ON THE NORMALIZER OF FINITELY GENERATED SUBGROUPS OF ABSOLUTE GALOIS GROUPS OF UNCOUNTABLE HILBERTIAN FIELDS OF CHARACTERISTIC 0

by

Wulf-Dieter Geyer and Moshe Jarden[1)]
Universität Erlangen — Tel Aviv University

1) This work was partially supported by an NSF grant #DMS–H603187, while the second author enjoyed the hospitality of Rutgers University.

Introduction

Our topic in this paper is the group-theoretic behavior of elements of the absolute Galois group of a Hilbertian field which are chosen at random. We continue the study that has been initiated in [J] and extended by Chatzidakis [C]. Indeed our main results can be viewed as completing those of [C].

We denote the absolute Galois group of a field K by $G(K)$. Equip $G(K)$ with the normalized Haar measure μ. For each positive integer e use μ also for the Haar measure of $G(K)^e$. Abbreviate an e-tuple $(\sigma_1, \ldots, \sigma_e)$ of elements of $G(K)$ by $\boldsymbol{\sigma}$ and let $\langle\boldsymbol{\sigma}\rangle$ be the closed subgroup of $G(K)$ generated by $\sigma_1, \ldots, \sigma_e$. Denote the fixed field of $\boldsymbol{\sigma}$ in the algebraic closure $\widetilde{K}$ of K by $\widetilde{K}(\boldsymbol{\sigma})$. Let $\widehat{F}_e$ be the free profinite group on e generators.

Theorem A (The free generators theorem [FJ, Thm. 16.13]): *Let K be a Hilbertian field. Then $\langle\boldsymbol{\sigma}\rangle \cong \widehat{F}_e$ for almost all $\boldsymbol{\sigma} \in G(K)^e$.*

Consider the centralizer $\mathrm{C}_{G(K)}\langle\boldsymbol{\sigma}\rangle$ and the normalizer $\mathrm{N}_{G(K)}\langle\boldsymbol{\sigma}\rangle$ of $\langle\boldsymbol{\sigma}\rangle$ in $G(K)$. Our main objects of investigation are the following subsets of $G(K)^e$:

$$\mathrm{C}_1(K) = \{\sigma \in G(K) \,|\, \mathrm{C}_{G(K)}\langle\sigma\rangle = \langle\sigma\rangle\}$$
$$\mathrm{C}_e(K) = \{\boldsymbol{\sigma} \in G(K)^e \,|\, \mathrm{C}_{G(K)}\langle\boldsymbol{\sigma}\rangle = 1\}, \qquad e \geq 2, \quad \textit{and}$$
$$\mathrm{N}_e(K) = \{\boldsymbol{\sigma} \in G(K)^e \,|\, \mathrm{N}_{G(K)}\langle\boldsymbol{\sigma}\rangle = \langle\boldsymbol{\sigma}\rangle\}, \qquad e \geq 1.$$

For Hilbertian fields there is a simple connection between $\mathrm{C}_e(K)$ and $\mathrm{N}_e(K)$.

Lemma B: *If K is a Hilbertian field, then for each $e \geq 1$, $\mathrm{N}_e(K)$ is contained in $\mathrm{C}_e(K)$ up to a set of measure 0.*

Proof: Consider $\boldsymbol{\sigma} \in G(K)^e$ such that $\langle\boldsymbol{\sigma}\rangle \cong \widehat{F}_e$. It is well known that the center of $\widehat{F}_e$ coincides with $\widehat{F}_e$ if $e = 1$ but is trivial if $e \geq 2$ [FJ, Cor. 24.8]. Hence if $\boldsymbol{\sigma} \in \mathrm{N}_e(K)$ and $\langle\boldsymbol{\sigma}\rangle \cong \widehat{F}_e$, then $\boldsymbol{\sigma} \in \mathrm{C}_e(K)$. Indeed, if $\tau^{-1}\boldsymbol{\sigma}\tau = \boldsymbol{\sigma}$, then $\tau \in \langle\boldsymbol{\sigma}\rangle$. So τ belongs to the center of $\langle\boldsymbol{\sigma}\rangle$ which coincides with $\langle\boldsymbol{\sigma}\rangle$ for $e = 1$ and is trivial if $e \geq 2$. Thus Lemma B is a consequence of Theorem A. ∎

The first result about $\mathrm{C}_e(K)$ (Theorem D) is valid for each K involved in Theorem C.

Theorem C: *If $K = \mathbb{Q}$ or $K = N(t)$, with N a real closed or algebraically closed field and t transcendental over N, then every closed abelian subgroup of $G(K)$ is procyclic.*

Proof: See [G, Thm. 2.3] or [R, p. 306] for the case $K = \mathbb{Q}$ and Lemma 5.1 for $K = N(t)$. ∎

Theorem D ([J, Thm. 14.1]): *Let K be a Hilbertian field. Suppose that every abelian closed subgroup of $G(K)$ is procyclic. Then $\mu(\mathrm{C}_e(K)) = 1$.*

Chatzidakis has proved a stronger theorem:

Theorem E (Chatzidakis [C, Thm. 2.2] or [FJ, 24.53]): *If K is a countable Hilbertian field, then $\mu(\mathrm{N}_e(K)) = 1$. Therefore, by Lemma B, $\mu(\mathrm{C}_e(K)) = 1$.*

It turns out that further generalization of Theorem E depends upon the roots of unity which are contained in K. We denote the extension of a field F generated by all roots of unity by F_{cyc}.

Theorem F: *Let K be a Hilbertian field with prime field F. If $F_{\mathrm{cyc}} \cap K$ is a finite extension of F, then $\mu(\mathrm{C}_e(K)) = 1$.*

Theorem G (Main result): *Let K_0 be a field of characteristic 0 that contains all roots of unity. Take a set T of cardinality $\aleph_1$, algebraically independent over K_0 and let $K = K_0(T)$. Then neither $\mathrm{N}_e(K)$ nor $\mathrm{C}_e(K)$ nor their complements in $G(K)^e$ contain a set of positive measure. In particular neither $\mathrm{N}_e(K)$ nor $\mathrm{C}_e(K)$ is a measurable set.*

Since K is Hilbertian this result shows that one cannot remove the hypotheses of countability from Theorem E.

In the last section we complete Theorem C:

Theorem H: *Let K be a finitely generated extension of $\mathbb{Q}$ of transcendence degree n.*

(a) *The rank of each closed abelian subgroup of $G(K)$ is at most $n+1$.*

(b) *$\hat{\mathbb{Z}}^{n+1}$ is isomorphic to a closed subgroup of $G(K)$.*

Our results for the measure of the sets $\mathrm{N}_e(K)$ and $\mathrm{C}_e(K)$ over uncountable Hilbertian fields are incomplete in two ways: we deal entirely with purely transcendental extensions, and only in characteristic 0.

1. Fields with only finitely many roots of unity.

A rather simple observation about fields with absolute Galois group isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ leads in this section to the proof of Theorem F. For a positive integer n we denote the n-th root of unity by ζ_n.

Lemma 1.1 ([L2, p. 221]): *Let K be a field and let n be an integer ≥ 2. Assume for $a \in K$, $a \neq 0$ that $a \notin K^p$ for each prime divisor p of n and that if $4|n$, then $a \notin -4K^4$. Then $X^n - a$ is irreducible in $K[X]$.*

Lemma 1.2: *Let K be a field with $G(K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Then $\mathrm{char}(K) \neq p$ and $\zeta_{p^i} \in K$ for every positive integer i.*

Proof: Note first that $\mathrm{char}(K) \neq p$, since otherwise $G(K)$, as a pro-p group, would be projective and therefore free [R, p. 257] (a theorem of Witt). Every finite extension of K is an abelian p-group. Since $[K(\zeta_p) : K]$ divides $p-1$, we have $\zeta_p \in K$.

Assume for $i \geq 2$ that $\zeta_{p^{i-1}} \in K$ but $\zeta_{p^i} \notin K$. Hence $[K(\zeta_{p^i}) : K] = p$ (Lemma 1.1). Since $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is a quotient of $\mathbb{Z}_p \times \mathbb{Z}_p$ there exists a cyclic extension $K(a^{1/p})$ of K, with $a \in K$, of degree p such that $K(\zeta_{p^i}) \cap K(a^{1/p}) = K$. In particular a is not a p-th power in $K(\zeta_{p^i})$. If $p = 2$ and $a \in -4K(\zeta_{2^i})^4$, then $\sqrt{a} \in \sqrt{-1}K(\zeta_{2^i})^2 \subseteq K(\zeta_{2^i})$, a contradiction. Conclude from Lemma 1.1 that $K(a^{1/p^i})$ is an abelian extension of K of degree p^i which is linearly disjoint from $K(\zeta_{p^i})$. In particular $K(a^{1/p^i})$ contains $\zeta_{p^i} a^{1/p^i}$ and therefore also ζ_{p^i}. This contradiction proves that $\zeta_{p^i} \in K$, as asserted. ∎

Consider now a Hilbertian field K such that

(1) each of the fields $K(\sqrt{-1})$ and $K(\zeta_p)$, p a prime and $p \neq \mathrm{char}(K)$, contains only finitely many roots of unity.

For example, if $\mathbb{Q}_{\mathrm{cyc}} \cap K$ is a finite extension of $\mathbb{Q}$, then K satisfies (1). Theorem F is therefore a consequence of Propositions 1.3 and 1.4 below.

Proposition 1.3: *Let K be a Hilbertian field that satisfies (1). Then $\mu(\mathrm{C}_1(K)) = 1$.*

Proof: For a prime $p \neq \mathrm{char}(K)$ let $K_{p^\infty} = K(\zeta_{p^i} \mid i = 1, 2, 3, \ldots)$. Also, let $\xi_p = \zeta_p$ for $p \neq 2$ and $\xi_2 = \zeta_4$. By assumption, there exists a positive integer m such that

$\zeta_{p^m} \in K(\xi_p)$ but $\zeta_{p^{m+1}} \notin K(\xi_p)$. By Lemma 1.1, $\zeta_{p^{m+i}}$ generates a cyclic extension of $K(\xi_p)$ of degree p^i, $i = 1, 2, 3, \ldots$. Hence $\mathcal{G}(K_{p^\infty}/K(\xi_p)) \cong \mathbb{Z}_p$.

The action of $\mathcal{G}(K_{p^\infty}/K)$ on the set $\{\zeta_{p^i} | \ i = 1, 2, 3, \ldots\}$ defines an embedding of $\mathcal{G}(K_{p^\infty}/K)$ into $\mathbb{Z}_p^\times$. Recall that $\mathbb{Z}_p^\times \cong A \oplus \mathbb{Z}_p$, where $A = \mathbb{Z}/(p-1)\mathbb{Z}$ if $p \neq 2$ and $A = \mathbb{Z}/2\mathbb{Z}$ if $p = 2$. Therefore $\mathcal{G}(K_{p^\infty}/K)$, being an infinite subgroup of $\mathbb{Z}_p^\times$, is isomorphic to a group $A_1 \oplus \mathbb{Z}_p$ with $A_1 \leq A$ (For $p = 2$ use that $\mathbb{Z}_p$ is a principal ideal domain and [L2, p. 393].) If K_p is the fixed field of the subgroup A_1 of $\mathcal{G}(K_{p^\infty}/K)$, then $\mathcal{G}(K_p/K) \cong \mathbb{Z}_p$.

As K_p/K is an infinite extension the subset $S_1 = \bigcup_{p \neq \mathrm{char}(K)} G(K_p)$ of $G(K)$ is of measure 0. By Theorem A, the set T_2 of all $\sigma \in G(K)$ such that $\langle \sigma \rangle \cong \hat{\mathbb{Z}}$ is of measure 1. By the bottom theorem [FJ, p. 216], the set T_3 of all $\sigma \in G(K)$ for which $\widetilde{K}(\sigma)$ is a proper finite extension of no proper field that contains K is of measure 0. It therefore suffices to prove that if

$$\sigma \in (G(K) - S_1) \cap T_2 \cap T_3,$$

then σ commutes with no element of $G(K) - \langle \sigma \rangle$.

Assume that there exists $\tau \in G(K) - \langle \sigma \rangle$ such that $\sigma\tau = \tau\sigma$. Then there is a prime p that divides $[\widetilde{K}(\sigma) : \widetilde{K}(\sigma, \tau)]$. Let a be the element of $\hat{\mathbb{Z}}$ with pth coordinate $a_p = 1$ and lth coordinate $a_l = 0$ for each prime $l \neq p$. Then, since $\sigma \in T_3$, the degree $[\widetilde{K}(\sigma) : \widetilde{K}(\sigma, \tau^a)]$ is an infinite power of p. As $\widetilde{K}(\sigma)/\widetilde{K}(\sigma, \tau^a)$ is an abelian extension with Galois group generated by one element, that group is isomorphic to $\mathbb{Z}_p$. It follows that $\mathcal{G}(\widetilde{K}(\tau^a)\widetilde{K}(\sigma)/\widetilde{K}(\tau^a)) \cong \mathbb{Z}_p$. By the choice of a, $G(\widetilde{K}(\tau^a))$ is a quotient of $\mathbb{Z}_p$. As each endomorphism of $\mathbb{Z}_p$ is an automorphism [FJ, Prop. 15.3], $\widetilde{K}(\tau^a)\widetilde{K}(\sigma) = \widetilde{K}$ and

$$G(\widetilde{K}(\sigma, \tau^a)) \cong G(\widetilde{K}(\tau^a)) \times G(\widetilde{K}(\sigma)) \cong \mathbb{Z}_p \times \hat{\mathbb{Z}}.$$

Conclude that $G(\widetilde{K}(\sigma^a, \tau^a)) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

By Lemma 1.2, $p \neq \mathrm{char}(K)$ and $\widetilde{K}(\sigma^a, \tau^a)$ contains ζ_{p^i} for every positive integer i. Hence also $\widetilde{K}(\sigma^a)$ contains ζ_{p^i} for all i and therefore $K_p \subseteq \widetilde{K}(\sigma^a)$. However the degree $[K_p\widetilde{K}(\sigma) : \widetilde{K}(\sigma)]$ as a divisor of $[\widetilde{K}(\sigma^a) : \widetilde{K}(\sigma)]$ is on one hand relatively prime to p, and as a divisor of $[K_p : K]$ is on the other hand a p-th power. It follows that

$K_p\widetilde{K}(\sigma) = \widetilde{K}(\sigma)$ and therefore that $K_p \subseteq \widetilde{K}(\sigma)$. This contradiction to $\sigma \notin S_1$ completes the proof of the Proposition. ∎

Note that the assumption "K contains only finitely many roots of unity" does not imply (1). Indeed the theory of cyclotomic extensions asserts that $\mathcal{G}(\mathbb{Q}_{p^\infty}/\mathbb{Q}) \cong A \oplus \mathbb{Z}_p$, where $A = \mathbb{Z}/(p-1)\mathbb{Z}$ if $p \neq 2$ and $A = \mathbb{Z}/2\mathbb{Z}$ if $p = 2$. Let K be the fixed field of A in $\mathbb{Q}_{p^\infty}$. As $\mathcal{G}(\mathbb{Q}_{p^\infty}/\mathbb{Q}(\xi_p)) \cong \mathbb{Z}_p$ the field $\mathbb{Q}(\xi_p)$ is not contained in K. Moreover, since $[\mathbb{Q}(\xi_p) : Q] = |A|$ we have $K(\xi_p) = \mathbb{Q}_{p^\infty}$. So, $K(\xi_p)$ contains infinitely many roots of unity.

On the other hand the only roots of unity in $\mathbb{Q}_{p^\infty}$ are the $\pm\zeta_{p^i}$'s. The field K contains only finitely many of them, since otherwise it would contain them all and therefore would coincide with $\mathbb{Q}_{p^\infty}$, a contradiction. Finally note that since $\mathcal{G}(K/\mathbb{Q}) \cong \mathbb{Z}_p$ the field K is Hilbertian [FJ, Prop. 15.5].

PROPOSITION 1.4: *Let K be a Hilbertian field of that satisfies (1) and let $e \geq 2$. Then $\mu(\mathrm{C}_e(K)) = 1$.*

Proof: Let S be the set of all $\boldsymbol{\sigma} \in G(K)^e$ such that $\langle\sigma_1\rangle \cap \langle\sigma_2\rangle = 1$ and $C_{G(K)}\langle\sigma_i\rangle = \langle\sigma_i\rangle$, $i = 1, 2$. By [J, Thm. 5.1] (or as an easy consequence of Theorem A) and by Proposition 1.3 the set S has measure 1.

Let $\boldsymbol{\sigma} \in S$ and let $\tau \in C_{G(K)}(\langle\boldsymbol{\sigma}\rangle)$. Then τ commutes with both σ_1 and σ_2. Conclude that $\tau \in \langle\sigma_1\rangle \cap \langle\sigma_2\rangle = 1$. Thus $C_{G(K)}\langle\boldsymbol{\sigma}\rangle = \langle\boldsymbol{\sigma}\rangle$, as desired. ∎

2. Irreducible polynomials over rational function fields.

Hilbert's irreducibility theorem takes a strong form over rational function fields $K = K_0(t)$: Separable irreducible polynomials $f \in K[X,Y]$ in two variables remain irreducible, if one variable is substituted by $a + bt$ with $(a,b) \in K_0^2$ arbitrary, satisfying only one inequality $g(a,b) \neq 0$ [FJ, Thm. 12.9].

For the rest of this section we fix an infinite field K_0 and set $K = K_0(t)$. Define the **rank** of an infinite separable algebraic extension as the cardinality of the family of all finite subextensions.

LEMMA 2.1: *Consider a tower $K \subseteq L \subseteq M$ of separable algebraic extensions with L/K finite and $\mathrm{rank}(M/K) < |K_0|$. Let $f_1, \ldots, f_m$ be irreducible polynomials in $M[X_1,, \ldots, X_r, Y]$ separable in Y. Let $g_1, \ldots, g_n$ be irreducible polynomials in $L[X_1,, \ldots, X_r, Y]$, separable in Y, and let $0 \neq h \in M[X_1,, \ldots, X_r]$. Then there exists $\mathbf{x} \in K^r$ such that $f_i(\mathbf{x}, Y)$ is separable irreducible in $M[Y]$, $i = 1, \ldots, m$, $g_j(\mathbf{x}, Y)$ is separable irreducible in $L[Y]$, $j = 1, \ldots, n$ and $h(\mathbf{x}) \neq 0$.*

Proof: Do induction on r to assume that $r = 1$. Then follow the proof of [FJ, Lemma 16.32], using that a separable Hilbert subset of a finite separable extension of K contains a separable Hilbert subset of K. (The proof of this statement is a simple modification of the proof of [FJ, Cor. 11.7].) ∎

PROPOSITION 2.2: *Let M be a separable algebraic extension of K with $\mathrm{rank}(M/K) < |K_0|$. Consider a finite Galois extension L of K with $G = \mathcal{G}(L/K)$. Suppose that G acts on a finite abelian group A. Let $A \rtimes G$ be the corresponding semidirect product and let α: $A \rtimes G \to G$ be the projection map. Then there exists an epimorphism γ: $G(K) \to A \rtimes G$ such that $\alpha \circ \gamma = \mathrm{res}_L$ and the fixed field $\widehat{L}$ of $\mathrm{Ker}(\gamma)$ is linearly disjoint from M over $L_0 = M \cap L$.*

Proof: Let $\widehat{F}/E$ be a Galois extension such that $E = K(x_1, \ldots, x_r)$ with $x_1, \ldots, x_r$ algebraically independent over K and $\widehat{F}$ is a regular extension of L for which there is an isomorphism θ: $\mathcal{G}(\widehat{F}/E) \to A \rtimes G$ such that $\alpha \circ \theta = \mathrm{res}_L$ [FJ, Lemma 24.46]. For $\mathbf{x} = (x_1, \ldots, x_r)$ find rings $R = K[\mathbf{x}, g(\mathbf{x})^{-1}]$ with $0 \neq g(\mathbf{x}) \in K[\mathbf{x}]$ and $\widehat{R} = R[z]$ where $\widehat{F} = E(z)$ and the discriminant of z over E is a unit of R. Then $\widehat{R}/R$ is a **ring cover**.

In particular $\widehat{R}$ is the integral closure of R in $\widehat{F}$ [FJ, end of §5.2]. Let $f(\mathbf{x}, Z) = \mathrm{irr}(\mathrm{z}, \mathrm{E})$ and $h(\mathbf{x}, Z) = \mathrm{irr}(\mathrm{z}, \mathrm{L}(\mathbf{x}))$. Since $\widehat{F}/L$ is regular h is absolutely irreducible.

Now choose $\mathbf{a} \in K^n$ such that $g(\mathbf{a}) \neq 0$, $f(\mathbf{a}, Z)$ is irreducible over K and $h(\mathbf{a}, Z)$ is irreducible over ML (Lemma 2.1). The K-specialization $\mathbf{x} \to \mathbf{a}$ extends to an epimorphism φ of $\widehat{R}$ onto a Galois extension $\widehat{L} = K(\varphi(z))$ of K that contains L such that $\varphi(b) = b$ for each $b \in L$. Since $f(\mathbf{a}, Z)$ is irreducible over K it induces an isomorphism $\varphi^*\colon \mathcal{G}(\widehat{L}/K) \to \mathcal{G}(\widehat{F}/E)$ such that $\mathrm{res}_{\hat{F}/L} \circ \varphi^* = \mathrm{res}_{\hat{L}/L}$ [FJ, Lemma 5.5]. The map $\gamma = \theta \circ \varphi^* \circ \mathrm{res}_{\hat{L}}$ from $G(K)$ satisfies $\alpha \circ \gamma = \mathrm{res}_L$. Also $[\widehat{L} : L] = \deg(h(\mathbf{a}, Z)) = [M\widehat{L} : ML]$. Hence $\widehat{L}$ is linearly disjoint from M over L_0. ∎

3. $\mathrm{N}_e(K)$ is big.

In this Section we assume that K_0 is an uncountable field of characteristic 0 and let $K = K_0(t)$ be the field of rational functions in t over K_0. Our goal is to show that for each $e \geq 1$ the complement of $\mathrm{N}_e(K)$ contains no set of positive measure, i.e., $\mathrm{N}_e(K)$ is a "big" set. This will give one half of Theorem G. The proof is based on the following version of [FJ, Lemma 16.30].

LEMMA 3.1: *Let G be a profinite group and let S be a subset of G^e. Suppose that $\mu_H(r(S)) = 1$ for each epimorphism $r\colon G \to H$ onto a profinite group H of rank $\leq \aleph_0$. (Here we also use r to denote the function from G^e to H^e induced by $r\colon G \to H$.) Then $G^e - S$ contains no set of positive measure. In particular this holds if $r(S) = H^e$ for each H as above.*

Proof: Let $\overline{B}$ be a measurable subset of $G^e - S$. Then there exists a set B with $B \subseteq \overline{B}$ such that $\mu(\overline{B} - B) = 0$ which belongs to the σ-algebra generated by all open-closed subsets of G^e [FJ, Lemma 16.29]. An induction on structure shows that B can be found in a σ-algebra $\mathcal{A}$ generated by countably many open-closed sets, $A_1, A_2, A_3, \ldots$. For each i there is a normal open subgroup N_i of G and there is a finite subset T_i of G^e such that $A_i = \bigcup_{\boldsymbol{\tau} \in T_i} \boldsymbol{\tau} N_i^e$. The group $N = \bigcap_{i=1}^{\infty} N_i$ is normal and closed in G and $\mathrm{rank}(G/N) \leq \aleph_0$. Let $r\colon G \to G/N$ be the canonical epimorphism. Clearly

$r^{-1}(r(A_i)) = A_i,\ \ i = 1, 2, 3, \ldots$. Since the collection of all $A \in \mathcal{A}$ with $A = r^{-1}(r(A))$ is closed under taking complements and under countable unions it coincides with $\mathcal{A}$. In particular $r^{-1}(r(G^e - B)) = G^e - B$. Since $G^e - B \supseteq S$ we have $r(G^e - B) \supseteq r(S)$ and $\mu_H(r(G^e - B)) \geq \mu_H(r(S)) = 1$. Hence $\mu(G^e - B) = \mu_H(r(G^e - B)) = 1$. Conclude that $\mu(\overline{B}) = \mu(B) = 0$, as desired. ∎

Our first application of Lemma 3.1 depends upon the following corollary of Proposition 2.2.

LEMMA 3.2: *Let M be a Galois extension of K with* $\mathrm{rank}(M/K) \leq \aleph_0$ *and let* $\boldsymbol{\sigma} \in \mathcal{G}(M/K)^e$. *Then K has a Galois extension M' which contains M with* $\mathrm{rank}(\mathcal{G}(M'/K)) \leq \aleph_0$ *and there exists an extension* $\boldsymbol{\tau} \in \mathcal{G}(M'/K)^e$ *of* $\boldsymbol{\sigma}$ *such that* $\mathrm{N}_{\mathcal{G}(M'/K)}\langle\boldsymbol{\tau}\rangle = \langle\boldsymbol{\tau}\rangle$.

Proof: Present M as a union $M = \bigcup_{i=1}^{\infty} K_i$ of an ascending sequence $K_1 \subseteq K_2 \subseteq \cdots$ of finite Galois extensions of K. Let $\boldsymbol{\sigma}_i = \mathrm{res}_{K_i}(\boldsymbol{\sigma})$, $i = 1, 2, 3, \ldots$. Inductively construct an ascending sequence $L_1 \subseteq L_2 \subseteq \ldots$ of finite Galois extensions of K and e-tuples $\boldsymbol{\tau}_i \in \mathcal{G}(L_i/K)^e$, $i = 1, 2, 3, \ldots$ such that

(a) $M \cap L_i = K_i$ and $\mathrm{res}_{K_i}(\boldsymbol{\tau}_i) = \boldsymbol{\sigma}_i$,

(b) $\boldsymbol{\tau}_{i+1}$ extends $\boldsymbol{\tau}_i$, $i = 1, 2, 3, \ldots$, and

(c) $\mathrm{res}_{L_i}(N_{\mathcal{G}(L_{i+1}/K)}\langle\boldsymbol{\tau}_{i+1}\rangle) = \langle\boldsymbol{\tau}_i\rangle$.

Indeed suppose that we have already constructed L_i and $\boldsymbol{\tau}_i$ for $i = 1, \ldots, n$ such that they satisfy conditions (a)–(c). In particular for $G = \mathcal{G}(K_{n+1}L_n/K)$ there exists $\boldsymbol{\rho} \in G^e$ that extends both $\boldsymbol{\sigma}_{n+1}$ and $\boldsymbol{\tau}_n$, and $M \cap K_{n+1}L_n = K_{n+1}$. Choose an integer $m \geq 2$ and let G operate on the group ring $(\mathbb{Z}/m\mathbb{Z})[G]$ by multiplication from the right. By Proposition 2.2, K has a Galois extension L_{n+1} that contains $K_{n+1}L_n$ such that $M \cap L_{n+1} = K_{n+1}$ and there exists a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{G}(L_{n+1}/K_{n+1}L_n) & \longrightarrow & \mathcal{G}(L_{n+1}/K) & \longrightarrow & \mathcal{G}(K_{n+1}L_n/K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})[G] & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})[G] \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

in which the vertical arrows are isomorphisms. Lemma 24.52 of [FJ] states that $\boldsymbol{\rho}$ extends to $\boldsymbol{\tau}_{n+1} \in \mathcal{G}(L_{n+1}/K)$ such that $\mathrm{res}_{K_{n+1}L_n}(N_{\mathcal{G}(L_{n+1}/K)}\langle\boldsymbol{\tau}_{n+1}\rangle) = \langle\boldsymbol{\rho}\rangle$. (The close "$H$ into G_0" at the end of that lemma should be corrected to "H onto G_0".) In particular $\boldsymbol{\tau}_{n+1}$ extends both $\boldsymbol{\sigma}_{n+1}$ and $\boldsymbol{\tau}_n$, and $\mathrm{res}_{L_n}(N_{\mathcal{G}(L_{n+1}/K)}\langle\boldsymbol{\tau}_{n+1}\rangle) = \langle\boldsymbol{\tau}_n\rangle$. This completes the induction.

Let $M' = \bigcup_{i=1}^{\infty} L_i$ and let $\boldsymbol{\tau}$ be the unique element of $\mathcal{G}(M'/K)^e$ that extends all $\boldsymbol{\tau}_i$. Then M' is a Galois extension of K of rank $\leq \aleph_0$, $\boldsymbol{\tau}$ extends $\boldsymbol{\sigma}$ and $\mathrm{N}_{\mathcal{G}(M'/K)}\langle\boldsymbol{\tau}\rangle = \langle\boldsymbol{\tau}\rangle$. Indeed if $\kappa \in \mathrm{N}_{\mathcal{G}(M'/K)}\langle\boldsymbol{\tau}\rangle$, then $\mathrm{res}_{L_{n+1}}(\kappa) \in N_{\mathcal{G}(L_{n+1}/K)}\langle\boldsymbol{\tau}_{n+1}\rangle$. Hence $\mathrm{res}_{L_n}(\kappa) \in \langle\boldsymbol{\tau}_n\rangle$, $n = 1, 2, 3, \ldots$. Conclude that $\kappa \in \langle\boldsymbol{\tau}\rangle$. ∎

LEMMA 3.3: *Suppose that $|K_0| = \aleph_1$ and let L/K be a Galois extension of rank $\leq \aleph_0$. Then each $\boldsymbol{\sigma}_1 \in \mathcal{G}(L/K)^e$ extends to $\boldsymbol{\sigma} \in G(K)^e$ such that $\mathrm{N}_{G(K)}\langle\boldsymbol{\sigma}\rangle = \langle\boldsymbol{\sigma}\rangle$.*

Proof: Order the collection of all finite Galois extensions of K in a transfinite sequence $\{K_\alpha | \, 1 \leq \alpha < \aleph_1\}$. Apply Lemma 3.2 in a transfinite induction to define for each ordinal $\alpha < \aleph_1$ a Galois extension L_α and $\boldsymbol{\sigma}_\alpha \in \mathcal{G}(L_\alpha/K)^e$ such that (a) $L_1 = L$, (b) $\mathrm{rank}(L_\alpha/K) = \aleph_0$, (c) $\alpha < \beta$ implies that $K_\alpha \subseteq L_\beta$, $L_\alpha \subseteq L_\beta$ and $\boldsymbol{\sigma}_\beta$ extends $\boldsymbol{\sigma}_\alpha$, and (d) $N_{\mathcal{G}(L_\alpha/K)}\langle\boldsymbol{\sigma}_\alpha\rangle = \langle\boldsymbol{\sigma}_\alpha\rangle$,

Then $K_s = \bigcup_{\alpha<\aleph_1} L_\alpha$ and $\boldsymbol{\sigma} = \varprojlim \boldsymbol{\sigma}_\alpha$ extends $\boldsymbol{\sigma}_1$ and satisfies $\mathrm{N}_{G(K)}\langle\boldsymbol{\sigma}\rangle = \langle\boldsymbol{\sigma}\rangle$. ∎

PROPOSITION 3.4: *Let $K = K_0(t)$ be the field of rational functions in t over a field K_0 of cardinality $\aleph_1$. Then $G(K)^e - \mathrm{N}_e(K)$ and $G(K)^e - \mathrm{C}_e(K)$ contain no set of positive measure.*

Proof: By Lemma B it suffices to prove only the assertion about $\mathrm{N}_e(K)$.

Apply Lemma 3.1 on the set $S = \mathrm{N}_e(K)$. Consider a Galois extension L/K of rank $\leq \aleph_0$. By Lemma 3.3, $\mathrm{res}_L S = \mathcal{G}(L/K)^e$. Hence, $G^e - S$ contains no set of positive measure. ∎

4. $\mathrm{N}_e(K)$ **is small.**

We apply the technique of power series fields to complete the proof of Theorem G.

Let K be a field of characteristic 0. For a transcendental element t over K choose for each positive integer e an e-th root $t^{1/e}$ of t such that whenever d divides e, $(t^{1/e})^{e/d} = t^{1/d}$. Puiseux's theorem states that the algebraic closure of the field of power series $\widetilde{K}((t))$ is the union of all fields $E_e = \widetilde{K}((t^{1/e}))$. In order to obtain the algebraic closure of the complete discrete valued field $E = K((t))$ we have to distinguish between unramified and purely ramified extensions. First note that each algebraic extension L of E is Henselian with residue field of characteristic 0. Therefore, if L' is a finite extension of L, then $[L' : L]$ is equal to the product of the ramification index and the residue degree [A, Prop. 15]. Now observe that $E_{\mathrm{ur}} = \widetilde{K}E$, as a separable constant field extension of E, is unramified with an algebraically closed residue field $\widetilde{K}$. Hence, each algebraic extension of E_{ur} is purely unramified. On the other hand, $F = \bigcup_{e=1}^{\infty} E(t^{1/e})$ is a purely ramified extension of E with a divisible value group, $\mathbb{Q}$. Hence, each algebraic extension of F is unramified. It follows that $E_{\mathrm{ur}} \cap F = E$ and $E_{\mathrm{ur}}F = \widetilde{E}$. For each e the field $E_{\mathrm{ur}}(t^{1/e})$ is a cyclic extension of E of degree e. Therefore $G(E_{\mathrm{ur}}) = \hat{\mathbb{Z}}$. As K is algebraically closed in E and therefore also in F this yields a presentation of $G(E)$ as a semidirect product of $G(K)$ and $\hat{\mathbb{Z}}$.

PROPOSITION 4.1: *Let K be a field of characteristic 0 and let $E = K((t))$.*

(a) *The field $E_{\mathrm{ur}} = \widetilde{K}E$ is the maximal unramified extension of E.*

(b) *The field $F = \bigcup_{e=1}^{\infty} E(t^{1/e})$ is a totally unramified extension of E,* $\mathrm{ord}(F^\times) = \mathbb{Q}$, *each algebraic extension of F is unramified, and K is algebraically closed in F.*

(c) *$E_{\mathrm{ur}} \cap F = E$ and $E_{\mathrm{ur}}F = \widetilde{E}$.*

(d) *$G(E_{\mathrm{ur}}) = \hat{\mathbb{Z}}$ and $G(F) \cong G(K)$.*

(e) *$G(E)$ is the semidirect product of $G(K)$ and $\hat{\mathbb{Z}}$.*

COROLLARY 4.2: *Let K be a field of characteristic 0 that contains all roots of unity.*

(a) *$G(K((t))) \cong G(K) \times \hat{\mathbb{Z}}$.*

(b) *There exists an isomorphism $\alpha\colon G(K) \times \hat{\mathbb{Z}} \to G(\widetilde{K(t)} \cap K((t)))$ such that $\mathrm{res}_{\widetilde{K}} \circ \alpha$ is the projection map of $G(K) \times \hat{\mathbb{Z}}$ onto $G(K)$.*

Proof: In this case F, of Proposition 4.1, is a Galois extension of E. ∎

PROPOSITION 4.3: *Let T be an uncountable set, algebraically independent over a field of characteristic 0 that contains all roots of unity. Let $K = K_0(T)$. Then $\mathrm{C}_e(K)$ and $\mathrm{N}_e(K)$ contains no set of positive measure.*

Proof: By Lemma B it suffices to prove that $\mathrm{C}_e(K)$ contains no set of positive measure. We apply Lemma 3.1 on $S = G(K)^e - \mathrm{C}_e(K)$ and consider an epimorphism $r\colon G(K) \to H$ onto a profinite group H of rank $\le \aleph_0$. Denote the fixed field of $\mathrm{Ker}(r)$ by L. Then L/K is a Galois extension of rank $\le \aleph_0$. Hence T has a countable subset T_1 for which there exists a Galois extension L_1 of $K_1 = K_0(T_1)$ such that $L_1K = L$. Choose $t \in T - T_1$ and let $K_2 = K_0(T - \{t\})$ and $L_2 = L_1K_2$. Then $K = K_2(t)$. Assume without loss that r is the epimorphism $\mathrm{res}_{L_2}\colon G(K) \to \mathcal{G}(L_2/K_2)$.

By Corollary 4.2(b) each $\boldsymbol{\sigma} \in \mathcal{G}(L_2/K_2)^e$ extends to $\boldsymbol{\tau} \in G(K)^e$ for which there exists $\rho \in G(K) - \langle\boldsymbol{\tau}\rangle$ such that $\tau_i\rho = \rho\tau_i$, $i = 1, \ldots, e$. Thus $\rho \in \mathrm{C}_{G(K)}\langle\boldsymbol{\tau}\rangle - \langle\boldsymbol{\tau}\rangle$. Therefore $\boldsymbol{\tau} \in S$.

Conclude from Lemma 3.1 that $\mathrm{C}_e(K)$ contains no set of positive measure. ∎

Combine now Propositions 3.4 and 4.3 to achieve the main result of this work.

THEOREM 4.4: *Let K_0 be a field of characteristic 0 that contains all roots of unity. Take a set T of cardinality $\aleph_1$, algebraically independent over K_0 and let $K = K_0(T)$. Then neither $\mathrm{N}_e(K)$ nor $\mathrm{C}_e(K)$ nor their complements in $G(K)^e$ contain a set of positive measure. In particular neither $\mathrm{N}_e(K)$ nor $\mathrm{C}_e(K)$ is a measurable set.*

5. Abelian subgroups of $G(K)$.

We give in this section some details about the possible ranks of closed abelian subgroups of absolute Galois groups of finitely generated extensions of $\mathbb{Q}$. First we prove the second part of Theorem C.

LEMMA 5.1: *Let N be either an algebraically closed or a real closed field. Let x be transcendental over N. Then every abelian closed subgroup C of $G(N(x))$ is procyclic.*

Proof: Suppose first that N is algebraically closed. As the cohomological dimension of $G(N)$ is 0, the cohomological dimension of $G(N(x))$ is 1 [R, p. 276]. In other words $G(N(x))$ is projective (Actually $G(N(x))$ is free. But this is a deeper theorem.) It follows that C is projective [FJ, Cor. 20.16]. Hence, for each p, the p-Sylow subgroup C_p of C is pro-p-free [FJ, Prop. 20.47]. Since C_p is abelian it must be procyclic. Conclude that C is also procyclic.

Now assume that N is real closed. If C is not procyclic, it contains a closed subgroup B isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, for some prime p [G, Satz 1.13]. By Lemma 1.2, the fixed field of B contains $\sqrt{-1}$ and therefore also $\widetilde{N}$. This contradicts the first part of the Lemma. ∎

PROPOSITION 5.2: *For almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$ each closed abelian subgroup C of $G(\tilde{\mathbb{Q}}(\boldsymbol{\sigma})(x))$, with x transcendental over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, is procyclic.*

Proof: Each of the extensions $\mathbb{Q}_{p^\infty} = \mathbb{Q}(\zeta_{p^i} \,|\, i = 1, 2, 3, \ldots)$ is infinite. Hence $\mu(\bigcup G(\mathbb{Q}_{p^\infty}^e)) = 0$. Let $\boldsymbol{\sigma} \in G^e - G(\mathbb{Q}_{p^\infty})^e$ and let $F = \tilde{\mathbb{Q}}(\boldsymbol{\sigma})(x)$. Assume that C is a closed abelian nonprocyclic subgroup of $G(F)$. As in the second paragraph of the proof of Lemma 5.1, F and therefore $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ contain ζ_{p^i}, $i = 1, 2, 3, \ldots$ for some prime p. Thus $\boldsymbol{\sigma} \in G(\mathbb{Q}_{p^\infty})^e$, a contradiction. ∎

PROPOSITION 5.3 (Haran): *Let K be an extension of $\mathbb{Q}$ of transcendence degree n. Then the rank of each closed abelian subgroup of $G(K)$ is bounded by $n+1$.*

Proof: If $n = 0$, then K is an algebraic extension of $\mathbb{Q}$, and Theorem C applies.

For $n > 0$ we may assume without loss that $K = K_0(x)$ for some extension K_0 of $\mathbb{Q}$ of transcendence degree $n-1$ and a transcendental element x over K_0. Let B

be a closed abelian closure of $G(K)$. The short exact sequence $1 \longrightarrow G(\widetilde{K}_0(x)) \longrightarrow G(K) \xrightarrow{\mathrm{res}} G(K_0) \longrightarrow 1$ induces a short exact sequence of abelian profinite groups $1 \longrightarrow C \longrightarrow B \longrightarrow A \longrightarrow 1$. The group A is contained in $G(K_0)$. By an induction hypothesis on n, $\mathrm{rank}(A) \le n$. Lemma 5.1 asserts that C, as an abelian closed subgroup of $G(\widetilde{K}_0)$ is procyclic. Hence $\mathrm{rank}(B) \le n+1$. This completes the induction and the proof of the proposition. ∎

Now we show that the bound in Proposition 5.3 can not be improved.

PROPOSITION 5.4: *Let K be a finitely generated extension of $\mathbb{Q}$ of transcendence degree n. Then $\hat{\mathbb{Z}}^{n+1}$ is isomorphic to a closed subgroup of $G(K)$.*

Proof: The field $L = \mathbb{Q}_{\mathrm{ab}}K$ is finitely generated over $\mathbb{Q}_{\mathrm{ab}}$ and of transcendence degree n. We prove by induction on n that $\hat{\mathbb{Z}}^{n+1}$ is even isomorphic to a closed subgroup of $G(L)$.

Indeed for $n = 0$, $L = \mathbb{Q}_{\mathrm{ab}}$ is Hilbertian [FJ, Thm. 15.6]. Hence, by Theorem A, almost each $\sigma \in G(L)$ generates a subgroup isomorphic to $\hat{\mathbb{Z}}$. For $n > 0$ choose a transcendental basis $t_1, \ldots, t_n$ for $L/\mathbb{Q}_{\mathrm{ab}}$ and let $E_0 = \mathbb{Q}_{\mathrm{ab}}(t_1, \ldots, t_{n-1})$ and $E = E_0(t_n)$. By the induction hypothesis $\hat{\mathbb{Z}}^n$ is isomorphic to a closed subgroup of $G(E_0)$. Since E contains all roots of unity Corollary 4.4(b) implies that $\hat{\mathbb{Z}}^{n+1}$ is isomorphic to a closed subgroup of $G(E)$. As $G(L) \cap A$ is an open subgroup of A it is also isomorphic to $\hat{\mathbb{Z}}^{n+1}$. The induction is complete. ∎

References

[A] J. Ax, *A mathematical approach to some problems in number theory,* AMS Proc. Symp. Pure Math. **XX** (1971), 161-190.

[C] Z. Chatzidakis, *Some properties of the absolute Galois group of a Hilbertian field,* Israel Journal of Mathematics **55** (1986), 173–183.

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

[G] W.-D. Geyer, *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist,* Journal of Number Theory **1** (1969), 346-374.

[J] M. Jarden, *Algebraic extensions of finite corank of Hilbertian fields,* Israel Journal of Mathematics **18** (1974), 279-307.

[Ja] G.J. Janusz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[L1] S. Lang, *Algebraic Number Theory,* Addison-Wesely, Reading, 1970.

[L2] S. Lang, *Algebra,* Addison-Wesely, Reading, 1965.

[Le] S. Lefschetz, *Algebraic Geometry,* Princeton University Press, Princeton, 1953.

[R] L. Ribes, *Introduction to pro-finite groups and Galois cohomology,* Queens papers in pure and applied Mathematics **24**, Queens's University, Kingston, 1970.

Addresses of the authors:

Wulf-Dieter Geyer
Mathematisches Institut
der Universität
Bismarckstr. $1\frac{1}{2}$
D-8520 Erlangen
WEST GERMANY

Moshe Jarden
School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL