# The inverse Galois problem for p-adic fields

David Roe

Department of Mathematics
Massachusetts Institute of Technology

September 10, 2019

# Inverse Galois Problem

- Classic Problem: determine if a finite $G$ is a Galois group.
- Depends on base field: every $G$ is a Galois group over $\mathbb{C}(t)$.
- Most work focused on $L/\mathbb{Q}$: $S_n$ and $A_n$, every solvable group, every sporadic group except possibly $M_{23}, \ldots$
- Generic polynomials $f_G(t_1, \ldots, t_r, X)$ are known for some $(G, K)$: every $L/K$ with group $G$ is a specialization.

## Computational Problems

Given a finite group $G$, find algorithms for

1. Existence problem: exist $L/\mathbb{Q}_p$ with Gal$(L/\mathbb{Q}_p) \cong G$?
2. Counting problem: how many such $L$ exist (always finite)?
3. Enumeration problem: list the $L$.

# Ramification Groups

Suppose

- $L/K$ is an extension of $p$-adic fields, $G = \mathrm{Gal}(L/K)$,
- $\pi$ is a uniformizer of $L$,
- $G_i = \{\sigma \in G : v_L(\sigma(x) - x) \geq i + 1 \forall x \in \mathcal{O}_L\}$ for $i \geq -1$,
- $U_L^{(0)} = \mathcal{O}_L^\times$ and $U_L^{(i)} = 1 + \pi^i \mathcal{O}_L$ for $i \geq 1$.

**Proposition ([2, Prop. IV.2.7])**

*For $i \geq 0$, the map $\theta_i : G_i/G_{i+1} \to U_L^{(i)}/U_L^{(i+1)}$ defined by $\theta_i(\sigma) = \sigma(\pi)/\pi$ is injective and independent of $\pi$.*

**Corollary**

- *$G/G_0$ is cyclic,*
- *$G_0/G_1$ is cyclic of order prime to $p$,*
- *$G_i/G_{i+1}$ is an elementary abelian $p$-group for $i \geq 1$.*

# $p$-realizable groups

## Definition

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, generated by some $\tau \in G_0$,
4. $\tau^\sigma = \tau^p$,
5. $G_1$ is a $p$-group.

It is *$p$-realizable* if there exists $L/\mathbb{Q}_p$ with $\text{Gal}(L/\mathbb{Q}_p) \cong G$.
It is *minimally unrealizable* if it is not $p$-realizable, but every proper quotient is.

# Counting for $p$-groups

When $G$ is a $p$-group, complete answer available. Suppose $K/\mathbb{Q}_p$ has degree $n$ and $K \not\supset \mu_p$.

**Theorem ([3])**

*The maximal pro-$p$ quotient of* Gal$(K)$ *is a free pro-$p$ group on $n+1$ generators.*

**Corollary**

*If $G$ is a $p$-group generated by $d$ elements (minimally), the number of extensions $L/K$ with Galois group $G$ is*

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

# Criterion for $p$-groups

We get an easy condition on when a $p$-group is $p$-realizable. Let $W = G^p G'$ be the Frattini subgroup; $G/W$ is the maximal elementary abelian quotient of $G$. A set of elements generates $G$ if and only if its projection onto $G/W$ spans $G/W$ as an $\mathbb{F}_p$-vector space.

**Corollary**

*If $p > 2$ and $G$ is a $p$-group then $G$ is $p$-realizable if and only if $G/W$ has dimension less than $3$.*

# Presentation of the absolute Galois group

For $p > 2$, Gal$(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the profinite group generated by $\sigma, \tau, x_0, x_1$ with $x_0, x_1$ pro-$p$ and the following relations (see [1])

$$\tau^\sigma = \tau^p$$

$$\langle x_0, \tau\rangle^{-1} x_0^\sigma = x_1^p \Big[ x_1, x_1^{\tau_2^{p+1}} \left\{x_1, \tau_2^{p+1}\right\}^{\sigma_2 \tau_2^{(p-1)/2}} \left\{\left\{x_1, \tau_2^{p+1}\right\}, \sigma_2 \tau_2^{(p-1)/2}\right\}^{\sigma_2 \tau_2^{(p+1)/2} + \tau_2^{(p+1)/2}} \Big]$$

---

$h \in \mathbb{Z}_p$ with mult. order $p-1$, $\quad$ $\mathrm{proj}_p : \hat{\mathbb{Z}} \to \mathbb{Z}_p$

$$\langle x_0, \tau\rangle := (x_0 \tau x_0^{h^{p-2}} \tau \ldots x_0^h \tau)^{\mathrm{proj}_p/(p-1)}$$

$$\beta : \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p) \to \mathbb{Z}_p^\times \qquad \beta(\tau) = h \qquad \beta(\sigma) = 1$$

$$\{x, \rho\} := (x^{\beta(1)} \rho^2 x^{\beta(\rho)} \rho^2 \ldots x^{\beta(\rho^{p-2})} \rho^2)^{\mathrm{proj}_p/(p-1)}$$

$$\sigma_2 := \mathrm{proj}_2(\sigma) \qquad \tau_2 := \mathrm{proj}_2(\tau)$$

# Counting in general

By the Galois correspondence, Galois extensions of $\mathbb{Q}_p$ correspond to finite index normal subgroups of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Thus the number of extensions $L/\mathbb{Q}_p$ with $\mathrm{Gal}(L/\mathbb{Q}_p) \cong G$ is

$$\frac{1}{\#\,\mathrm{Aut}(G)} \# \left\{ \varphi : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \twoheadrightarrow G \right\}$$

So we count the tuples $\sigma, \tau, x_0, x_1 \in G$ (up to automorphism) that

1. satisfy the relations from $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$,
2. generate $G$.

## Basic Strategy

Loop over $\sigma$ generating the unramified quotient and $\tau$ generating the tame inertia (with $\tau^\sigma = \tau^p$). For each such $(\sigma, \tau)$ up to automorphism, count the valid $x_0, x_1$.

# Iterative approach

Counting for many $G$, so we can build up from quotients.

**Iterative Strategy**

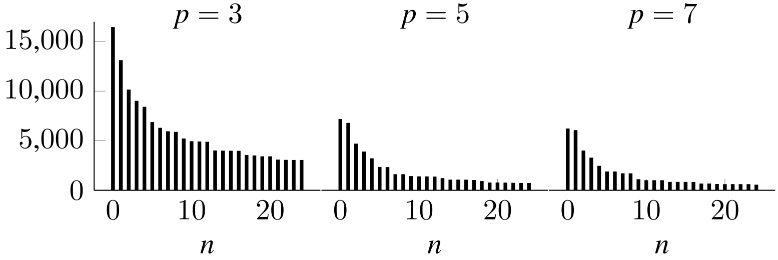
- Pick a minimal normal subgroup $N \triangleleft G$, then try to lift $(\sigma, \tau, x_0, x_1)$ from $G/N$ to $G$.
- Tame $G$ form a base case.

Two subtleties.

- If $N$ is not characteristic, it will not be preserved by Aut$(G)$ so not all automorphisms descend;
- The map $\mathrm{Stab}_{\mathrm{Aut}(G)}(N) \to \mathrm{Aut}(G/N)$ may not be surjective, so equivalent quadruples may become inequivalent.

# Counts

Potentially $p$-realizable $G$ with the count of $L/\mathbb{Q}_p$ at least $n$.




The largest counts occurred for cyclic groups or products of large cyclic groups with small nonabelian groups:

- $C_{1458}$ ($p = 3$) with $2916$,
- $C_{1210}$ ($p = 11$) with $2376$,
- $C_{243} \times S_3$ ($p = 3$) with $1944$.

But also 1458G553, $(C_{27} \rtimes C_{27}) \rtimes C_2$ ($p = 3$) with $1323$.

# Realizability Criteria

Given potentially $p$-realizable $G$, let $V$ be it's $p$-core and $W = V^p V'$. Then $V/W$ is an $\mathbb{F}_p$ vector space with action of $G/V$. Let $T_G$ be the set of pairs $(\sigma, \tau) \in G^2$ generating $G/V$ and satisfying $\tau^\sigma = \tau^p$.

**Definition**

$G$ is *strongly-split* if $\mathrm{ord}_G(\sigma) = \mathrm{ord}_{G/V}(\sigma)$ for all $(\sigma, \tau) \in T_G$.
$G$ is *tame-decoupled* if $\tau$ acts trivially on $V/W$ for all $(\sigma, \tau) \in T_G$.
$G$ is $x_0$-*constrained* if $x_0^\sigma \langle x_0, \tau \rangle^{-1} \in W \Rightarrow x_0 \in W$ for all $(\sigma, \tau) \in T_G$.

Set $n_{G,ss} = 0$ if strongly-split, $1$ o/w; $n_{G,xc} = 0$ if $x_0$-constrained, $1$ o/w.

**Theorem**

*Let $n$ be the largest multiplicity of an indecomposable factor of $V/W$.*

- *If $G$ is tame-decoupled then it is $x_0$-constrained.*
- *If $n > 1 + n_{G,ss} + n_{G,xc}$ then $G$ is not $p$-realizable.*
- *If $W = 1$ and $V$ is a sum of distinct irreducibles, $G$ is $p$-realizable.*

# Minimally unrealizable $G$ with abelian $V$, $p = 3$

| Label | Description | $V$ | SS | TD | XC | $1 + n_{G,ss} + n_{G,xc}$ |
|---|---|---|---|---|---|---|
| 27G5 | $\mathbb{F}_3^3$ | $1^3$ | N | Y | Y | 2 |
| 36G7 | $\mathbb{F}_3^2 \rtimes C_4$ | $1^2$ | Y | Y | Y | 1 |
| 54G14 | $\mathbb{F}_3^3 \rtimes C_2$ | $1^3$ | Y | N | N | 2 |
| 72G33 | $\mathbb{F}_3^2 \rtimes D_8$ | $1^2$ | Y | Y | Y | 1 |
| 162G16 | $C_9^2 \rtimes C_2$ | $1^2$ | Y | N | N | 2 |
| 324G164 | $\mathbb{F}_3^4 \rtimes C_4$ | $2^2$ | Y | N | Y | 1 |
| 324G169 | $\mathbb{F}_3^4 \rtimes (C_2 \times C_2)$ | $1^2 \oplus 1^2$ | Y | N | N | 2 |
| 378G51 | $\mathbb{F}_3^2 \rtimes (C_7 \rtimes C_6)$ | $1^2$ | Y | Y | Y | 1 |
| 648G711 | $\mathbb{F}_3^4 \rtimes C_8$ | $2^2$ | Y | N | Y | 1 |

# 162G16 and 324G169

There are two instances not explained by the theorem.

- For 324G169, $V \cong 1^2 \oplus 1^2$. There are nontrivial $x_0$ satisfying $x_0^\sigma \langle x_0, \tau \rangle^{-1} = 1$, 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

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

  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 $V$.

# Minimally unrealizable $G$ with nonabelian $V$, $p = 3$

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

# Sketch for $G$ not $p$-realizable

**Proof.**

To prove that $G$ is not $p$-realizable, we show that a map $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to G$ cannot possibly be surjective. In any attempt at surjectivity, we need to choose $(\sigma, \tau) \in T_G$. Having done so, we must generate all of $V$, which is equivalent to generating $V/W$. There are only three ways to produce elements of $V$: the image of $x_0$, the image of $x_1$ and a power of $\sigma$. When $G$ is $x_0$-constrained, $x_0$ must map to $0 \in V/W$. When $G$ is strongly split, every power of $\sigma$ lying in $V$ also lies in $W$. So there are $1 + n_{G,ss} + n_{G,xc}$ generators available.

The action of $G/V$ on $V/W$ spreads out these generators: we can get anything in the $G/V$ submodule spanned by them. But when $n > 1 + n_{G,ss} + n_{G,xc}$, this submodule can't possibly be everything. □

# Sketch for $G$ $p$-realizable

**Proof.**

We show that when $W = 1$ and $V$ is a sum of distinct irreducibles, then $G$ is $p$-realizable. In this case, the relations simplify and we can just choose to map $x_0$ to $1$ and $x_1$ to an element projecting nontrivially on each irreducible $G/V$-submodule of $V$. The resulting homomorphism is surjective. □

# References


[1] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of number fields*. Springer, Berlin, 2015, pg 419.

[2] J.-P. Serre. *Local fields*. Springer, Berlin, 1979, pg 67.

[3] I. Shafarevich. *On $p$-extensions*. Mat. Sb. **20** (1947), no. 62, 351–363.