LARGE NORMAL EXTENSIONS OF HILBERTIAN FIELDS*

by

Moshe Jarden
School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv, 69978, Israel
e-mail: jarden@math.tau.ac.il

Abstract: Let K be a countable separably Hilbertian field. Denote the absolute Galois group of K by $G(K)$. For each $\boldsymbol{\sigma} \in (\sigma_1, \ldots, \sigma_e) \in G(K)^e$ let $K_s[\boldsymbol{\sigma}]$ be the maximal Galois extension of K which is fixed by $\sigma_1, \ldots, \sigma_e$. We prove that for almost all $\boldsymbol{\sigma} \in G(K)^e$ (in the sense of the Haar measure) the field $K_s[\boldsymbol{\sigma}]$ is PAC and its absolute Galois group is isomorphic to $\hat{F}_\omega$.

Mathematische Zeitschrift **224** (1997), 555-565

* This research was supported by The Israel Science Foundation administered by The Israel Academy of Sciences and Humanities

Introduction

The goal of this note is to consider a certain natural family of closed normal subgroups of $G(\mathbb{Q})$ and to prove that each group in this family is free. More generally, consider a countable separably Hilbertian field K. Denote the absolute Galois group of K by $G(K)$. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$ the field $K_s(\boldsymbol{\sigma})$ is PAC and e-free [FJ2, Thms. 16.13 and 16.18]. Here K_s is the separable closure of K and $K_s(\boldsymbol{\sigma})$ is the fixed field of $\boldsymbol{\sigma}$ in K_s. Being **PAC** means that every nonvoid absolutely irreducible variety defined over $K_s(\boldsymbol{\sigma})$ has a $K_s(\boldsymbol{\sigma})$-rational point. We say that $K_s(\boldsymbol{\sigma})$ is e-**free** if $G(K_s(\boldsymbol{\sigma}))$ (i.e., the closed subgroup $\langle \sigma_1, \ldots, \sigma_e \rangle$ of $G(K)$ generated by $\sigma_1, \ldots, \sigma_e$) is free on e generators.

Denote the largest Galois extension of K which is contained in $K_s(\boldsymbol{\sigma})$ by $K_s[\boldsymbol{\sigma}]$. It is the intersection of all K-conjugates of $K_s(\boldsymbol{\sigma})$ and also the fixed field of the smallest closed normal subgroup of $G(K)$ which contains $\sigma_1, \ldots, \sigma_e$. If $\mathrm{char}(K) = 0$, then, for almost all $\boldsymbol{\sigma} \in G(K)^e$ the field $K_s[\boldsymbol{\sigma}]$ is PAC [FJ2, Thm. 16.47]. Lemma 1.2 below generalizes this result to arbitrary characteristic. If we knew that $K_s[\boldsymbol{\sigma}]$ is separably Hilbertian, then a theorem of Fried-Völklein and Pop would imply that $K_s[\boldsymbol{\sigma}]$ is ω-free. That is, $G(K_s[\boldsymbol{\sigma}])$ is isomorphic to the free profinite group $\hat{F}_w$ on countably many generators. Unfortunately, it is not clear how to prove the Hilbertianity of almost all $K_s[\boldsymbol{\sigma}]$ directly. So, we use instead a forerunner to the above mentioned theorem of Fried-Völklein-Pop and a recent theorem of Neumann [Neu] to prove directly that $G(K_s[\boldsymbol{\sigma}]) \cong \hat{F}_\omega$ for almost all $\boldsymbol{\sigma} \in G(K)^e$. A theorem of Roquette, then implies that $K_s[\boldsymbol{\sigma}]$ is also separably Hilbertian.

Let $\tilde{K}$ be the algebraic closure of K. Denote the maximal purely inseparable extension of $K_s[\boldsymbol{\sigma}]$ by $\tilde{K}[\boldsymbol{\sigma}]$. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $\tilde{K}[\boldsymbol{\sigma}]$ is PAC and ω-free. If K is a given finitely generated field, this information leads, via Galois stratification, to a primitive recursive decision procedure for the elementary theory of the family of almost all fields $\tilde{K}[\boldsymbol{\sigma}]$.

Acknowledgement: The author is indebted to Aharon Razon and Dan Haran for critical reading which led to improvement of an earlier version of this work.

1. The field $K_s[\sigma_1, \ldots, \sigma_e]$

Let G be a profinite group, and let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e)$ be an e-tuple of elements of G. The closed subgroup generated by $\boldsymbol{\sigma}$ is usually denoted by $\langle \boldsymbol{\sigma} \rangle$. We denote the **closed normal subgroup of G generated by $\boldsymbol{\sigma}$** by $[\boldsymbol{\sigma}]_G$ or by $[\boldsymbol{\sigma}]$ if G is clear from the context. It is the closed subgroup $\langle \sigma_i^\tau \mid \tau \in G,\ i = 1, \ldots, e \rangle$. It is also the intersection of all closed normal subgroups of G which contain $\sigma_1, \ldots, \sigma_e$.

Let A be a normal subgroup of G. We say that A is **normally generated in G by e elements** if there exist $\sigma_1, \ldots, \sigma_e \in G$ such that $A = [\boldsymbol{\sigma}]_G$. If G is normally generated in itself by e elements, we just say that G is **normally generated by e elements**.

If $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_f)$ is an f-tuple of elements of G, then, by definition, $[\boldsymbol{\sigma}, \boldsymbol{\tau}] = [\boldsymbol{\sigma}] \cdot [\boldsymbol{\tau}]$. If $h\colon H \to G$ is an epimorphism of profinite groups, then $h\langle \boldsymbol{\sigma} \rangle = \langle h(\boldsymbol{\sigma}) \rangle$ and $h([\boldsymbol{\sigma}]_H) = [h(\boldsymbol{\sigma})]_G$. If G is abelian, then $[\boldsymbol{\sigma}] = \langle \boldsymbol{\sigma} \rangle$.

Let now N/K be a Galois extension, $G = \mathcal{G}(N/K)$ and $\boldsymbol{\sigma} \in G^e$. Then $N(\boldsymbol{\sigma})$ is the fixed field of $\boldsymbol{\sigma}$ in N, and $N[\boldsymbol{\sigma}]_K$ (or $N[\boldsymbol{\sigma}]$, if K is clear from the context) is the maximal Galois extension of K which is contained in $N(\boldsymbol{\sigma})$. It is also the fixed field of $[\boldsymbol{\sigma}]$ in N. For each $\boldsymbol{\tau} \in G^f$ we have $N[\boldsymbol{\sigma}] \cap N[\boldsymbol{\tau}] = N[\boldsymbol{\sigma}, \boldsymbol{\tau}]$. If N' is a Galois extension of K which contains N, $\boldsymbol{\sigma}' \in \mathcal{G}(N'/K)^e$ and $\boldsymbol{\sigma} = \mathrm{res}_N \boldsymbol{\sigma}'$, then $N \cap N'[\boldsymbol{\sigma}'] = N[\boldsymbol{\sigma}]$. In particular if $N = K_s$, then $K_s[\boldsymbol{\sigma}]$ is the maximal Galois extension of K which is contained in $K_s(\boldsymbol{\sigma})$.

Recall [FJ2, p. 381] that a field M is **ω-free** if every finite embedding problem for $G(M)$ is solvable. If in addition $G(M)$ has rank $\le \aleph_0$ and in particular if M is countable, then the latter condition is equivalent to $G(M) \cong \hat{F}_\omega$ (Iwasawa [FJ2, Cor. 24.2]).

Our goal in this section and in the next one is to prove that if K is a countable separably Hilbertian field, then for almost all $\boldsymbol{\sigma} \in G(K)^e$ the field $K_s[\boldsymbol{\sigma}]$ is ω-free and PAC.

One of the two major ingredients in the proof is Proposition 1.1 below. It has been first proved for fields K of characteristic 0 in [FJ1, Thm. 3.4] and then has been generalized to infinite perfect fields in [GeJ, Cor. I]. Finally Neumann [Neu] has completed the proof for arbitrary K.

Recall that a field extension F/K is **regular** if F is linearly disjoint from $\tilde{K}$ over K. If F/K is finitely generated, then this condition is equivalent to 'K is algebraically closed in F and F/K has a separating transcendence base' [FJ2, §9.2].

PROPOSITION 1.1: *Let F be a finitely generated regular extension of a field K. Then there exist a positive integer n and a separating transcendence base $t_1, \ldots, t_r$ for F/K such that the Galois closure $\hat{F}$ of $F/K(\mathbf{t})$ is regular over K and $\mathcal{G}(\hat{F}/K(\mathbf{t}))$ is isomorphic to the symmetric group S_n.*

The transcendence base $t_1, \ldots, t_r$ of Proposition 1.1 is called a **stabilizing base** for F/K.

LEMMA 1.2: *Let K be a countable separably Hilbertian field. Then, $K_s[\boldsymbol{\sigma}]$ is PAC for almost all $\boldsymbol{\sigma} \in G(K)^e$.*

Proof: The special case of the lemma in which $\mathrm{char}(K) = 0$ is stated as Theorem 16.47 of [FJ2]. The general case is proved in the same way, using Proposition 1.1. We reproduce the proof here for the convenience of the reader.

By [FJ2, Thm. 10.4], it suffices to prove that each absolutely irreducible variety V defined over K has a $K_s[\boldsymbol{\sigma}]$-rational point for almost all $\boldsymbol{\sigma} \in G(K)^e$. So, let $\mathbf{x} = (x_1, \ldots, x_n)$ be a generic point of V over K and consider the function field $F = K(\mathbf{x})$ of V over K. It is a regular extension of K. Let $\mathbf{t} = (t_1, \ldots, t_r)$ be a stabilizing base for F/K (Proposition 1.1) and let $\hat{F}$ be the Galois closure of $F/K(\mathbf{t})$. Choose a primitive element y for $\hat{F}/K(\mathbf{t})$ which is integral over $K[\mathbf{t}]$. Since $\hat{F}/K$ is a regular extension, $\mathrm{irr}(y, K(\mathbf{t})) = f(\mathbf{t}, Y)$ is an absolutely irreducible polynomial.

The discriminant of $f(\mathbf{t}, Y)$ is a nonzero polynomial $d \in K[\mathbf{t}]$. Write $x_j = p_j(\mathbf{t}, y)/p_0(\mathbf{t})$ with $p_j \in K[\mathbf{t}, Y]$, $j = 1, \ldots, n$, and $0 \neq p_0 \in K[\mathbf{t}]$. Let $y^{(1)}, \ldots, y^{(s)}$ be the conjugates of y over $K(\mathbf{t})$. Write $y^{(k)} = q_k(\mathbf{t}, y)/q_0(\mathbf{t})$ with $q_k \in K[\mathbf{t}, Y]$, $k = 1, \ldots, s$, and $0 \neq q_0 \in K[\mathbf{t}]$. Since K is separably Hilbertian, we may use [FJ2, Cor. 11.7] and inductively construct a sequence of points $(\mathbf{t}_i, y_i)$ such that $\mathbf{t}_i \in K^r$, the polynomial $f(\mathbf{t}_i, Y)$ is irreducible over $K(y_1, \ldots, y_{i-1})$, $f(\mathbf{t}_i, y_i) = 0$, and $d(\mathbf{t}_i)p_0(\mathbf{t}_i)q_0(\mathbf{t}_i) \neq 0$.

Then $L_i = K(y_i)$ is a Galois extension of degree s, with $\mathcal{G}(L_i/K) \cong \mathcal{G}(\hat{F}/K(\mathbf{t}))$ [Lan, p. 248, Prop. 15]. Also, with $x_{ij} = p_j(\mathbf{t}_i, y_i)/p_0(\mathbf{t}_i)$, the point $\mathbf{x}_i = (x_{i1}, \ldots, x_{in})$

belongs to $V(L_i)$. Finally, the sequence $L_1, L_2, L_3, \ldots$ of Galois extensions is linearly disjoint over K.

By [FJ2, Lemma 16.11], for almost all $\boldsymbol{\sigma} \in G(K)^e$ there exists i such that $L_i \subseteq K_s(\boldsymbol{\sigma})$. Since L_i is Galois, it is contained in $K_s[\boldsymbol{\sigma}]$. In particular, $\mathbf{x}_i$ is $K_s[\boldsymbol{\sigma}]$-rational. ∎

Lemma 1.3: *Let K be a separably Hilbertian field. For almost all $(\boldsymbol{\sigma}, \tau) \in G(K)^{e+1}$, the field $K_s[\boldsymbol{\sigma}, \tau]$ is properly contained in $K_s[\boldsymbol{\sigma}]$.*

Proof: For each finite abelian group A, [FJ2, Lemma 24.46] gives a purely transcendental extension $E = K(t_1, \ldots, t_r)$ of K and a Galois extension F of E which is regular over K such that $\mathcal{G}(F/E) \cong A$. Since K is separably Hilbertian, [FJ2, Lemma 15.8] allows us to specialize $\mathbf{t}$ infinitely many times onto an r-tuple with coordinates in K and to get a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K with Galois group A.

Apply this construction to $A = (\mathbb{Z}/2\mathbb{Z})^{e+1}$. For each i let $\sigma_{i1}, \ldots, \sigma_{ie}, \tau_i$ be a system of generators for $\mathcal{G}(L_i/K)$. For almost all $(\boldsymbol{\sigma}, \tau) \in G(K)^{e+1}$ there exists i such that $\mathrm{res}_{L_i}(\boldsymbol{\sigma}, \tau) = (\boldsymbol{\sigma}_i, \tau_i)$ [FJ2, Lemma 16.11]. Since A is not generated by e elements and since A is abelian, $K = L_i(\boldsymbol{\sigma}_i, \tau_i) = L_i[\boldsymbol{\sigma}_i, \tau_i]$ is properly contained in $L_i(\boldsymbol{\sigma}_i) = L_i[\boldsymbol{\sigma}_i]$. Hence, if $(\boldsymbol{\sigma}, \tau)$ is as above, $L_i[\boldsymbol{\sigma}_i, \tau_i] = L_i \cap K_s[\boldsymbol{\sigma}, \tau]$ and $L_i[\boldsymbol{\sigma}_i] = L_i \cap K_s[\boldsymbol{\sigma}]$. So, $K_s[\boldsymbol{\sigma}, \tau] \subset K_s[\boldsymbol{\sigma}]$. This concludes the proof of the lemma. ∎

The following result is a special case of [FJ2, Cor. 12.15].

Proposition 1.4 (Weissauer): *Let N be a Galois extension of a separably Hilbertian field K. Then every proper finite separable extension M of N is separably Hilbertian.*

Proposition 1.5 ([FV2, Thm. A] for characteristic 0 and [Pop, Thm. 1] for arbitrary characteristic): *Every PAC separably Hilbertian field is ω-free.*

Lemma 1.6: *Let K be a countable separably Hilbertian field. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $K_s[\boldsymbol{\sigma}]$ is a Galois extension of an ω-free PAC field.*

Proof: By Lemmas 1.2 and 1.3, almost all $(\boldsymbol{\sigma}, \tau) \in G(K)^{e+1}$ have these properties:

(1a) $K_s[\boldsymbol{\sigma}, \tau]$ is PAC, and

(1b) $K_s[\boldsymbol{\sigma}]$ is a proper extension of $K_s[\boldsymbol{\sigma},\tau]$.

So, $K_s[\boldsymbol{\sigma},\tau]$ has a proper finite extension M which is contained in $K_s[\boldsymbol{\sigma}]$. By Proposition 1.4, M is separably Hilbertian. Since by (1a), M is a separable algebraic extension of a PAC field, it is itself PAC [FJ2, Cor. 10.7]. Conclude from Proposition 1.5 that M is ω-free. ∎

2. The absolute Galois group of $K_s[\sigma_1, \ldots, \sigma_e]$

By Lemma 1.6 and by [FJ2, Cor. 24.4], for almost all $\boldsymbol{\sigma} \in G(K)^e$ the group $[\boldsymbol{\sigma}]$ has the **embedding property**. That is, every finite embedding problem (φ: $[\boldsymbol{\sigma}] \to A$, α: $B \to A$) has a solution provided B is a quotient of $[\boldsymbol{\sigma}]$. Thus, in order to prove that $K_s[\boldsymbol{\sigma}]$ is ω-free, it would suffice now to prove that each finite group is realizable over it. This, I have not been able to do. Fortunately, the following result of Melnikov allows us to get away with less:

LEMMA 2.1: *A closed normal subgroup N of $\hat{F}_\omega$ is isomorphic to $\hat{F}_\omega$ if and only if the following groups are quotients of N:*
(a) *S^n, for each finite nonabelian simple group S and for each positive integer n; and*
(b) *$\mathbb{Z}/p\mathbb{Z}$, for each prime number p.*

Proof: For each finite simple group S let $M_S(N)$ be the intersection of all open normal subgroups M of N such that $N/M \cong S$. Then $N/M_S(N) \cong S^m$, where m is a cardinal number between 0 and $\aleph_0$, which we denote by $r_N(S)$. If $S = \mathbb{Z}/p\mathbb{Z}$, then $r_N(S)$ is either 0 or $\aleph_0$ [Mel, Thm. 3.2]. Hence, if all finite groups in (a) and (b) are quotients of N, then $r_N(S) = \aleph_0$ for all S. In addition $r_{\hat{F}_\omega}(S) = \aleph_0$ for all S. Since the function $r_N(S)$ characterizes N among all closed normal subgroups of $\hat{F}_\omega$ up to an isomorphism [Mel, Thm. 3.1], this implies that $N \cong \hat{F}_\omega$. ∎

It is a consequence of the realizability of the symmetric groups over a Hilbertian field K, that for each finite group G there exists a finite separable extension L of K over which G is realizable. Harbater [Ha1, Prop. 1.4] (and possibly others) observed that if K is a number field, then the Riemann existence theorem implies that L can be chosen to be Galois over K. Since for each field K (even if $\mathrm{char}(K) > 0$), each finite group G occurs as a Galois group over $K_s(t)$ [Ha2, Cor. 1.5] (See also a recent more elementary proof of this result by Haran and Völklein [HV].), the same conclusion holds now for each Hilbertian field K, irrespective of its characteristic. Proposition 2.3 below uses Propositions 1.1 and 2.2 to strengthen the above result.

Given a finite group G and a positive integer r, Fried and Völklein [FV1] parametrize all Galois covers of the projective line over $\mathbb{C}$ with Galois group G and with r branch points by a nonsingular algebraic set over $\mathbb{Q}$. They show that for each G there is some r such that this set has an absolutely irreducible component $\mathcal{H}$ defined over $\mathbb{Q}$. In particular $\mathcal{H}$ has the **realization property** with respect to G over each field K of characteristic 0: Let u be a transcendental element over K. If $\mathcal{H}(K)$ is nonempty, then $K(u)$ has a Galois extension N which is regular over K such that $\mathcal{G}(N/K(u)) \cong G$.

The existence of such a variety for fields of arbitrary characteristic is a consequence of a theorem of Harbater:

PROPOSITION 2.2: *Let K be a field and let G be a finite group. Then there exists an absolutely irreducible variety $\mathcal{H}$ which is defined over K and with the realization property with respect to G over every extension of K.*

Proof: Consider the field of formal power series $E = K((t))$. By [Ha1, Thm. 2.3], [Liu], or [HaV, Thm. 4.4], $E(u)$ has a Galois extension F which is regular over E such that $\mathcal{G}(F/E(u)) \cong G$. Choose a primitive element z for $F/E(u)$ which is integral over $E[u]$. Since F/E is a regular extension, $f(u, Z) = \mathrm{irr}(z, E(u))$ is an absolutely irreducible polynomial with coefficients in E.

Let $z_1, \ldots, z_s$ be all conjugates of z over $E(u)$. Then $z_i = p_i(u, z)/p_0(u)$ with polynomials $p_i \in E[u, Z]$, $i = 1, \ldots, s$, and $0 \neq p_0 \in E[u]$. Also, the discriminant of $f(u, Z)$ is a nonzero polynomial $d \in E[u]$.

Let $x_1, \ldots, x_n$ be all the elements of E which appear in the coefficients of $f, p_0, p_1, \ldots, p_s, d$. Let $g_0, g_1 \in K[\mathbf{X}]$ be polynomials such that $g_0(\mathbf{x})$ is a nonzero coefficient of $p_0(u)$ and $g_1(\mathbf{x})$ is a nonzero coefficient of $d(u)$. Finally let $h \in K[\mathbf{X}, u, Z]$ be a polynomial such that $h(\mathbf{x}, u, Z) = f(u, Z)$.

By Bertini-Noether theorem [FJ2, Prop. 8.8] there exists a nonzero polynomial $g_2 \in K[\mathbf{X}]$ such that for each extension L of K which is algebraically independent of $K(u)$ over K and for each specialization $\mathbf{a} \in L^n$ of $\mathbf{x}$ such that $g_2(\mathbf{a}) \neq 0$, the polynomial $h(\mathbf{a}, u, Z)$ is absolutely irreducible. In particular, if $\bar{z}$ satisfies $h(\mathbf{a}, u, \bar{z}) = 0$, then $L(u, \bar{z})$ is a regular extension of L. If in addition $g_0(\mathbf{a})g_1(\mathbf{a}) \neq 0$, then $L(u, \bar{z})/L(u)$ is a Galois extension with Galois group isomorphic to G (use [Lan, p. 248, Prop. 15]).

Finally, note that E is a regular extension of K (e.g., $K[[t]]$ is a valuation ring with residue field K; now use [Jar, Lemma 1.2]). Hence $K(\mathbf{x})$ is also a regular extension of K. Let $g = g_0g_1g_2$ and $y = g(\mathbf{x})^{-1}$. Then $(\mathbf{x}, y)$ generates an absolutely irreducible variety $\mathcal{H}$ over K.

Let now L be an extension of K and let $(\mathbf{a}, b) \in \mathcal{H}(L)$. Then $\mathbf{a}$ is an L-specialization of $\mathbf{x}$ and $g(\mathbf{a}) \neq 0$. Assume without loss that u is transcendental over L. Hence, by the preceding paragraph, $L(u)$ has a Galois extension with Galois group isomorphic to G. Conclude that $\mathcal{H}$ has the realization property over L. ∎

PROPOSITION 2.3: *Let K be a separably Hilbertian field and let G be a finite group. Then there exists a positive integer n and there exists a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K with $\mathcal{G}(L_i/K) \cong S_n$, $i = 1, 2, 3, \ldots$, such that for each i, L_i has a linearly disjoint sequence $L_{i1}, L_{i2}, L_{i3}, \ldots$ of Galois extensions with $\mathcal{G}(L_{ij}/L_i) \cong G$, $j = 1, 2, 3, \ldots$.*

Proof: Let $\mathcal{H}$ be a variety defined over K with the realization property with respect to G over each extension of K (Proposition 2.2). Let $\mathbf{x}$ be a generic point of $\mathcal{H}$ over K and consider the function field $F = K(\mathbf{x})$ of $\mathcal{H}$ over K. It is a regular extension of K of, say, transcendence degree r. Take the integer n and the stabilizing base $t_1, \ldots, t_r$ for F/K that Proposition 1.1 provides. Thus, the Galois closure $\hat{F}$ of $F/K(\mathbf{t})$ is a regular extension of K and $\mathcal{G}(\hat{F}/K(\mathbf{t})) \cong S_n$.

Since K is separably Hilbertian, we may specialize $\mathbf{t}$ into K in infinitely many ways and get a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K with $\mathcal{G}(L_i/K) \cong S_n$ and with a point $\mathbf{x}_i \in \mathcal{H}(L_i)$ [FJ2, Lemma 15.8].

By the realization property of $\mathcal{H}$, for each i, the field $L_i(u)$ has a Galois extension F_i which is regular over L_i such that $\mathcal{G}(F_i/L_i(u)) \cong G$. Since L_i is separably Hilbertian [FJ2, Cor. 11.7], it has a linearly disjoint sequence $L_{i1}, L_{i2}, L_{i3}, \ldots$ of Galois extensions with Galois groups isomorphic to G, as claimed. ∎

LEMMA 2.4: *Let K be a separably Hilbertian field and let G be a finite group which is normally generated by e elements. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the group G is realizable over $K_s[\boldsymbol{\sigma}]$.*

Proof: Apply Proposition 2.3 to G and use its notation. For each pair (i, j) choose

$\boldsymbol{\sigma}_{ij} \in \mathcal{G}(L_{ij}/L_i)^e$ such that $L_{ij}[\boldsymbol{\sigma}_{ij}]_{L_i} = L_i$. If $\boldsymbol{\sigma} \in G(L_i)^e$ is a lifting of $\boldsymbol{\sigma}_{ij}$, then $K_s[\boldsymbol{\sigma}] = K_s[\boldsymbol{\sigma}]_K$ is a Galois extension of L_i and $L_{ij} \cap K_s[\boldsymbol{\sigma}] \subseteq L_{ij}(\boldsymbol{\sigma}_{ij})$. It follows that $L_{ij} \cap K_s[\boldsymbol{\sigma}]$ is contained in $L_{ij}[\boldsymbol{\sigma}_{ij}]_{L_i}$. So, by the choice of $\boldsymbol{\sigma}_{ij}$, we have $L_{ij} \cap K_s[\boldsymbol{\sigma}] = L_i$. By Galois theory, $\mathcal{G}(L_{ij}K_s[\boldsymbol{\sigma}]/K_s[\boldsymbol{\sigma}]) \cong \mathcal{G}(L_{ij}/L_i) \cong G$.

Finally let μ be the normalized Haar measure of $G(K)^e$. Since the L_i's, are linearly disjoint over K with a fixed degree, we have $\mu(\bigcup_{i=1}^\infty G(L_i)^e) = 1$ [FJ2, Lemma 16.11]. Similarly, as the L_{ij} are linearly disjoint over L_i with a fixed degree, we have $\mu(G(L_i)) = \mu\big(\bigcup_{j=1}^\infty \{\boldsymbol{\sigma} \in G(L_i)^e \| \mathrm{res}_{L_{ij}}\boldsymbol{\sigma} = \boldsymbol{\sigma}_{ij}\}\big)$. It follows that almost each $\boldsymbol{\sigma} \in G(K)^e$ is a lifting of some $\boldsymbol{\sigma}_{ij}$. Combined with the preceding paragraph, this concludes the proof of the lemma. ∎

Lemma 2.5: *Let S be a finite simple nonabelian group. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for all n, the group S^n occurs as a Galois group over $K_s[\boldsymbol{\sigma}]$.*

Proof: By Lemma 2.4, it suffices to prove that S^n is normally generated by one element. Indeed, rewrite S^n as $\prod_{i=1}^n S_i$ with $S_i \cong S$ for $i = 1, \ldots, n$. Choose $\boldsymbol{\sigma} \in S^n$ such that none of its coordinates is 1. Then $[\boldsymbol{\sigma}]$ as a normal subgroup of S^n is equal to $\prod_{i\in I} S_i$ where I is a subset of $\{1, \ldots, n\}$ [Hup, p. 51]. By the choice of $\boldsymbol{\sigma}$, I must be the whole set. Conclude that $[\boldsymbol{\sigma}] = G$, as desired. ∎

Lemma 2.6: *Let K be a separably Hilbertian field. Let p be a prime and let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the group $\mathbb{Z}/p\mathbb{Z}$ occurs as a Galois group over $K_s[\boldsymbol{\sigma}]$.*

Proof: The first paragraph of the proof of Lemma 1.3 gives a linearly disjoint sequence $K_1, K_2, K_3, \ldots$, of Galois extensions of K with Galois group $\mathbb{Z}/p\mathbb{Z}$. For each j let $\bar{\sigma}_j$ be a generator of $\mathcal{G}(K_j/K)$. By [FJ2, Lemma 16.11], for almost all $\boldsymbol{\sigma} \in G(K)^e$ there exists j such that $\mathrm{res}_{K_j}\sigma_1 = \bar{\sigma}_j$. For this j we have, $\mathcal{G}(K_j \cdot K_s[\boldsymbol{\sigma}]/K_s[\boldsymbol{\sigma}]) \cong \mathbb{Z}/p\mathbb{Z}$, as desired. ∎

We may now sum up and prove our main result:

Theorem 2.7: *Let K be a countable separably Hilbertian field. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $K_s[\boldsymbol{\sigma}]$ is PAC and ω-free. In particular $K_s[\boldsymbol{\sigma}]$ is separably*

Hilbertian.

Proof: By Lemma 1.2, Lemma 1.6, Lemma 2.5, and Lemma 2.6, almost all $\boldsymbol{\sigma} \in G(K)^e$ have these properties:

(1a) $K_s[\boldsymbol{\sigma}]$ is PAC.

(1b) $K_s[\boldsymbol{\sigma}]$ is a Galois extension of an ω-free field M.

(1c) For each finite nonabelian simple group S and each positive integer n, the group S^n occurs as a Galois group over $K_s[\boldsymbol{\sigma}]$.

(1d) For each prime p, the group $\mathbb{Z}/p\mathbb{Z}$ occurs as a Galois group over $K_s[\boldsymbol{\sigma}]$.

Since M is countable, $G(M) \cong \hat{F}_\omega$. Hence, by Lemma 2.1, $[\boldsymbol{\sigma}] = G(K_s[\boldsymbol{\sigma}]) \cong \hat{F}_\omega$. Finally recall that the Hilbertianity of $K_s[\boldsymbol{\sigma}]$ is a consequence of being PAC and ω-free [FJ2, Cor. 24.38]. ∎

3. Applications

A special case of Theorem 2.7 yields a group theoretic result*:

Corollary 3.1: *Consider the free profinite group $\hat{F}_\omega$ on countably many generators. Then, for almost all $\boldsymbol{\sigma} \in \hat{F}_\omega^e$ we have $[\boldsymbol{\sigma}] \cong \hat{F}_\omega$.*

Proof: Choose a PAC field K of characteristic 0 such that $G(K) \cong \hat{F}_\omega$. E.g., $K = \tilde{\mathbb{Q}}[\tau]$, where $\tau \in G(\mathbb{Q})$ is chosen at random (Theorem 2.7), or use [FJ2, Cor. 20.14 and Cor. 23.38]. By [FJ2, Cor. 24.38], K is Hilbertian. Now apply Theorem 2.7 to K.

Note however, that one may also start from Lemma 2.1 and replace the construction of special Galois extensions of K in the proof of Theorem 2.7 by a construction of special open normal subgroups of $\hat{F}_\omega$. This will give a group theoretical proof of the corollary. ∎

The following corollary to Theorem 2.7 seems peculiar. I wonder if it could be proved directly. Here we say that a group $\hat{G}$ **covers** a group G if there exists an epimorphism of $\hat{G}$ onto G.

Corollary 3.2: *Let K be a countable separably Hilbertian field. Then every finite group G has a finite cover $\hat{G}$ which can be embedded into a finite group H such that*

(a) *$\hat{G}$ is normally generated in H by one element,*

(b) *H occurs as a Galois group over K.*

Proof: Take $\sigma \in G(K)$ such that $K_s[\sigma]$ is ω-free (Theorem 2.7). In particular $K_s[\sigma]$ has a Galois extension M such that $\mathcal{G}(M/K_s[\sigma]) \cong G$. Let N be a finite Galois extension of K such that $\hat{M} = N \cdot K_s[\sigma] \supseteq M$. Then $\hat{G} = \mathcal{G}(\hat{M}/K_s[\sigma])$ is a finite cover of G. Moreover, $\hat{G} \cong \mathcal{G}(N/N \cap K_s[\sigma])$ is a subgroup of $H = \mathcal{G}(N/K)$ which is normally generated in H by $\mathrm{res}_N \sigma$. ∎

Remark 3.3: A group theoretic construction of H (Dan Haran). The existence of H as in Corollary 3.2, possibly without Condition (b), can be proved by a simple group theoretic argument:

* The author is indebted to Helmut Völklein for this observation.

Choose a positive integer e such that G is generated by e elements. Let N be the intersection of the kernels of all epimorphisms $\hat{F}_e \to G$. Since there are only finitely many of them, N is open. Hence $\hat{G} = \hat{F}_e/N$ is a finite cover of G. Let $g_1, \ldots, g_e$ be the images of generators of $\hat{F}_e$ in $\hat{G}$. Then, for each i between 1 and e, there exists an automorphism α of $\hat{G}$ such that $g_1^\alpha = g_i$. Thus $\hat{G}$ is normally generated by one element in the semidirect product $H = \hat{G} \rtimes \mathrm{Aut}(\hat{G})$.

Of course, as the inverse Galois problem has not yet been settled, we do not know whether H occurs as a Galois group over K. ∎

4. Decidability

We have already mentioned in Remark 2.10 that the absolute Galois groups of $K_s[\boldsymbol{\sigma}]$ and $\tilde{K}[\boldsymbol{\sigma}]$ are isomorphic. Hence, if $K_s[\boldsymbol{\sigma}]$ is a PAC ω-free field, then so is $\tilde{K}[\boldsymbol{\sigma}]$ [FJ2, Cor. 10.7]. This leads to decidability results of several families of ω-free PAC fields associated with these fields.

Fix a base field K. If K is finitely generated over its prime field (e.g., $K = \mathbb{Q}$ or $K = \mathbb{F}_p$) and is presented in the sense of [FJ2, Def. 17.1] we will speak about the **explicit case**. In a discussion of a sentence θ, this will also include the assumption that θ is explicitly given. Denote the first order language of rings with a constant symbol for each element of K by $\mathcal{L}(\mathrm{ring}, K)$. A richer language is the language of **Galois sentences** over K [FJ2, Sect. 25.4].

Let $\mathcal{N}(K)$ be the class of all perfect ω-free PAC fields M which contain K such that $K_s \cap M$ is a Galois extension of K. In particular, each M in $\mathcal{N}(K)$ is a Frobenius field [FJ2, Def. 23.1]. For each e let $\mathcal{N}_e(K)$ be the subclass of all $M \in \mathcal{N}(K)$ such that $G(K_s \cap M)$ is normally generated in $G(K)$ by e elements. We denote the set of all Galois sentences over K which are true in all $M \in \mathcal{N}(K)$ (resp., $M \in \mathcal{N}_e(K)$) by $\mathrm{Th}(\mathcal{N}(K))$ (resp., $\mathrm{Th}(\mathcal{N}_e(K))$). This set contains the elementary theory of $\mathcal{N}(K)$ (resp., $\mathcal{N}_e(K)$) in the language $\mathcal{L}(\mathrm{ring}, K)$.

The stratification procedure developed in [FJ2, Chap. 25] gives us a tool to establish various primitive recursive decidability results:

LEMMA 4.1: *Let θ be a Galois sentence. Then we can find (effectively, in the explicit case) a finite Galois extension L of K and a conjugacy domain* Con *of subgroups of $\mathcal{G}(L/K)$ such that if M is a perfect ω-free PAC field containing K, then $M \models \theta$ if and only if $\mathcal{G}(L/L \cap M) \in$* Con.

Proof: This is a special case of [FHJ, Thm. 3.8] in which the field M of that theorem is ω-free. See also the discussion on the bottom of [FJ2, p. 415]. ∎

THEOREM 4.2 (Decidability): *Let K be a countable separably Hilbertian field and let θ be a Galois sentence over K.*

(a) *Let e be a positive integer. Then the set $S_e(\theta)$ of all $\boldsymbol{\sigma} \in G(K)^e$ such that θ is* *true in* $\tilde{K}[\boldsymbol{\sigma}]$ *has a rational measure, which in the explicit case can be effectively computed.*

(b) *The sentence* θ *belongs to* $\mathrm{Th}(\mathcal{N}_e(K))$ *if and only if it is true in* $\tilde{K}[\boldsymbol{\sigma}]$ *for almost all* $\boldsymbol{\sigma} \in G(K)^e$.

(c) *In the explicit case,* $\mathrm{Th}(\mathcal{N}_e(K))$ *is a primitive recursive theory.*

(d) *The sentence* θ *belongs to* $\mathrm{Th}(\mathcal{N}(K))$ *if and only if* θ *is true in all perfect* ω*-free PAC fields which are normal over* K.

(e) θ *belongs to* $\mathrm{Th}(\mathcal{N}(K))$ *if and only if there exists a positive integer* e_0 *such that* $\theta \in \mathrm{Th}(\mathcal{N}_e(K))$ *for all* $e \geq e_0$. *In the explicit case, it is possible to compute* e_0 *effectively.*

(f) *In the explicit case,* $\mathrm{Th}(\mathcal{N}(K))$ *is a primitive recursive theory.*

Proof: Let P_e be the set of all $\boldsymbol{\sigma} \in G(K)^e$ such that $\tilde{K}[\boldsymbol{\sigma}]$ is an ω-free PAC field. By Theorem 2.7, $\mu(P_e) = 1$. Let L and Con be as in Lemma 4.1.

Proof of (a): Consider the set $\bar{S}_e(\theta)$ of all $\boldsymbol{\sigma}_0 \in \mathcal{G}(L/K)^e$ such that $[\boldsymbol{\sigma}_0] \in \mathrm{Con}$. Let $\boldsymbol{\sigma} \in P_e$. By Lemma 4.1, $\boldsymbol{\sigma}$ belongs to $S_e(\theta)$ if and only if $\mathrm{res}_L\boldsymbol{\sigma} \in \bar{S}_e(\theta)$. Hence, $\mu(S_e(\theta)) = |\bar{S}_e(\theta)|/[L:K]^e$.

In the explicit case one can effectively compute $|\bar{S}_e(\theta)|$ and therefore also $\mu(S_e(\theta))$.

Proof of (b): Suppose that θ is true in all $M \in \mathcal{N}_e(K)$. By Theorem 2.7, θ is true in $\tilde{K}[\boldsymbol{\sigma}]$ for almost all $\boldsymbol{\sigma} \in G(K)^e$.

Conversely, suppose that θ is true in $\tilde{K}[\boldsymbol{\sigma}]$ for almost all $\boldsymbol{\sigma} \in G(K)^e$. By the proof of (a), $\bar{S}_e(\theta) = \mathcal{G}(L/K)^e$. If $M \in \mathcal{N}_e(K)$, then $L \cap M = L[\boldsymbol{\sigma}_0]$ for some $\boldsymbol{\sigma}_0 \in \mathcal{G}(L/K)^e$. Hence $\mathcal{G}(L/L \cap M) \in \mathrm{Con}$ and therefore, by Lemma 4.1, θ is true in M.

Proof of (c): Combine (a) and (b).

Proof of (d): Suppose that θ is true in each perfect ω-free PAC field which is normal over K. Let $M \in \mathcal{N}(K)$. Choose generators $\sigma_{01}, \ldots, \sigma_{0e}$ for the normal subgroup $\mathcal{G}(L/L \cap M)$ of $\mathcal{G}(L/K)$. By Theorem 2.7, we can lift $\boldsymbol{\sigma}_0$ to $\boldsymbol{\sigma} \in G(K)^e$ such that $\tilde{K}[\boldsymbol{\sigma}]$ is ω-free PAC field. In particular $L \cap \tilde{K}[\boldsymbol{\sigma}] = L[\boldsymbol{\sigma}_0] = L \cap M$. By Lemma 4.1, $\mathcal{G}(L/L \cap M) \in \mathrm{Con}$. Hence, again by Lemma 4.1, θ is true in M.

Proof of (e): A possible value for e_0 is the maximum of the minimal number of normal generators of A, where A ranges over all normal subgroups of $\mathcal{G}(L/K)$. In the explicit case, this number can be effectively calculated.

Proof of (f): $\theta \in \mathrm{Th}(\mathcal{N}(K))$ if and only if each normal subgroup of $\mathcal{G}(L/K)$ belongs to Con. ∎

References

[FHJ] M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields,* Advances of Mathematics, **51** (1984), 1–35.

[FJ1] M. Fried and M. Jarden, *Stable extensions with the global density property,* Canadian Journal of Mathematics **28** (1976), 774–787.

[FJ2] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[FV1] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces,* Mathemtische Annalen **290** (1991), 771–800.

[FV2] M. D. Fried and H. Völklein, The embedding problem over a Hilbertian PAC-field, Annals of Mathematics **135** (1992), 469–481.

[GeJ] W.-D. Geyer and M. Jarden, *On stable fields in positive characteristic,* geometria dedicata **29** (1989), 335–375.

[Ha1] D. Harbater, *Galois coverings of the arithmetic line,* in Number Theory — New York 1984–85, ed. by D.V. and G.V Chudnovsky, Lecture Notes in Mathematics **1240**, Springer, Berlin, 1987, pp. 165–195.

[Ha2] D. Harbater, *Mock covers and Galois extensions,* Journal of Algebra **91** (1984), 281–293.

[HaV] D. Haran and H. Völklein, *Galois groups over complete valued fields,* Israel Journal of Mathematics **93** (1996), 9–27.

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

[Jar] M. Jarden, *The inverse Galois problem over formal power series fields,* Israel Journal of Mathemtics **85** (1994), 263–275.

[Lan] S. Lang, *Algebra,* Addison-Wesley, Reading, 1970.

[Liu] Q. Liu, *Tout groupe fini est un groupe de Galois sur* $\mathbb{Q}_p(T)$, Contemporary Mathematics **186** (1995), 261–265.

[Mel] O. V. Melnikov, *Normal subgroups of free profinite groups,* Math. USSR Izvestija **12** (1978), 1–20.

[Neu] K. Neumann, *Israel Journal of Mathematics,*

[Pop] F. Pop, *Hilbertian fields with a universal local global principle,* preprint, Heidelberg, 1993.