The inverse Galois problem for p-adic fields

David Roe

Department of Mathematics
University of Pittsburgh

November 13, 2017
Outline

1. Counting Problem
2. Enumeration Problem
3. Algebraic Tori
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 $\text{Gal}(L/\mathbb{Q}_p) \cong G$?
2. Counting problem: how many such $L$ exist (always finite)?
3. Enumeration problem: list the $L$. 
If $L/K$ is an extension of $p$-adic fields, it decomposes:

$\begin{align*}
L & \\
\mid & \text{wild} \\
L_t & \\
\mid & \text{tame} \\
L_u & \\
\mid & \text{unram} \\
K &
\end{align*}$

- **Wild** – totally ramified, degree a power of $p$.
- **Tame** – totally ramified, degree relatively prime to $p$. Have $L_t = L_u(\sqrt[p]{\pi})$ for some uniformizer $\pi \in L_u$.
- **Unramified** – there is a unique unramified extension of each degree: equivalence of categories with extensions of the residue field.
Filtrations of $p$-adic Galois groups

The splitting of $L/K$ into unramified, tame and wild pieces induces a filtration on $\text{Gal}(L/K)$. We can refine this filtration to

$$G \supset G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = 1.$$ 

- For every $i$, $G_i \trianglelefteq G$;
- $G/G_0 = \langle \sigma \rangle$ is cyclic, and $L^{G_0} = L_u$;
- $G_0/G_1 = \langle \tau \rangle$ is cyclic, order prime to $p$ and $\sigma^{-1}\tau \sigma = \tau^q$;
- For $0 < i < r$, $G_i/G_{i+1} \cong \mathbb{F}_p^{k_i}$.

Necessary condition: $G$ must be solvable with such a filtration.
Absolute Galois groups

In the projective limit, get a tower of infinite extensions:

\[ \overline{K} \]

\[ K^t \] \hspace{1cm} \text{wild}

\[ K^u \] \hspace{1cm} \text{tame}

\[ K \] \hspace{1cm} \text{unram}

\[ \text{Gal}(K^u/K) = \langle \sigma \rangle \cong \hat{\mathbb{Z}} \]

\[ \text{Gal}(K^t/K^u) = \langle \tau \rangle \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \]

\[ \sigma^{-1} \tau \sigma = \tau^\ell \]

\[ \text{Gal}(\overline{K}/K^t) \text{ is pro-} p. \]
Presentation of the absolute Galois group

For \( p > 2 \), \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \) is the profinite group generated by \( \sigma, \tau, x_0, x_1 \) with \( x_0, x_1 \) pro-\( p \) and the following relations (see [7])

\[
\tau^\sigma = \tau^p
\]

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

\[
\left\{ \left\{ x_1, \tau^{p+1} \right\}, \sigma_2 \tau_2^{(p-1)/2} \right\}^{\sigma_2 \tau_2^{(p+1)/2} + \tau_2^{(p+1)/2}}
\]

\( h \in \mathbb{Z}_p \) with mult. order \( p - 1 \), \( \text{proj}_p : \hat{\mathbb{Z}} \to \mathbb{Z}_p \)

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

\[
\beta : \text{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p) \to \mathbb{Z}_p^\times \quad \beta(\tau) = h \quad \beta(\sigma) = 1
\]

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

\[
\sigma_2 := \text{proj}_2(\sigma) \quad \tau_2 := \text{proj}_2(\tau)
\]
The number of extensions $L/Q_p$ with $\text{Gal}(L/Q_p) \cong G$ is

$$\frac{1}{\# \text{Aut}(G)} \# \left\{ \varphi : \text{Gal}(\overline{Q}_p/Q_p) \twoheadrightarrow G \right\}$$

So it suffices to count the tuples $\sigma, \tau, x_0, x_1 \in G$ that

1. satisfy the relations from $\text{Gal}(\overline{Q}_p/Q_p)$,
2. generate $G$.

**Overall 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 $x_0, x_1$. 
Counting $x_0, x_1$

- The hard relation has $x_0$ in LHS only, $x_1$ in RHS only.
- If we didn’t have to worry about $(\sigma, \tau, x_0, x_1)$ generating, could count collisions: for each $y$ in the $p$-core, the product of the number of ways it can be represented as LHS with the number as RHS.
- Can make this work when the $p$-core is multiplicity free as a representation of the tame quotient, using a lemma on generating sets for $p$-groups.
- Naive looping faster for small $G$. 
Conclusions

Assume $p > 2$. Call a group potentially $p$-adic if
1. it has a valid filtration,
2. in the case that the order is a power of $p$, it has one or two generators.

### Notable Examples ($p = 3$)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>36G7</td>
<td>$(C_3 \times C_3) \rtimes C_4$</td>
<td>0</td>
</tr>
<tr>
<td>54G6</td>
<td>$(C_9 \rtimes C_3) \rtimes C_2$</td>
<td>49</td>
</tr>
<tr>
<td>54G14</td>
<td>$(C_3 \times C_3 \times C_3) \rtimes C_2$</td>
<td>0</td>
</tr>
<tr>
<td>54G15</td>
<td>$C_6 \times C_3 \times C_3$</td>
<td>0</td>
</tr>
<tr>
<td>72G33</td>
<td>$(C_{12} \times C_3) \rtimes C_2$</td>
<td>0</td>
</tr>
<tr>
<td>18T89</td>
<td>$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes C_2$</td>
<td>0</td>
</tr>
<tr>
<td>18T128</td>
<td>$(C_3 \times C_3 \times C_3 \times C_3) \rtimes C_4$</td>
<td>0</td>
</tr>
<tr>
<td>18T138</td>
<td>$((C_3 \times C_3) \rtimes C_2) \times ((C_3 \times C_3) \rtimes C_2)$</td>
<td>0</td>
</tr>
<tr>
<td>15T64</td>
<td>$(C_3 \times (((C_3 \times C_3 \times C_3 \times C_3) \rtimes C_5) \rtimes C_4)) \rtimes C_2$</td>
<td>200</td>
</tr>
</tbody>
</table>
Inductive Approach

Want an algorithm to list the $L$ with a given Galois group.

**Solution for tame case**

Lift irreducible polynomials from residue field for unramified, then adjoin $n^{th}$ roots of $p \cdot u$.

Thus, it suffices to solve:

**Problem**

Fix a Galois extension $L/K$, set $H = \text{Gal}(L/K)$ and suppose $G$ is an extension of $H$:

$$1 \to A \to G \to H \to 1,$$

with $A \cong \mathbb{F}_p^k$. Find all $M/L$ s.t. $M/K$ Galois and $\text{Gal}(M/K) \cong G$. 
Interlude: Local Class Field Theory

Let $M/L/\mathbb{Q}_p$ with $[M : L] = m$ and $\Gamma = \text{Gal}(M/L)$.

**Theorem (Local Class Field Theory [8, Part IV])**

- $H^2(\Gamma, M^\times) = \langle u_{M/L} \rangle \cong \frac{1}{m}\mathbb{Z}/\mathbb{Z}$
- $\cup u_{M/L} : \Gamma^{\text{ab}} = \hat{H}^{-2}(\Gamma, \mathbb{Z}) \supseteq \hat{H}^0(\Gamma, M^\times) = L^\times / \text{Nm}_{M/L} M^\times$.
- The map $M \mapsto \text{Nm}_{M/L} M^\times$ gives a bijection between abelian extensions $M/L$ and finite index subgroups of $L^\times$.

Monge [5] gives algorithms for finding a defining polynomial of the extension associated to a given norm subgroup.

**Upshot**

Since $A = \mathbb{F}_p^k$ abelian, can use LCFT to find possible $M/L$ in terms of subgroups of $L^\times$. 
A Mod-$p$ Representation

Given

\[ 1 \to A \to G \to H \to 1 \]

and \( L/K \), let \( V = (1 + \mathcal{P}_L)/(1 + \mathcal{P}_L)^p \), an \( \mathbb{F}_p[H] \)-module.

- Since \( A = \text{Gal}(M/L) \) has exponent \( p \), it corresponds to a subgp \( N \supseteq (1 + \mathcal{P}_L)^p \) and \( L^\times/N \cong (1 + \mathcal{P}_L)/(N \cap (1 + \mathcal{P}_L)) \).
- Let \( W = (N \cap (1 + \mathcal{P}_L))/(1 + \mathcal{P}_L)^p \), a subspace of \( V \).
- \( M/K \) is Galois iff \( W \) is stable under \( H = \text{Gal}(L/K) \).
- The MeatAxe algorithm finds such subrepresentations.
- For each \( W \), check \( V/W \cong A \) as \( \mathbb{F}_p[H] \)-modules.
- Given \( W \), easy to find a list of \( N \).
- The corresponding \( M/K \) are candidates for \( \text{Gal}(M/K) \cong G \).
Extension Classes

There may be multiple extensions

\[ 1 \to A \to G' \to H \to 1 \]

yielding the same action of \( H \) on \( A \). Use group cohomology to distinguish them.

- Choosing a section \( s : H \to G' \), define a 2-cocycle by
  \[ (g, h) \mapsto s(g)s(h)s(gh)^{-1} \in A. \]

- Get bijection \( H^2(H, A) \leftrightarrow \{ 1 \to A \to G' \to H \to 1 \}/\sim \).

Two approaches to picking out \( G \):

1. Try to find the extension class, given \( W \),
2. Use \( W \) to attempt to construct an action of \( G \) on \( M \), failing if extension class wrong.
A Theorem of Shafarevich and Weil

**Theorem ([1, Ch. 14, Thm. 6])**

Let $N \subset L^\times$ correspond to $M/L$ under LCFT and set $G = \text{Gal}(M/K)$, $H = \text{Gal}(L/K)$ and $A = \text{Gal}(M/L)$. Then the image of $u_{L/K}$ under the natural map

$$H^2(H, L^\times) \to H^2(H, L^\times/N) \cong H^2(H, A)$$

is the extension class for

$$1 \to \text{Gal}(M/L) \to \text{Gal}(M/K) \to \text{Gal}(L/K) \to 1.$$ 

We can compute a 2-cocycle representing $u_{L/K}$ and use it for each $W$. 
Summary of Algorithm

Data: $G \succeq G_0 \succeq G_1 \succeq G_2 \succeq \cdots \succeq G_r = 1$
Result: List of all Galois $F/\mathbb{Q}_p$ with $\text{Gal}(F/\mathbb{Q}_p) \cong G$

Find tame extensions $L_1/\mathbb{Q}_p$ with $\text{Gal}(L_1/\mathbb{Q}_p) \cong G/G_1$;

for $0 < i < r$ do
  Find class $\sigma_i$ of $1 \to G_i/G_{i+1} \to G/G_{i+1} \to G/G_i \to 1$;
  for each $L = L_i$ do
    Compute a 2-cocycle representing $u_{L/\mathbb{Q}_p}$;
    Find all stable submodules $W$ with $L^\times/W \cong G_i/G_{i+1}$;
    for each $W$ do
      if $u_{L/\mathbb{Q}_p} \mapsto \sigma_i \in H^2(L/\mathbb{Q}_p, L^\times/W)$ then
        Add the $M/L$ matching $W$ to the list of $L_{i+1}$;
      end
    end
  end
end
Tori over \( \mathbb{R} \)

**Definition**

An *algebraic torus* over a field \( K \) is a group scheme, isomorphic to \( (\mathbb{G}_m)^n \) after tensoring with a finite extension.

We use tori over \( \mathbb{R} \) as an example, since classification is easy:

- \( U \), with \( U(\mathbb{R}) = \{ z \in \mathbb{C}^\times : z\bar{z} = 1 \} \),
- \( \mathbb{G}_m \), with \( \mathbb{G}_m(\mathbb{R}) = \mathbb{R}^\times \),
- \( S \), with \( S(\mathbb{R}) = \mathbb{C}^\times \).

**Theorem (c.f. [2, Thm 2])**

*Every algebraic torus over \( \mathbb{R} \) is a product of these tori.*

Over \( \mathbb{Q}_p \), different field extensions help create a much wider variety of tori.
Character lattices

**Definition**

The *character lattice* of $T$ is $X^*(T) = \text{Hom}_{\bar{K}}(T, \mathbb{G}_m)$,

$X^*(T)$ is a free rank-$n$ $\mathbb{Z}$-module with a $\text{Gal}(\bar{K}/K)$ action. Can take $\{\chi_i : (z_1, \ldots, z_n) \mapsto z_i\}$ as a basis for $X^*(\mathbb{G}_m^n)$.

- $X^*(\mathbb{G}_m) = \mathbb{Z}$ with trivial action,
- $X^*(U) = \mathbb{Z}$ with conjugation acting as $x \mapsto -x$,
- $X^*(S) = \mathbb{Z}v \oplus \mathbb{Z}w$ with conjugation exchanging $v$ and $w$.

**Theorem**

*The functor $T \mapsto X^*(T)$ defines a contravariant equivalence of categories $K\text{-Tori} \rightarrow \text{Gal}(\bar{K}/K)-\text{Lattices}$.***
Finding $p$-adic tori

**Goal**

Create a database of algebraic tori over $p$-adic fields.

We can break up the task of finding tori into two pieces:

1. For each dimension $n$, list all finite groups $G$ that act (faithfully) on $\mathbb{Z}^n$. For fixed $n$, the set of $G$ is finite.

2. For each $G$ and $p$, list all Galois extensions $L/\mathbb{Q}_p$ with $\text{Gal}(L/\mathbb{Q}_p) \cong G$. For fixed $G$ and $p$, the set of $L$ is finite. Moreover, when $p$ does not divide $|G|$, this question is easy.
Finite Subgroups of $\text{GL}_n(\mathbb{Z})$

- With a choice of basis, a faithful action of $G$ on $\mathbb{Z}^n$ is the same as an embedding $G \subset \text{GL}_n(\mathbb{Z})$.
- Two $G$-lattices are isomorphic if and only if the corresponding subgroups are conjugate within $\text{GL}_n(\mathbb{Z})$.
- Two $G$-lattices are \textit{isogenous} if the corresponding subgroups are conjugate within $\text{GL}_n(\mathbb{Q})$.

$\mathbb{G}_m \times \textbf{U}$ and $\textbf{S}$ are isogenous but not isomorphic, since $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are conjugate in $\text{GL}_n(\mathbb{Q})$ but not in $\text{GL}_n(\mathbb{Z})$. 
Previous Computations

**CARAT [3]**
Up to dimension 6, the software package CARAT lists all of the finite subgroups of $GL_n(\mathbb{Z})$, up to $\mathbb{Z}$- and $\mathbb{Q}$-conjugacy.

**IMF GAP Library [6]**
The group theory software package GAP has a library for maximal finite subgroups where the corresponding lattice is irreducible as a $G$-module. The $\mathbb{Q}$-classes are known for $n \leq 31$, the $\mathbb{Z}$-classes for $n \leq 11$ and $n \in \{13, 17, 19, 23\}$. 
A $G$-lattice is *indecomposable* if it does not split as a direct sum of $G$-submodules.

For example, $X^*(S)$ is not irreducible, since $\langle v + w \rangle$ is a stable submodule, as is $\langle v - w \rangle$.

But it is indecomposable; the sum of these submodules has index 2.

For $n > 6$, work remains to recover a list of indecomposable subgroups. Note that the decomposition into indecomposable submodules is NOT unique.
### Number of Subgroups (up to $\text{GL}_n(\mathbb{Z})$-conjugacy)

<table>
<thead>
<tr>
<th>Dimension</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Unramified</td>
<td>2</td>
<td>7</td>
<td>16</td>
<td>45</td>
<td>96</td>
<td>240</td>
</tr>
<tr>
<td>Tame</td>
<td>2</td>
<td>13</td>
<td>51</td>
<td>298</td>
<td>1300</td>
<td>6661</td>
</tr>
<tr>
<td>7-adic</td>
<td>2</td>
<td>10</td>
<td>38</td>
<td>192</td>
<td>802</td>
<td>3767</td>
</tr>
<tr>
<td>5-adic</td>
<td>2</td>
<td>11</td>
<td>41</td>
<td>222</td>
<td>890</td>
<td>4286</td>
</tr>
<tr>
<td>3-adic</td>
<td>2</td>
<td>13</td>
<td>51</td>
<td>348</td>
<td>1572</td>
<td>9593</td>
</tr>
<tr>
<td>2-adic</td>
<td>2</td>
<td>11</td>
<td>60</td>
<td>536</td>
<td>4820</td>
<td>65823</td>
</tr>
<tr>
<td>Local</td>
<td>2</td>
<td>13</td>
<td>67</td>
<td>633</td>
<td>5260</td>
<td>69584</td>
</tr>
<tr>
<td>All</td>
<td>2</td>
<td>13</td>
<td>73</td>
<td>710</td>
<td>6079</td>
<td>85308</td>
</tr>
</tbody>
</table>

Note that each subgroup corresponds to multiple tori, since there are multiple field extensions with that Galois group.
## Order of Largest Subgroup

<table>
<thead>
<tr>
<th>Dimension</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Unramified</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>12</td>
<td>30</td>
</tr>
<tr>
<td>Tame</td>
<td>2</td>
<td>12</td>
<td>12</td>
<td>40</td>
<td>72</td>
<td>144</td>
</tr>
<tr>
<td>7-adic</td>
<td>2</td>
<td>8</td>
<td>12</td>
<td>40</td>
<td>40</td>
<td>120</td>
</tr>
<tr>
<td>5-adic</td>
<td>2</td>
<td>12</td>
<td>12</td>
<td>40</td>
<td>72</td>
<td>144</td>
</tr>
<tr>
<td>3-adic</td>
<td>2</td>
<td>12</td>
<td>12</td>
<td>72</td>
<td>72</td>
<td>432</td>
</tr>
<tr>
<td>2-adic</td>
<td>2</td>
<td>12</td>
<td>48</td>
<td>576</td>
<td>1152</td>
<td>2304</td>
</tr>
<tr>
<td>Irreducible</td>
<td>2</td>
<td>12</td>
<td>48</td>
<td>1152</td>
<td>3840</td>
<td>103680</td>
</tr>
<tr>
<td>Weyl</td>
<td>$A_1$</td>
<td>$G_2$</td>
<td>$B_3$</td>
<td>$F_4$</td>
<td>$B_5$</td>
<td>$2 \times E_6$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dim</th>
<th>Largest Irreducible Subgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>$2903040 \ (E_7)$</td>
</tr>
<tr>
<td>8</td>
<td>$696729600 \ (E_8)$</td>
</tr>
<tr>
<td>31</td>
<td>$176584115499894161336717308363957862400000000 \ (B_{31})$</td>
</tr>
</tbody>
</table>
Database of \( p \)-adic Fields

Jones and Roberts [4] have created a database of \( p \)-adic fields.

- Lists all \( L/\mathbb{Q}_p \) with a given degree, including non-Galois;
- Includes up to degree 10;
- Gives Galois group and other data about the extension;
- Biggest table is \([L : \mathbb{Q}_2] = 8\), of which there are 1823.
- I want \( G \) in degree up to 96 (tame) or 14, 60, 144, 144 (wild, \( p = 7, 5, 3, 2 \) resp.)

Their database solves the problem for small \( G \), but most of the target \( G \) fall outside it.
Future Work

1. Flesh out details of algorithm and implement it,
2. Extend group theoretic analysis to dimension 7 and 8,
3. Compute additional data for each torus: cohomology groups, embeddings into induced tori, Moy-Prasad filtrations, conductors, component groups of Néron models...
Thank you for your attention!
References


