A database of p-adic tori

David Roe

Department of Mathematics
Massachusetts Institute of Technology

Representation Theory of Groups Defined over Local Fields
CMS19, Regina, SK

June 8, 2019

Algebraic tori

Definition

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

Can also give $T(\bar{K})$ plus a continuous action of Gal$(\bar{K}/K)$ on it.

Examples over $\mathbb{R}$

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

Theorem (c.f. [1, Thm 2])

Every algebraic torus over $\mathbb{R}$ is a product of these 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 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** $\to$ Gal$(\bar{K}/K)$-**Lattices** (with continuous action).*

Building tori over $\mathbb{Q}_p$

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

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

1. For each dimension n, list all finite subgroups G of $\text{GL}_n(\mathbb{Z})$ (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 $\text{Gal}(L/\mathbb{Q}_p) \cong G$. For fixed G and p, the set of L is finite. Moreover, when p does not divide $|G|$, doing so is easy.
3. For each G, compute the automorphisms of G (up to $\text{GL}_n(\mathbb{Z})$-conjugacy).

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

Ambiguity of embedding

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

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

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

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

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

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 [3]

- Included in LMFDB
- 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 [2, 4]

- 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 $GL_n(\mathbb{Z})$-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 $G \cong \text{Gal}(L/\mathbb{Q}_p)$, 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})

p-realizable groups

We say a group G is p-*realizable* if there is an extension $L/\mathbb{Q}_p$ with $G \cong \mathrm{Gal}(L/\mathbb{Q}_p)$. The group 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 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.

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 *core* 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

- 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 [5]. Wild tori in exceptional groups only occur in small characteristic and dimension, making them a perfect target for a database.

References

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

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

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

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

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