ANNALES SCIENTIFIQUES DE L'É.N.S.

D. HARAN
M. JARDEN

Compositum of Galois extensions of hilbertian fields

Annales scientifiques de l'É.N.S. 4e série, tome 24, nº 6 (1991), p. 739-748
<http://www.numdam.org/item?id=ASENS_1991_4_24_6_739_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 24, 1991, p. 739 à 748.

COMPOSITUM OF GALOIS EXTENSIONS OF HILBERTIAN FIELDS

BY D. HARAN AND M. JARDEN (1)

Introduction

Hilbert [H] proved in 1892 that for given irreducible polynomials $f_i(T_1, \ldots, T_r, X)$, $i=1, \ldots, m$, and a nonzero polynomial $g(T_1, \ldots, T_r)$ with rational coefficients there exists $(a_1, \ldots, a_r) \in \mathbb{Q}^r$ such that $f_1(\mathbf{a}, X), \ldots, f_m(\mathbf{a}, X)$ are irreducible in $\mathbb{Q}[X]$ and $g(\mathbf{a}) \neq 0$.

Numerous proofs of Hilbert's irreducibility theorem have since been given. Many of them apply to other fields. So, each field K which satisfies the theorem has been called **Hilbertian.** The sets of $\mathbf{a} \in K^r$ whose substitution in the polynomials leaves them irreducible and nonzero have been called **Hilbert sets.**

The investigation of Hilbertian fields has been extended in the last 98 years since Hilbert's original paper in several directions:

(*a*) *Study of Hilbert subsets of Hilbertian fields* (e. g. Dörge [D], Geyer [G], Sprindžuk [S], and Fried [F]).

(*b*) *Search for arithmetical conditions on a field which make it Hilbertian.* Beyond the classical example of fields of rational function over any field (Inaba [I] and Franz [Fr]) two results stand out: "Each ω-free PAC field is Hilbertian" (Roquette [FJ], Cor. 24.38) and "The field of formal power series in at least two variables over any field is Hilbertian" (Weissauer [FJ], Cor. 14.18).

(*c*) *Infinite algebraic extensions of Hilbertian fields.* The first result in this direction is due to Kuyk [K]: "Every abelian extension of Hilbertian field is Hilbertian" In particular the field $\mathbb{Q}_{cycl}$ obtained from $\mathbb{Q}$ by adjoining all roots of unity is Hilbertian. Uchida [U] extended a result of Kuyk and proved that if an algebraic extension L of a Hilbertian field K is contained in a nilpotent extension and if the supernatural number [L : K] (*see* [FJ], Section 20.9) is divisible by at least two prime numbers, then L is Hilbertian. The strongest result however in this direction, is again due to Weissauer: "Every finite proper

(1) Partially supported by a grant from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

extension of a galois extension of a Hilbertian field is Hilbertian". (*See* [W], Satz 9.7, for a nonstandard proof and [FJ], Cor. 12.15 for a standard proof.) We make an extensive use of this result and refer to it as **Weissauer's theorem**.

(*d*) *Realization of finite groups over Hilbertian fields, especially over number fields via Riemann existence theorem* (*see* Matzat's exposition [M]).

(*e*) *Properties of almost all e-tuples* $(\sigma_1, \ldots, \sigma_e)$ *of elements of the absolute Galois group of a Hilbertian field* K. For example, the group generated by almost all $(\sigma_1, \ldots, \sigma_e)$ is a free profinite group [FJ], Thm, 16.13, and if K is countable, then the fixed field $K_s(\sigma_1, \ldots, \sigma_e)$ of $\sigma_1, \ldots, \sigma_e$ in the separable closure K_s of K is PAC [FJ], Thm. 16.18.

This note is a contribution to the study of infinite algebraic extensions of Hilbertian fields. Weissauer's theorem implies that the compositum of a Galois extension M_1 of a Hilbertian field K and a finite extension M_2 of K which is not contained in M_1 is Hilbertian. So, it is natural to ask whether the compositum N of two (infinite) linearly disjoint proper Galois extensions M_1 and M_2 of K is Hilbertian. Indeed, this has been stated as Problem 12.18 of [FJ]. However, the question goes back at least to Kuyk [K] (*see* Remark 2.6) and Weissauer. Kuyk proved that N is Hilbertian if an extra condition holds: "For each finite Galois extension L of K which is contained in N we have $L \cap M_1 \neq K$ or $L \cap M_2 \neq K$." In particular this is the case if the degrees $[N:M_1]$ and $[N:M_2]$ are relatively prime. The main tool in Kuyk's proof is the possibility to realize wreath products over K. Zorn [Z] gave a clearer exposition of Kuyk's proof while strengthening Kuyk's extra condition to: "Each open normal sugroup of an open normal subgroup of $\mathcal{G}(N/K)$ is the direct product $\mathcal{G}(N/M'_1) \times \mathcal{G}(N/M'_2)$, where M'_i is a finite extension of M_i contained in N."

We extend here Kuyk's result to a complete affirmative solution of Problem 12.18 of [FJ]. Our proof is an elaboration of Zorn's in the case where $[N:M_1]$ and $[N:M_2]$ are relatively prime. For the case where the degrees are not relatively prime we generalize a lemma of Chatzidakis on normalizers of elements in wreath products [FJ], Lemma 52. Then we apply the setup used in the first case to conclude the proof in the second case.

An application of Weissauer's theorem gives even a sharper result:

THEOREM. — *The composition of two Galois extensions of a Hilbertian field, neither of which is contained in the other, is Hilbertian.*

Of course, the solution of Problem 12.18 of [FJ] immediately supplies an affirmative solution to Problem 12.19 of [FJ]:

COROLLARY. — *The separable closure of a Hilbertian field* K *cannot be presented as the compositum of two Galois extensions of* K, *neither of which is contained in the other.*

1. Wreath products

Recall that the wreath product $H = A \operatorname{wr} G$ os finite groups A and G is the semidirect product $G \ltimes A^G$, where A^G is the group of all functions $f: G \to A$ with the canonical multiplication rule, and G acts on A^G by the formula $f^\tau(\sigma)=f(\tau\sigma)$. Thus each element of H is a pair (σ,f) with $\sigma\in G$ and $f\in A^G$. The product and the inverse in H are given by

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

Let $\pi:H\to G$ be the canonical projection. Embed A in A^G by identifying each $a\in A$ with the function which maps 1 to a and σ to 1 for each $\sigma\neq 1$. Then A^G may also be considered as a direct product, $A^G=\prod_{\sigma\in G}A^\sigma$, and each element of A^σ has the form a^σ with $a\in A$.

Our first result generalizes a lemma of Chatzidakis [FJ], Lemma 24.52.

LEMMA 1.1. — *Let* G *and* A *be finite groups. For* $\sigma_1,\ldots,\sigma_e\in G$ *and* $1\neq a\in A$ *let* $G_0=\langle\sigma_1,\ldots,\sigma_e\rangle$ *and* $H_0=\langle(\sigma_1,a),\ldots,(\sigma_e,a)\rangle$. *Then* π *maps the normalizer* $N=N_H(H_0)$ *of* H_0 *in* H *onto* G_0.

Proof. – Since $\pi(H_0)=G_0$ it suffices to prove that $\pi(N)\leqq G_0$. Consider A^{G_0} as the subgroup of A^G consisting of all functions $f:G\to A$ for which $f(\tau)=1$ for each $\tau\in G-G_0$. It follows from (1) that $H_1=\{(\sigma,f)\mid\sigma\in G_0 \text{ and } f\in A^{G_0}\}$ is a subgroup of H. The main point to be observed here is that if (σ,f), $(\tau,g)\in H_1$ and $\rho\in G-G_0$, then $\tau\rho$, $\sigma^{-1}\rho\notin G_0$ and therefore $(f^\tau g)(\rho)=f(\tau\rho)g(\rho)=1$ and $f^{-\sigma^{-1}}(\rho)=f(\sigma^{-1}\rho)^{-1}=1$. As $(\sigma_i,a)\in H_1$, $i=1,\ldots,e$, we have $H_0\leqq H_1$. In other words

$$(2)\qquad (\sigma,f)\in H_0 \quad\text{implies that } \sigma\in G_0 \text{ and } f\in A^{G_0}.$$

Let $(\tau,g)\in N$. Then $(\sigma,f)=(\tau,g)^{-1}(\sigma_1,a)(\tau,g)\in H_0$. By (1) and (2),

$$\sigma=\tau^{-1}\sigma_1\tau\in G_0 \qquad\text{and}\qquad f=g^{-\sigma}a^\tau g\in A^{G_0}.$$

Let $n=\operatorname{ord}(\sigma)$ and act with the powers of σ on f to get

$$f=g^{-\sigma}a^\tau g,\qquad f^\sigma=g^{-\sigma^2}a^{\tau\sigma}g^\sigma,\qquad\ldots,\qquad f^{\sigma^{n-1}}=g^{-\sigma^n}a^{\tau\sigma^{n-1}}g^{\sigma^{n-1}}.$$

Hence

$$(3)\quad f^{\sigma^{n-1}}\cdots f^\sigma f=(g^{-1}a^{\tau\sigma^{n-1}}g^{\sigma^{n-1}})\cdots(g^{-\sigma^2}a^{\tau\sigma}g^\sigma)(g^{-\sigma}a^\tau g)=g^{-1}a^{\tau\sigma^{n-1}}\cdots a^{\tau\sigma}a^\tau g$$

As $\sigma\in G_0$ and $f\in A^{G_0}$, the left hand side of (3) belongs to A^{G_0}. Therefore, so does the right hand side of (3). So if $\tau\notin G_0$, then the value of the right hand side of (3) at τ^{-1} is 1. Thus

$$(4)\qquad g(\tau^{-1})^{-1}a(\tau\sigma^{n-1}\tau^{-1})\cdots a(\tau\sigma\tau^{-1})a(1)g(\tau^{-1})=1.$$

Finally, note that for j between 1 and $n-1$ we have $\tau\sigma^j\tau^{-1}\neq 1$. Hence (4) reduces to $a=1$. This contradiction to the choice of a proves that $\tau\in G_0$, as desired. ■

As a result, a certain embedding problem for a direct product of profinite groups cannot be properly solved:

LEMMA 1.2. — *Let* C_1, C_2 *be nontrivial profinite groups. Let* G_1, G_2 *be nontrivial finite quotients of* C_1, C_2, *respectively, such that either*

(*a*) *the orders* G_1 *and* G_2 *are not relatively prime, or*

(*b*) *the orders of* C_1 *and* C_2 *are relatively prime.*

Let $G=G_1\times G_2$ *and let* $\rho: C_1\times C_2\to G$ *be the product of the quotient maps.*

Let A *be a nontrivial finite group,* $H=A\,\mathrm{wr}\,G$, *and* $\pi: H\to G$ *the canonical projection. Then there exists no epimorphism* $\theta: C_1\times C_2\to H$ *such that* $\pi\circ\theta=\rho$.

Proof. — Assume that there exists an epimorphism $\theta: C_1\times C_2\to H$ such that $\pi\circ\theta=\rho$, We derive a contradiction in each of the two cases.

Case (*a*): *There exists a prime p and elements* $\sigma_i\in G_i$, $i=1, 2$, *of order p.* Then the order of $\sigma=\sigma_1\sigma_2$ is also p. Use Lemma 1.1 for $e=1$ to find $h\in H$ such that $\pi(h)=\sigma$ *and* $\pi(N)=\langle\sigma\rangle$, with $N=N_H\langle h\rangle$. Write $h=h_1 h_2$, with $h_i=\theta(c_i)$ and $c_i\in C_i$. Then c_1 commutes with c_2 and therefore $h_i\in N$. Hence $\pi(h_i)=\rho(c_i)\in\langle\sigma\rangle\cap G_i=1$. It follows that $\sigma=\pi(h)=1$. This is a contradiction.

Case (*b*): *The orders of* C_1 *and* C_2 *are relatively prime.* For $i=1, 2$ put $H_i=\theta(C_i)$. Then $H_i\lhd H$, $\pi(H_i)=G_i$ and there exists $h\in H_i$ such that $\sigma=\pi(h)\neq 1$. Thus $h=(\sigma, f)$, where $f\in A^G$. As $A^\sigma\lhd A^G$, we have $A^h=(A^\sigma)^f=A^\sigma$. It follows that $A=(A^\sigma)^{h^{-1}}\leqq H_i.A^\sigma$, and therefore

$$A^G=A\cdot\prod_{\substack{\tau\in G\\ \tau\neq 1}}A^\tau\leqq H_i\cdot\prod_{\substack{\tau\in G\\ \tau\neq 1}}A^\tau.$$

Hence, with $n=|G|$, the order of A^n divides $|H_i|\cdot|A|^{n-1}$, and therefore $|A|$ divides $|H_i|$, for $i=1, 2$. This is a contradiction, since $|H_1|$ and $|H_2|$ are relatively prime. ∎

REMARK 1.3. — *Characterization of wreath products.* Although we shall not use it in the sequel it is interesting to note that wreath products can be characterized by less data than above:

Given an extension of finite groups

$$1\to B\to H\to G\to 1, \tag{5}$$

the lifting of elements of G to elements of H determines a homomorphism $\psi: G\to \mathrm{Aut}(B)/\mathrm{In}(B)$. The set of all congruence classes of extensions with the same ψ bijectively corresponds to the group $H^2(G, Z(B))$ [Mc], p. 128. In particular let $B=A^G$ and ψ be the homomorphism obtained from the natural action of G on B. Then the G-module $Z(B)=Z(A)^G$ is the induced module $\mathrm{Ind}_1^G Z(A)$. Hence $H^2(G, Z(B))$ is trivial [R], p. 146. It follows that the only extension (5) such that ψ is induced by the natural action of G on $B=A^G$ is the wreath product.

REMARK 1.4. — *Interpretation of wreath products in Galois theory.* Consider a tower of fields $K \subseteq L \subseteq F \subseteq \hat{F}$ where L/K, F/L and $\hat{F}$/K are finite Galois extensions. Let also K′ be a field such that $K' \cap L = K$ and $LK' = \hat{F}$. Put $G = \mathcal{G}(L/K) \cong \mathcal{G}(\hat{F}/K')$ and $A = \mathcal{G}(F/L)$. Suppose that the fields F^σ, $\sigma \in \mathcal{G}(\hat{F}/K')$ are linearly disjoint over L and their compositum is $\hat{F}$. Then there exists an isomorphism $\varphi : \mathcal{G}(\hat{F}/K) \to A \operatorname{wr} G$ which maps $\mathcal{G}(\hat{F}/L)$ onto A^G and induces the identity maps $\mathcal{G}(F/L) = A$ and $\mathcal{G}(L/K) = G$. We say in this set up that the fields L, F, $\hat{F}$ **realize the wreath product** $A \operatorname{wr} G$ **over** K.

$K'_0 = \hat{F}_0 \cap K'$, and $A_0 = \mathcal{G}(F_0/L)$. Then $K'_0 \cap L = K$ and $LK'_0 = \hat{F}_0$. Hence L, F_0, $\hat{F}_0$ realize $A_0 \operatorname{wr} G$ over K, as above.

2. Main results

We take the crucial step toward the solution to Problem 12.18 of [FJ] in the following lemma. It involves a construction of wreath products over fields of rational functions as in [K], Prop. 1.

LEMMA 2.1. — *Let* M_1, M_2 *be linearly disjoint infinite Galois extensions of a field* K, *and let* $N = M_1 M_2$. *Let* $f \in K[T, X]$ *be an absolutely irreducible polynomial, monic in* X, *and Galois over* K(T). *Then there exists a finite Galois extension* L *of* K *contained in* N *such that for every basis* $c_1, \ldots, c_n$ *of* L *over* K *there is a Hilbert subset* B *of* K^n *such that for each* $(b_1, \ldots, b_n) \in B$ *the polynomial* $f(b_1 c_1 + \ldots + b_n c_n, X)$ *is irreducible over* N.

Proof. — There are three parts in the proof.

Part A: Construction of L. Let $C_1 = \mathcal{G}(N/M_1)$ and $C_2 = \mathcal{G}(N/M_2)$. Then $\mathcal{G}(N/M) = C_1 \times C_2$. Choose nontrivial finite quotients G_1, G_2 of C_1, C_2, respectively. If the orders of C_1 and C_2 are not relatively prime, choose G_1 and G_2 with orders having a common prime divisor. Let $\rho : C_1 \times C_2 \to G_1 \times G_2$ be the product of the quotient maps. Consider the fixed field L of $\operatorname{Ker}(\rho)$ in N. Then $G = \mathcal{G}(L/K) = G_1 \times G_2$. By Lemma 1.2, for no nontrivial finite group A_0 there exist fields $L \subseteq E \subseteq \hat{E} \subseteq N$ such that L, E, $\hat{E}$ realize $A_0 \operatorname{wr} G$ over K.

Part B: Construction of wreath product over a field of rational functions. Choose a set $\{u^\sigma \mid \sigma \in G\}$ of algebraically independent elements over K. For each $\sigma \in G$ let x^σ be a root of $f(u^\sigma, X)$. As f is absolutely irreducible, the field $K(u^\sigma, x^\sigma)$ is a regular extension of K. Hence $L(u^\sigma, x^\sigma)$ is a regular extension of L. As these fields are algebraically independent over L, the field $\hat{Q} = L(u^\sigma, x^\sigma \mid \sigma \in G)$ is a regular extension of L [FJ], p. 112. Moreover, the field $Q = L(u^\sigma \mid \sigma \in G)$ is linearly disjoint from $K(u^\sigma, x^\sigma)$ over $K(u^\sigma)$. Hence $Q(x^\sigma)/Q$ is a Galois extension with Galois group isomorphic to $A = \mathcal{G}(f(T, X), K(T))$. The set of all $Q(x^\sigma)$ is linearly disjoint over Q. So, $\mathcal{G}(\hat{Q}/Q) \cong A^G$.

Put $n=[\mathrm{L}:\mathrm{K}]=|\mathrm{G}|$, and let $c_1, \ldots, c_n$ be a basis for L/K. Let $t_1, \ldots, t_n$ be the unique solution of the following system of linear equations:

$$(1) \qquad \mathrm{T}_1 c_1^\sigma + \ldots + \mathrm{T}_n c_n^\sigma = u^\sigma, \qquad \sigma \in \mathrm{G}$$

As the matrix (c_i^σ) is invertible [L], p. 212, $\mathrm{L}(t_1, \ldots, t_n)=\mathrm{L}(u^\sigma \mid \sigma \in \mathrm{G})=\mathrm{Q}$. 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.

Extend the action of G on L to an action on $\hat{\mathrm{Q}}$ in a natural way: $(u^\sigma)^\tau = u^{\sigma\tau}$ and $(x^\sigma)^\tau = x^{\sigma\tau}$. 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 leaves each element of $\mathrm{P}=\mathrm{K}(t_1, \ldots, t_n)$ element wise fixed. So, the fixed field Q(G) of G in Q contains P. In particular $n \leqq [\mathrm{Q}:\mathrm{P}]$. As LP=Q, this implies that P=Q(G) and that $\mathrm{L} \cap \mathrm{P}=\mathrm{K}$.

The subgroup H of $\mathrm{Aut}(\hat{\mathrm{Q}})$ generated by G and $\mathcal{G}(\hat{\mathrm{Q}}/\mathrm{Q})$ is contained in $\mathrm{Aut}(\hat{\mathrm{Q}}/\mathrm{P})$. As $\hat{\mathrm{Q}}/\mathrm{P}$ is separable, the latter group is finite and therefore so is H. Since P is the fixed field of H, the field $\hat{\mathrm{Q}}$ is Galois over P and $\mathrm{H}=\mathcal{G}(\hat{\mathrm{Q}}/\mathrm{P})$.

Now consider the fixed field $\mathrm{P}'=\hat{\mathrm{Q}}(\mathrm{G})$. Its intersection with Q is P and their compositum is $\hat{\mathrm{Q}}$. So, Q, Q(x), $\hat{\mathrm{Q}}$ realize A wr G over P.

Part C: Definition of B *and conclusion of the proof.* Write $\hat{\mathrm{Q}}$ as $\mathrm{P}(z)$ with z integral over $\mathrm{K}[t_1, \ldots, t_n]$ and let $h(t_1, \ldots, t_n, \mathrm{Z})=\mathrm{irr}(z, \mathrm{P})$. Then $f(\mathrm{T}_1 c_1 + \ldots + \mathrm{T}_n c_n, \mathrm{X})$ is irreducible over L. Use [FJ], Lemma 12.12 and Cor. 11.7, to find a Hilbert subset B of K^n such that for each $\mathbf{b} \in \mathrm{B}$ and for $a=\sum_{i=1}^{n} b_i c_i$.

$$(2a) \qquad \mathcal{G}(h(\mathbf{b}, \mathrm{Z}), \mathrm{K}) \cong \mathcal{G}(h(\mathbf{t}, \mathrm{Z}), \mathrm{P}),$$

$$(2b) \qquad f(a, \mathrm{X}) \quad \text{is irreducible over L},$$

and the specialization $\mathbf{t} \mapsto \mathbf{b}$ extends to a place of $\hat{\mathrm{Q}}$ over K such that the residue fields of P, Q, $\mathrm{Q}(x^\sigma)$, P′, $\hat{\mathrm{Q}}$, respectively, are K, L, F^σ, K′, $\hat{\mathrm{F}}$, where F^σ is the splitting field of $f(a^\sigma, \mathrm{X})$ over L, for $\sigma \in \mathrm{G}$. In particular L, F, $\hat{\mathrm{F}}$ realize A wr G over K and $[\mathrm{F}:\mathrm{L}]=\deg(f(a, \mathrm{X}))$.

Let $\mathbf{b} \in \mathrm{B}$, $a=\sum_{i=1}^{n} b_i c_i$, and assume that $f(a, \mathrm{X})$ is reducible over N. Then $\mathrm{E}=\mathrm{N} \cap \mathrm{F}$ is a proper Galois extension of L. Extend each $\sigma \in \mathcal{G}(\hat{\mathrm{F}}/\mathrm{K}')$ to an element σ of the absolute Galois group G(K) of K to observe that $\mathrm{E}^\sigma = \mathrm{N} \cap \mathrm{F}^\sigma$ is contained in N. Let $\mathrm{A}_0=\mathcal{G}(\mathrm{E}/\mathrm{L})$ and $\hat{\mathrm{E}}=\prod_{\sigma \in \mathcal{G}(\mathrm{F}/\mathrm{K}')} \mathrm{E}^\sigma$. Then $\hat{\mathrm{E}} \subseteq \mathrm{N}$ and, by Remark 1.4, L, E, $\hat{\mathrm{E}}$ realize A_0 wr G over K. This contradiction to Part A proves that $f(a, \mathrm{X})$ is irreducible over N, as desired. ■

LEMMA 2.2. — *Let* N *be a field,* N′ *a finite Galois extension of* N, $f \in \mathrm{N}[\mathrm{T}, \mathrm{X}]$ *an irreducible polynomial, which is separable in* X, *and* $g \in \mathrm{N}'[\mathrm{T}, \mathrm{X}]$ *a factor of f which is irreducible over* N′. *Then, for almost all* $a \in \mathrm{N}$, *if* $g(a, \mathrm{X})$ *is irreducible over* N′, *then* $f(a, \mathrm{X})$ *is irreducible over* N.

Proof. — The polynomial f decomposes over N′ as $f(T, X) = \prod_{i=1}^{m} g_i(T, X)$ where each g_i is conjugate to g over N and for $i \neq j$, g_i is not a multiple of g_j by an element of N′(T). Suppose that for $a \in N$ and each $i \neq j$, $g_i(a, X)$ is not a multiple of $g_j(a, X)$ by an element of N′ (this happens for almost all $a \in N$) and $g(a, X)$ is irreducible over N′. Then $f(a, X)$ is irreducible over N. Indeed, let $f(a, X) = h_1(X) h_2(X)$ be a decomposition over N. Then $h_1(X) h_2(X) = \prod_{i=1}^{m} g_i(a, X)$. As $g(a, X)$ is irreducible, it divides, say, $h_1(X)$. Since each $g_i(a, X)$ is conjugate to $g(a, X)$ over N, it also divides $h_1(X)$. As $g_1(a, X), \ldots, g_m(a, X)$ are relatively prime, $f(a, X) = \prod_{i=1}^{m} g_i(a, X)$ divides $h_1(X)$. Conclude that $f(a, X)$ is irreducible over N. ■

PROPOSITION 2.3. — *Let* M_1 *and* M_2 *be infinite Galois extensions of Hilbertian field* K *such that* $M_1 \cap M_2 = K$. *Then their compositum* $N = M_1 M_2$ *is Hilbertian. Moreover, given an irreducible polynomial* $f \in N[T, X]$, *separable in* X, *there exist* $c_1, \ldots, c_n \in N$ *and a Hilbert subset* B *of* K^n *such that for each* $(b_1, \ldots, b_n) \in B$, *and for* $a = \sum_{i=1}^{n} b_i c_i$, *the polynomial* $f(a, X)$ *is irreducible over* N.

Proof. — Note that the second statement means that if K is only separably Hilbertian [FJ], p. 147, then so is N. If K is Hilbertian, as we suppose, then it is imperfect. Hence, the second statement implies in this case that N is Hilbertian [FJ], Prop. 11.16.

To prove the second statement consider a transcendental element t over K. Let $\hat{N}$ be the splitting field of $f(t, X)$ over $N(t)$. Choose a primitive element y for $\hat{N}$ over $N(t)$ such that $h = \mathrm{irr}(y, N(t))$ has coefficients in $N[t]$. Then h is monic and Galois in X. If we find $c_1, \ldots, c_n \in N$ and a Hilbert subset B of K^n such that for each $(b_1, \ldots, b_n) \in B$ and with $a = \sum_{i=1}^{n} b_i c_i$, the polynomial $h(a, X)$ is irreducible over N, then K^n has a Hilbert subset B_0 of B such that for $(b_1, \ldots, b_n) \in B_0$ the polynomials $f(a, X)$ is also irreducible over N. Indeed, the proof of [FJ], Lemma 12.12, shows that if a is not a zero of a certain nonzero polynomial with coefficients in N and $h(a, X)$ is irreducible, then $\mathcal{G}(f(a, X), N)$ and $\mathcal{G}(f(t, X), N(t))$ are isomorphic as permutation groups of the roots. In particular the former group operates transitively on the roots of $f(a, X)$. This implies that $f(a, X)$ is irreducible. Note that the exclusion of finitely many values $a_1, \ldots, a_k$ for a imposes the extra condition

$$\prod_{j=1}^{k} \left(\sum_{i=1}^{n} b_i c_i - a_j \right) \neq 0$$

on $(b_1, \ldots, b_n) \in B$. This defines B_0. So, without loss, assume that f is monic and Galois in X.

Choose an absolutely irreducible factor g of f. Let K'_0 be a finite Galois extension of K which contains the coefficients of g. Let K_1 and K_2 be finite Galois extensions of K contained in M_1 and M_2, respectively, such that $K'_0 \cap N \subseteq K_1 K_2$. Then $K' = K_1 K_2 K'_0$ satisfies $N \cap K' = K_1 K_2$ and $M_1 K_2 \cap M_2 K_1 = K_1 K_2$ (use the tower property of linear disjointness [FJ], Lemma 9.3).

Let $M'_1 = M_1 K_2 K'$, $M'_2 = M_2 K_1 K'$, $N' = NK'$. Then M'_1, M'_2 are linearly disjoint Galois extensions of K' and $N' = M'_1 M'_2$. By Lemma 2.1 there is a finite Galois extension L' of K' contained in N' such that for every basis $c_1, \ldots, c_n$ of L'/K' there is a Hilbert subset B' of $(K')^n$ such that for each $b_1, \ldots, b_n \in B'$ the polynomial $g(b_1 c_1 + \ldots + b_n c_n, X)$ is irreducible over N'. As $\mathcal{G}(N'/K') = \mathcal{G}(N/K_1 K_2)$, there is a finite Galois extension L of $K_1 K_2$ in N such that $L' = LK'$. A basis $c_1, \ldots, c_n$ of $L/K_1 K_2$ is also a basis of L'/K'. By Lemma 2.2 and by [FJ], Cor. 11.7, K^n has a Hilbert subset $B \subseteq B'$ such that $f(b_1 c_1 + \ldots + b_n c_n, X)$ is irreducible over N, for every $b_1, \ldots, b_n \in B$. ■

We are now ready to solve Problem 12.18 of [FJ] in a much stronger form:

THEOREM 2.4. — *Let* M_1 *and* M_2 *be Galois extensions of Hilbertian field* K *neither of which is contained in the other. Then their compositum* $N = M_1 M_2$ *is Hilbertian.*

Proof. — If N is a finite extension of M_1 or of M_2, then it is Hilbertian, by Weissauer's theorem. So, assume that N is an infinite extension of both M_1 and M_2. In particular $K_1 = M_1 \cap M_2$ has a finite proper Galois extension K' which is contained in M_2. Let $M'_1 = M_1 K'$. By Weissauer's theorem, K' is Hilbertian. Also, M'_1 and M_2 are infinite extensions of K' whose intersection is K' and whose compositum is N. Conclude from Proposition 2.3 that N is Hilbertian. ■

One of the consequences of Theorem 2.4 is a solution of Problem 12.19 of [FJ]:

COROLLARY 2.5. — *The separable (resp. solvable, p−) closure* K_s *(resp.* K_{solv}, $K^{(p)}$*) of a Hilbertian field* K *is not the compositum of two Galois extensions of* K *neither of which is equal to* K_s *(resp.,* K_{solv}, $K^{(p)}$*).*

Proof. — None of the above fields is Hilbertian. So the corollary follows from Theorem 2.4.

Nevertheless, as the separable case was the subject of an open question we sketch a short cut in the above proof in this case.

Assume that M_1 and M_2 are Galois extensions of K which are not separably closed such that $M_1 M_2 = K_s$. Use Weissauer's theorem to replace M_1, M_2, and K, if necessary, by algebraic extensions to assume that M_1, M_2 are Hilbertian and $M_1 \cap M_2 = K$. In particular M_i has a cyclic extension M'_i of degree p, $i = 1, 2$ [FJ], Thm. 24.48.

Let $K_1 = M_1 \cap M'_2$, $K_2 = M_2 \cap M'_1$ and $L = K_1 K_2$. Then

$$G = \mathcal{G}(L/K) = \mathcal{G}(L/K_1) \times \mathcal{G}(L/K_2) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}.$$

By [FJ], Prop. 24.47, there exists a Galois extension F of K which contains L and there exists an isomorphism $\varphi : (\mathbf{Z}/p\mathbf{Z}) \operatorname{wr} G \to \mathcal{G}(F/K)$ such that $\operatorname{res}_L \circ \varphi$ is the canonical projection of the wreath product on G.

Now choose a generator σ_i of $\mathcal{G}(L/K_i)$, $i=1,2$ and let $\sigma=\sigma_1\sigma_2$. Chatzidakis' Lemma [FJ], Lemma 24.52, extends σ to an element τ of $\mathcal{G}(F/K)$ such what restriction to L maps the normalizer of $\langle\tau\rangle$ onto $\langle\sigma\rangle$. This gives a group theoretic contradiction as in Lemma 1.2.

Note that this proof actually works for each normal extension N of K which admits no p-extensions. In particular it works also for K_{solv} and $K^{(p)}$. ■

REMARK 2.6. – Kuyk [K], p. 120, states, contrary to Theorem 2.4, that the compositum of linearly disjoint Galois extensions of a Hilbertian field need not be Hilbertian. He adjoins p-th roots of all elements of $\mathbb{Q}$ to $K=\mathbb{Q}(\zeta_p)$ to get a Galois extension $\mathbb{Q}^{()p)}$ of K. Then $\mathcal{G}(\mathbb{Q}^{(p)}/K)$ is isomorphic to the direct product of infinitely many cyclic extensions of order p. Kuyk claims, without a proof, that $\mathbb{Q}^{(p)}$ is not Hilbertian. However, as $\mathbb{Q}^{(p)}$ is the compositum of a linearly disjoint finite Galois extension and an infinite Galois extensions, already Weissauer's theorem implies that $\mathbb{Q}^{(p)}$ is Hilbertian, contrary to Kuyk's statement.

REFERENCES

[D] K. DÖRGE, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes* (*Math. Annal.*, Vol. 96, 1927, pp. 176-182).

[F] M. FRIED, *Irreducibility Results for Separated Variables Equations* (*J. Pure Appl. Alg.*, Vol. 48, 1987, pp. 9-22).

[FJ] M. D. FRIED and M. JARDEN, *Field Arithmetic* (*Ergebnisse der Mathematik III*, Vol. 11, Springer, Heidelberg, 1986).

[Fr] W. FRANZ, *Untersuchungen zum Hilbertschen Irreduzibilitätssatz* (*Math. Z.*, Vol. 33, 1931, pp. 275-293).

[G] W.-D. GEYER, *Galois Groups of Intersections of Local Fields* (*Israel J. Math.*, Vol. 30, 1978, pp. 382-396).

[H] D. HILBERT, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten* (*J. reine angew. Math.*, Vol. 110, 1892, pp. 104-129).

[I] E. INABA, *Über den Hilbertschen Irreduzibilitätssatz* (*Jap. J. Math.*, Vol. 19, 1944, pp. 1-25).

[K] W. KUYK, *Extensions de corps hilbertiens* (*J. Alg.*, Vol. 14, 1970, pp. 112-124).

[L] S. LANG, *Algebra*, Addison-Wesley, Reading, 1970.

[M] B. H. MATZAT, *Über das Umkehrproblem der Galoisschen Theorie* (*Jahresbericht Deutschen Mathematiker-Vereinigung*, Vol. 90, 1988, pp. 155-183).

[Mc] S. MACLANE, *Homology*, Springer, Berlin, 1963.

[R] L. RIBES, *Introduction to Profinite Groups and Galois Cohomology* (*Queen's Papers Pure Appl. Math.*, No. 24, Queen's University, Kingston, 1970).

[S] V. G. SPRINDŽUK, *Reducibility of Polynomials and Rational Points on Algebraic Curves* (*Seminar on Number Theory*, Paris, 1979-1980).

[U] K. UCHIDA, *Separably Hilbertian Fields* (*Kodai Math. J.*, Vol. 3, 1980, pp. 83-95).

[W] R. WEISSAUER, *Der Hilbertsche Irreduzibilitätssatz* (*J. reine angew. Math.*, Vol. 334, 1982, pp. 203-220).

[Z] P. ZORN, *Der Hilbertsche Irreduzibilitätssatz*, Zulassungsarbeit zur wissenschaftlichen Prüfung für das Höhere Lehramt, written under the supervision of W.-D. GEYER, Erlangen, 1975.

(Manuscript received March 22, 1990,
revised June 22, 1990.)

D. HARAN and M. JARDEN,
School of Mathematical Sciences,
Raymond and Beverly Sackler Faculty of Exact Sciences,
Tel Aviv University,
Ramat Aviv, Tel Aviv 69978, Israel.