The inverse Galois problem for p-adic fields

David Roe

Department of Mathematics
University of Pittsburgh

November 13, 2017

Outline

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

Extensions of p-adic fields

If L/K is an extension of p-adic fields, it decomposes:

$$\begin{tikzcd} L \arrow[d, dash, "\text{wild}"] \\ L_t \arrow[d, dash, "\text{tame}"] \\ L_u \arrow[d, dash, "\text{unram}"] \\ K \end{tikzcd}$$

- **Wild** – totally ramified, degree a power of p.
- **Tame** – totally ramified, degree relatively prime to p. Have $L_t = L_u(\sqrt[n]{\pi})$ 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 Gal(L/K). We can refine this filtration to

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

- 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:

$$\begin{array}{c} \bar{K} \\ \Big| \text{ wild} \\ K^t \\ \Big| \text{ tame} \\ K^u \\ \Big| \text{ unram} \\ K \end{array}$$

- $\mathrm{Gal}(K^u/K) = \langle \sigma \rangle \cong \hat{\mathbb{Z}}$
- $\mathrm{Gal}(K^t/K^u) = \langle \tau \rangle \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$
- $\sigma^{-1}\tau\sigma = \tau^q$
- $\mathrm{Gal}(\bar{K}/K^t)$ is pro-p.

Presentation of the absolute Galois group

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

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

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

$h \in \mathbb{Z}_p$ 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 algorithm

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

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

Overall Strategy

Loop over σ generating the unramified quotient and τ generating the tame inertia (with $\tau^\sigma = \tau^p$). For each such (σ, τ) 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 (σ, τ, 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 ($p = 3$)

Label	Description	Num
36G7	$(C_3 \times C_3) \rtimes C_4$	0
54G6	$(C_9 \rtimes C_3) \rtimes C_2$	49
54G14	$(C_3 \times C_3 \times C_3) \rtimes C_2$	0
54G15	$C_6 \times C_3 \times C_3$	0
72G33	$(C_{12} \times C_3) \rtimes C_2$	0
18T89	$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes C_2$	0
18T128	$(C_3 \times C_3 \times C_3 \times C_3) \rtimes C_4$	0
18T138	$((C_3 \times C_3) \rtimes C_2) \times ((C_3 \times C_3) \rtimes C_2)$	0
15T64	$(C_3 \times (((C_3 \times C_3 \times C_3 \times C_3) \rtimes C_5) \rtimes C_4)) \rtimes C_2$	200

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 $\Gamma = \mathrm{Gal}(M/L)$.

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

- $\mathrm{H}^2(\Gamma, M^\times) = \langle u_{M/L} \rangle \cong \frac{1}{m}\mathbb{Z}/\mathbb{Z}$
- $- \cup u_{M/L} : \Gamma^{\mathrm{ab}} = \hat{\mathrm{H}}^{-2}(\Gamma, \mathbb{Z}) \xrightarrow{\sim} \hat{\mathrm{H}}^{0}(\Gamma, M^\times) = L^\times / \mathrm{Nm}_{M/L} M^\times$.
- *The map $M \mapsto \mathrm{Nm}_{M/L} M^\times$ 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 $\mathrm{H}^2(H, A) \leftrightarrow \{1 \to A \to G' \to H \to 1\}/\sim$.

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 $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(L/K)$ and $A = \mathrm{Gal}(M/L)$. Then the image of $u_{L/K}$ under the natural map

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

is the extension class for

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

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

Summary of Algorithm

Data: $G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = 1$
Result: List of all Galois $F/\mathbb{Q}_p$ with Gal$(F/\mathbb{Q}_p) \cong G$
Find tame extensions $L_1/\mathbb{Q}_p$ with Gal$(L_1/\mathbb{Q}_p) \cong G/G_1$;
for $0 < i < r$ **do**
    Find class σ_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 $u_{L/\mathbb{Q}_p} \mapsto \sigma_i \in \mathrm{H}^2(L/\mathbb{Q}_p, L^\times/W)$ **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 $\mathbf{U}(\mathbb{R}) = \{z \in \mathbb{C}^\times \ : \ z\bar{z} = 1\}$,
- $\mathbb{G}_m$, with $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^\times$,
- **S**, with $\mathbf{S}(\mathbb{R}) = \mathbb{C}^\times$.

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 $X^*(T) = \mathrm{Hom}_{\bar{K}}(T, \mathbb{G}_m)$,

$X^*(T)$ is a free rank-n $\mathbb{Z}$-module with a $\mathrm{Gal}(\bar{K}/K)$ 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,
- $X^*(\mathbf{U}) = \mathbb{Z}$ with conjugation acting as $x \mapsto -x$,
- $X^*(\mathbf{S}) = \mathbb{Z}v \oplus \mathbb{Z}w$ with conjugation exchanging v and w.

Theorem

*The functor $T \mapsto X^*(T)$ defines a contravariant equivalence of categories K-**Tori** $\to$ $\mathrm{Gal}(\bar{K}/K)$-**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 $\mathrm{Gal}(L/\mathbb{Q}_p) \cong G$. 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 $\mathrm{GL}_n(\mathbb{Z})$

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

$\mathbb{G}_m \times$ **U** and **S** are isogenous but not isomorphic, since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ are conjugate in $\mathrm{GL}_n(\mathbb{Q})$ but not in $\mathrm{GL}_n(\mathbb{Z})$.

Previous Computations

CARAT [3]

Up to dimension 6, the software package CARAT lists all of the finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$, 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 $n \in \{13, 17, 19, 23\}$.

Indecomposible subgroups

- A G-lattice is *indecomposible* if it does not split as a direct sum of G-submodules.
- For example, $X^*(\mathbf{S})$ is not irreducible, since $\langle v + w \rangle$ is a stable submodule, as is $\langle v - w \rangle$.
- But it is indecomposible; the sum of these submodules has index 2.

For $n > 6$, work remains to recover a list of indecomposible subgroups. Note that the decomposition into indecomposible submodules is NOT unique.

Number of Subgroups (up to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy)

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

Note that each subgroup corresponds to multiple tori, since there are multiple field extensions with that Galois group.

Order of Largest Subgroup

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

Dim	Largest Irreducible Subgroup
7	2903040 (E_7)
8	696729600 (E_8)
31	17658411549989416133671730836395786240000000 (B_{31})

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...
4. Put data online at `www.lmfdb.org`.

Thank you for your attention!

References

[1] E. Artin, J. Tate. *Class Field Theory*. W.A. Benjamin, 1968.

[2] B. Casselman. *Computations in real tori*, Representation theory of real groups, Contemporary Mathematics **472**, A.M.S. (2007).

[3] C. Cid, J. Opgenorth, W. Plesken, T. Schulz. *CARAT*. `wwwb.math.rwth-aachen.de/carat/`.

[4] J. Jones, D. Roberts. *A database of local fields*, J. Symbolic Comput **41** (2006), 80-97.

[5] M. Monge. *A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields*, Int. J. Number Theory **10** (2014), 1699-1727.

[6] G. Nebe, W. Pleskin, M. Pohst, B. Souvignier. *Irreducible maximal finite integral matrix groups*. GAP Library.

[7] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of Number Fields*. Springer, Berlin, 2015.

[8] J.-P. Serre. *Local fields*. Springer, New York, 1979.