Local-global principle, isogenies, and Tamagawa numbers of algebraic tori

Thomas Rüd

February 2021

Local-global principle

Local-global principle: The study of properties (e.g. isomorphism) holding *locally* but not *globally*.

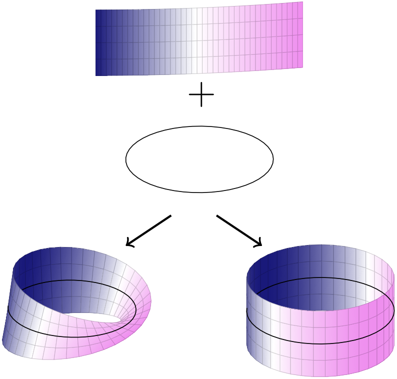


Figure: Examples of line bundles over S^1

Number-theoretical version

Look at integer solution for polynomial equations...

$$\begin{array}{c} x^2 - 3xy + 9y^2 = 8 \\ \text{no solution in } \mathbb{Z} \end{array} \Longleftarrow \begin{array}{c} x^2 \equiv 2 \pmod 3 \\ \text{no solution in } \mathbb{Z}/3\mathbb{Z} \end{array}.$$

The lack of "local" solutions implies the lack of "global" solutions, but the converse brings two related questions:

- Do local solutions imply a solution in $\mathbb{Q}$?
- If everything is defined over $\mathbb{Z}$, can we find a solution in $\mathbb{Z}$?

Answer: It depends.

- (Hasse) Homogeneous quadratic polynomials with roots modulo every n and in $\mathbb{R}$ also have roots in $\mathbb{Q}$.
- (Selmer) The equation $3x^3 + 4y^3 + 5z^3 = 0$ has solutions modulo every integer, but no solution in $\mathbb{Q}$.
- If a monic polynomial in $\mathbb{Z}[x]$ has a solution in $\mathbb{Q}$, then it has a solution in $\mathbb{Z}$.

Number-theoretical version

Globally: Over a global fields (e.g. $\mathbb{Q}$, number fields, $k(X)$, ...).

Locally: Over *completions* over the global fields.

For the field $\mathbb{Q}$, the completions are $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$, where p is a prime number.

Class, Genus, and Mass formulae

For $k = \mathbb{Q}$, the completions $\mathbb{Q}_p$ have rings of integers $\mathbb{Z}_p$. By the Chinese Remainder Theorem, we have $\prod_p \mathbb{Z}_p = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Given an algebraic object A defined over $\mathbb{Z}$, we can define its

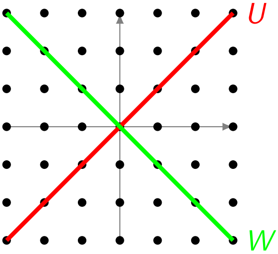
- **Genus:** Set of objects defined over $\mathbb{Z}$ that are isomorphic to A modulo every $n \in \mathbb{N}$.
- **Class:** Isomorphism class of A over $\mathbb{Z}$.
- **Mass:** Number of classes in its genus.

Example. The symmetric bilinear forms given by the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 82 \end{pmatrix}$ and $\begin{pmatrix} 2 & 0 \\ 0 & 41 \end{pmatrix}$ are in the same genus but not in the same class.

Other "example" if 2 were invertible.

Take

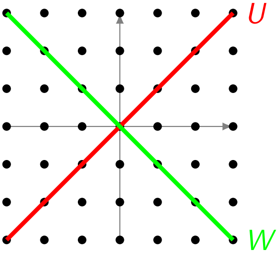
- $G = \mathbb{Z}/2\mathbb{Z} = \langle \sigma \rangle$.
- $V = \mathbb{Z}^2 = \mathbb{Z}[G]$
  as G-module ($\sigma(a, b) = (b, a)$).
- $U = \mathrm{span}_{\mathbb{Z}}((1, 1))$, and
  $W = \mathrm{span}_{\mathbb{Z}}((1, -1))$.
- $\varphi : U \times W \to V$.



Other "example" if 2 were invertible.

Take

- $G = \mathbb{Z}/2\mathbb{Z} = \langle \sigma \rangle$.
- $V = \mathbb{Z}^2 = \mathbb{Z}[G]$
  as G-module ($\sigma(a, b) = (b, a)$).
- $U = \mathrm{span}_{\mathbb{Z}}((1, 1))$, and
  $W = \mathrm{span}_{\mathbb{Z}}((1, -1))$.
- $\varphi : U \times W \to V$.



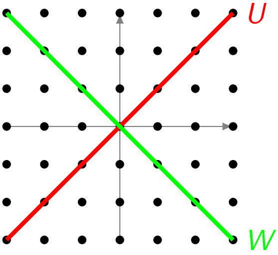
Then

- $\mathrm{Ker}(\varphi) = 0$, $\mathrm{Coker}(\varphi) = \mathbb{Z}/2\mathbb{Z}$.

Other "example" if 2 were invertible.

Take

- $G = \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle$.
- $V = \mathbb{Z}^2 = \mathbb{Z}[G]$ as G-module $(\sigma(a, b) = (b, a))$.
- $U = \mathrm{span}_{\mathbb{Z}}((1, 1))$, and $W = \mathrm{span}_{\mathbb{Z}}((1, -1))$.
- $\varphi : U \times W \to V$.



Then

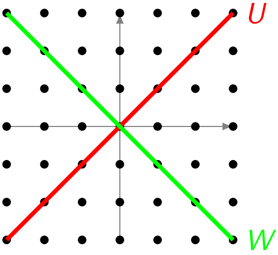
- $\mathrm{Ker}(\varphi) = 0$, $\mathrm{Coker}(\varphi) = \mathbb{Z}/2\mathbb{Z}$.
- If n is odd, φ is an isomorphism modulo n:

$$(U \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \times (W \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \cong (V \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}).$$

Other "example" if 2 were invertible.

Take

- $G = \mathbb{Z}/2\mathbb{Z} = \langle \sigma \rangle$.
- $V = \mathbb{Z}^2 = \mathbb{Z}[G]$
  as G-module ($\sigma(a, b) = (b, a)$).
- $U = \mathrm{span}_{\mathbb{Z}}((1, 1))$, and
  $W = \mathrm{span}_{\mathbb{Z}}((1, -1))$.
- $\varphi : U \times W \to V$.



Then

- $\mathrm{Ker}(\varphi) = 0$, $\mathrm{Coker}(\varphi) = \mathbb{Z}/2\mathbb{Z}$.
- If n is odd, φ is an isomorphism modulo n:

$$(U \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \times (W \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \cong (V \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}).$$

- φ induces an isomorphism over $\mathbb{Q}$ but not $\mathbb{Z}$:

$$(U \otimes_{\mathbb{Z}} \mathbb{Q}) \times (W \otimes_{\mathbb{Z}} \mathbb{Q}) \cong (V \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Modern setting: cohomological reformulation

In the modern setting, the classification of the objects of interest arise as Galois cohomology groups $H^1(k, \mathsf{G}(\overline{k}))$ where G is an algebraic group G defined over a global field k.

G	$H^1(k, \mathsf{G}(\overline{k}))$
$\mathrm{GL_n}$	isomorphism classes of n-dimensional k-vector spaces
$\mathrm{PGL_n}$	isomorphism classes of n-dimensional central simple algebras over k
O_n	isomorphism classes of non-degenerate n-dimensional quadratic forms over k
Sp_{2n}	isomorphism classes of $2n$-dimensional symplectic forms over k

Modern setting: cohomological reformulation

For simplicity, let us take $k = \mathbb{Q}$. One is interested in the local-global principle for G-torsors, i.e. the injectivity of

$$H^1(\mathbb{Q}, \mathrm{G}(\overline{\mathbb{Q}})) \longrightarrow \prod_{p \text{ prime}} H^1(\mathbb{Q}_p, \mathrm{G}(\overline{\mathbb{Q}_p})) \times H^1(\mathbb{R}, \mathrm{G}(\mathbb{C})).$$

The kernel of this map is denoted by $Ш^1(\mathrm{G})$, the *Tate-Shafarevich group*. We say that the *Hasse principle* holds when $Ш^1(\mathrm{G}) = \{0\}$.

The Hasse principle was proven for classical groups over number fields over many years with the work of Kneser, Springer, Harder, and Chernousov.

Algebraic tori

The specific algebraic groups we are interested in are *algebraic tori*.

$$\mathbb{G}_m = \text{multiplicative group}, \quad \mathbb{G}_m(k) = k^\times .$$

Algebraic torus: Algebraic group, isomorphic to $\mathbb{G}_m$ over $\overline{k}$.
Examples:

- $\mathrm{R}_{K/k}\mathbb{G}_m$: *restriction of scalars*, $\mathrm{R}_{K/k}\mathbb{G}_m(k) = K^\times$.
  Example: $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{R}) = \mathbb{C}^\times$.
- $\mathrm{R}^{(1)}_{K/k}\mathbb{G}_m = \mathrm{Ker}(N_{K/k} : \mathrm{R}_{K/k}\mathbb{G}_m \to \mathbb{G}_m)$: *norm-one torus.*
  Example: $\mathrm{R}^{(1)}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{R}) = SO_2(\mathbb{R}) = S^1$.

Theorem

There is a categorical equivalence

$$\{\textit{algebraic tori over } k\} \leftrightarrow \{\mathbb{Z} - \textit{lattices with } \mathrm{Gal}(\overline{k}/k) - \textit{action}\} .$$

$$\mathrm{T} \mapsto \mathrm{X}^\star(\mathrm{T}) = \mathrm{Hom}(\mathrm{T}, \mathbb{G}_m) \text{ (character lattice).}$$

Isogenies

Similarly, for algebraic groups, we consider **isogenies**: surjective (over the algebraic closure) morphisms of algebraic groups with finite kernel.

Examples.

- $\mathrm{GL}_n \to \mathbb{G}_m \times \mathrm{PGL}_n$ defined by $M \mapsto (\det(M), [M])$. It has kernel $\boldsymbol{\mu}_n$ and is surjective (over the algebraic closure).
- $\mathrm{R}_{K/k}\mathbb{G}_m$ is isogenous to $\mathrm{R}^{(1)}_{K/k}\mathbb{G}_m \times \mathbb{G}_m$.
  Example: For $k = \mathbb{R}$ and $K = \mathbb{C}$, we get polar coordinates:
    - a surjection $S^1 \times \mathbb{R}^\times \to \mathbb{C}^\times : (s, r) \mapsto rs$ with kernel $\{\pm 1\}$.
    - an injection $\mathbb{C}^\times \to S^1 \times \mathbb{R}^\times : z \mapsto (\mathrm{Arg}(z), |z|)$ with cokernel $\mathbb{Z}/2\mathbb{Z}$.

  The corresponding character lattices are U, V, W from before.

Isogenies

Theorem (Achter, Altug, Garcia, Gordon)

Let $[X, \lambda]$ be a principally polarized abelian variety of dimension g defined over a finite field $\mathbb{F}_q$ with commutative endomorphism ring. If q is prime or if X is ordinary, then its mass is

$$q^{\frac{g(g-1)}{4}} \tau_{\mathsf{T}} \nu_\infty([X, \lambda]) \prod_\ell \nu_\ell([X, \lambda]),$$

where τ_{T} is the Tamagawa number of T, some maximal algebraic torus in $\mathrm{GSp}_{2g}(\mathbb{Q})$.

The work presented here aims to compute

$$\tau_{\mathsf{T}} = \frac{|H^1(\mathbb{Q}, \mathsf{X}^\star(\mathsf{T}))|}{|\text{Ш}^1(\mathsf{T})|}.$$

Remark. Tamagawa numbers are defined for any algebraic group G over a number field k as a specific volume of $\mathsf{G}^1(\mathbb{A}_k)/\mathsf{G}(k)$. The formula above was established by Ono (1965) (and Voskresenski), and was generalized later to connected algebraic groups by Sansuc (1981) by the formula

$$\tau_{\mathsf{G}} = \frac{|\mathrm{Pic}(\mathsf{G})|}{|Ш^1(\mathsf{G})|}.$$

The torus

$$\begin{array}{c} K \\ \big|\, 2 \\ K^+ \\ \big| \\ \mathbb{Q} \end{array}$$

Let $K/\mathbb{Q}$ be a field extension of degree $2g$ with intermediate field extension K^+ such that K/K^+ is imaginary and $K^+/\mathbb{Q}$ is totally real. Define

$$\mathrm{T}(k) = \{x \in K^\times : x\overline{x} \in \mathbb{Q}\},$$

or in other words ...

The torus

$$\begin{array}{c} K \\ \big| \, 2 \\ K^+ \\ \big| \\ \mathbb{Q} \end{array}$$

Let $K/\mathbb{Q}$ be a field extension of degree $2g$ with intermediate field extension K^+ such that K/K^+ is imaginary and $K^+/\mathbb{Q}$ is totally real. Define

$$\mathsf{T}(k) = \{x \in K^\times : x\overline{x} \in \mathbb{Q}\},$$

or in other words ...

$$\mathsf{T} = \mathrm{Ker}\left(\mathbb{G}_m \times_{\mathrm{Spec}(\mathbb{Q})} \mathsf{R}_{K/\mathbb{Q}}(\mathbb{G}_m) \underset{(x,y)\mapsto x^{-1}N_{K/K^+}(y)}{\longrightarrow} \mathsf{R}_{K^+/\mathbb{Q}}(\mathbb{G}_m)\right).$$

What was known?

This specific torus is maximal in $\mathrm{GSp}_{2g}(\mathbb{Q})$, and was already studied in the context of local-global principle for bilinear forms. However very little was known.

- If $g = 1, 2, 3$ then $\text{Ш}^1(\mathsf{T}) = 0$ by elementary computations.
- If $g = 4$, there is $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) = Q_8$ the quaternion group, such that $\text{Ш}^1(\mathsf{T}) \neq 0$ (Cortella).

Implementation of algebraic tori in SageMath

There was no software to create and study specific tori so I implemented algebraic tori and their character lattices in Sagemath.

To build our lattice, we simply look at the embedding $\mathrm{GSp}_{2g} \hookrightarrow \mathrm{GL}_{2g}$, yielding an embedding $\mathsf{T} \hookrightarrow \mathsf{R}_{K/\mathbb{Q}}\mathbb{G}_m$. The corresponding map on character lattices is a surjection $\mathsf{X}^\star(\mathsf{R}_{K/\mathbb{Q}}\mathbb{G}_m) = \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})] \to \mathsf{X}^\star(\mathsf{T})$. We then just need to compute the quotient by the corresponding kernel.

Results

Assuming $K/\mathbb{Q}$ is Galois, we get ...

Theorem

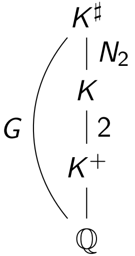
Let $G = \mathrm{Gal}(K/\mathbb{Q})$*.*

- *If the 2-Sylow subgroups of G are cyclic, then* $H^1(\mathbb{Q}, \mathsf{X}^\star(\mathsf{T})) = 0$*, otherwise* $H^1(\mathbb{Q}, \mathsf{X}^\star(\mathsf{T})) = \mathbb{Z}/2\mathbb{Z}$*. In particular,* $\tau_{\mathsf{T}} \leq 2$*.*
- *If* $H^1(\mathbb{Q}, \mathsf{X}^\star(\mathsf{T})) = 0$ *then* $\text{Ш}^1(\mathsf{T}) = 0$ *and* $\tau_{\mathsf{T}} = 1$*, else* $\text{Ш}^1(\mathsf{T}) \subset G^{\mathrm{ab}}[2]$*.*

Remark. In particular, if g is odd, then $\tau_{\mathsf{T}} = 1$.
Remark. We can replace 2's by p's.

Non-Galois Case

Let $K^\sharp$ be the Galois closure of K.



Theorem

We have $H^1(G, \mathrm{X}^\star(\mathrm{T})) \subset \mathbb{Z}/2\mathbb{Z}$. Moreover, $H^1(G, \mathrm{X}^\star(\mathrm{T})) = 0$ if and only if there is $g \in G$ such that $|\langle g \rangle \backslash G/N_2|$ is odd, where $G = \mathrm{Gal}(K^\sharp/\mathbb{Q})$ and $N_2 = \mathrm{Gal}(K^\sharp/K)$.

- $[K : \mathbb{Q}] = 4$: $\tau_\mathrm{T} = 1$ unless $K/\mathbb{Q}$ is Galois and $G = (\mathbb{Z}/2\mathbb{Z})^2$.
- $[K : \mathbb{Q}] = 6$: $\tau_\mathrm{T} = 1$.
- $[K : \mathbb{Q}] = 8$: see this page.

Most general case: CM-étale algebras

Now $K = \bigoplus_{i=1}^{m} K_i$ with totally real subalgebra $K^+ = \bigoplus_{i=1}^{m} K_i^+$.

- We have a method to compute $H^1(\mathbb{Q}, \mathrm{X}^\star(\mathrm{T}))$.

Theorem

Let K/k be an étale CM-algebra and let T^K be the corresponding torus. Assume $K = \bigoplus_{i=1}^{r} K_i^{\oplus j_i}$ for some pairwise non-isomorphic fields $K_1, \cdots, K_r$, and $j_1, \cdots, j_r \in \mathbb{N}$. Let $\tilde{K} = \bigotimes_{i=1}^{r} K_i$. If each K_i is a Galois CM-field and $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) = \prod_{i=1}^{r} \mathrm{Gal}(K_i/\mathbb{Q})$, then

$$\tau(\mathrm{T}^K) = \prod_{i=1}^{r} 2^{j_i - 1} \tau(\mathrm{T}^{K_i}),$$

where T^{K_i} is the torus defined for each field. In particular, if $r = 1$ we can obtain arbitrarily large Tamagawa numbers.

$K = K_1^{\oplus r}$ gives arbitrarily large numbers, $j_i = 1$ may give arbitrarily small ones.

Thank you!

Idea

We can define an auxilliary torus $\mathsf{T}_1 = R_{K^+/\mathbb{Q}} R^{(1)}_{K/K^+}(\mathbb{G}_m)$.

$$\mathsf{T}_1(\mathbb{Q}) = \{x \in K^\times : x\overline{x} = 1\}.$$

$$1 \to \mathsf{T}_1 \to \mathsf{T} \to \mathbb{G}_m \to 1.$$

We can compute the cohomology of T_1, and link it to the cohomology of T by careful examination of the group-theoretic *transfer map* (verlagerung) $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(K/K^+) = \mathbb{Z}/2\mathbb{Z}$ and its relation to 2-Sylow subgroups.

Remark. We can also (painfully) compute H^1 directly, by linking the transfer map to point counts, existence of complement subgroup of the 2-Sylows, and their "cyclicity".

The denominator

To compute $\text{Ш}^1(\mathsf{T})$ in the general case, it depends heavily on K and ramification of the prime ideals of $\mathcal{O}_K$.

In general, we have

$$\text{Ш}^1(\mathsf{T}) \subset \text{Ш}^1_{\mathscr{C}}(\mathsf{T}) := \mathrm{Ker}\left(H^1(\mathbb{Q}, \mathsf{T}) \to \prod_{\alpha \in G} H^1(\langle \alpha \rangle, \mathsf{T})\right).$$

We have a simple criteria for the computation of $\text{Ш}^1_{\mathscr{C}}(\mathsf{T})$ and $\text{Ш}^1(\mathsf{T})$.
In particular, assuming G is abelian, the only possibility for $\text{Ш}^1(\mathsf{T}) \neq 0$ is that its 2-Sylow is of the form $\mathbb{Z}/2^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{n_r}\mathbb{Z}$ with $r > 1$, $n_r > n_1, \cdots, n_{r-1}$, and $\mathrm{Gal}(K/K^+) \subset \mathbb{Z}/2^{n_r}\mathbb{Z}$.

How?

We use Tate-Nakayama duality to get $Ш^1(\mathsf{T}) = Ш^2(\mathsf{X}^\star(\mathsf{T}))$. Let $S \leq G$ and $N = \mathrm{Gal}(K/K^+)$. If S has cyclic 2-Sylow then $H^2(S, \mathsf{X}^\star(\mathsf{T})) = G^{\mathrm{ab}}/N$, otherwise $H^2(S, \mathsf{X}^\star(\mathsf{T})) = G^{\mathrm{ab}}$. $Ш^1_{\mathscr{C}}(\mathsf{T})$ becomes the kernel of

$$G^{\mathrm{ab}} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \prod_{\substack{\alpha \in G \\ N \subset \langle\alpha\rangle}} \langle\alpha\rangle/N \times \prod_{\substack{\alpha \in G \\ N \not\subset \langle\alpha\rangle}} \langle\alpha\rangle,$$

$$f \mapsto \prod_{\substack{\alpha \in G \\ N \subset \langle\alpha\rangle}} f(\alpha) \bmod \frac{1}{2}\mathbb{Z} \times \prod_{\substack{\alpha \in G \\ N \not\subset \langle\alpha\rangle}} f(\alpha).$$

Partial results for 2-groups of order ≤ 256 are available here. In all cases $|Ш^1_{\mathscr{C}}(\mathsf{T})| \leq 8$.

Examples

Example 1. Assume $G = \langle \alpha, \beta | \alpha^4 = \beta^2 = 1,\ \beta\alpha\beta = \alpha^3 \rangle$ the dihedral group D_4 with $N = \langle \alpha^2 \rangle$.
$G^{\mathrm{ab}} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^2 = \langle t_\alpha, t_\beta \rangle$ with
$t_\alpha(\alpha) = t_\beta(\beta) = \frac{1}{2}\mathbb{Z}$.

$$\left.\begin{array}{r} t_\beta(\beta) \neq 0 \text{ and } N \not\subset \langle \beta \rangle \\ t_\alpha(\alpha\beta) \neq 0 \text{ and } N \not\subset \langle \alpha\beta \rangle \end{array}\right\} \to Ш^1(\mathrm{T}) = Ш^1_{\mathscr{C}}(\mathrm{T}) = 0.$$

Example 2. Assume $G = Q_8$ the quaternion group. Here
$N = Z(G)$, and every proper subgroup is cyclic, containing N, so
$G^{\mathrm{ab}} = (\mathbb{Z}/2\mathbb{Z})^2 = Ш^1_{\mathscr{C}}(\mathrm{T})$.
Therefore, $\tau_{\mathrm{T}} = \frac{2}{1} = 2$ if a prime number of $\mathbb{Q}$ remains prime in K,
otherwise $\tau_{\mathrm{T}} = \frac{2}{4} = \frac{1}{2}$.
Find examples in the LMFDB