Automorphisms and isometries of lattices over algebraic integers

Thomas Camus

Institut Fourier, partially supported by LabEx PERSYVAL-Lab (ANR-11-LABX-0025)

PARI/GP Workshop, January 9th–13th 2017

Introduction

- **Algebraic lattice:** classical lattice with an additional algebraic structure (coming from a number field).

- **Theory under development:** lots of results are still missing.

- **Lack of algorithms and implementations:** many algorithms are non-existent or not implemented.

- **Motivations:**
  - Relative algebraic number theory.
  - Lattice-based cryptography.
  - Torsion in the K-theory of $\mathbb{Z}_K$ [Soulé, '03], effective computations of the cohomology of $\mathrm{GL}_N(\mathbb{Z})$ [Elbaz-Vincent *& al.*, '13].

Euclidean structure on $(K \otimes_{\mathbb{Q}} \mathbb{R})^n$

Let K be a number field with signature (r, s) and $\mathbb{Z}_K$ be its ring of integers. For all $n \geqslant 1$, we set $K_{\mathbb{R}}^n := (K \otimes_{\mathbb{Q}} \mathbb{R})^n$.

The $\mathbb{R}$-vector space $K_{\mathbb{R}}^n$ is equipped with an euclidean inner product:

$$\langle x \,|\, y \rangle := \sum_{i=1}^{n} \sum_{\sigma \in \Sigma} \rho_\sigma \overline{\sigma}(x)\sigma(y),$$

with $\rho_\sigma := 1$ if σ is a real embedding and $\rho_\sigma := 1/2$ otherwise.

The "natural" identification between $K_{\mathbb{R}}^n$ and $\mathbb{R}^{n[K:\mathbb{Q}]}$ is an isometry.

In practice, we want to avoid as much as possible the use of this isometry.

Algebraic lattices

Definition

A subgroup Λ of $K_{\mathbb{R}}^n$ is called an algebraic lattice of rank n over K if:

- Λ is a lattice in $K_{\mathbb{R}}^n$, i.e. a discrete subgroup of $K_{\mathbb{R}}^n$ of rank $n[K:\mathbb{Q}]$.
- Λ is a sub-$\mathbb{Z}_K$-module of $K_{\mathbb{R}}^n$.

Fundamental examples: sub-$\mathbb{Z}_K$-modules of rank n of K^n.

Fundamental structure of algebraic lattices

Theorem [Steinitz, 1912] [Laca *& al.*, 2009]

Let Λ be an algebraic lattices of rank n over K.

- There exists a $K_{\mathbb{R}}$-basis $(b_1, \dots, b_n)$ of $K_{\mathbb{R}}^n$ and fractional ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ of K such that
$$\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n.$$
- The class of the product ideal $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ fully determines Λ modulo $\mathrm{GL}_n(K_{\mathbb{R}})$.

Ideal class group of K.

$\uparrow\downarrow$

Algebraic lattices of rank n over K up to isomorphism.

Stabilizer in $\mathrm{GL}_n(K_{\mathbb{R}})$ of an algebraic lattice

Let $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ be an algebraic lattice. The orbit of Λ under $\mathrm{GL}_n(K_{\mathbb{R}})$ can be identified to $\mathrm{GL}_n(K_{\mathbb{R}})/\mathrm{GL}(\Lambda)$, where $\mathrm{GL}(\Lambda)$ is the stabilizer of Λ in $\mathrm{GL}_n(K_{\mathbb{R}})$.

Proposition

Let u be a $K_{\mathbb{R}}$-automorphism of $K_{\mathbb{R}}^n$ with matrix A in the basis $(b_1, \ldots, b_n)$. Then

$$u(\Lambda) = \Lambda \Leftrightarrow \begin{cases} \det(A) \in \mathbb{Z}_K^{\times}, \\ a_{i,j} \in \mathfrak{a}_i \mathfrak{a}_j^{-1} \quad \forall\, 1 \leqslant i, j \leqslant n. \end{cases}$$

Example: $\mathrm{GL}(\Lambda) \cong \mathrm{GL}_n(\mathbb{Z}_K)$ if $\mathfrak{a}_1 = \cdots = \mathfrak{a}_n = \mathbb{Z}_K$. But this is not always the case!

Automorphism and isometry of algebraic lattices

We can associate two automorphism groups to an algebraic lattice Λ of rank n over K:

Definition

- The group $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ formed of the euclidean automorphisms of $K_{\mathbb{R}}^n$ which preserve Λ is the automorphism group of Λ viewed as a (classical) lattice.
- The $K_{\mathbb{R}}$-linear elements of $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ form a subgroup $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, called the $K_{\mathbb{R}}$-automorphism group of Λ.

We have the identifications

$$\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda) \cong \mathrm{GL}(\Lambda) \cap \mathrm{O}_n(K_{\mathbb{R}}) \quad \text{and} \quad \mathrm{Aut}_{\mathbb{R}}(\Lambda) \cong \mathrm{GL}(\Lambda) \cap \mathrm{O}_{nd}(\mathbb{R}) \ .$$

The notion of $K_{\mathbb{R}}$-isometry between algebraic lattices is defined analogously.

Computing automorphisms and isometries of algebraic lattices

Problems

1. How to determine the group $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$?
2. How to decide whether two algebraic lattices are $K_{\mathbb{R}}$-isometric?

The case of classical lattices is tackled by the algorithm of Plesken & Souvignier [Plesken & Souvignier, '97], implemented by the functions `qfisom` and `qfauto` in GP.

Is it possible to adapt this algorithm for algebraic lattices?

Partial automorphism

Let us fix $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ an algebraic lattice in $K_{\mathbb{R}}^n$ and let $(\omega_1, \ldots, \omega_d)$ be a $\mathbb{Q}$-basis of K.

Proposition

A $K_{\mathbb{R}}$-endomorphism f is orthogonal if and only if for all $1 \leqslant i, j \leqslant n$ and $1 \leqslant k, l \leqslant d$

$$\langle \omega_k f(b_i) \,|\, \omega_l f(b_j) \rangle = \langle \omega_k b_i \,|\, \omega_l b_j \rangle.$$

Definition

Let $1 \leqslant m \leqslant n$. A m-partial automorphism of Λ is a m-tuple $\boldsymbol{v} = (v_1, \ldots, v_m)$ of elements in Λ such that for all $1 \leqslant i, j \leqslant m$ and $1 \leqslant k, l \leqslant d$

$$\langle \omega_k v_i \,|\, \omega_l v_j \rangle = \langle \omega_k b_i \,|\, \omega_l b_j \rangle.$$

A pool for partial automorphisms

A partial automorphism of $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ has its values in

$$S = \bigcup_{j=1}^{n} \left\{ x \in \mathfrak{a}_1 \mathfrak{a}_j^{-1} b_1 \oplus \cdots \oplus \mathfrak{a}_n \mathfrak{a}_j^{-1} b_n \;:\; \|x\| = \|b_j\| \right\}.$$

How to compute such sets?

1. By combining $\mathbb{Z}$-bases of $\mathfrak{a}_i \mathfrak{a}_j^{-1}$ for all i, identify $\mathfrak{a}_1 \mathfrak{a}_j^{-1} b_1 \oplus \cdots \oplus \mathfrak{a}_n \mathfrak{a}_j^{-1} b_n$ to a $\mathbb{Z}$-lattice of rank $n[K:\mathbb{Q}]$.
2. Now, we can use an enumerating algorithm [Fincke & Pohst, '85] to compute these sets of "short" vectors (`qfminim` function in PARI/GP).

Computing S is the most complex part of the algorithm. In fact, computing $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ knowing S can be done in quasi-polynomial (in $|S|$) time.

How to compute a $K_{\mathbb{R}}$-automorphism?

Idea

Recursively extend a 1-partial automorphism of Λ into a $K_{\mathbb{R}}$-automorphism by choosing a suitable $v_i \in \Lambda$ at each step.

Issue

It may happen that a partial automorphism cannot be extended to a $K_{\mathbb{R}}$-automorphism of Λ.

We want invariants that allow us the reject "bad candidates" as soon as possible in the backtrack search.

Invariant 1: fingerprint of a $K_{\mathbb{R}}$-basis

Proposition

If $\boldsymbol{v}$ can be extended into a $K_{\mathbb{R}}$-automorphism of Λ, the number of extensions of $\boldsymbol{v}$ to a $(m+1)$-partial automorphism is equal to the number of extensions of $(b_1, \ldots, b_m)$ to a $(m+1)$-partial automorphism.

How to use it:

- Naively precompute the number of extensions of $(b_1, \ldots, b_{m-1})$ to a m-partial automorphism of Λ for all $2 \leqslant m \leqslant n$.
- Determine a permutation of the initial basis minimizing these values.

Invariant 2: the scalar combinations

Let $\boldsymbol{s} = (s_{k,l,j})_{\substack{1 \leqslant k,l \leqslant d \\ 1 \leqslant j \leqslant m}} \in \mathbb{R}^{md^2}$ and $\boldsymbol{v}$ be a m-partial automorphism of Λ.
We set:

Definition

$$X_{\boldsymbol{s}}(\boldsymbol{v}) := \{x \in \Lambda \, : \, \langle \omega_k x \,|\, \omega_l v_j \rangle = s_{k,l,j} \ \forall\, k,l,j\}\,.$$

$$\widehat{X}_{\boldsymbol{s}}(\boldsymbol{v}) := \sum_{x \in X_{\boldsymbol{s}}(\boldsymbol{v})} x.$$

Proposition

Let $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. For all $\boldsymbol{s} \in \mathbb{R}^{md^2}$, we have

$$f(\widehat{X}_{\boldsymbol{s}}(b_1, \ldots, b_m)) = \widehat{X}_{\boldsymbol{s}}(f(b_1), \ldots, f(b_m)).$$

How to use it: a bit messy and complex...

The backtrack search for a $K_{\mathbb{R}}$-automorphism

❶ Compute the set C_1 of all 1-partial automorphisms of Λ and choose $v_1 \in C_1$.

❷ Let us assume that $\boldsymbol{v}$ is a m-partial automorphism of Λ (with $m < n$). Compute the set C_{n+1} of all elements of Λ extending $\boldsymbol{v}$ and choose $x \in C_{n+1}$.

- ✓ If $(\boldsymbol{v}, x)$ is "good candidate", go to the next step.
- ✗ Otherwise, choose another $x \in C_{n+1}$. If all possibilities are exhausted, return to the previous step.

From one $K_{\mathbb{R}}$-automorphism to $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$

It is generally not a good idea to enumerate all elements of $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, even in small dimension and degree...

Question

How to compute a generating set of $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$?

The group $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ **can be identified to a permutation group:** hence, we can use a Schreier & Sims-like algorithm to compute it.

Conclusions

✓ Theoretical algorithm effective for all number fields and all algebraic lattices.

✓ C code using the PARI library ($\approx$ 3000 lines).
✓ Works for lattices in K^n.
✗ With minor modifications should work in $K_{\mathbb{R}}^n$...

✗ What about the complexity analysis?
✗ We don't have one, even for the euclidean algorithm...
✓ But we have a general result for the isometric lattices problem.

✗ Partially effective certification.