A database of p-adic tori

David Roe

Department of Mathematics
Massachusetts Institute of Technology

UBC Number Theory Seminar
Vancouver, BC

November 21, 2019

Goal

Goal

Explicitly compute all algebraic tori over p-adic fields with dimension up to some bound.

Building tori over $\mathbb{Q}_p$

- A continuous action of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ on a lattice $\mathbb{Z}^n$ will factor through a finite quotient $G = \mathrm{Gal}(L/\mathbb{Q}_p)$,
- and a faithful action of G on $\mathbb{Z}^n$ is the same as an embedding $G \hookrightarrow \mathrm{GL}_n(\mathbb{Z})$.

We may thus break up the task of finding tori into three parts:

1. For each dimension n, list all finite subgroups G of $\mathrm{GL}_n(\mathbb{Z})$ (up to conjugacy). For fixed n, the set of such 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 $|G|$, doing so is easy.
3. For each G, compute the automorphisms of G (up to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy).

We will refer to such a pair (G, L) as a prototorus.

Ambiguity of embedding

The difference between a conjugacy class of embeddings $G \hookrightarrow \mathrm{GL}_n(\mathbb{Z})$ and a conjugacy class of subgroups $G \subset \mathrm{GL}_n(\mathbb{Z})$ is measured by the quotient A/W, where

$$A = \mathrm{Aut}(G) \qquad\qquad W = N_{\mathrm{GL}_n(\mathbb{Z})}(G)/C_{\mathrm{GL}_n(\mathbb{Z})}(G).$$

We refer to the size a of A/W as the ambiguity of G. Given a prototorus (G, L), there are a corresponding isomorphism classes of tori, each with splitting field L.

Example

The subgroup generated by

$$\alpha_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \alpha_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is isomorphic to C_2^2, and has both normalizer and centralizer $\langle \alpha_1, \alpha_2, -I \rangle \cong C_2^3$. Since $A \cong S_3$, we have $a = 6$.
Suppose p is odd and L is the compositum of the three quadratic extensions L_1, L_2 and L_3 of $\mathbb{Q}_p$. Let $\sigma_i \in \mathrm{Gal}(L/\mathbb{Q}_p)$ be the nontrivial element fixing L_i, and T the torus corresponding to the map $\sigma_i \mapsto \alpha_i$. Then $T(\mathbb{Q}_p) \cong \mathrm{Nm}^1_{L_1/\mathbb{Q}_p} \times L_2^\times$. Each of the six labelings of the L_i produces a distinct torus.

Isogenies

- Two G-lattices are isomorphic iff the corresponding maps $G \to \mathrm{GL}_n(\mathbb{Z})$ are $\mathrm{GL}_n(\mathbb{Z})$-conjugate.
- Two G-lattices are isogenous iff the corresponding maps are $\mathrm{GL}_n(\mathbb{Q})$-conjugate.
- Just as $a = A/W$ measures the number of isomorphism classes of tori for a given prototorus, $a' = A/W'$ measures the number of isogeny classes for a given pair (G', L), where G' is now up to $\mathrm{GL}_n(\mathbb{Q})$-conjugacy. Here

$$W' = N_{\mathrm{GL}_n(\mathbb{Q})}(G)/C_{\mathrm{GL}_n(\mathbb{Q})}(G).$$

$\mathbb{G}_m \times \mathrm{U}$ 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 $\mathrm{GL}_n(\mathbb{Z})$.

Inverse Galois problem

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.

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

Non-realizable examples

The group $W(F_4)$ generated by

$$\left\langle \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ -1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & -1 \\ -1 & -1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \right\rangle$$

has order 1152. It is not potentially p-realizable for any p.
In a p-adic Galois group, the quotient by wild inertia must be metacyclic (cyclic subgroup with cyclic quotient).

- G is not metacyclic, so only $p = 2$ and $p = 3$ possible
- For $p = 2$, the quotient by the p-core (largest normal p-subgroup) is S_3^2 which is not metacyclic.
- For $p = 3$, the p-core is trivial.

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

Write V for the p-core of G, as a representation of G/V, W for the Frattini subgroup of V.

Label	Description	V/W
27G5	$\mathbb{F}_3^3$	1^3
36G7	$\mathbb{F}_3^2 \rtimes C_4$	1^2
54G14	$\mathbb{F}_3^3 \rtimes C_2$	1^3
72G33	$\mathbb{F}_3^2 \rtimes D_8$	1^2
162G16	$C_9^2 \rtimes C_2$	1^2
324G164	$\mathbb{F}_3^4 \rtimes C_4$	2^2
324G169	$\mathbb{F}_3^4 \rtimes (C_2 \times C_2)$	$1^2 \oplus 1^2$
378G51	$\mathbb{F}_3^2 \rtimes (C_7 \rtimes C_6)$	1^2
648G711	$\mathbb{F}_3^4 \rtimes C_8$	2^2

Criterion for p-groups

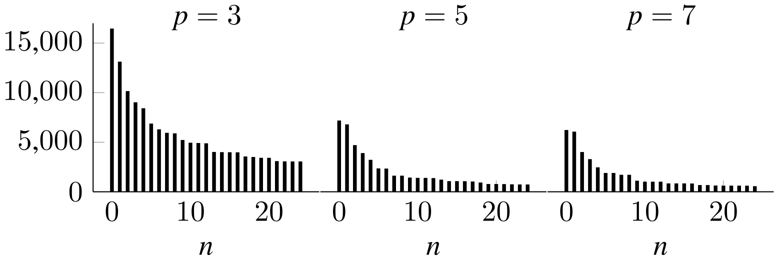
We get an easy condition on when a p-group is p-realizable. Let $W = G^p G'$ be the Frattini subgroup; G/W is the maximal elementary abelian quotient of G. A set of elements generates G if and only if its projection onto G/W spans G/W as an $\mathbb{F}_p$-vector space.

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.

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.

LMFDB

The L-functions and modular forms database (LMFDB) aims to make interesting objects in number theory and arithmetic geometry available for researchers to browse and search. It currently includes

- Global and local number fields,
- Classical, Hilbert, Bianchi and Maass modular forms,
- Elliptic curves over $\mathbb{Q}$ and number fields, genus-2 curves over $\mathbb{Q}$, abelian varieties over finite fields,
- Galois groups and Sato-Tate groups,
- L-functions for many of these objects.

Improved group theory, including subgroups of $\mathrm{GL}_n(\mathbb{Z})$, is under active development.

Existing ingredients

Jones-Roberts database of local fields [2]

- Included in LMFDB, by permutation degree
- p-adic fields of degree up to 15 for $p < 200$
- Missing sibling information (other fields with same closure)
- Only gives ramification breaks, not ramification subgroups

Matrix groups

GAP and Magma include databases of matrix groups [1, 3]

- All $G \subset \mathrm{GL}_n(\mathbb{Z})$ for $n \leq 6$, up to conjugacy
- Maximal irreducible $G \subset \mathrm{GL}_n(\mathbb{Z})$ for $n \leq 31$, up to $\mathrm{GL}_n(\mathbb{Q})$-conjugacy
- Maximal irreducible $G \subset \mathrm{GL}_n(\mathbb{Z})$ for $n \leq 11$ and $n \in \{13, 17, 19, 23\}$, up to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy

A database of tori

Demo

tori.lmfdb.xyz

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

Each subgroup can correspond to many tori: multiple $L/\mathbb{Q}_p$ with $G \cong \mathrm{Gal}(L/\mathbb{Q}_p)$, and ambiguity.

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})

What to compute?

- Easy: $\mathbb{Q}_p$-rank; whether unramified, tame, anisotropic, split, induced; dual torus
- Artin and swan conductors, discriminants
- Alternate descriptions: units in étale algebras (possibly with involution)
- Description of $T(\mathbb{Q}_p)$, Moy-Prasad filtration
- Néron models, behavior under base change
- Embeddings into reductive groups
- Fixed set for action on Bruhat-Tits building
- Tate cohomology groups $\hat{\mathrm{H}}(\mathbb{Q}_p, X^*(T))$
- Rationality, stable rationality, retract rationality, unirationality; flasque and coflasque
- Resolutions: $0 \to F \to M \to T \to 0$ with M induced and F flasque.

Computing with large field extensions

Definition

Let L/K be a Galois extension of fields. A stem field for L/K is an extension C/K so that L is the Galois closure of C.

The degree $[C : K]$ can be exponentially smaller than $[L : K]$: if $\mathrm{Gal}(L/K) = S_n$ we can find $[C : K] = n$ while $[L : K] = n!$.

Question

$T(K) \cong (X_*(T) \otimes L^\times)^{\mathrm{Gal}(L/K)}$ is usually expressed in terms of L. Can it be computed directly from some C (along with knowledge of $\mathrm{Gal}(L/C) \subset \mathrm{Gal}(L/K)$)?

Applications

- Jiu-Kang Yu's construction of supercuspidal representations isn't known to be exhaustive in small residue characteristic; I hope the database can be useful in working with examples of such representations.
- The behavior of Néron models under wild base change has always been a mystery to me. I hope examples can help clarify the situation.
- Understanding maximal tori in exceptional groups. Tame tori in exceptional groups have been studied by Reeder [4]. Wild tori in exceptional groups only occur in small characteristic and dimension, making them a perfect target for a database.

Integral Galois representations

We have been using the equivalence of categories to relate tori to representations

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_n(\mathbb{Z}).$$

The methods apply equally well to other base fields, such as number fields. In this case the integral Galois representations themselves are also of interest, and are connected to other sections of the LMFDB.

- If K is a number field, then $\mathcal{O}_K^\times$ is a finitely generated abelian group and the torsion-free quotient is an integral representation of $\mathrm{Gal}(K/\mathbb{Q})$.
- If E is an elliptic curve over a number field K, then $E(K)$ is a finitely generated abelian group and the torsion-free quotient is an integral representation of $\mathrm{Gal}(K/\mathbb{Q})$.

References

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

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

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

[4] M. Reeder. Elliptic centralizers in Weyl groups and their coinvariant representations. Representation Theory 15 (2011), 63–111.