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
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 $\text{Gal}(\bar{K}/K)$ on it.
Examples over $\mathbb{R}$

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

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

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

**Theorem**

*The functor $T \mapsto X^*(T)$ defines a contravariant equivalence of categories $K\text{-Tori} \to \text{Gal}(\bar{K}/K)\text{-Lattices}$ (with continuous action).*
Building tori over $\mathbb{Q}_p$

- A continuous action of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ 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 $G \rightarrow \text{GL}_n(\mathbb{Z})$.

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

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

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

The subgroup generated by

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

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 $\sigma_i \in \text{Gal}(L/\mathbb{Q}_p)$ be the nontrivial element fixing $L_i$, and $T$ the torus corresponding to the map $\sigma_i \mapsto \alpha_i$. Then $T(\mathbb{Q}_p) \cong \text{Nm}^1_{L_1/\mathbb{Q}_p} \times L_2^\times$. Each of the six labelings of the $L_i$ produces a distinct torus.
Isogenies

- Two $G$-lattices are isomorphic iff the corresponding maps $G \rightarrow \text{GL}_n(\mathbb{Z})$ are $\text{GL}_n(\mathbb{Z})$-conjugate.
- Two $G$-lattices are isogenous iff the corresponding maps are $\text{GL}_n(\mathbb{Q})$-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 $\text{GL}_n(\mathbb{Q})$-conjugacy. Here

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

$\mathbb{G}_m \times \mathbf{U}$ and $\mathbf{S}$ 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 $\text{GL}_n(\mathbb{Z})$. 
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 \( \text{GL}_n(\mathbb{Z}) \), 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 \( G \subset \text{GL}_n(\mathbb{Z}) \) for \( n \leq 6 \), up to conjugacy
- Maximal irreducible \( G \subset \text{GL}_n(\mathbb{Z}) \) for \( n \leq 31 \), up to \( \text{GL}_n(\mathbb{Q}) \)-conjugacy
- Maximal irreducible \( G \subset \text{GL}_n(\mathbb{Z}) \) for \( n \leq 11 \) and \( n \in \{13, 17, 19, 23\} \), up to \( \text{GL}_n(\mathbb{Z}) \)-conjugacy
A database of tori

tori.lmfdb.xyz
### 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>

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

<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>17658411549989416133671730836395786240000000 ((B_{31}))</td>
</tr>
</tbody>
</table>
**$p$-realizable groups**

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

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

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 $\hat{H}(\mathbb{Q}_p, X^*(T))$
- 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 $\text{Gal}(L/K) = S_n$ we can find $[C : K] = n$ while $[L : K] = n!$.

Question

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


