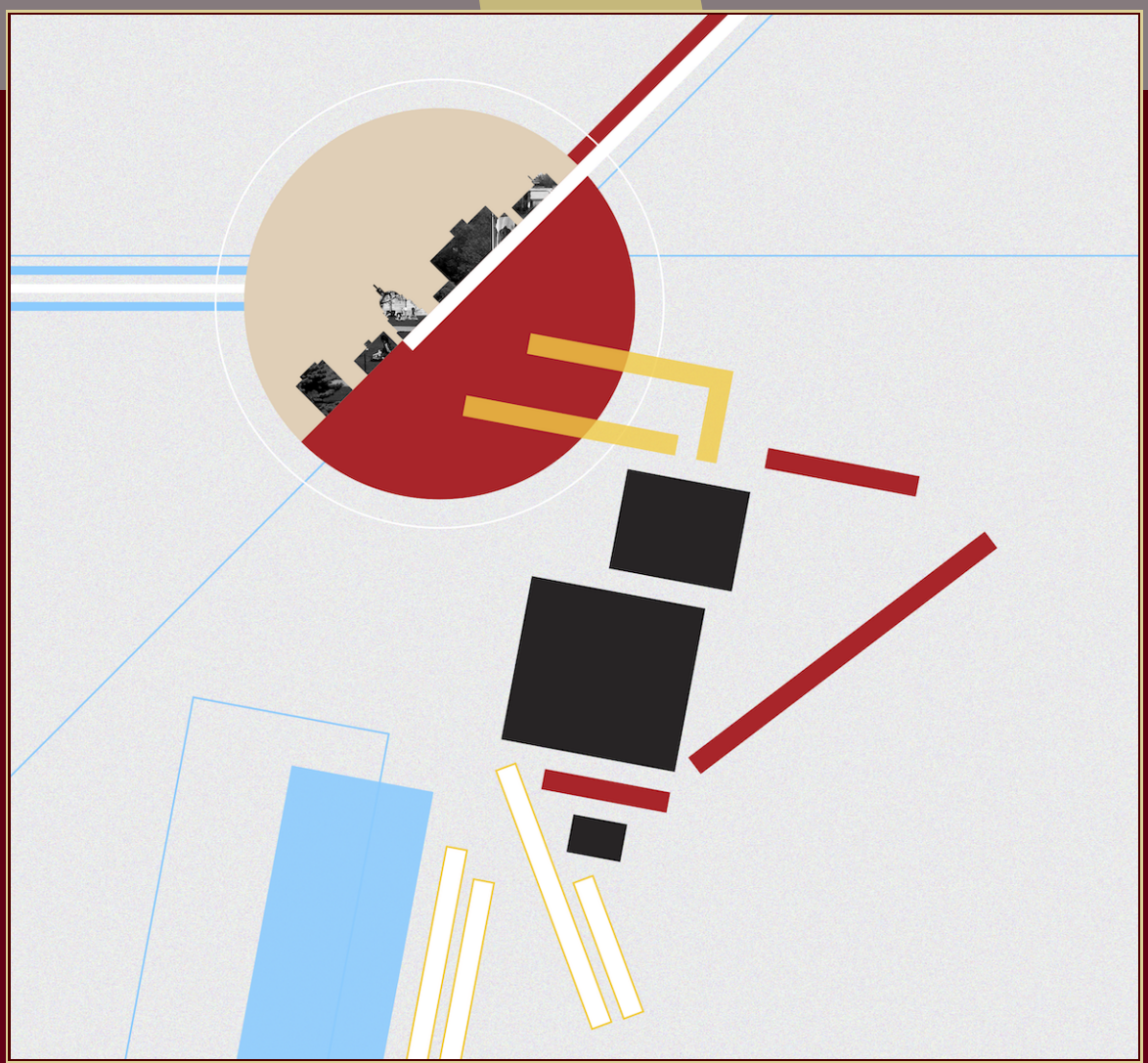
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

The inverse Galois problem for p-adic fields

David Roe



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.393

msp

The inverse Galois problem for p-adic fields

David Roe

We describe a method for counting the number of extensions of $\mathbb{Q}_p$ with a given Galois group G, founded upon the description of the absolute Galois group of $\mathbb{Q}_p$ due to Jannsen and Wingberg. Because this description is only known for odd p, our results do not apply to $\mathbb{Q}_2$. We report on the results of counting such extensions for G of order up to 2000 (except those divisible by 512), for $p = 3, 5, 7, 11, 13$. In particular, we highlight a relatively short list of minimal G that do not arise as Galois groups. Motivated by this list, we prove two theorems about the inverse Galois problem for $\mathbb{Q}_p$: one giving a necessary condition for G to be realizable over $\mathbb{Q}_p$ and the other giving a sufficient condition.

1. Introduction

The inverse Galois problem is most commonly studied over $\mathbb{Q}$. There, a theorem of Shafarevich [13; 18, Theorem 9.6.1] shows that every solvable group is realizable as the Galois group of an extension of $\mathbb{Q}$. Attention has thus focused on simple groups, and many have been shown to be realizable; see [11] for background.

Over $\mathbb{Q}$, if a given group arises as a Galois group it will arise for infinitely many extensions. Thus the constructive version of the problem, finding extensions with a given Galois group, has been approached by the method of generic polynomials. A generic polynomial for a group G is a monic polynomial with coefficients in a function field $\mathbb{Q}(c_1, \ldots, c_n)$ so that every extension of $\mathbb{Q}$ with Galois group G will arise via specializing the c_i to elements of $\mathbb{Q}$. Even if G is realizable, it may not have a generic polynomial parametrizing all extensions.

Over $\mathbb{Q}_p$, for fixed p and G, there are only finitely many isomorphism classes of Galois extensions $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. Thus, rather than trying to produce them via a generic polynomial, one could hope to enumerate them directly. As a first step toward such an enumeration, in this paper we study the less refined question of counting such K.

The counting and enumeration of p-adic fields has a rich history, mostly separate from the study of the inverse Galois problem. Rather than focusing on the Galois group, most approaches have studied the

Supported by Simons Foundation grant 550033.
MSC2010: primary 12F12; secondary 11S15, 11Y40, 12Y05, 20C40.
Keywords: p-adic extensions, inverse Galois theory, profinite groups.

extensions of a given degree, or with a given degree and discriminant. Foundational work of Krasner [10, Theorem 2] gave counts for the number of extensions of degree n in a fixed algebraic closure, and Serre [17] gives a "mass formula" where the counts are weighted appropriately. More recently, Hou and Keating [7] and Monge [12] have described how to count isomorphism classes of extensions with prescribed ramification and inertia degrees.

There has been some work on counting extensions with a given Galois group. When G is a p-group generated by d elements (minimally) and $k/\mathbb{Q}_p$ has degree n, Shafarevich [19] has obtained the following formula for the number of extensions of k with Galois group G, using his description of the maximal pro-p quotient of the absolute Galois group:

$$\frac{1}{|\mathrm{Aut}(G)|}\left(\frac{|G|}{p^d}\right)^{n+1}\prod_{i=0}^{d-1}(p^{n+1}-p^i). \tag{1}$$

The result only holds for k that do not contain the p-th roots of unity, but Yamagishi [20] has generalized it, obtaining a formula involving characters of G.

Other authors have pursued the problem of enumerating p-adic fields [14; 9] of a given degree. Theoretically, this would solve the problem of enumerating with a given Galois group, since one can determine from G the smallest degree where a field can have a normal closure with Galois group G. However, for many groups this degree is prohibitively large for the methods employed, since you also get many other, much larger, Galois groups at the same time.

In this paper, we count Galois extensions with Galois group G by exploiting the explicit description of the absolute Galois group of $\mathbb{Q}_p$. This approach has the benefit of completely avoiding computations with polynomials, allowing for a large number of groups to be considered. The downside is that we do not get any information on many invariants of number theoretic interest, such as the discriminant or the ramification filtration, beyond distinguishing between tame and wild inertia.

We have chosen to focus on the case of $\mathbb{Q}_p$ because it has the most intrinsic interest, and because the number of extensions grows exponentially with the absolute degree of the base field, as illustrated by (1). The code, which uses GAP [3] and SageMath [16], can be found at https://github.com/roed314/padicIGP.

1A. ***Summary.*** We begin Section 2 with the notion of a *potentially p-realizable group*, which encapsulates the obvious conditions on G that come from the first few steps of the ramification filtration. This notion is closed under quotients, and we conjecture that any potentially p-realizable group can be expressed as a semidirect product of its p-core and its tame quotient. This conjecture is supported by experimental evidence, and has consequences for the existence of subextensions complementary to the maximal tame subextension. We close with Section 2B, where we give algorithms to test whether a group is potentially p-realizable and to enumerate such groups.

In Section 3 we review the structure of the absolute Galois group, which plays a key role in our approach to counting extensions. We use the description to show that our notion of a potentially p-realizable group has the property that any such group will be realized over some p-adic field k.

Section 4 describes the algorithms used to count extensions $K/\mathbb{Q}_p$ with a given Galois group G. We give an explicit enumeration in the case of abelian groups, since we need this as a base case for inductive lifting methods later. We then summarize the tame case, which follows from the well-known structure of the tame quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Finally we give a lifting method for counting extensions for arbitrary G, and briefly discuss its runtime.

In Section 5 we apply the counting algorithms to the question of whether a potentially p-realizable group is actually realized over $\mathbb{Q}_p$. We start by listing minimal examples of groups that are unrealizable. We then proceed, in Section 5B, to prove Theorems 5.3 and 5.4 giving one necessary and one sufficient condition for p-realizability. Both conditions relate to the structure of the p-core of G as a representation of the tame quotient.

1B. ***Notation and terminology.*** We work throughout with a prime $p \neq 2$ and a finite group G. There are some naturally defined subgroups of G that will play an important role throughout the paper. The p-core V of G is the intersection of all of the p-Sylow subgroups of G:

$$V = \bigcap_{P \ p\text{-Sylow}} P.$$

It is the maximal normal p-group inside G. The quotient $T = G/V$ has the structure of a metacyclic group (an extension of a cyclic group by a cyclic group), but not canonically. It acts on V by conjugation. We call G *tame* if V is trivial and $G = T$.

We will also use the Frattini subgroup W of V, defined as

$$W = V^p V',$$

where V' is the commutator subgroup of V. The quotient V/W is the maximal quotient of V that is an elementary abelian p-group. The action of T on V descends to an action on V/W, yielding a representation of T on an $\mathbb{F}_p$-vector space.

We will refer to groups by their ID in GAP's SmallGroups library [2] using the notation $n\mathrm{G}k$, where n is the order of G and k enumerates groups of that order.

Write $\mathcal{G}$ for the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

2. Potentially p-realizable groups

2A. ***The structure of p-adic Galois groups.*** The structure of p-adic field extensions [4, Chapter 16] imposes constraints on the possible Galois groups that can arise. Any finite extension $K \supseteq \mathbb{Q}_p$ can be decomposed into a tower $K \supseteq K_t \supseteq K_u \supseteq \mathbb{Q}_p$, where $K_u/\mathbb{Q}_p$ is unramified, K_t/K_u is tame and totally ramified, and K/K_t is totally wildly ramified. When $K/\mathbb{Q}_p$ is Galois, this tower corresponds to the first parts of the ramification filtration on $G = \mathrm{Gal}(K/\mathbb{Q}_p)$:

$$G = G_{-1} \supseteq G_0 \supseteq G_1. \tag{2}$$

The fixed field of G_0 is the unramified subfield K_u and the quotient G/G_0 must be cyclic. The fixed field of G_1 is the tame subfield K_t and the quotient G_0/G_1 must be cyclic of order relatively prime to p. Finally, $G_1 \cong \mathrm{Gal}(K/K_t)$ is a p-group. Moreover, G_0 and G_1 are normal subgroups of G.

By a theorem of Iwasawa [8, Theorem 2], the Frobenius element of G/G_0 acts on G_0/G_1 by raising to the p-th power.

Definition 2.1. A group G is *potentially p-realizable* if it has a filtration $G \supseteq G_0 \supseteq G_1$ so that

(1) G_0 and G_1 are normal in G,

(2) G/G_0 is cyclic, generated by some $\sigma \in G$,

(3) G_0/G_1 is cyclic of order relatively prime to p, generated by some $\tau \in G_0$,

(4) $\tau^\sigma = \tau^p$,

(5) G_1 is a p-group.

We will call such a filtration on G a *tame structure*. A group G is *p-realizable* if there exists an extension $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$.

Remark 2.2. By the discussion above, any p-realizable group is potentially p-realizable, justifying the terminology. We will also see in Proposition 3.2 that if G is potentially p-realizable then it arises as a Galois group after some finite extension, conforming with the common usage of "potentially."

Remark 2.3. Since every p-group is nilpotent, the condition that G is potentially p-realizable implies that G is solvable. However, some groups G may have multiple tame structures. The simplest example is $G = C_2$ and p odd, where we can take $G_0 = G$ or $G_0 = 1$. An example with varying G_1 is $G = C_{p^2}$, where we can take $G_0 = G_1 = C_p$ or $G_0 = G_1 = 1$.

Proposition 2.4. *Any quotient of a potentially p-realizable group is potentially p-realizable.*

Proof. Suppose G has tame structure $G \supseteq G_0 \supseteq G_1$ and $N \trianglelefteq G$. It suffices to show that $G/N \supseteq G_0N/N \supseteq G_1N/N$ is a tame structure on G/N.

By the third isomorphism theorem, $(G/N)/(G_0N/N) \cong G/(G_0N)$ is a quotient of G/G_0 and thus cyclic, generated by the image of σ. The natural map

$$G_0 \to (G_0N/N)/(G_1N/N) \cong (G_0N)/(G_1N) \cong G_0/(G_1(G_0 \cap N))$$

has kernel containing G_1, showing that $(G_0N/N)/(G_1N/N)$ is cyclic and generated by the image of τ.

Since the relation $\tau^\sigma = \tau^p$ holds in G, it also holds for the images of σ and τ in G/N. Finally, $G_1N/N \cong G_1/(G_1 \cap N)$ is a p-group since G_1 is. □

If G is potentially realizable, the maximal choice for G_1 is the p-core V. We may always enlarge a tame structure on G to make $G_1 = V$:

Proposition 2.5. *If $G \supseteq G_0 \supseteq G_1$ is a tame structure on G, so is $G \supseteq G_0V \supseteq V$.*

Proof. Since G_0 and V are normal subgroups of G, so is G_0V. Moreover, $G/(G_0V)$ is a quotient of G/G_0 and thus cyclic generated by the same $\sigma \in G$. Since the order of G_0/G_1 is prime to p, $G_0 \cap V = G_1$ and the second isomorphism theorem implies that $(G_0V)/V \cong G_0/G_1$ with the image of τ still generating $(G_0V)/V$. □

Define $T = G/V$, the smallest possible tame quotient of G.

Conjecture 2.6. *If G is potentially p-realizable, then $G \cong V \rtimes T$.*

The conjecture holds for $p \in \{3, 5, 7, 11, 13\}$ and potentially p-realizable groups G with $|G| \leq 2000$. It also holds when T has order prime to p, by the Schur–Zassenhaus theorem. Note that we may not replace V with an arbitrary G_1, as the example of $C_{p^2} \supseteq C_p \supseteq C_p$ shows. Moreover, attempting to decompose the pieces further fails. The tame quotient T is not necessarily the semidirect product of G_0/G_1 by G/G_0: the quaternion group of order 8 is p-realizable for $p \equiv 3 \pmod 4$ but not a semidirect product of cyclic subgroups.

The conjecture has an interesting corollary for p-adic fields.

Corollary 2.7. *Assume Conjecture 2.6 holds, and suppose that $K/\mathbb{Q}_p$ is Galois. If $K_t/\mathbb{Q}_p$ is the maximal tamely ramified subextension of $K/\mathbb{Q}_p$ and $\mathrm{Gal}(K/K_t)$ is the p-core of $\mathrm{Gal}(K/\mathbb{Q}_p)$ then there is a totally wildly ramified complement $K_0/\mathbb{Q}_p$ with $K = K_0K_t$.*

2B. ***Enumerating small examples.*** The first step toward counting p-adic fields by Galois group is computing a list of potential G. Since GAP's database of small groups [2] can identify groups of order n for $n \leq 2000$ except $n = 512, 1024, 1536$, groups of these orders were screened.

When n is prime to p, we may use the classification of metacyclic groups [5, Lemma 2.1] to screen G. This process is described in Algorithm 1.

When n has p-adic valuation 1, we can build groups as extensions of metacyclic groups. Any group of order n will arise either as an extension of a group of order n/p by C_p, or as a metacyclic group

Algorithm 1: Finding potentially p-realizable groups: the tame case

Input : an integer n
Output : the list of potentially p-realizable groups of order n with trivial G_1

```
groups = [];
for positive k, m with n = k · m do
    if m divides p^k − 1 then
        step = m / gcd(m, p − 1);
        for ℓ from 0 to m by step do
            find the GAP id of ⟨x, y | x^k = y^ℓ, y^m = 1, y^x = y^p⟩;
            add id to groups if not present;
return sorted(groups);
```

Algorithm 2: Finding potentially p-realizable groups: valuation 1

Input : an integer n with $v_p(n) = 1$
Output : the list of potentially p-realizable groups of order n

```
groups = [];
foreach tame group T of order n/p do
    foreach homomorphism φ from T to Aut(C_p) do
        foreach group G in Extensions(T, φ) do
            if x and y lift to elements of G satisfying the tame relation then
                find the GAP id of G;
                add id to groups if not present;
foreach tame group T of order n do
    find the id of T;
    add id to groups if not present;
return sorted(groups);
```

produced by Algorithm 1. The extensions are computable using GAP's `Extensions` method, and we describe the process in Algorithm 2.

When n has larger p-adic valuation, this extension method becomes more complicated, since there are more possibilities for V. Moreover, some of the possible V are not elementary abelian p-groups, so GAP's `Extensions` method does not apply. While it would be possible to try to construct the extensions manually using GAP's `GrpConst` package [1], in practice it suffices to check whether each group in the small group database [2] with order n is potentially p-realizable using Algorithm 3 (see next page).

3. The absolute Galois group of a local field

Our approach to counting p-adic fields rests on the following description of the absolute Galois group of $\mathbb{Q}_p$. Let $p \neq 2$, k be a p-adic field, $N = [k : \mathbb{Q}_p]$, q be the cardinality of the residue field of k, and p^s be the order of the group of p-power roots of unity in the maximal tame extension k^t/k. Choose $g, h \in \mathbb{Z}_p$ with

$$\zeta^\sigma = \zeta^g, \zeta^\tau = \zeta^h \quad \text{for } \zeta \in \mu_{tr},$$

where $\sigma, \tau \in \mathrm{Gal}(k^t/k)$ with $\tau^\sigma = \tau^q$ as in [8], and μ_{tr} are the p-power roots of unity in k^t.

Let $\pi = \pi_p$ be the element of $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ with coordinate 1 in the $\mathbb{Z}_p$-component and 0 in the $\mathbb{Z}_\ell$ components for $\ell \neq p$. Then for x, y in a profinite group,[1] set

$$\langle x, y \rangle = (x^{h^{p-1}} y x^{h^{p-2}} y \cdots x^h y)^{\pi/(p-1)}.$$

Theorem 3.1 [13, Theorem 7.5.14]. *The absolute Galois group* $\mathrm{Gal}(\bar{k}/k)$ *is isomorphic to the profinite group generated by* $N + 3$ *generators* $\sigma, \tau, x_0, \ldots, x_N$, *subject to the following conditions and relations.*

(1) *The closed subgroup topologically generated by* $x_0, \ldots, x_N$ *is normal in* G *and is a pro-*p*-group.*

[1] See [15], especially Sections 3.3 and 4.1, for relevant background on profinite groups.

Algorithm 3: Determining whether a group is potentially p-realizable

Input : a group G
Output : whether or not G is potentially p-realizable

```
V = PCore(G);
T = G/ V;
if IsCyclic(T) then
    return True;
D = DerivedSubgroup(G);
if IsCyclic(D) then
    for N in NormalSubgroupsContaining(D) do
        if IsCyclic(N) and IsCyclic(G/N) then
            let e be the order of N and f the order of G/N;
            let a be the exponent in the conjugation action of G/N on N;
            find b with a^b ≡ p (mod e), or continue if not possible;
            let m be the order of a (mod e);
            if gcd(m, b, f) = 1 then
                return True;
return False;
```

(2) *The elements σ, τ satisfy the tame relation*

$$\tau^{\sigma} = \tau^{q}.$$

(3) *The generators satisfy the wild relation*

$$x_0^{\sigma} = \langle x_0, \tau\rangle^{g} x_1^{p^s}[x_1, x_2][x_3, x_4]\cdots[x_{N-1}, x_N] \quad \textit{if } N \textit{ is even},$$
$$x_0^{\sigma} = \langle x_0, \tau\rangle^{g} x_1^{p^s}[x_1, y_1][x_2, x_3]\cdots[x_{N-1}, x_N] \quad \textit{if } N \textit{ is odd};$$

here g and s are defined above and y_1 is an explicit element in the span of x_1, σ, and τ, specified below when $k = \mathbb{Q}_p$.

We will mostly be interested in the case where $k = \mathbb{Q}_p$; recall that we write $\mathcal{G}$ for $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Now $q = p$, $g = 1$ and h is a $(p-1)$-st root of unity in $\mathbb{Z}_p$. In order to define y_1, let $\mathbb{Q}_p^t$ be the maximal tamely ramified extension of $\mathbb{Q}_p$ and define $\beta : \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p) \to \mathbb{Z}_p^{\times}$ by setting $\beta(\sigma) = 1$ and $\beta(\tau) = h$. For ρ in the subgroup of $\mathcal{G}$ generated by σ and τ and $x \in \mathcal{G}$, set

$$\{x, \rho\} = (x\rho^2 x^{\beta(\rho)}\rho^2 \cdots x^{\beta(\rho^{p-2})}\rho^2)^{\pi/(p-1)}.$$

Let $\pi_2 \in \hat{\mathbb{Z}}$ be the element with $\pi_2\hat{\mathbb{Z}} = \mathbb{Z}_2$, and set $\tau_2 = \tau^{\pi_2}$ and $\sigma_2 = \sigma^{\pi_2}$. Set

$$y_1 = x_1^{\tau_2^{p+1}}\{x_1, \tau_2^{p+1}\}^{\sigma_2\tau_2^{(p-1)/2}}\left\{\{x_1, \tau_2^{p+1}\}, \sigma_2\tau_2^{(p-1)/2}\right\}^{\sigma_2\tau_2^{(p+1)/2}+\tau_2^{(p+1)/2}}. \tag{3}$$

The wild relation for $\mathbb{Q}_p$ then becomes

$$x_0^\sigma = \langle x_0, \tau \rangle x_1^p [x_1, y_1]. \tag{4}$$

We can use this description of absolute Galois groups to show that any potentially p-realizable group occurs as a Galois group over some k with $k/\mathbb{Q}_p$ finite.

Proposition 3.2. *If G is potentially p-realizable and V/W has dimension m then G will be realized over k if $[k : \mathbb{Q}_p] \geq 2m + 1$.*

Proof. It suffices to exhibit a surjective homomorphism $\mathrm{Gal}(\bar{k}/k) \to G$, which we define by specifying the images of the generators. Map $x_0, x_1, x_3, x_5, \ldots, x_{2m+1}$ and $x_{2m+2}, \ldots, x_N$ to 1. Then the wild relation is automatically satisfied, and we may freely choose the images of $x_2, \ldots, x_{2m}$. As long as we map them to elements of V that project to an $\mathbb{F}_p$-basis of V/W, Burnside's basis theorem implies that they will generate V. The fact that G is potentially p-realizable then implies that we may extend this homomorphism to a surjective map on all of $\mathrm{Gal}(\bar{k}/k)$. □

Note that one can decrease $2m + 1$ in some cases using the representation of T on V, and even then this bound is certainly not sharp.

4. Counting p-adic fields

4A. ***Parametrizing extensions.*** Following [20], we count the extensions of $\mathbb{Q}_p$ with Galois group G by counting the surjections $\mathcal{G} \to G$, modulo automorphisms of G. We can then translate the description of $\mathcal{G}$ from Theorem 3.1 to a counting problem in G. Let n be the order of G and factor $n = u_p p^r = u_2 2^s$ with $(u_p, p) = 1$ and u_2 odd. Using the Chinese remainder theorem, define integers a and b so that

$$a = 0 \pmod{u_p}, \qquad (p-1)a = 1 \pmod{p^r},$$
$$b = 0 \pmod{u_2}, \qquad b = 1 \pmod{2^s}.$$

Since the images of x_0 and x_1 have p-power order, they lie in V.

Definition 4.1. Define T_G to be the set of pairs $(\sigma, \tau) \in G^2$ so that

(1) $\tau^\sigma = \tau^p$,

(2) the images of σ and τ in G/V generate G/V.

Define X_G to be the set of quadruples $(\sigma, \tau, x_0, x_1) \in G^4$ satisfying the following properties:

(1) $\tau^\sigma = \tau^p$.

(2) $x_0, x_1 \in V$.

(3) σ, τ, x_0, x_1 generate G.

(4) $x_0^\sigma = \langle x_0, \tau \rangle x_1^p [x_1, y_1]$, where y_1 is defined as in (3).

Note that we may compute the projections $\pi/(p-1)$ and π_2 by raising to the a and b powers, respectively.

Proposition 4.2. *The Galois extensions of $\mathbb{Q}_p$ with Galois group G are in bijection with the orbits of X_G under the action of* $\mathrm{Aut}(G)$.

Proof. Finite extensions K of $\mathbb{Q}_p$ within a fixed algebraic closure of $\mathbb{Q}_p$ correspond to finite index subgroups H_K of $\mathcal{G}$. The condition that K is Galois with Galois group G translates to the condition that H_K is normal with $\mathcal{G}/H_K \cong G$. Different subgroups H cannot yield isomorphic K since an isomorphism of fields would extend to an automorphism of $\overline{\mathbb{Q}}_p$ conjugating one H to the other, which is impossible since both are normal. Finally, elements of X_G correspond to homomorphisms $\mathcal{G} \to G$ by the description of $\mathcal{G}$ in Theorem 3.1, and the kernel of such a homomorphism is preserved by composition with an automorphism of G. □

We will be inductively constructing representatives for the orbits of $\mathrm{Aut}(G)$ on X_G; write Y_G for a choice of such representatives. Then Y_G will be in bijection with the extensions of $\mathbb{Q}_p$ with Galois group G.

4B. ***Abelian groups.*** When G is abelian, the wild relation simplifies to $x_0 = x_1^p$. Thus x_0 is determined by x_1, and the wild relation imposes no constraint on x_1. The order of τ must divide $p-1$, the order of x_1 must be a power of p, and the three elements σ, τ, and x_1 must generate G.

Write

$$G \cong \prod_{\ell} \prod_{i=1}^{m_\ell} \mathbb{Z}/\ell^{n_{\ell,i}}\mathbb{Z}, \tag{5}$$

where $n_{\ell,1} \le \cdots \le n_{\ell,m_\ell}$ for each ℓ. We can enumerate the elements of X_G as a function of the $n_{\ell,i}$. Let α_ℓ be the element of G with a 1 in the $\ell,1$ component and 0s elsewhere, and let β_ℓ be the element with a 1 in the $\ell,2$ component and 0s elsewhere. Since we will be analyzing the ℓ-components separately, we drop ℓ from the notation, writing a for $n_{\ell,1}$, b for $n_{\ell,2}$, α for α_ℓ and β for β_ℓ.

(1) In the case $m_\ell \ge 3$, set $c_\ell = 0$ and $C_\ell = \{\}$.

(2) In the case $m_\ell = 2$, if $a \ne b$ and $\ell = p$, set $c_\ell = 2$ and $C_\ell = \{(\alpha, 0, p\beta, \beta), (\beta, 0, p\alpha, \alpha)\}$.

(3) In the case $m_\ell = 2$, if $a \ne b$ and ℓ^b divides $p-1$, set $c_\ell = 2$ and $C_\ell = \{(\alpha, \beta, 0, 0), (\beta, \alpha, 0, 0)\}$.

(4) In the case $m_\ell = 2$, if $a = b$ and $\ell = p$, set $c_\ell = 1$ and $C_\ell = \{(\alpha, 0, p\beta, \beta)\}$.

(5) In the case $m_\ell = 2$, if ℓ^a divides $p-1$ but case (3) does not apply, set $c_\ell = 1$ and $C_\ell = \{(\beta, \alpha, 0, 0)\}$.

(6) In the case $m_\ell = 2$, if $\ell \ne p$ and $\ell^a \nmid p-1$, set $c_\ell = 0$ and $C_\ell = \{\}$.

(7) In the case $m_\ell = 1$, if $\ell = p$, set $c_\ell = p^{a-1}(p+1)$ and

$$C_\ell = \{(\alpha, 0, pk\alpha, k\alpha) : 0 \le k < p^a\} \cup \{(pk\alpha, 0, p\alpha, \alpha) : 0 \le k < p^{a-1}\}.$$

(8) In the case $m_\ell = 1$, if ℓ^a divides $p-1$, set $c_\ell = \ell^{a-1}(\ell+1)$ and

$$C_\ell = \{(\alpha, k\alpha, 0, 0) : 0 \le k < \ell^a\} \cup \{(pk\alpha, \alpha, 0, 0) : 0 \le k < \ell^{a-1}\}.$$

(9) In the case $m_\ell = 1$, if ℓ^a does not divide $p-1$, set $c_\ell = \gcd(\ell^a, p-1)$ and

$$C_\ell = \left\{(\alpha, \frac{\ell^a}{c_\ell}k\alpha, 0, 0) : 0 \le k < c_\ell\right\}.$$

Proposition 4.3. *Let G be abelian, with elementary factors as in* (5)*. Then the number of Galois extensions $K/\mathbb{Q}_p$ with Galois group G is $\prod_\ell c_\ell$ and the set $\left\{\sum_\ell \eta_\ell : \eta_\ell \in C_\ell\right\}$ forms a set of representatives for the orbits of* $\mathrm{Aut}(G)$ *on X_G.*

Proof. The role of x_1 at p is almost the same as the role of τ away from p, except that the order of τ must divide $p-1$. For $\ell \neq p$, the ℓ-component of x_1 must be 0; the p-component of τ must be 0. Therefore, if any m_ℓ is at least 3, it is impossible for σ, τ and x_1 to generate G.

For $m_\ell = 2$, generating sets for $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$ are permuted transitively by $\mathrm{Aut}(G)$ [6, Theorem 3.6], and if $a = b$ then the two generators can be interchanged by an automorphism. When ℓ^b divides $p-1$ then τ can be taken as either generator, whereas if ℓ^a divides $p-1$ but ℓ^b does not then τ can only be the generator of order ℓ^a. If $\ell \neq p$ and ℓ^a does not divide $p-1$ then σ and τ cannot generate G.

When $m_\ell = 1$ then either σ or τ (or both) must be a generator. The descriptions of C_ℓ then follow from the fact that $\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. □

Remark 4.4. It is also possible to count abelian extensions using local class field theory, but the orbits on X_G are used in the lifting algorithm (Algorithm 5) of Section 4D.

4C. ***Tame groups.*** If G has order relatively prime to p, or more generally if V is trivial, then we must have $x_0 = x_1 = 1$. We search for elements of X_G by enumerating the normal subgroups that can contain τ, and then finding pairs (σ, τ) that satisfy the tame relation and generate G. We summarize the steps in Algorithm 4.

Algorithm 4: Enumerating extensions: tame case

Input : a group G with trivial p-core
Output : a list of pairs (σ, τ) representing the $\mathrm{Aut}(G)$-orbits in X_G

```
1  D = DerivedSubgroup(G);
2  pairs = [];
3  if IsCyclic(D) then
4      for N in NormalSubgroupsAbove(D) do
5          if IsCyclic(N) and IsCyclic(G/N) then
6              for s in G that induce p-th powering on N do
7                  for t in N that generate G along with s do
8                      if (s, t) not marked then
9                          append (s, t) to pairs;
10                         mark images of (s, t) under Aut(G);
11 return pairs;
```

4D. ***Lifting homomorphisms.*** For potentially p-realizable groups G that are neither tame nor abelian, we choose a minimal normal subgroup $N \triangleleft G$ (such an N always exists since G is solvable) and set $Q = G/N$. Inductively, we may assume that we have computed a list Y_Q of representatives for the orbits of $\mathrm{Aut}(Q)$ on X_Q. In particular, if Q is abelian or tame then we may use Section 4B or Algorithm 4; otherwise we will recursively use Algorithm 5, described below.

The idea is to just test all lifts of quadruples $(\sigma, \tau, x_0, x_1) \in Y_Q$ to see if they are valid elements of X_G. There is a subtlety however: there may be automorphisms of Q which are not induced by automorphisms of G. This problem comes in two parts. First, if N is not a characteristic subgroup then it may not be stabilized by all of $\mathrm{Aut}(G)$, so not all automorphisms descend. Second, the map $\mathrm{Stab}_{\mathrm{Aut}(G)}(N) \to \mathrm{Aut}(Q)$ is not necessarily surjective, so elements of X_Q that are equivalent under $\mathrm{Aut}(Q)$ may lift to elements that are inequivalent under $\mathrm{Aut}(G)$.

We solve the problem by computing a list of coset representatives for the image of $\mathrm{Stab}_{\mathrm{Aut}(G)}(N) \to \mathrm{Aut}(Q)$. Then, instead of just lifting elements of Y_Q, we lift all translates under these automorphisms. We summarize this process in Algorithm 5.

The runtime of Algorithm 5 depends on the structure of G. If $N \triangleleft G$ is the minimal normal subgroup used, C is the list of coset representatives in $\mathrm{Aut}(Q)$, Y_Q is the list of representatives for the quotient Q, and R is the time it takes to compute the wild relation, then the runtime is bounded by $O(|C| \cdot |Y_Q| \cdot |N|^4 R)$. The actual runtime may be better for some N since we can short circuit some of the loops if the lifts of (x_1, x_0, τ, σ) do not satisfy the appropriate conditions.

Algorithm 5: Enumerating extensions: lifting method

Input : a potentially p-realizable group G and lists of representatives Y_Q for quotients Q of G
Output : a list Y_G of quadruples (σ, τ, x_0, x_1) representing the $\mathrm{Aut}(G)$-orbits in X_G.

```
choose a minimal normal subgroup N ◁ G;
Set Q = G/N;
compute the stabilizer A of N in Aut(G);
compute a list cokreps of representatives for the cosets of the image of A in Aut(Q);
Xreps = [];
foreach (σ, τ, x_0, x_1) ∈ Y_Q do
    foreach α ∈ cokreps do
        foreach lift x_1 of α(x_0) to G that lies in V do
            foreach lift x_0 of α(x_1) to G that lies in V do
                foreach lift τ of α(τ) to G with order prime to p do
                    foreach lift σ of α(σ_0) with τ^σ = τ^p do
                        if (σ, τ, x_0, x_1) not marked then
                            mark images of (σ, τ, x_0, x_1) under Aut(G);
                            if σ, τ, x_0, x_1 generate G then
                                append (σ, τ, x_0, x_1) to Xreps;
return Xreps;
```

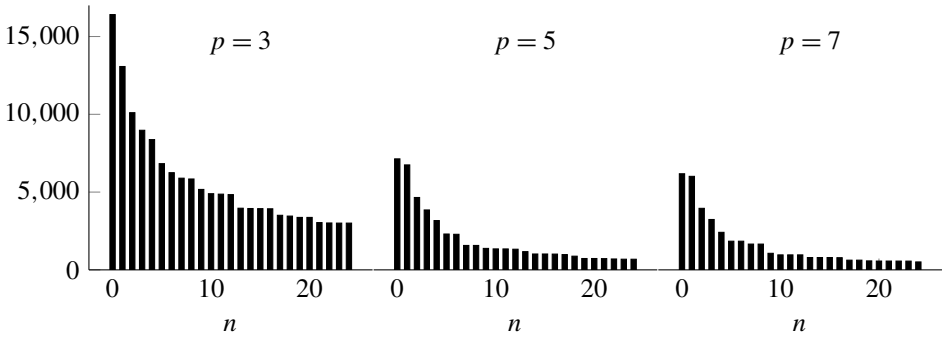


Figure 1. Number of potentially p-realizable G with $|G| \le 2000$ and $|Y_G| \ge n$.

Running Algorithm 5 on groups of order up to 2000 for p up to 13 required a few weeks of CPU time. The largest counts found occurred for cyclic groups such as $C_{1458} : p = 3$ (2916) and $C_{1210} : p = 11$ (2376), or for products of cyclic groups with small nonabelian groups such as $C_{243} \times S_3 : p = 3$ (1944). For $p = 3$, other nonabelian groups had large counts such as 1458G553: $(C_{27} \rtimes C_{27}) \rtimes C_2$ (1323) suggesting that the dominance of cyclic groups may not last as the order increases.

Figure 1 shows these counts in aggregate, ignoring the group structure. Specifically, recall that Y_G is in bijection with the set of Galois extensions of $\mathbb{Q}_p$ with Galois group G. Figure 1 plots the function $f(n)$ that counts the number of potentially realizable G with $|G| \le 2000$ and $|Y_G| \ge n$. The difference between the first and second bars in each chart gives the number of groups that are potentially p-realizable but not actually p-realizable. We have truncated the charts at 25 since they have long tails; the previous paragraph gives examples of G with large $|Y_G|$.

We have no theoretical results on the possible sizes of N and C, but experimental results are summarized in Tables 1 and 2. The first shows the number of G that have a specified minimum size of N, and the second shows the number of pairs (G, N) with a specified size of C, called the *automorphism index*.

Large indices did occur, but rarely. There were 20 cases of index larger than 10000 for $p = 3$, the largest being 4586868. For $p = 5$, the only index larger than 124 was 3100, occurring 3 times; for other p no index larger than 120 occurred.

	number of groups whose N has the given size				
size	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$
2	8765	2437	1419	638	588
3	3800	423	228	104	110
5	27	392	70	26	45
7	10	6	168	11	18
9	87	0	0	0	0
11	0	3	0	56	7
13	0	3	0	0	68
> 13	9	17	12	12	2

Table 1. Smallest $N \triangleleft G$ for nonabelian, nontame G.

	number of $N \triangleleft G$ with given automorphism index				
index	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
1	8594	2393	1210	561	663
2	1798	594	421	111	117
3	468	24	73	25	19
4	396	157	59	107	17
5	0	7	0	4	0
6	333	10	58	0	6
8	217	42	47	17	13
9	91	0	4	0	0
10	2	0	0	0	0
12	153	7	4	7	1
13	21	0	0	0	0
16	37	0	8	0	1
18	61	0	2	0	0
20	0	4	0	1	0
24	99	30	4	12	1
> 24	428	12	7	2	0

Table 2. Automorphism index for nonabelian, nontame G.

5. The inverse Galois problem for p-adic fields

5A. ***Examples of nonrealizable groups.*** Recall that G is *p-realizable* if there exists an extension $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. If G is p-realizable, then every quotient of G is as well, leading us to consider the following class of groups.

Definition 5.1. A group G is *minimally unrealizable* if G is not p-realizable but it is potentially p-realizable and every proper quotient of G is p-realizable.

In Table 3 we list the minimally unrealizable G that have abelian p-core. The label is from the GAP SmallGroups library, which makes precise the description of the group; we write $\mathbb{F}_p^n$ for C_p^n to emphasize the vector space structure. The column V describes the decomposition of V into indecomposable submodules: n^k refers to a submodule of dimension n occurring with multiplicity k. The columns SS, TD, and XC will be described in Section 5B.

5B. ***Realizability criteria.*** We may explain many of the groups in Table 3 by considering V/W as a representation of $T = G/V$ on an $\mathbb{F}_p$-vector space. Note that $|T|$ may be divisible by p: this will occur precisely when there is more than one p-Sylow subgroup in G. In this case V/W may not have a decomposition as a direct sum of irreducible subrepresentations, but it still has a decomposition as a direct sum of indecomposable subrepresentations. The multiplicity of an indecomposable factor is the number of times it appears in such a representation.

Recall from Definition 4.1 that T_G is the set of pairs $(\sigma, \tau) \in G^2$ generating G/V and satisfying the tame relation. In order to show that a potentially p-realizable group G is not p-realizable, we will show that any possible $(\sigma, \tau, x_0, x_1) \in X_G$ that satisfy the tame and wild relations cannot generate G. We will

p	label	description	V	SS	TD	XC
3	27G5	$\mathbb{F}_3^3$	1^3	N	Y	Y
3	36G7	$\mathbb{F}_3^2 \rtimes C_4$	1^2	Y	Y	Y
3	54G14	$\mathbb{F}_3^3 \rtimes C_2$	1^3	Y	N	N
3	72G33	$\mathbb{F}_3^2 \rtimes D_8$	1^2	Y	Y	Y
3	162G16	$C_9^2 \rtimes C_2$	1^2	Y	N	N
3	324G164	$\mathbb{F}_3^4 \rtimes C_4$	2^2	Y	N	Y
3	324G169	$\mathbb{F}_3^4 \rtimes (C_2 \times C_2)$	$1^2 \oplus 1^2$	Y	N	N
3	378G51	$\mathbb{F}_3^2 \rtimes (C_7 \rtimes C_6)$	1^2	Y	Y	Y
3	648G711	$\mathbb{F}_3^4 \rtimes C_8$	2^2	Y	N	Y
5	50G4	$\mathbb{F}_5^2 \rtimes C_2$	1^2	Y	Y	Y
5	125G5	$\mathbb{F}_5^3$	1^3	N	Y	Y
5	200G20	$\mathbb{F}_5^2 \rtimes C_8$	1^2	Y	Y	Y
5	300G34	$\mathbb{F}_5^2 \rtimes (C_3 \rtimes C_4)$	1^2	Y	Y	Y
5	400G149	$\mathbb{F}_5^2 \rtimes (C_8 \times C_2)$	1^2	Y	Y	Y
5	500G48	$\mathbb{F}_5^3 \rtimes C_4$	1^3	Y	N	Y
5	1300G29	$\mathbb{F}_5^2 \rtimes (C_{13} \rtimes C_4)$	1^2	Y	Y	Y
5	1300G30	$\mathbb{F}_5^2 \rtimes (C_{13} \rtimes C_4)$	1^2	Y	Y	Y
5	1875G21	$\mathbb{F}_5^4 \rtimes C_3$	2^2	Y	Y	Y
7	98G4	$\mathbb{F}_7^2 \rtimes C_2$	1^2	Y	Y	Y
7	147G4	$\mathbb{F}_7^2 \rtimes C_3$	1^2	Y	Y	Y
7	343G5	$\mathbb{F}_7^3$	1^3	N	Y	Y
7	588G22	$\mathbb{F}_7^2 \rtimes C_{12}$	1^2	Y	Y	Y
7	882G23	$\mathbb{F}_7^2 \rtimes C_{18}$	1^2	Y	Y	Y
7	1176G130	$\mathbb{F}_7^2 \rtimes (C_3 \times D_8)$	1^2	Y	Y	Y
11	242G4	$\mathbb{F}_{11}^2 \rtimes C_2$	1^2	Y	Y	Y
11	605G4	$\mathbb{F}_{11}^2 \rtimes C_5$	1^2	Y	Y	Y
11	1331G5	$\mathbb{F}_{11}^3$	1^3	N	Y	Y
13	338G4	$\mathbb{F}_{13}^2 \rtimes C_2$	1^2	Y	Y	Y
13	507G4	$\mathbb{F}_{13}^2 \rtimes C_3$	1^2	Y	Y	Y
13	676G10	$\mathbb{F}_{13}^2 \rtimes C_4$	1^2	Y	Y	Y
13	1014G9	$\mathbb{F}_{13}^2 \rtimes C_6$	1^2	Y	Y	Y

Table 3. Minimally unrealizable groups with abelian p-core.

say that G is *strongly split* (SS) if, for every $(\sigma, \tau) \in T_G$, the order of σ in G equals the order of its image in G/V. Note that Conjecture 2.6 would imply that there is some σ with the same order in G as in G/V, but some lifts of σ from G/V to G may have larger order.

We will say that G is *tame-decoupled* (TD) if τ acts trivially on V/W for every $(\sigma, \tau) \in T_G$. Finally, we will say that G is x_0-*constrained* (XC) if the implication

$$x_0^\sigma \langle x_0, \tau \rangle^{-1} \in W \Rightarrow x_0 \in W$$

holds for all $(\sigma, \tau) \in T_G$. The last three columns of Table 3 record whether G is strongly split, tame-decoupled and x_0-constrained, respectively.

Proposition 5.2. *If G is tame-decoupled then it is x_0-constrained.*

Proof. Each condition holds for G if and only if it holds for G/W, so we may assume that V is an elementary abelian p-group and $W = 1$. Since every τ acts trivially on V by conjugation and h is a $(p-1)$-st root of unity,

$$\langle x_0, \tau\rangle = (x_0^{1+h+\cdots+h^{p-2}}\tau^{p-1})^{\pi/(p-1)} = \tau^{\pi} = 1.$$

So if $x_0^{\sigma}\langle x_0, \tau\rangle^{-1} = 1$ then $x_0^{\sigma} = 1$ and thus $x_0 = 1$. □

Let $n_{G,\mathrm{ss}}$ be 0 if G is strongly split and 1 otherwise; let $n_{G,\mathrm{xc}}$ be 0 if G is x_0-constrained and 1 otherwise.

Theorem 5.3. *Suppose G is potentially p-realizable. Let n be the largest multiplicity of an indecomposable factor of V/W as a representation of T. If $n > 1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$, then G is not p-realizable.*

Proof. We first reduce to the case where $W = 1$. This is easily done, since the definitions of n, $n_{G,\mathrm{ss}}$ and $n_{G,\mathrm{xc}}$ are invariant under quotienting by W, and if we can show that G/W is not p-realizable then G will be unrealizable as well. We may therefore replace V by V/W and assume that V is an elementary abelian p-group.

For sake of contradiction, suppose that G is p-realizable, with $(\sigma, \tau, x_0, x_1) \in X_G$. Suppose that we have an arbitrary word in these generators, and assume that the word is an element of V. Using the conjugation action of T on V and the tame relation, we may rewrite it as $\sigma^c\tau^d x$, where x is a product of conjugates of x_0 and x_1 under the action of T. Thus $\sigma^c\tau^d \in V$, so we may use the fact that τ has order prime to p to rewrite $\sigma^c\tau^d$ as $\sigma^{c'} \in V$. If G is strongly split then we must have $\sigma^{c'} = 1$; otherwise it could be some nonzero element of V.

Since V is an elementary abelian p-group, the wild relation (4) simplifies to

$$x_0^{\sigma}\langle x_0, \tau\rangle^{-1} = 1. \tag{6}$$

If G is x_0-constrained, we must have $x_0 = 1$; otherwise x_0 can be nontrivial.

Since x_1 is unconstrained, we can write any word in terms of a fixed set of $1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$ elements of V, where we are allowed to act on these elements by T. Let A be a homogeneous component of V with multiplicity n, and consider the projections of our $1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$ elements onto A. Their $\mathbb{F}_p[T]$-span is a proper subspace of A since A has multiplicity $n > 1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$, contradicting the assumption that (σ, τ, x_0, x_1) generate G. □

We can get a partial converse, but we now need to assume that $W = 1$.

Theorem 5.4. *Suppose that G is potentially p-realizable with $W = 1$, and that V decomposes as a multiplicity-free direct sum of irreducible T-submodules. Then G is p-realizable.*

Proof. It suffices to construct an element of X_G. Since V is an elementary abelian p-group, we again have the relation (6), which is satisfied for $x_0 = 1$ and arbitrary x_1. Since G is potentially p-realizable, by Proposition 2.5 there are $\sigma, \tau \in G$ satisfying the tame relation and generating G/V. Choose $x_1 \in V$ with nonzero projection onto each irreducible component. The conjugates of x_1 under T generate V, since if they were contained in a proper subspace that subspace would have zero projection onto some

p	label	description	G/W	V/W
3	486G146	$(\mathbb{F}_3^4 \rtimes C_3) \rtimes C_2$	54G13	$1^2 \oplus 1$
3	648G218	$(C_{27} \rtimes C_3) \times D_8$	72G37	1^2
3	648G219	$(\mathbb{F}_3^3 \rtimes C_3) \times D_8$	72G37	1^2
3	648G220	$((C_9 \times C_3) \rtimes C_3) \times D_8$	72G37	1^2
3	648G221	$((C_9 \times C_3) \rtimes C_3) \times D_8$	72G37	1^2
3	972G816	$(\mathbb{F}_3^2 \times (\mathbb{F}_3^2 \rtimes C_3)) \rtimes (C_2^2)$	324G170	$1^2 \oplus 1 \oplus 1$
3	1458G613	$((C_{81} \times C_3) \rtimes C_3) \rtimes C_2$	18G4	1^2
3	1458G640	$(C_9^2 \rtimes C_9) \rtimes C_2$	18G4	1^2

Table 4. Minimally unrealizable groups with nonabelian p-core.

irreducible component, contradicting the choice of x_1. Now the fact that σ and τ generate G/V means that x_1, σ and τ generate G. □

Remark 5.5. There are two groups in Table 3 that are not explained by Theorem 5.3. For 324G169, there are nonzero x_0 satisfying (6), but they all lie in a 1-dimensional indecomposable subrepresentation. The other subrepresentation can't be spanned by x_1 on its own. For 162G16, the quotient by W is p-realizable. Here V is abelian but has exponent 9 rather than 3, so the wild relation takes the form

$$x_0^{\sigma} \langle x_0, \tau \rangle^{-1} = x_1^p. \tag{7}$$

In order to get a nontrivial x_1, we need to find x_0 with $x_0^{\sigma} \langle x_0, \tau \rangle^{-1}$ of order 3. Such x_0 exist, but they all have the property that $x_0^{\sigma} \langle x_0, \tau \rangle^{-1}$ is a multiple of x_0, preventing x_1 from spanning the rest of V.

Remark 5.6. Table 4 gives the groups of order up to 2000 with nonabelian V that are minimally unrealizable. In each case, G/W will be p-realizable, so the methods of this section do not apply. In order to provide an explanation for why they are not p-realizable, one would need to analyze the wild relation more thoroughly.

References

[1] Hans Ulrich Besche and Bettina Eick, GAP: *GrpConst - constructing the groups of a given order, version 2.5*, software package, 2015.

[2] Hans Ulrich Besche, Bettina Eick, and Eamonn O'Brien, GAP: *the SmallGroups library*, software package, 2002.

[3] The GAP group, *GAP – Groups, Algorithms, and Programming*.

[4] Helmut Hasse, *Number theory*, Grundlehren der Mathematischen Wissenschaften, no. 229, Springer, 1980. MR 562104

[5] C. E. Hempel, *Metacyclic groups*, Comm. Algebra **28** (2000), no. 8, 3865–3897. MR 1767595

[6] Christopher J. Hillar and Darren L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. 10, 917–923. MR 2363058

[7] Xiang-Dong Hou and Kevin Keating, *Enumeration of isomorphism classes of extensions of p-adic fields*, J. Number Theory **104** (2004), no. 1, 14–61. MR 2021625

[8] Kenkichi Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. **80** (1955), 448–469. MR 0075239

[9] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887

[10] Marc Krasner, *Nombre des extensions d'un degré donné d'un corps* $\mathfrak{p}$*-adique*, Les Tendances Géom. en Algèbre et Théorie des Nombres, Editions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 143–169. MR 0225756

[11] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer, 1999. MR 1711577

[12] Maurizio Monge, *Determination of the number of isomorphism classes of extensions of a* $\mathfrak{p}$*-adic field*, J. Number Theory **131** (2011), no. 8, 1429–1434. MR 2793885

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, no. 323, Springer, 2008. MR 2392026

[14] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a* p*-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659. MR 1836924

[15] Luis Ribes and Pavel Zalesskii, *Profinite groups*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, no. 40, Springer, 2010. MR 2599132

[16] The Sage Development Team, *SageMath, the Sage Mathematics Software System*, 2005-2013.

[17] Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 22, A1031–A1036. MR 500361

[18] I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 525–578. MR 0071469

[19] I. Shafarevitch, *On* p*-extensions*, Rec. Math. N.S. **20(62)** (1947), 351–363. MR 0020546

[20] Masakazu Yamagishi, *On the number of Galois* p*-extensions of a local field*, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2373–2380. MR 1264832

Received 2 Mar 2018. Revised 17 Jun 2018.

DAVID ROE: roed@mit.edu
Department of Mathematics, MIT, Cambridge, MA, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine