A \triangleleft \mathcal{G}(F/K')$ by conjugation in $\mathcal{G}(F/K')$. We claim that there exists an isomorphism

$\varphi\colon A \operatorname{wr}_{G'} G \to \mathcal{G}(\hat{F}/K)$ which is identity on G and maps $\operatorname{Ind}_{G'}^{G}(A)$ onto $\mathcal{G}(\hat{F}/L)$. We say in this setup that the fields $K, K', L, F, \hat{F}$ **realize the wreath product** $A \operatorname{wr}_{G'} G$.

Proof: By (c), $\hat{F}/L$ is a Galois extension of degree $|A|^{(G:G')}$. It follows from (d) that $\mathcal{G}(\hat{F}/K) = \mathcal{G}(\hat{F}/\hat{K}) \ltimes \mathcal{G}(\hat{F}/L) = G \ltimes \mathcal{G}(\hat{F}/L)$.

Extend each $\sigma \in \mathcal{E}(K'/K)$ to an element of $G = \mathcal{G}(L/K)$. This gives a system Σ of representatives of the right cosets of G' in G. Let $\sigma \in \Sigma$. The group $\operatorname{Ind}_{G'}^{G}(A)$ acts on F^σ by

$$z^f = \left((z^{\sigma^{-1}})^{f(\sigma^{-1})}\right)^\sigma, \qquad z \in F^\sigma. \tag{5}$$

This does not depend on Σ: If $\rho \in G'$, then $F^{\rho\sigma} = F^\sigma$, since F/K' is Galois, and

$$\rho^{-1} f(\sigma^{-1}\rho^{-1})\rho = f(\sigma^{-1}\rho^{-1})^\rho = f(\sigma^{-1}\rho^{-1}\rho) = f(\sigma^{-1})$$

from which it follows that $\left((z^{(\rho\sigma)^{-1}})^{f((\rho\sigma)^{-1})}\right)^{\rho\sigma} = \left((z^{\sigma^{-1}})^{f(\sigma^{-1})}\right)^\sigma$.

Observe that action (5) fixes L, since $f(\sigma^{-1}) \in A$ fixes L. Thus (5) defines a homomorphism $\varphi_\sigma\colon \operatorname{Ind}_{G'}^{G}(A) \to \mathcal{G}(F^\sigma/L) \cong A$. Clearly, $\operatorname{Ker}\varphi_\sigma = N^\sigma$.

Using (c), the φ_σ's define a homomorphism

$$\varphi'\colon \operatorname{Ind}_{G'}^{G}(A) \to \prod_{\sigma\in\Sigma} \mathcal{G}(F^\sigma/L) = \mathcal{G}(\hat{F}/L).$$

As $\operatorname{Ker}\varphi' = \bigcap_{\sigma\in\Sigma} = 1$, and $|\operatorname{Ind}_{G'}^{G}(A)| = |A|^{|\Sigma|} = |\mathcal{G}(\hat{F}/L)|$, we get that φ' is an isomorphism.

Now, let $z \in F^\sigma$ and $\tau \in G$. Then $z^{\tau^{-1}} \in F^{(\sigma\tau^{-1})}$ and so

$$\begin{aligned}\left((z^{\tau^{-1}})^f\right)^\tau &= \left(\left(\left((z^{\tau^{-1}})^{(\tau\sigma^{-1})}\right)^{f(\tau\sigma^{-1})}\right)^{(\sigma\tau^{-1})}\right)^\tau = \left((z^{\sigma^{-1}})^{f(\tau\sigma^{-1})}\right)^\sigma \\ &= \left((z^{\sigma^{-1}})^{f^\tau(\sigma^{-1})}\right)^\sigma = z^{f^\tau},\end{aligned}$$

and hence $\tau^{-1}\varphi'(f)\tau = \varphi'(f^\tau)$. Thus φ' together with the identity map of $G = \mathcal{G}(L/K)$ gives an isomorphism $A \operatorname{wr}_{G'} G \to \mathcal{G}(\hat{F}/K)$. ∎

Remark 1.3: Let $K, K', L, F, \hat{F}$ realize $A \operatorname{wr}_{G'} G$. Let $\hat{K}$ be a field that satisfies condition (d) of Remark 1.2. If F_0 is a Galois extension of K' such that $L \subseteq F_0 \subseteq F$, let

$A_0 = \mathcal{G}(F_0/L)$ and $\hat{F}_0 = \prod_{\sigma\in\Sigma} F_0^\sigma$. Then $\hat{F}_0$ is a Galois extension of K contained in $\hat{F}$. Furthermore, let $\hat{K}_0 = \hat{F}_0 \cap \hat{K}$. Then $L \cap \hat{K}_0 = K$ and $L\hat{K}_0 = \hat{F}_0$. By Remark 1.2(ii), $K, K', L, F_0, \hat{F}_0$ realize $A_0 \,\mathrm{wr}_{G'}\, G$, as above. ∎

Our central application requires the following property of twisted wreath products:

LEMMA 1.4: *Let $\pi\colon A \,\mathrm{wr}_{G'}\, G \to G$ be a twisted wreath product, where $A \neq 1$. Let $B = \mathrm{Ind}_{G'}^G(A) = \mathrm{Ker}\,\pi$. Let $H_1 \triangleleft A \,\mathrm{wr}_{G'}\, G$ and $h_2 \in A \,\mathrm{wr}_{G'}\, G$. Let $G_1 = \pi(H_1)$.*

(a) *If $\pi(h_2) \notin G'$ and $(G_1G' : G') > 2$, then there is $f \in B \cap H_1$ such that $f^{h_2} \notin \langle f\rangle$.*

(b) *If $G_1 \not\subseteq G'$ and $\pi(h_2) \notin G_1G'$, there is $f \in B \cap H_1$ such that $f^{h_2} \notin \langle f\rangle^{h'}$ for each $h' \in \pi^{-1}(G_1G')$.*

In particular, in both cases $[f, h_2] \neq 1$.

Proof: Let $\sigma_2 = \pi(h_2)$. Consider $\sigma_1 \in G_1$ and $g \in B$. There is $f_1 \in B$ such that $(\sigma_1, f_1) \in H_1$. Let $f = g^{(\sigma_1,f_1)}g^{-1}$. Then $f \in [H_1, B] \subseteq H_1 \cap B$. We have

$$f(\tau) = \big((g^{\sigma_1})^{f_1}\big)(\tau)g(\tau)^{-1} = g(\sigma_1\tau)^{f_1(\tau)}g(\tau)^{-1}, \qquad \text{for every } \tau \in G.$$

There is $f_2 \in B$ such that $h_2 = (\sigma_2, f_2)$. Let $\tau \in G$ and $f' \in B$. Then

$$\begin{aligned} f^{h_2}(1) &= (f^{\sigma_2})^{f_2}(1) = f(\sigma_2)^{f_2(1)} = g(\sigma_1\sigma_2)^{f_1(\sigma_2)f_2(1)}g(\sigma_2)^{-f_2(1)},\\ f^{(\tau,f')}(1) &= f(\tau)^{f'(1)} = g(\sigma_1\tau)^{f_1(\tau)f'(1)}g(\tau)^{-f'(1)},\\ f(1) &= g(\sigma_1)^{f_1(\tau)}g(1)^{-1}. \end{aligned} \tag{6}$$

We now use these general formulae in special cases (a) and (b), with a particular choice of σ_1 and g.

(a) Since $(G_1G' : G') > 2$, there are $\tau_1, \tau_2 \in G_1$ such that $G', \tau_1^{-1}G', \tau_2^{-1}G'$ are distinct. Let σ_1 be τ_1 if $\sigma_2 \in \tau_2^{-1}G'$, and τ_2 otherwise. Then $\sigma_1 \in G_1 \smallsetminus G'$ and $\sigma_2 \notin \sigma_1^{-1}G'$.

So none of the cosets $\sigma_1G', \sigma_2G', \sigma_1\sigma_2G'$ is G'. Therefore we may choose $g \in B$ such that $g(1) = a^{-1}$, where $1 \neq a \in A$, and $g(\sigma_1G') = g(\sigma_2G') = g(\sigma_1\sigma_2G') = 1$. By (6), $f^{h_2}(1) = 1$, while $f(1) = a \neq 1$. It follows that $f \notin \langle f^{h_2}\rangle$, which implies that $f^{h_2} \notin \langle f\rangle$.

(b) As $G_1^{\sigma_2} = G_1 \not\subseteq G'$, we have $G_1 \not\subseteq (G')^{\sigma_2^{-1}}$. Thus $G_1 \cap G'$ and $G_1 \cap (G')^{\sigma_2^{-1}}$ are two proper subgroups of G_1. Since no group is the union of two proper subgroups, there is $\sigma_1 \in G_1$ such that $\sigma_1 \notin G'$ and $\sigma_1 \notin (G')^{\sigma_2^{-1}}$. Then $\sigma_2 \notin \sigma_1\sigma_2 G'$. Recall that $\sigma_2 \notin G_1G'$. Therefore we may choose $g \in B$ such that

$$g(G_1G') = 1, \quad g(\sigma_1\sigma_2) = 1, \quad g(\sigma_2) = a^{-1},$$

where $1 \neq a \in A$. Let $\tau \in G_1G'$ and $f' \in B$. By (6), $f^{h_2}(1) = a^{f_2(1)} \neq 1$, while $f^{(\tau,f')}(1) = 1$. It follows that $f^{h_2} \notin \langle f \rangle^{(\tau,f')}$. Thus $f^{h_2} \notin \langle f \rangle^{h'}$ for each $h' \in \pi^{-1}(G_1G')$. ∎

2. A Hilbertianity criterion

Observe that if E/K is a separable extension of fields such that E has a K-rational place, then E/K is regular. Indeed, a K-place $\varphi\colon E \to K \cup \{\infty\}$ maps the algebraic closure L of K in E into K. But the restriction of φ to L is an embedding of fields, whence $L = K$.

Let K be a field and let t be transcendental over K.

Definition 2.1: We say that a Galois extension $F/K(t)$ is **K-rationally split**, if there are field extensions L/K and $E/K(t)$ such that $F = EL$ and E has a K-rational place, unramified over $K(t)$. In particular, E/K is regular and L/K is Galois. ∎

LEMMA 2.2: *Let K be an infinite field and let $F/K(t)$ be a finite Galois extension. Then there exists a finite K-rationally split Galois extension $F'/K(t)$ such that $F \subseteq F'$.*

Proof: As K is infinite, there is a K-rational place $K(t) \to K \cup \{\infty\}$ that extends to a place $\varphi\colon F \to K_s \cup \{\infty\}$, unramified over $K(t)$. Let L be the residue field of φ; this is a Galois extension of K. Let $F' = FL$. Extend φ to a place $\varphi'\colon F' \to K_s \cup \{\infty\}$. Then φ' is unramified over $K(t)$ and L is its residue field [FJ, Proposition 2.14].

Let E be the decomposition field of φ'. Then $\mathrm{res}_E\,\varphi'$ is a K-rational place, unramified over $K(t)$. This implies that E/K is regular. Hence $[EL : E] = [L : K]$. But $[L : K] = [F' : E]$, since the decomposition group of φ' is isomorphic to the Galois group of the residue field extension. Thus $F' = EL$, and so F' is K-rationally split. ∎

Let L be a field. An irreducible polynomial $f \in L[X]$ is said to be **Galois over** L if a root of f generates a Galois extension of L, that is, the field $L[X]/(f)$ is Galois over L.

Remark 2.3: Let L/K be a Galois extension of fields, and let $f \in K[X]$. Assume that f is irreducible and Galois over L. Let $x = x_1, x_2, \ldots, x_n$ be the roots of f (in an algebraic closure of L). Then $L(x)/K$ is Galois. Indeed, $L(x)$ is the compositum of two Galois extensions of K, namely, L and $K(x_1, \ldots, x_n)$. Furthermore, $K(x)$ and L are linearly disjoint over K. Hence $\mathcal{G}(L(x)/K) = \mathcal{G}(L/K) \ltimes \mathcal{G}(L(x)/L)$. In particular, $\mathcal{G}(L/K)$ acts on $\mathcal{G}(L(x)/L)$. ∎

LEMMA 2.4: *Let M be a field and let t be transcendental over M. Then M is separably Hilbertian if and only if the following condition holds:*

(*) *Given an absolutely irreducible polynomial $f \in M[T,X]$, monic in X, and a finite Galois extension M' of M such that $f(t,X)$ is Galois over $M'(t)$, there are infinitely many $a \in M$ such that $f(a,X) \in M[X]$ is irreducible over M'.*

Proof: The condition is necessary, by [FJ, Corollary 11.7].

To show that it is sufficient, let $g(T,Z) \in M[T,Z]$ be monic and separable in Z and irreducible over $M(T)$. Let z be a root of $g(t,Z)$ in some algebraic closure of $M(t)$. Each $a \in M$ defines a specialization $t \to a$ that extends to an M-place $\varphi\colon M(t,z) \to M_s$. There is $0 \neq h(T) \in M[T]$ such that $M[t,z,h(t)^{-1}]$ is the integral closure of $M[t,h(t)^{-1}]$ in $M(t,z)$ [FJ, Lemma 5.3]. Thus for all a's, except for the finitely many zeros of h, the residue field extension of $M(t,z)/M(t)$ with respect to φ is $M(\varphi(z))/M$. We have $\deg_Z g(t,Z) = [M(t,z) : M(t)]$ and $\varphi(z)$ is a root of $g(a,Z)$. It therefore suffices to find infinitely many $a \in M$ for which the extension $M(t,z)/M(t)$ is inert, i.e., the residue field degree is the degree of the extension.

By Lemma 2.2 there is a a finite M-rationally split Galois extension $F/M(t)$ such that $z \in F$. Thus there is a Galois extension M'/M and a regular extension E/M such that $M(t) \subseteq E$ and $F = EM'$. Let $f(t,X)$ be the irreducible polynomial of a primitive element x for $E/M(t)$. Then f is absolutely irreducible and $f(t,X)$ is Galois over $M'(t)$.

By (*) there exist finitely many $a \in M$ such that $f(a,X) \in M[X]$ is irreducible over M'. For each such a let $\varphi\colon F \to M_s \cup \{\infty\}$ extend $t \to a$; then $\varphi(x)$ is of degree $[F : M'(t)] \cdot [M' : M] = [F : M(t)]$ over M. Hence $F/M(t)$ is inert with respect to φ. Therefore so is the subextension $M(t,z)/M(t)$. ∎

3. Twisted wreath products over fields of rational functions and specializations

We now realize the twisted wreath products of Section 1 over fields of rational functions in several variables.

LEMMA 3.1: *Let L/K be a finite Galois extension, let K' be an intermediate field of L/K, and let $c_1, \ldots, c_n$ be a basis of K' over K. Let $f \in K'[T,X]$ be an absolutely irreducible polynomial, monic in X and Galois over $L(T)$, and let $A = \mathcal{G}(f, L(T))$. Let $\mathbf{t} = (t_1, \ldots, t_n)$ be an n-tuple of algebraically independent elements over K'. Put $G = \mathcal{G}(L/K) = \mathcal{G}(L(\mathbf{t})/K(\mathbf{t}))$ and $G' = \mathcal{G}(L/K') = \mathcal{G}(L(\mathbf{t})/K'(\mathbf{t}))$. Then G' acts on A and there exist fields F, $\hat{F}$ such that*

(a) *$K(\mathbf{t}), K'(\mathbf{t}), L(\mathbf{t}), F, \hat{F}$ realize $A \operatorname{wr}_{G'} G$ and $\hat{F}$ is regular over L.*

(b) *$F = L(\mathbf{t})(z)$, where $\operatorname{irr}(z, L(\mathbf{t})) = f(\sum_{i=1}^{n} c_i t_i, Z) \in K'[\mathbf{t}, Z]$.*

Proof: Fix a root x of $f(T,X) \in K'[T][X]$ in an algebraic closure of $L(T)$. Identify G' with $\mathcal{G}(L(T,x)/K'(T,x))$ to define the action on $A = \mathcal{G}(L(T,x)/L(T))$ (Remark 2.3).

Let Σ be the family of cosets $G'\sigma$ of G' in G. For $C \in \Sigma$ and $a \in K'$ let a^C denote a^σ, where $\sigma \in C$; also, let f^C denote f^σ, where $\sigma \in C$.

$$\begin{tikzcd}
L(u^{C'}, z^{C'} \mid C' \neq C) \arrow[r, dash] \arrow[d, dash] & L(\mathbf{u})(z^{C'} \mid C' \neq C) \arrow[r, dash, "A"] \arrow[d, dash] & L(u^{C'}, z^{C'} \mid C' \in \Sigma) = \hat{F} \arrow[d, dash] \\
L(u^{C'} \mid C' \neq C) \arrow[r, dash] \arrow[d, dash] & L(\mathbf{t}) = L(\mathbf{u}) = Q \arrow[r, dash, "A"] \arrow[d, dash] & L(\mathbf{u}, z^C) = F^C \arrow[d, dash] \\
L \arrow[r, dash] \arrow[d, dash] & L(u^C) \arrow[r, dash, "A"] \arrow[d, dash] & L(u^C, z^C) \arrow[d, dash] \\
K'^C \arrow[r, dash] & K'^C(u^C) \arrow[r, dash] & K'^C(u^C, z^C)
\end{tikzcd}$$

Choose a set $\{u^C \mid C \in \Sigma\}$ of algebraically independent elements over K and put $Q = L(u^C \mid C \in \Sigma)$. For each $C \in \Sigma$ let z^C be a root of $f^C(u^C, Z)$ in a fixed algebraic closure of Q and let $F^C = Q(z^C)$. As f^C is absolutely irreducible, the field $K'^C(u^C, z^C)$ is a regular extension of K'^C. Hence $L(u^C, z^C)$ is a regular extension of L. As $(L(u^C, z^C) \mid C \in \Sigma)$ are free over L, they are linearly disjoint over L, and their compositum $\hat{F} = L(u^C, z^C \mid C \in \Sigma) = Q(z^C \mid C \in \Sigma)$ is a regular extension of L [FJ, p. 112]. It follows [FJ, Lemma 9.3] that any two fields in the above diagram are linearly disjoint over the field that lies in the lower left corner of the rectangle determined by them. In particular, F^C/Q is a Galois extension with Galois group isomorphic to A, the set of all F^C is linearly disjoint over Q, and $\hat{F}$ is their compositum. Therefore $\hat{F}/Q$ is Galois.

Let $t'_1, \ldots, t'_n$ be the unique solution of the following system of linear equations:

$$(1) \qquad T_1 c_1^C + \cdots + T_n c_n^C = u^C, \qquad C \in \Sigma.$$

As the matrix $(c_i^C) \in \mathrm{M}_n(L)$ is invertible [L, p. 212], $L(t'_1, \ldots, t'_n) = L(u^C \mid C \in \Sigma) = Q$. Since n is the transcendence degree of Q over L, the elements $t'_1, \ldots, t'_n$ are algebraically independent over L and hence also over K. So we may assume that $t'_i = t_i$, for $i = 1, \ldots, n$. Hence $Q = L(\mathbf{t})$.

Extend the action of G on L to an action on $\hat{F}$ in a natural way: $(u^C)^\tau = u^{C\tau}$ and $(z^C)^\tau = z^{C\tau}$. In particular, τ permutes the equations of the system (1). As $(t_1^\tau, \ldots, t_n^\tau)$ is also a solution of (1), it coincides with $(t_1, \ldots, t_n)$. Thus τ fixes $t_1, \ldots, t_n$. It follows that the action of G on $Q = L(\mathbf{t})$ is the unique extension of the given action on L that fixes $t_1, \ldots, t_n$. In particular, $K(\mathbf{t})$ is the fixed field of G in Q.

Let $F = F^{G'1}$. Then $F^C = F^\sigma$ for each $\sigma \in C$. Therefore $\hat{F} = \prod_\sigma F^\sigma$, where σ runs through a system of representatives of Σ.

As $\hat{F}/L(\mathbf{t})$ and $L(\mathbf{t})/K(\mathbf{t})$ are Galois, and every $\tau \in G = \mathcal{G}(L(\mathbf{t})/K(\mathbf{t}))$ lifts to an automorphism of $\hat{F}$, we obtain that $\hat{F}/K(\mathbf{t})$ is Galois. Similarly, $F/L(\mathbf{t})$ and $L(\mathbf{t})/K'(\mathbf{t})$ are Galois, and every $\tau \in G' = \mathcal{G}(L(\mathbf{t})/K'(\mathbf{t}))$ lifts to an automorphism of F, so $F/K'(\mathbf{t})$ is Galois.

Let $\hat{K}$ be the fixed field of G in $\hat{F}$. Then $\hat{K} \cap L(\mathbf{t}) = K(\mathbf{t})$, the fixed field of G in

$L(\mathbf{t})$, and $\hat{K}L(\mathbf{t}) = \hat{F}$. By Remark 1.2, $K(\mathbf{t})$, $K'(\mathbf{t})$, $L(\mathbf{t})$, F, $\hat{F}$ realize $A\,\mathrm{wr}_{G'}\,G$.

Put $u = u^{G'1}$ and $z = z^{G'1}$. By (1), $u = \sum_{i=1}^n c_i t_i \in K'(\mathbf{t})$. Now, $f(u,z) = 0$ and $f(u,Z)$ is irreducible over $K'(u)$. As $Q = L(\mathbf{u})$ and $K'(u,z)$ are linearly disjoint over $K'(u)$, we get that $f(u,Z)$ is irreducible over $Q = L(\mathbf{t})$. This shows (b). ∎

We now apply the above construction to prove that certain separable extensions of separably Hilbertian fields are separably Hilbertian. Recall [FJ, Proposition 11.13 and Proposition 11.16] that a field is Hilbertian if and only if it is separably Hilbertian and either imperfect or of characteristic 0. Therefore in the rest of this section we could replace 'separably Hilbertian' by 'Hilbertian'.

THEOREM 3.2: *Let M be a separable algebraic extension of a separably Hilbertian field K. Suppose that for every $\alpha \in M$ and every $\beta \in M_s$ there exist:*

(i) *a finite Galois extension L of K that contains β; let $G = \mathcal{G}(L/K)$;*

(ii) *a field K' such that $K \subseteq K' \subseteq M \cap L$ and K' contains α; let $G' = \mathcal{G}(L/K')$;*

(iii) *a Galois extension N of K that contains both M and L,*

such that for every finite nontrivial 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 M is separably Hilbertian.

Proof:

PART A: *Preliminaries.* We will apply the criterion of Lemma 2.4. So let $f \in M[T,X]$ be an absolutely irreducible polynomial, monic in X, and let M'/M be a finite Galois extension such that $f(T,X)$ is Galois over $M'(T)$, We have to show that there are infinitely many $a \in M$ such that $f(a,X) \in M[X]$ is irreducible over M'. Let $A = \mathcal{G}(f, M'(T)) = \mathcal{G}(f, M_s(T))$.

There is $\alpha \in M$ such that $f \in K(\alpha)[T,X]$ and there is $\beta \in M_s$ such that $M' \subseteq M(\beta)$ and $f(T,X)$ is Galois over $K(\beta)(T)$. For these α, β let K', L, and N be as in (i) - (iii). Then $f \in K'[T,X]$ and $f(T,X)$ is Galois over $L(T)$.

As $K' \subseteq M$ and $M' \subseteq N$, it suffices to find infinitely many $a \in K'$ such that $f(a,X)$ is irreducible over N.

PART B: *Specialization of the wreath product.* Let $c_1, \ldots, c_n$ be a basis of K' over K.

By Lemma 3.1 there are fields P and $\hat{P}$ such that

(a) $K(\mathbf{t}), K'(\mathbf{t}), L(\mathbf{t}), P, \hat{P}$ realize $A \operatorname{wr}_{G'} G$ (with respect to some action of G' on A).

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

As K is separably Hilbertian, for infinitely many n-tuples $\mathbf{b} = (b_1, \ldots, b_n) \in K^n$ the specialization $\mathbf{t} \mapsto \mathbf{b}$ gives an L-place of $\hat{P}$ onto a Galois extension $\hat{F}$ of K with group isomorphic to $\mathcal{G}(\hat{P}/K(\mathbf{t}))$, that is, there are fields F and $\hat{F}$ such that

(a′) $K, K', L, F, \hat{F}$ realize $A \operatorname{wr}_{G'} G$ (with respect to some action of G' on A).

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

For simplicity, fix such $\mathbf{b}$ and let $a = \sum_{i=1}^n c_i b_i$. Then $a \in K'$, so $f(a, X) \in K'[X]$.

PART C: $L = N \cap F$. Indeed, let $F_0 = N \cap F$. This is a Galois extension of K'. Let $A_0 = \mathcal{G}(F_0/L)$. By Remark 1.3 there is a Galois extension $\hat{F}_0$ of K such that

(a″) $K, K', L, F_0, \hat{F}_0$ realize $A_0 \operatorname{wr}_{G'} G$ (with respect to some action of G' on A_0).

In particular, $\hat{F}_0$ is the Galois closure of F_0 over K. As $F_0 \subseteq N$, 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, $f(a, y) = 0$. By Part C, $[N(y) : N] = [NF : N] = [F : L] = [L(y) : L]$. Thus $f(a, X) = \operatorname{irr}(y, N)$. In particular, $f(a, X)$ is irreducible over N. ∎

4. Applications

Our main result is the following theorem, that could be considered a generalization of Weissauer's Theorem [W, Satz 9.7] on one hand and [HJ, Theorem 2.4] on the other hand. It answers [J1, Problem 2.3(a)].

THEOREM 4.1: *Let K be a Hilbertian field and let M_1, M_2 be two Galois extensions of K. Let M be an intermediate field of M_1M_2/K such that $M \not\subseteq M_1$ and $M \not\subseteq M_2$. Then M is Hilbertian.*

Proof: By [FJ, Corollary 11.7] we may assume that $[M : K] = \infty$.

PART A: *We may assume that*

(a) *either* $M_1 \cap M_2 = K$ *or* $[M : (M_1 \cap M)] > 2$.

Indeed, we cannot have $[M : (M_1 \cap M)] = 1$, since $M \not\subseteq M_1$. Suppose that $[M : (M_1 \cap M)] = 2$. Then there is $d \in M_1 \cap M$ such that $M = (M_1 \cap M)(\delta)$, where either $\delta^2 - \delta = d$ (in characteristic 2) or $\delta^2 = d$ (otherwise). Observe that M_1 and $K(\delta)$ are Galois extensions of $K(d)$, their intersection is $K(d)$, and $K(d) \subseteq M \subseteq M_1K(\delta)$. Furthermore, $M \not\subseteq K(\delta)$, since M/K is infinite. Replace K by $K(d)$ and M_2 by $K(\delta)$ to achieve (a).

PART B: *Construction of N and L.* We apply the criterion of Theorem 3.2. Let $\alpha \in M$ and $\beta \in M_s$. Let L_0 be the Galois closure of $K(\alpha, \beta)$ over K, and let $N = L_0M_1M_2$. Then N/K is Galois, and $\mathcal{G}(N/M_1), \mathcal{G}(N/M_2) \triangleleft \mathcal{G}(N/K)$.

Choose a finite Galois extension L/K such that $L_0 \subseteq L \subseteq N$, let $G = \mathcal{G}(L/K)$, and let $\varphi\colon \mathcal{G}(N/K) \to G$ be the restriction map. Let G_1, G_2, and G' be the images in G of $\mathcal{G}(N/M_1)$, $\mathcal{G}(N/M_2)$, and $\mathcal{G}(N/M)$, respectively, under φ. Put $K' = M \cap L$; then $\alpha \in K'$ and $G' = \mathcal{G}(L/K')$. Then

(b) $G_1, G_2 \triangleleft G$.

Condition $M \not\subseteq M_i$ means that $\mathcal{G}(N/M_i) \not\subseteq \mathcal{G}(N/M)$, for $i = 1, 2$. Thus if L is sufficiently large (that is, if G is a sufficiently large finite quotient of $\mathcal{G}(N/K)$) then

(c) $G_1, G_2 \not\subseteq G'$.

Similarly, $[M : K] = \infty$ implies, with L sufficiently large, that

(d) $(G : G') > 2$.

Finally, (a) implies, with L sufficiently large, that

(e) either $G_1G_2 = G$ or $(G_1G' : G') > 2$.

In particular,

(e$'$) either $G_2 \not\subseteq G_1G'$ or $(G_1G' : G') > 2$.

Indeed, otherwise $G_2 \subseteq G_1G'$ and $(G_1G' : G') \leq 2$. By (e), $G_1G_2 = G$, and therefore $G = G_1G'$. Hence, by (d), $(G_1G' : G') > 2$, a contradiction.

PART C: *A realization.* Let $A \neq 1$ be a finite group on which G' acts, and let $H = A\,\mathrm{wr}_{G'}\,G$. By Theorem 3.2 it suffices to show that there is no realization $K, K', L, F, \hat{F}$ of H with $\hat{F} \subseteq N$.

Suppose there is such a realization. Identify H with $\mathcal{G}(\hat{F}/K)$ so that the restriction map $\mathcal{G}(\hat{F}/K) \to \mathcal{G}(L/K)$ coincides with the projection $\pi\colon H \to G$. Then $\pi \circ \mathrm{res}_{\hat{F}} = \mathrm{res}_L$, where $\mathrm{res}_L : \mathcal{G}(N/K) \to G$ and $\mathrm{res}_{\hat{F}} : \mathcal{G}(N/K) \to H$ are the restriction maps.

For $i = 1, 2$ let $H_i = \mathrm{res}_{\hat{F}}(\mathcal{G}(N/M_i))$. Then $H_i \triangleleft H$ and $\pi(H_i) = \mathrm{res}_L(\mathcal{G}(N/M_i)) = G_i$. We claim that 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, if the first statement of (e$'$) holds, then there exists $h_2 \in H_2$ such that $\pi(h_2) \notin G_1G'$. The claim then follows from (c) and Lemma 1.4(b) with $h_1 = f$. If the second statment of (e$'$) holds, then by (c) there exists $h_2 \in H_2$ such that $\pi(h_2) \notin G'$. The claim then follows from Lemma 1.4(a) with $h_1 = f$.

For $i = 1, 2$ choose $\gamma_i \in \mathcal{G}(N/M_i)$ such that $\mathrm{res}_{\hat{F}}(\gamma_i) = h_i$. Then $\mathrm{res}_L\,\gamma_1 = \pi(h_1) = 1$ and

$$[\gamma_1, \gamma_2] \neq 1. \tag{1}$$

However, as $\mathcal{G}(M_1M_2/M_1 \cap M_2) = \mathcal{G}(M_1M_2/M_1) \times \mathcal{G}(M_1M_2/M_2)$, the subgroups $\mathcal{G}(M_1M_2/M_1)$ and $\mathcal{G}(M_1M_2/M_2)$ of $\mathcal{G}(M_1M_2/k)$ commute. Therefore

$$\mathrm{res}_{M_1M_2}[\gamma_1, \gamma_2] = [\mathrm{res}_{M_1M_2}\,\gamma_1, \mathrm{res}_{M_1M_2}\,\gamma_2] = 1.$$

Furthermore,

$$\mathrm{res}_L[\gamma_1, \gamma_2] = [\mathrm{res}_L\,\gamma_1, \mathrm{res}_L\,\gamma_2] = [1, \mathrm{res}_L\,\gamma_2] = 1.$$

As $N = (M_1M_2)L$, it follows that $[\gamma_1, \gamma_2] = 1$, a contradiction to (1). ∎

Put $\hat{M} = M_1 M_2$ in the preceding theorem. The main ingredient in the proof is the fact that there are two normal subgroups $\mathcal{G}(\hat{M}/M_1)$ and $\mathcal{G}(\hat{M}/M_2)$ of $\mathcal{G}(\hat{M}/K)$ that commute. That is, for every $\gamma_1 \in \mathcal{G}(\hat{M}/M_1)$ and every $\gamma_2 \in \mathcal{G}(\hat{M}/K)$ we have $\gamma_1^{\gamma_2} = \gamma_1$. However, we can considerably weaken this condition:

An automorphism σ of a profinite group G is said to be **families preserving** if, for all $g \in G$, the closed subgroup $\langle g^\sigma \rangle$ generated by g^σ is conjugate in G to $\langle g \rangle$ [JR]. In particular, every inner automorphism is families preserving.

THEOREM 4.2: *Let K be a Hilbertian field and let $M_1 \subseteq \hat{M}$ be two Galois extensions of K. Assume that there is $\gamma_2 \in \mathcal{G}(\hat{M}/K) \smallsetminus \mathcal{G}(\hat{M}/M_1)$ such that conjugation by γ_2 induces a families preserving automorphism of $\mathcal{G}(\hat{M}/M_1)$. Let M be an intermediate field of $\hat{M}/K$ such that $M \not\subseteq M_1$ and $M_1 \cap M \not\subseteq M_1(\gamma_2)$, the fixed field of γ_2 in M_1. Then M is Hilbertian. In particular, $\hat{M}$ is Hilbertian.*

$$\begin{tikzcd}[arrows=dash]
M_1(\gamma_2) \arrow[r] \arrow[d] & M_1 \arrow[r] \arrow[d] & \hat{M} \arrow[d] \\
K \arrow[r] & M_1 \cap M \arrow[r] & M
\end{tikzcd}$$

Proof: We apply the criterion of Theorem 2.2. Let $\alpha \in M$ and $\beta \in M_s$. Let L_0 be the Galois closure of $K(\alpha, \beta)$ over K, and let $N = L_0 \hat{M}$. Then N/K is Galois, $\mathcal{G}(N/M_1) \triangleleft \mathcal{G}(N/K)$, and $\mathcal{G}(N/M_1) \not\subseteq \mathcal{G}(N/M)$. Extend γ_2 to $\delta_2 \in \mathcal{G}(N/K)$. Then $\delta_2 \notin \mathcal{G}(N/M_1 \cap M) = \mathcal{G}(N/M_1)\mathcal{G}(N/M)$.

Let L be a finite Galois extension L/K such that $L_0 \subseteq L \subseteq N$, let $G = \mathcal{G}(L/K)$, and let φ: $\mathcal{G}(N/K) \to G$ be the restriction map. Let G_1, σ_2, and G' be the images in G of $\mathcal{G}(N/M_1)$, δ_2, and $\mathcal{G}(N/M)$, respectively, under φ. Put $K' = M \cap L$; then $\alpha \in K'$ and $G' = \mathcal{G}(L/K')$. If L is sufficiently large then $G_1 \not\subseteq G'$ and $\sigma_2 \notin G_1 G'$.

CLAIM: *For each $\delta_1 \in \mathcal{G}(N/M_1)$ such that $\mathrm{res}_L\, \delta_1 = 1$ there is $\delta \in \mathcal{G}(N/M_1)$ such that $\delta_1^{\delta_2} \in \langle \delta_1^{\delta} \rangle$.* Indeed, by assumption there is $\delta \in \mathcal{G}(N/M_1)$ such that $\mathrm{res}_{\hat{M}}\, \delta_1^{\delta_2} \in \langle \mathrm{res}_{\hat{M}}\, \delta_1^{\delta} \rangle$. Clearly $\mathrm{res}_L\, \delta_1^{\delta_2} = 1 = \mathrm{res}_L\, \delta_1^{\delta}$. As $N = L\hat{M}$, the claim follows.

Let $A \neq 1$ be a finite group on which G' acts, let $H = A \,\mathrm{wr}_{G'}\, G$, and suppose there is a realization $K, K', L, F, \hat{F}$ of H with $\hat{F} \subseteq N$. As in the preceding theorem identify H with $\mathcal{G}(\hat{F}/K)$ and the restriction $\mathcal{G}(\hat{F}/K) \to \mathcal{G}(L/K)$ with the projection $\pi: H \to G$.

Let $H_1 = \mathrm{res}_{\hat{F}}(\mathcal{G}(N/M_1))$ and $h_2 = \mathrm{res}_{\hat{F}}(\delta_2)$. Then $H_1 \triangleleft H$, $\pi(H_1) = G_1$, and $\pi(h_2) = \sigma_2$. By the above Claim, for each $f \in H_1 \cap \mathrm{Ker}\,\pi$ there is $h' \in H_1$ such that $f^{h_2} \in \langle f^{h'} \rangle$. This contradicts Lemma 1.4(b). ∎

COROLLARY 4.3: *Let M_1 be a proper Galois extension of a Hilbertian field K. Then its absolute Galois group $G(M_1)$ has outer automorphisms.*

Proof: Put $M = \hat{M} = K_s$ in Theorem 4.2 and let $\gamma_2 \in G(K) \smallsetminus G(M_1)$. Then γ_2 induces an outer automorphism of $G(M_1)$. Otherwise, by Theorem 4.2, $M = K_s$ is Hilbertian, a contradiction. ∎

Remark 4.4: Examples of fields with whose absolute Galois group has no outer automorphisms. The famous theorem of Ikeda, Iwasawa, Uchida [J2, Section 8.5] states that each automorphism of $G(\mathbb{Q})$ is inner.

More generally, let L be a number field that is Galois over no proper subfield (e.g., $L = \mathbb{Q}(\sqrt[3]{2})$). Let α be an automorphism of $G(L)$. By a theorem of Uchida and Iwasawa [J2, Section 8.5] α is of the form $\tau \mapsto \sigma^{-1}\tau\sigma$, where $\sigma \in G(\mathbb{Q})$. In particular, $G(L)^\sigma = G(L)$, and hence $L^\sigma = L$. As L is Galois over the fixed field $L(\sigma)$ of σ in L, we have $L(\sigma) = L$. Thus $\sigma \in G(L)$, whence α is inner.

Thus by Corollary 4.3, $G(L) \not\cong G(M_1)$ for each proper Galois extension M_1 of $\mathbb{Q}$. ∎

We now show how cases (F1)–F(6) from the Introduction can be deduced from Theorems 3.2 and 3.3. First, we slightly generalize (F2):

PROPOSITION 4.5 (cf. [FJ, Proposition 15.5]): *Let M be a separable extension of a Hilbertian field K. Let $\hat{M}$ be its Galois closure over K and assume that $\mathcal{G}(\hat{M}/K)$ is finitely generated. Then M is Hilbertian.*

Proof: Apply the criterion of Theorem 3.2. Let $\alpha \in M$ and $\beta \in M_s$. Let L_0 be the Galois closure of $K(\alpha, \beta)$ over K, and let $N = L_0\hat{M}$. Then N/K is Galois and $\mathcal{G}(N/K)$

is finitely generated. Let $K' = K(\alpha)$ and let A_0 be a non-trivial finite group. Put $n = [K' : K]$ and $m = |A_0| > 1$.

As $\mathcal{G}(N/K)$ is finitely generated (and hence small), there are only finitely many extensions of K of degree at most $[K' : K] \cdot |A_0|$ contained in N. Their compositum L is a finite Galois extension of K and $K \subseteq K' \subseteq L \subseteq N$.

Let $G = \mathcal{G}(L/K)$ and $G' = \mathcal{G}(L/K')$, and let G' act on A_0. Suppose that there are fields $F', F, \hat{F} \subseteq N$ such that $K, K', L, F, \hat{F}$ realize $A_0 \operatorname{wr}_{G'} G$ over K. By Remark 1.2(e) there is a field F' such that $L \cap F' = K'$ and $F = LF'$. Then $[F' : K'] = |A_0|$, and hence $[F' : K] = [K' : K] \cdot |A_0|$, whence $F' \subseteq L$. A contradiction to $L \cap F' = K'$. ∎

Proposition 4.5 also implies case (F1). Cases (F3) and (F5) follow from Theorem 4.1. So does (F6): For each prime p let K_p be the maximal pro-p-extension of K. If $p_1, p_2 | [M : K]$, then $M \subseteq \prod_p K_p = M_1 M_2$, where $M_1 = K_{p_1}$ and $M = \prod_{p \neq p_1} K_p$, but $M \not\subseteq M_1, M_2$.

Case (F4) can be deduced from (F2) and (F3) [FJ, Proposition 15.6], but also directly from Theorem 3.2 (in the spirit of the original proof of Kuyk [Ku] that uses wreath products). The essential point is that $A_0 \operatorname{wr}_{G'} G$ is not commutative, if $(G : G') > 2$. This follows, e.g., from Lemma 1.4(a) with $G_1 = G$.

Finally, we remark that the peculiar case (F7) could be deduced from a slight generalization of Theorem 3.3. However, the original proof [JL, Proposition 5.2] is more straightforward.

References

[Br] K. Brown, *Cohomology of groups*, GTM 87, Springer Verlag 1982.

[FJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[HJ] D. Haran, M. Jarden, *Compositum of Galois extensions of Hilbertian fields*, Annales Scientifiques de l'École Normale Supérieure **24**, (1991), 739–748.

[Hi] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Journal für die reine und angewandte Mathematik **110** (1892), 104–129.

[Hp] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer Verlag, Berlin, 1967.

[J1] M. Jarden, *Hilbertian fiels and free profinite groups II*, an unpublished manuscript, 1994.

[J2] M. Jarden, *Infinite Galois Theory* in *Handbook of Algebra*, (ed. M. Hazewinkel) Volume 1, Elsevier Science B.V., 1996.

[JL] M. Jarden, A. Lubotzky, *Hilbertian fields and free profinite groups*, J. London Math. Soc. **46** (1992), 205–227.

[JR] M. Jarden, J. Ritter, *Normal automorphisms of absolute Galois groups of p-adic fields*, Duke Math. Journal **47** (1980), 47–56.

[Ku] W. Kuyk, *Extensions de corps hilbertiens*, Journal of Algebra **14** (1970), 112–124.

[La] S. Lang, *Algebra, third edition*, Addison-Wesley, Reading, 1994.

[Ma] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics **1284**, Springer-Verlag 1987.

[Mc] S. Mac Lane, *Homology (third corrected printing)*, Springer, Berlin, 1975.

[R] L. Ribes, *Introduction to profinite groups and Galois Cohomology*, Queen's papers in pure and applied Mathematics 24, Queen's University, Kingston, 1970.

[U] K. Uchida, *Separably Hilbertian fields*, Kodai Mathematical Journal **3** (1980), 83–95.

[W] R. Weissauer, *Der Hilbertsche Irreduzibilitätssatz*, Journal für die reine und angewandte Mathematik **334** (1982), 203–220.

October 26, 1999