ISRAEL JOURNAL OF MATHEMATICS **214** (2016), 193–207
DOI: 10.1007/s11856-016-1356-z

FIELDS WITH ALMOST SMALL ABSOLUTE GALOIS GROUP

BY

Arno Fehm

Fachbereich Mathematik und Statistik, University of Konstanz
78457 Konstanz, Germany
e-mail: arno.fehm@uni-konstanz.de

AND

Franziska Jahnke

Institut für Mathematische Logik und Grundlagenforschung
University of Münster, Einsteinstr. 62, 48149 Münster, Germany
e-mail: franziska.jahnke@wwu.de

ABSTRACT

We construct and study fields F with the property that F has infinitely many extensions of some fixed degree, but $E^\times/(E^\times)^n$ is finite for every finite extension E/F and every $n \in \mathbb{N}$.

1. Introduction

We study the following closely related algebraic conditions on a field F:

(F1) For every $n \in \mathbb{N}$, the field F has only finitely many extensions of degree n (sometimes referred to as F is **bounded**).

(F2) For every $n \in \mathbb{N}$ and every finite extension E of F, the subgroup of n-th powers $(E^\times)^n$ has finite index in the multiplicative group $E^\times$.

Both conditions appear already in Serre's *Cohomologie Galoisienne* [Ser65, Ch. III §4] and have recently acquired importance in the model theory of fields:

Received December 12, 2014 and in revised form March 26, 2015

For example, it is known that every supersimple field satisfies (F1) (Pillay–Poizat), and for perfect pseudo-algebraically closed fields also the converse holds (Hrushovski). Condition (F2) is satisfied by every superrosy field and also by every strongly^2-dependent field, and it appears in a conjecture of Shelah–Hasson on definable valuations in NIP fields, as well as in related results by Krupiński. For details on all of this see [Kru15], [KS13, Cor. 2.7].

It is well-known (we recall this in Proposition 2.3 below) that for perfect fields (F1) implies (F2); it was, however, an open question whether the converse holds. For example, finite or pseudo-finite fields and local fields like $\mathbb{R}$ and $\mathbb{Q}_p$ are known to satisfy both (F1) and (F2), while global fields like $\mathbb{Q}$ or $\mathbb{F}_q(t)$ satisfy neither of them. Similarly, it is obvious that (F1) is preserved under elementary equivalence of fields, but it was an open question, asked by S. Kuhlmann in 2010, whether so is (F2).

We answer both questions negatively:

Theorem 1.1: *If a field F satisfies* (F2) *and F^* is a field elementarily equivalent to F, then F^* need not satisfy* (F2).

Theorem 1.2: *Even if all fields elementarily equivalent to F satisfy* (F2), *F need not satisfy* (F1).

The theorems are proven by constructing counterexamples. These counterexamples are obtained by first translating the problem into group theory and then realizing suitable profinite groups—the universal Frattini cover of products over certain finite groups derived from wreath products—as absolute Galois groups. The fields obtained by such a construction can be chosen either pseudo-algebraically closed or henselian valued. In the last section we take a closer look at the henselian case and relate (F1) and (F2) to the residue field.

2. Translation to group theory

We now explain the translation of (F1) and (F2) into properties of the absolute Galois group G_F of F and recall why (F1) implies (F2). For simplicity, we will from now on always assume that F is of characteristic zero. Let G be a profinite group and consider the following two conditions on G:

(G1) G is a **small** profinite group, i.e., for every $n \in \mathbb{N}$ there are only finitely many open subgroups $H \leq G$ of index n.

(G2) For every $n \in \mathbb{N}$, every open subgroup $H \leq G$ has only finitely many open normal subgroups $N \lhd H$ with H/N cyclic of order n.

For (F1) the translation follows directly from Galois correspondence:

Fact 2.1: F satisfies (F1) if and only if $G = G_F$ satisfies (G1).

Let E be a field of characteristic zero and let $\overline{E}$ be an algebraic closure of E. For $n \in \mathbb{N}$ we denote by $\mu_n \subseteq \overline{E}$ the group of n-th roots of unity, and let $\mu_\infty = \bigcup_{n\in\mathbb{N}} \mu_n$.

Lemma 2.2: *If $G = G_E$ is small, then $E^\times/(E^\times)^n$ is finite for any $n \in \mathbb{N}$.*

Proof. The short exact sequence

$$1 \to \mu_n \to \overline{E}^\times \overset{\cdot^n}{\to} \overline{E}^\times \to 1$$

gives rise to the long cohomology sequence

$$1 \to \mu_n^G \to E^\times \overset{\cdot^n}{\to} E^\times \to H^1(G,\mu_n) \to H^1(G,\overline{E}^\times) \to \cdots$$

where μ_n^G denotes the G-invariant subgroup of μ_n [GS06, Proposition 4.3.1]. Since $H^1(G,\overline{E}^\times) = 1$ holds by Hilbert's Theorem 90 [GS06, Lemma 4.3.7], we conclude that $E^\times/(E^\times)^n \cong H^1(G,\mu_n)$. Let $N = G_{E(\mu_n)}$, which is an open normal subgroup of G, and let μ_n^N denote the N-invariant subgroup of μ_n. The inflation-restriction sequence [GS06, Corollary 4.3.5]

$$1 \to H^1(G/N,\mu_n^N) \overset{\text{inf}}{\to} H^1(G,\mu_n) \overset{\text{res}}{\to} H^1(N,\mu_n)$$

shows that $H^1(G,\mu_n)$ is finite, as $H^1(G/N,\mu_n^N)$ is finite (since G/N and μ_n are finite) and $H^1(N,\mu_n) = \mathrm{Hom}(N,\mu_n)$ is finite (since N is small and μ_n is finite). ∎

Proposition 2.3: *If F satisfies* (F1), *then it satisfies* (F2).

Proof. Since (F1) implies that G_E is small for every finite extension E/F, the claim follows from Lemma 2.2. ∎

In the case where F contains all roots of unity, this follows more directly from the following considerations.

Lemma 2.4: *Suppose that $\mu_n \subseteq E$. Then $E^\times/(E^\times)^n$ is finite if and only if E has only finitely many cyclic extensions of degree dividing n.*

Proof. Let $B \leq E^\times$ be a subgroup containing $(E^\times)^n$, and denote by E_B the field obtained from E by adjoining n-th roots of all elements of B. By Kummer theory, the map $B \mapsto E_B$ gives a bijection between the set of such subgroups B and the abelian extensions of E of exponent n, and if $(B : (E^\times)^n) < \infty$, then $\mathrm{Gal}(E_B/E) \cong B/(E^\times)^n$; cf. [Lan02, Ch. VI §8]. In particular, the cyclic subgroups of $E^\times/(E^\times)^n$ correspond to cyclic extensions of E of degree dividing n. Since $E^\times/(E^\times)^n$ has infinitely many cyclic subgroups if and only if it is infinite, the claim follows. ∎

Proposition 2.5: *If $\mu_\infty \subseteq F$, then F satisfies* (F2) *if and only if $G = G_F$ satisfies* (G2).

Proof. This follows from Lemma 2.4 applied to the finite extensions E of F. ∎

In order to deal with the fields elementarily equivalent to F we also need a uniform variant of (G2). We denote by C_n the cyclic group of order n. We write $H \leq G$ and $H \lhd G$ to denote that H is a closed respectively closed normal subgroup of G.

Definition 2.6: For $n, m \in \mathbb{N}$ we let

$$I_G(n) = |\{N \lhd G : G/N \cong C_n\}|$$

and

$$I_G(n,m) = \sup\{I_H(n) : H \leq G, (G:H) \leq m\}.$$

With this definition, (G2) means that $I_H(n) < \infty$ for all open $H \lhd G$, and the uniform variant of (G2) can now be formulated as follows:

(G2*) For every $n, m \in \mathbb{N}$, $I_G(n,m) < \infty$.

In other words, G_F satisfies (G2*) if and only if there is a uniform bound on the number of cyclic extensions of degree n of finite extensions E of F of degree at most m.

Proposition 2.7: *If $\mu_\infty \subseteq F$, then $G = G_F$ satisfies* (G2*) *if and only if all fields $F^* \equiv F$ satisfy* (F2).

Proof. For every $m, n, k \in \mathbb{N}$, there is a sentence $\varphi_{m,n,k}$ in the language of fields such that $F \models \varphi_{m,n,k}$ if and only if every extension E of F with $[E:F] \leq m$ has at most k cyclic extensions of degree n.

If G_F satisfies (G2*), then $F \models \varphi_{m,n,I_{G_F}(n,m)}$ for every m, n, so if $F^* \equiv F$, then also $F^* \models \varphi_{m,n,I_{G_F}(n,m)}$, and therefore $I_{G_{F^*}}(n,m) \leq I_{G_F}(n,m) < \infty$ for all m, n. In particular, G_{F^*} satisfies (G2), so F^* satisfies (F2) by Proposition 2.5.

Conversely, if G_F does not satisfy (G2*), then there exist m, n such that $F \models \neg\varphi_{m,n,k}$ for every k. Let F^* be an $\aleph_1$-saturated elementary extension of F; cf. [CK90, Lemma 5.1.4] or [FJ08, Lemma 7.7.4]. Since $F^* \equiv F$, for every k we have $F^* \models \neg\varphi_{m,n,k}$, i.e., F^* has an extension E_k with $[E_k : F^*] \leq m$ which has more than k cyclic extensions of degree n. By saturation, F^* has an extension E^* with $[E^* : F^*] \leq m$ which has infinitely many cyclic extensions of degree n. Therefore, F^* does not satisfy (F2), by Lemma 2.4. ∎

Remark 2.8: If G is small, then the supremum in the definition of $I_G(n,m)$ runs over only finitely many H, so (G1) implies (G2*). We thus have the following implications for a profinite group G:

$$G \text{ is finitely generated} \implies \text{(G1)} \implies \text{(G2}^*\text{)} \implies \text{(G2)}.$$

For the first implication see [FJ08, 16.10.2]. It is well-known that the first implication cannot be reversed (see [FJ08, 16.10.4]), and what we show in the next section is that the same holds for the other two implications.

We mention here without proof that G satisfies (G2) if and only if every open subgroup of G has only finitely many solvable quotients of given order n, cf. [Ser65, p. III-30 Exercice], so if G is pro-solvable, then the last two arrows are equivalences. Moreover, for pro-p groups, all four conditions are equivalent; cf. [Ser65, p. III-28 Corollaire].

3. Constructing profinite groups

We now construct a profinite group that satisfies (G2*) but not (G1), which is relatively straightforward, and another one that satisfies (G2) but not (G2*), which requires more group theory.

PROPOSITION 3.1: *Let S be any non-abelian finite simple group, κ an infinite cardinal number, and $G = S^\kappa$. Then G satisfies* (G2*) *but not* (G1).

Proof. Note that every open normal subgroup of G is isomorphic to G itself, with quotient of the form S^k with $k \in \mathbb{Z}_{\geq 0}$; cf. [RZ00, Lemma 8.2.4]. In particular, $I_G(n) = 0$ for all n. If $H \leq G$ with $(G : H) \leq m$, let N be the biggest normal subgroup of G contained in H. Then $(G:N) \leq m!$ and $I_N(n) = 0$ for all n. If $M \lhd H$ with $H/M \cong C_n$, then $M \cap N \lhd N$ and $N/(M \cap N) \cong MN/M \leq H/M \cong C_n$ is cyclic, hence trivial. Thus, $N \leq M \leq H$, and so $I_H(n)$ is bounded by the number of subgroups of H/N. Therefore, $I_G(n,m) \leq 2^{m!}$. Since G has at least κ many quotients isomorphic to S, it is not small. ■

Lemma 3.2: *Let G be a profinite group and $n \in \mathbb{N}$. Then we have $I_G(n) \leq 2^{n^s}$ with $s = \sum_{p|n \text{ prime}} I_G(p)$.*

Proof. Let $N_1, \dots, N_r \lhd G$ be distinct normal subgroups with $G/N_i \cong C_n$. Let $N = \bigcap_{i=1}^r N_i$. Then $A := G/N$ embeds into C_n^r, hence $A \cong C_{d_1} \times \cdots \times C_{d_k}$ with $k \in \mathbb{N}$ and $d_i | n$ for all i. If $p | d_i$ is prime, then there is an epimorphism $\rho_i : C_{d_i} \to C_p$, and the maps

$$\delta_i : G \to A \overset{\cong}{\to} C_{d_1} \times \cdots \times C_{d_k} \overset{\pi_i}{\to} C_{d_i} \overset{\rho_i}{\to} C_p$$

are surjective and mutually distinct $(1 \leq i \leq k)$. Thus, if $I_G(p) < \infty$ for all $p|n$, then $k \leq s := \sum_{p|n} I_G(p)$. As $N_1/N, \dots, N_r/N$ are distinct subsets of A, we see that r is bounded by the number of subsets of A. Hence, $r \leq 2^{|A|} \leq 2^{n^s}$. ■

Remark 3.3: Let p be a prime number, and let $M_p(G)$ be the intersection over all $N \lhd G$ with $G/N \cong C_p$. Then $G/M_p(G) \cong C_p^{r_p(G)}$, where $r_p(G)$ is the p-rank of G; cf. [RZ00, Sec. 8.2]. Since $V = C_p^{r_p(G)}$ is an $\mathbb{F}_p$-vector space of dimension $r_p(G)$, and the C_p-quotients of V correspond to 1-dimensional subspaces of the dual space V^*, we see that

$$I_G(p) = |\mathbb{P}V^*| = \frac{p^{r_p(G)} - 1}{p - 1}$$

if $r_p(G)$ is finite, and $I_G(p) = \infty$ otherwise. We also see that if F is a field of characteristic zero with $\mu_p \subseteq F$, then $|F^\times/(F^\times)^p| = |G_F/M_p(G_F)| = p^{r_p(G_F)}$; cf. the proof of Lemma 2.4.

Lemma 3.4: *If a profinite group G has, for every prime p, a basis of neighborhoods of* 1 *consisting of open normal subgroups U with $r_p(U) < \infty$, then it satisfies* (G2).

Proof. Let $H \leq G$ be an open subgroup and let p be a prime number. By assumption, H contains an open normal subgroup U of G with $r_p(U) < \infty$.

Thus,

$$U/(U \cap M_p(H)) \cong M_p(H)U/M_p(H) \leq H/M_p(H) \cong C_p^{r_p(H)},$$

so $M_p(U) \leq U \cap M_p(H)$, which implies that

$$(H : M_p(H)) \leq (G : U) \cdot (U : M_p(U)) < \infty,$$

and hence $r_p(H)$ is finite. Since this holds for every p, Lemma 3.2 shows that G satisfies (G2). ∎

Recall that a profinite group G is **perfect** if $G' = G$, where $G' = [G,G]$ denotes the closed subgroup of G generated by the commutators

$$[x,y] = x^{-1}x^y = x^{-1}y^{-1}xy.$$

Thus, G is perfect if and only if $r_p(G) = 0$ for all primes p.

Lemma 3.5: *Every direct product $G = \prod_{i\in I} G_i$ of finite perfect groups G_i satisfies* (G2).

Proof. Note that the open normal subgroups $G_J = \prod_{i\in I\smallsetminus J} G_i$, $J \subseteq I$ finite, form a basis of neighborhoods of 1 of G. Moreover, each G_J is perfect as a direct product of perfect groups. Thus, the claim follows from Lemma 3.4. ∎

Lemma 3.6: *Let S be a non-abelian finite simple group and p a prime number. For every k_0 there exists $k \geq k_0$ and a group extension of S by C_p^k which is perfect.*

Proof. Let $A = C_p^{k_0}$ and let $\Gamma = A \wr S$ be the wreath product, which is defined as the semidirect product $B \rtimes S$, where S acts on the group B of functions $f : S \to A$ from the right by $f^\sigma(\tau) = f(\tau\sigma)$, where $\sigma, \tau \in S$. Then

$$\Gamma'' = \Gamma' = B_0 \rtimes S,$$

where

$$B_0 = \left\{ f \in B : \prod_{\sigma\in S} f(\sigma) = 1 \right\} \cong A^{|S|-1},$$

so Γ' is a perfect extension of S by C_p^k, where $k = (|S| - 1)k_0 \geq k_0$. This fact can be found in the literature (see, e.g., [Mel95, Ch. I §4], [Isa77, bottom of p. 721], [Gur10]), but we briefly recall the proof for the convenience of the reader:

Note that $\Gamma = BS$. Since $B \lhd \Gamma$, we have $[B,S] \leq B$ and $[B,S] \lhd \Gamma$ (for the last statement see [Isa08, Lemma 4.1]). Since $\Gamma/[B,S] \cong B/[B,S] \times S$ we conclude that $\Gamma/[B,S]S \cong B/[B,S]$ is abelian, hence $\Gamma' \subseteq [B,S]S$, which together with the obvious inclusions $[B,S] \subseteq \Gamma'$ and $S = [S,S] \subseteq \Gamma'$ gives that $\Gamma' = [B,S]S$.

For $x \in S$ and $g \in B$, we have $\prod_{\sigma\in S} g^x(\sigma) = \prod_{\sigma\in S} g(\sigma x) = \prod_{\sigma\in S} g(\sigma)$, so we get $\prod_{\sigma\in S}(g^{-1}g^x)(\sigma) = 1$, hence $[B,S] \subseteq B_0$. Conversely, if $f \in B_0$, write $f = \prod_{\sigma\in S} f_\sigma$ with $f_\sigma \in B$ defined by $f_\sigma(\tau) = f(\tau)$ if $\tau = \sigma$ and $f_\sigma(\tau) = 1$ otherwise. Define $g := \prod_{\sigma\in S}(f_\sigma)^\sigma$. Then $g = 1$. Indeed,

$$g(1) = \prod_{\sigma\in S} f_\sigma(\sigma) = \prod_{\sigma\in S} f(\sigma) = 1$$

since $f \in B_0$, and for $1 \neq \tau \in S$, we have $g(\tau) = \prod_{\sigma\in S} f_\sigma(\sigma\tau) = \prod_{\sigma\in S} 1 = 1$. But each $(f_\sigma)^{-1}(f_\sigma)^\sigma \in [B,S]$, hence $f[B,S] = g[B,S] = [B,S]$ and therefore $B_0 \subseteq [B,S]$. It follows that $[B,S] = B_0$. Therefore,

$$\Gamma' = [B,S]S = B_0S = B_0 \rtimes S.$$

Finally, write $[X,Y,Z]$ for $[[X,Y],Z]$. We claim that $N := [B,S,S]$ is normal in Γ. Note that N is normal in $\langle [B,S],S\rangle$ (see again [Isa08, Lemma 4.1]) and thus invariant under conjugation with elements from S. Furthermore, $[B,S] \lhd \Gamma$ implies $N \subseteq [B,S] \subseteq B$. Thus, as B is abelian, we also get that N is invariant under conjugation with elements from B. As $\Gamma = BS$, we conclude that N is normal in Γ. This proves the claim. Moreover, we have $[B,S,S] = [S,B,S]$. Therefore, the 'three-subgroups lemma' [Isa08, Corollary 4.10] gives that $[S,S,B] \subseteq N$. We conclude that

$$[\Gamma',\Gamma'] \supseteq [B,S,S] \supseteq [S,S,B] = [S,B] = [B,S].$$

Together with the trivial inclusion $[\Gamma',\Gamma'] \supseteq [S,S] = S$ we conclude that

$$\Gamma'' = [B,S]S = \Gamma'. \qquad \blacksquare$$

Proposition 3.7: *Let S be a non-abelian finite simple group and p a prime number. Let G be the direct product over all perfect extensions of S by C_p^k for all $k \in \mathbb{N}$. Then G satisfies* (G2) *but not* (G2*).

Proof. By Lemma 3.6, for every k_0 there exists $k \geq k_0$ and a perfect extension P of S by C_p^k, which by definition is a quotient of G. Since P has an open subgroup Q of index $m = |S|$ with $r_p(Q) \geq k$, the group G has an open subgroup H of index m with $r_p(H) \geq k$. Therefore, $I_G(p, m) \geq k \geq k_0$. Since this holds for every k_0, G does not satisfy (G2*). On the other hand, Lemma 3.5 implies that G satisfies (G2). ∎

4. Constructing fields

We saw that the desired properties of fields are reflected by the properties (G1), (G2) and (G2*) of their absolute Galois groups and we already constructed suitable profinite groups. However, the groups we constructed do not occur as absolute Galois groups of fields—they have too much torsion. Instead, we want to construct fields using the following result; cf. [FJ08, 23.1.2]:

Proposition 4.1 (Lubotzky–van den Dries): *For every field K and every projective profinite group G there is a perfect pseudo-algebraically closed field $F \supseteq K$ with $G_F \cong G$.*

In order to apply this result, we have to replace the profinite groups we constructed by projective ones with similar properties, for which we will make use of the **universal Frattini cover** $\tilde{G}$ of a profinite group G; cf. [FJ08, Chapter 22]. We do not give the full definition but rather list the properties of $\tilde{G}$ that we need:

(1) $\tilde{G}$ is a projective profinite group and there is an epimorphism $\phi : \tilde{G} \to G$; see [FJ08, 22.6.1].

(2) For each quotient Δ of $\tilde{G}$ there is an epimorphism $\Delta \to \Gamma$ onto some quotient Γ of G such that $\mathrm{rk}(\Delta) = \mathrm{rk}(\Gamma)$; see [FJ08, 22.6.3, 22.5.3].

Here, $\mathrm{rk}(G)$ denotes the profinite rank of G, cf. [FJ08, Chapter 17.1], which for finite G is just the minimal cardinality of a set of generators. We now show that the properties (G2) and (G2*) are preserved by taking the universal Frattini cover, which is the technical heart of our construction.

Lemma 4.2: *For every prime p and every $H \leq \tilde{G}$ with $(\tilde{G} : H) = m$ there exists $G_0 \leq G$ with $(G : G_0) \leq m!$ such that $r_p(H) \leq (m!)^2(r_p(G_0) + 2)$.*

Proof. If H_0 is the biggest normal subgroup of $\tilde{G}$ contained in H, then $(\tilde{G} : H_0) \leq m!$. Furthermore, we have

$$r_p(H) \leq r_p(H_0) + r_p(H/H_0) \leq r_p(H_0) + \log_p(m!)$$

with the first inequality following from [RZ00, 8.2.5(d)].

Let $N = M_p(H_0)$. Since $H_0 \lhd \tilde{G}$ and N is characteristic in H_0, we conclude that $N \lhd \tilde{G}$. Let $\Delta = \tilde{G}/N$ and $\Delta_0 = H_0/N \cong C_p^{r_p(H_0)}$. By (2), there exist epimorphisms $\phi : \Delta \to \Gamma$, $\pi : G \to \Gamma$ with $\mathrm{rk}(\Gamma) = \mathrm{rk}(\Delta)$. Let

$$\Gamma_0 = \phi(\Delta_0) \lhd \Gamma \quad \text{and} \quad G_0 = \pi^{-1}(\Gamma_0) \lhd G$$

and note that $(G : G_0) = (\Gamma : \Gamma_0)$ divides $(\Delta : \Delta_0) = (\tilde{G} : H_0) \leq m!$.

Trivially, $r_p(G_0) \geq r_p(\Gamma_0)$. Since Γ_0 is an elementary abelian p-group, we have $\mathrm{rk}(\Gamma_0) = r_p(\Gamma_0)$ and so the inequality

$$\mathrm{rk}(\Gamma) \leq \mathrm{rk}(\Gamma_0) + \mathrm{rk}(\Gamma/\Gamma_0) \leq r_p(\Gamma_0) + m!$$

holds. By the Nielsen–Schreier formula [FJ08, 17.6.3], we get

$$\mathrm{rk}(\Delta_0) \leq 1 + (\Delta : \Delta_0)(\mathrm{rk}(\Delta) - 1).$$

Thus,

$$\begin{aligned} r_p(H_0) =& \mathrm{rk}(\Delta_0) \leq 1 + m! \cdot (\mathrm{rk}(\Gamma) - 1) \leq 1 + m! \cdot (r_p(\Gamma_0) + m! - 1) \\ \leq& m! \cdot r_p(G_0) + (m!)^2, \end{aligned}$$

which gives

$$r_p(H) \leq \log_p(m!) + m! \cdot r_p(G_0) + (m!)^2 \leq (m!)^2(r_p(G_0) + 2). \qquad \blacksquare$$

PROPOSITION 4.3: *The universal Frattini cover $\tilde{G}$ of G satisfies* (G2) *resp.* (G2*) *if and only if G does.*

Proof. If $\tilde{G}$ satisfies (G2) or (G2*), then so does its quotient G.

Conversely, assume that G satisfies (G2) and let $H \leq \tilde{G}$ with $(\tilde{G} : H) \leq m$. By Lemma 4.2 there exists $G_0 \leq G$ with $(G : G_0) \leq m!$ such that $r_p(H)$ is bounded in terms of $r_p(G_0)$ and m. In particular, $I_H(p)$ is finite. By Lemma 3.2 we get for every n that $I_H(n)$ is finite, so $\tilde{G}$ satisfies (G2).

If G satisfies even (G2*) then $I_{G_0}(p) \leq I_G(p, m!)$ is uniformly bounded just in terms of m and p, hence so is $r_p(G_0)$, and therefore also $I_H(p)$. Thus, by Lemma 3.2, $I_H(n)$ is bounded in terms of m and n, so $I_{\tilde{G}}(n, m) < \infty$, which means that $\tilde{G}$ satisfies (G2*). $\blacksquare$

We now have all the ingredients to construct the counterexamples that prove Theorem 1.1 and Theorem 1.2:

Proposition 4.4: *There exists a pseudo-algebraically closed field F of characteristic zero such that every $F^* \equiv F$ satisfies* (F2), *but F does not satisfy* (F1).

Proof. Let S be a non-abelian finite simple group, for example $S = A_5$, and let $G = S^{\aleph_0}$. By Proposition 3.1, G satisfies (G2*) but not (G1). Thus, by Proposition 4.3, also $\tilde{G}$ satisfies (G2*), and, since it has G as a quotient, it does not satisfy (G1). Let K be any field of characteristic zero that contains all roots of unity, for example $K = \mathbb{C}$. By Proposition 4.1 there exists a field $F \supseteq K$ which is pseudo-algebraically closed and has absolute Galois group $G_F \cong \tilde{G}$, so all $F^* \equiv F$ satisfy (F2) by Proposition 2.7, but F does not satisfy (F1) (Fact 2.1). ∎

Proposition 4.5: *There exists a pseudo-algebraically closed field F of characteristic zero that satisfies* (F2), *but some $F^* \equiv F$ does not satisfy* (F2).

Proof. Let S be a non-abelian finite simple group, for example $S = A_5$, let p be any prime number, for example $p = 2$, and let G be the direct product over all perfect extensions of S by C_p^k for all $k \in \mathbb{N}$. By Proposition 3.7, G satisfies (G2) but not (G2*). Thus, by Proposition 4.3, also $\tilde{G}$ satisfies (G2) but not (G2*). Let again K be any field of characteristic zero that contains all roots of unity and apply Proposition 4.1 to get a field $F \supseteq K$ which is pseudo-algebraically closed and has absolute Galois group $G_F \cong \tilde{G}$. By Proposition 2.5, F satisfies (F2), but by Proposition 2.7 there is some $F^* \equiv F$ that does not satisfy (F2). ∎

Remark 4.6: We remark that much more concrete realizations of projective profinite groups are known. For example, since the groups we constructed have countable rank, they could be realized as absolute Galois groups of algebraic extensions of $\mathbb{Q}$. For instance, if $\mathbb{Q}^{\mathrm{tr}}$ denotes the field of totally real algebraic numbers—the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{R}$—then one can find algebraic extensions of $\mathbb{Q}^{\mathrm{tr}}(\mu_\infty)$ with the properties of Proposition 4.4 or Proposition 4.5; cf. [Jar11, Example 5.10.7].

5. Henselian fields

Since (F1) and (F2) are essentially properties of the absolute Galois group, and every absolute Galois group occurs as the absolute Galois group of a henselian valued field, it is clear that one can also construct such examples with F henselian:

Proposition 5.1: *There exists a henselian valued field F of characteristic zero that satisfies* (F2) *but not* (F1).

Proof. Let F be the field constructed in Proposition 4.4, and let $F' = F((\mathbb{Q}))$ be the field of generalized power series over F with exponents in $\mathbb{Q}$; cf. [Efr06, §4.2]. Then F' is henselian valued with residue field F and divisible value group $\mathbb{Q}$; see [Efr06, 18.4.2]. Thus, $G_{F'} \cong G_F$, as follows from [EP05, 5.2.7 and 5.3.3]. Since F' contains all roots of unity, it satisfies (F2) but not (F1), as above. ∎

In this construction, the property that F' satisfies (F2) but not (F1) is inherited from the residue field. We now show that, at least in characteristic 0, this is in fact the only way to construct henselian fields with this property, or, more generally, with properties like in Proposition 4.4 and Proposition 4.5. In order to do that, we need the following lemmas.

Lemma 5.2: *Let (F, v) be a henselian valued field with residue field Fv of characteristic* 0 *and value group Γ, and let $n \in \mathbb{N}$. Then*

$$|F^\times/(F^\times)^n| = |\Gamma/n\Gamma| \cdot |Fv^\times/(Fv^\times)^n|$$

holds. In particular, if $\mu_n \subseteq F$, then $I_{G_F}(n)$ is finite if and only if both $[\Gamma : n\Gamma]$ and $I_{G_{Fv}}(n)$ are finite.

Proof. Take $A = \{a_i\}_{i\in I} \subseteq \mathcal{O}_v$ such that $\{v(a_i)\}_{i\in I}$ form a system of representatives for $\Gamma/n\Gamma$ and $B = \{b_i\}_{i\in J} \subseteq \mathcal{O}_v^\times$ such that $\{\overline{b_i}\}_{i\in J}$ form a system of representatives for $Fv^\times/(Fv^\times)^n$.

We first show

$$|F^\times/(F^\times)^n| \geq |\Gamma/n\Gamma| \cdot |Fv^\times/(Fv^\times)^n|$$

for any valued field (F, v): Consider (a, b), $(a', b') \in A \times B$. Assume that we have $ab \equiv a'b' \bmod (F^\times)^n$. Without loss of generality, $ab = r^n a'b'$ for some $r \in \mathcal{O}_v$. Then

$$v(a) = v(ab) = nv(r) + v(a'b') = nv(r) + v(a'),$$

so $a = a'$, since the values of A form a system of representatives for $\Gamma/n\Gamma$. Thus, $b = r^n b'$ holds, so we get $\overline{b} \equiv \overline{b'} \bmod (Fv^\times)^n$ and hence $b = b'$, which proves the claim.

On the other hand, take any $x \in F^\times$. We want to show that there is some $(a, b) \in A \times B$ such that we have $xab \in (F^\times)^n$. Choose $a \in A$ with $v(xa) \in n\Gamma$ and take some $u \in F^\times$ with $v(u^n) = v(xa)$. Then for $c = \frac{xa}{u^n}$ we get $v(c) = 0$, so there is some $b \in B$ with $\overline{t}^n = \overline{cb}$ for some $t \in F^\times$. By henselianity (see [EP05, 4.1.3]), $f(X) = X^n - \frac{cb}{t^n}$ has a zero $\alpha \in F^\times$, as $\mathrm{char}(Fv) = 0$. This implies $xab = \alpha^n t^n u^n \in (F^\times)^n$. Thus $|F^\times/(F^\times)^n| \leq |\Gamma/n\Gamma| \cdot |Fv^\times/(Fv^\times)^n|$ holds.

The last part now follows immediately from Lemma 2.4. ∎

Lemma 5.3: *Let G be a profinite group and assume that there are subgroups H and K of G with $G = K \rtimes H$. If both K and H are small, then so is G.*

Proof. Consider a continuous epimorphism f from G onto a finite group of order n. Note that the restriction f_K (respectively f_H) of f to K (respectively H) induces an epimorphism of K (respectively H) onto a group of order at most n. Since $G = KH$ holds by assumption, the map f is completely determined by its restrictions f_K and f_H. Hence, if both K and H have only finitely many continuous quotients of order at most n, then G has only finitely many continuous quotients of order n. Thus, if both K and H are small, then so is G. ∎

Proposition 5.4: *Let (F, v) be a henselian valued field with residue field Fv and value group Γ. Assume that* $\mathrm{char}(Fv) = 0$ *and* $\mu_\infty \subseteq F$.

(1) *If* $[\Gamma : p\Gamma] = \infty$ *for some prime p, then F satisfies neither* (F1) *nor* (F2).

(2) *If* $[\Gamma : p\Gamma]$ *is finite for all primes p, then*

   (a) (F1) *holds for F if and only if it holds for Fv,*

   (b) (F2) *holds for F if and only if it holds for Fv, and*

   (c) (F2) *holds for every $K \equiv F$ if and only if it holds for every $k \equiv Fv$.*

Proof. (1) Note that since (F, v) is henselian of characteristic $(0, 0)$ and F contains all roots of unity, Lemma 5.2 applies. Thus, $[\Gamma : p\Gamma] = \infty$ for some prime p implies $|F^\times/(F^\times)^p| = \infty$ and so neither (F1) nor (F2) hold for F.

(2) For the remainder of the proof, assume that $i_p := [\Gamma : p\Gamma]$ is finite for all primes p. By [EP05, 5.2.6 and 5.3.3] and [Neu68, Satz 2], we have

$$G_F \cong \left(\prod_{p \text{ prime}} \mathbb{Z}_p^{i_p} \right) \rtimes G_{Fv}.$$

(a) Since $\prod_p \mathbb{Z}_p^{i_p}$ is small, Lemma 5.3 implies that G_F is small if and only if G_{Fv} is small, i.e., F satisfies (F1) if and only if Fv does (Fact 2.1).

(b) If G_F satisfies (G2) then so does its quotient G_{Fv}.

Conversely, assume that (G2) holds for G_{Fv}. Let E be a finite extension of F, say $[E : F] = m$. Let Δ denote the value group and Ev the residue field of the unique prolongation of v to E. Define $f := [Ev : Fv]$ and $e = [\Delta : \Gamma]$. Then—by [EP05, 3.3.4]—we have $ef \leq m$. For every prime p, $I_{G_{Ev}}(p)$ and thus $Ev^\times/(Ev^\times)^p$ is finite, and $[\Delta : p\Delta] \leq [\Gamma : p\Gamma] \cdot e < \infty$, so by applying Lemma 5.2 to E, we get $|E^\times/(E^\times)^p| < \infty$ for every p, which by Remark 3.3 and Lemma 3.2 implies that G_F satisfies (G2).

(c) Again, if G_F satisfies (G2*), then so does its quotient G_{Fv}. For the other direction, assume that G_{Fv} satisfies (G2*). Fix any prime p and let E be a finite extension of F with $[E : F] \leq m$ and define Ev, Δ and $e = [\Delta : \Gamma]$ as before. Then, making repeated use of Remark 3.3, we see that

$$\begin{aligned} I_{G_E}(p) &= \frac{p^{r_p(G_E)} - 1}{p-1} = \frac{1}{p-1} \cdot (|E^\times/(E^\times)^p| - 1) \\ &\overset{5.2}{\leq} \frac{1}{p-1} \cdot ([\Delta : p\Delta] \cdot |Ev^\times/(Ev^\times)^p|) \\ &\leq \frac{1}{p-1}([\Gamma : p\Gamma] \cdot e \cdot p^{r_p(G_{Ev})}) \\ &\leq [\Gamma : p\Gamma] \cdot m \cdot (I_{G_{Ev}}(p) + 1) \\ &\leq [\Gamma : p\Gamma] \cdot m \cdot (I_{G_{Fv}}(p, m) + 1). \end{aligned}$$

Now Lemma 3.2 implies that for any subgroup $H \leq G_F$ of index at most m, $I_H(n)$ is uniformly bounded in terms of m and n, i.e., $I_{G_F}(n, m) < \infty$. Thus, (G2*) holds also for G_F, so any $K \equiv F$ satisfies (F2) (Proposition 2.7). ∎

Acknowledgments. The authors would like to thank Lior Bary-Soroker for suggesting the use of the universal Frattini cover, and Assaf Hasson, Itay Kaplan, Krzysztof Krupiński, Salma Kuhlmann and Moshe Jarden for helpful discussions and comments on a previous version.

References

[CK90] C. C. Chang and H. J. Keisler, *Model Theory*, Studies in Logic and the Foundations of Mathematics, Vol. 73, North-Holland, Amsterdam, 1990.

[Efr06] I. Efrat, *Valuations, Orderings, and Milnor K-Theory*, Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2006.

[EP05] A. Engler and A. Prestel, *Valued Fields*, Springer Monographs in Mathematics, Springer, Berlin, 2005.

[FJ08] M. D. Fried and M. Jarden, *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 11, Springer, Berlin, 2008.

[GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, Vol. 101, Cambridge University Press, Cambridge, 2006.

[Gur10] R. M. Guralnick, *Commutators and wreath products*, in *Character Theory of Finite Groups*, Contemporary Mathematics, Vol. 524, American Mathematical Society, Providence, RI, 2010, pp. 79–82.

[Isa77] I. M. Isaacs, *Commutators and the commutator subgroup*, American Mathematical Monthly **84** (1977), 720–722.

[Isa08] I. M. Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, Vol. 92, American Mathematical Society, Providence, RI, 2008.

[Jar11] M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics, Springer, Heidelberg, 2011.

[KS13] I. Kaplan and S. Shelah, *Chain conditions in dependent groups*, Annals of Pure and Applied Logic **164** (2013), 1322–1337.

[Kru15] K. Krupiński, *Superrosy fields and valuations*, Annals of Pure and Applied Logic **166** (2015), 342–357.

[Lan02] S. Lang, *Algebra*, Graduate Texts in Mathematics, Vol. 211, Springer, New York, 2002.

[Mel95] J. D. P. Meldrum, *Wreath products of groups and semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 74, Longman, Harlow, 1995.

[Neu68] J. Neukirch, *Zur Verzweigungstheorie der allgemeinen Krullschen Bewertungen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **32** (1968), 207–215.

[RZ00] L. Ribes and P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 40, Springer, Berlin, 2000.

[Ser65] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, vol. 5, Springer, Berlin–New York, 1965.