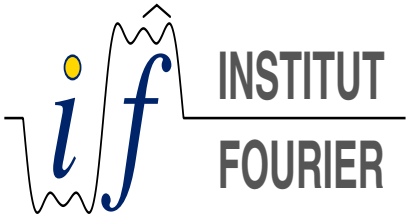
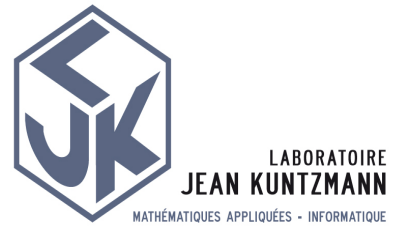
Calcul des isométries de réseaux algébriques

Thomas Camus

Institut Fourier, partiellement supporté par le LabEx PERSYVAL-Lab (ANR-11-LABX-0025)

Journées Nationales du Calcul Formel 2015





Réseaux euclidiens classiques (sur $\mathbb{Z}$)

- Théorie bien connue :
  - Inégalités géométriques (Hadamard, Hermite, Mordell...).
  - Dictionnaire réseaux / formes quadratiques.
  - Théorie de Voronoï (extremalité, perfection et eutaxie).

- Algorithmique développée et implantée :
  - Algorithmes de réduction (LLL, BKZ,...).
  - Calcul des automorphismes (Plesken et Souvignier, 1997).
  - Algorithme de Voronoï (effectif en dimension $\leqslant 8$).

Introduction

Réseaux sur un anneau d'entiers algébriques

- Théorie en développement :
  - Travaux pour des familles restreintes de réseaux.
  - Correspondance partielle entre réseaux et formes.
  - Extension de la théorie de Voronoï (Okuda et Yano, 2010).

- Algorithmique incomplète et peu implantée :
  - Réduction partiellement polynomiale (Fieker et Stehlé, 2010).
  - Algorithme de Voronoï (Watanabe, Yano et Hayashi, 2013).

Motivations

- Géométrie algorithmique des nombres dans un contexte *relatif*.
- Cryptographie basée sur la complexité de l'algorithmique des réseaux.
- Cohomologie des groupes linéaires.

Plan

1. Le $K_{\mathbb{R}}$-espace euclidien $(K \otimes_{\mathbb{Q}} \mathbb{R})^n$
2. Réseaux sur un anneau d'entiers algébriques
3. Calcul des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique

Plan

Le $\mathbb{R}$-espace vectoriel $(K \otimes_{\mathbb{Q}} \mathbb{R})^n$

Soient K un corps de nombres de degré d et $\mathcal{O}_K$ son anneau d'entiers.
Pour tout $n \geqslant 1$, on note $K_{\mathbb{R}}^n := (K \otimes_{\mathbb{Q}} \mathbb{R})^n$. C'est un

- $\mathbb{R}$-espace vectoriel de dimension nd.
- $K_{\mathbb{R}}$-module libre de rang n.

Comme $\mathbb{R}$-espace vectoriel, $K_{\mathbb{R}}^n$ s'identifie à $\mathbb{R}^{nr} \times \mathbb{C}^{ns}$ (et donc à $\mathbb{R}^{nd}$), où r désigne le nombre de plongements réels de K et $2s$ le nombre de plongements complexes de K.

Si $\Sigma = \{\sigma_1, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}\}$ désigne l'ensemble des plongements de K dans $\mathbb{C}$, cette identification est induite par :

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{R}^r \times \mathbb{C}^s \\ x & \longmapsto & (\sigma_1(x), \ldots, \sigma_{r+s}(x)) \end{array} .$$

Structure euclidienne sur $(K \otimes_{\mathbb{Q}} \mathbb{R})^n$

Le $\mathbb{R}$-espace vectoriel $K_{\mathbb{R}}^n$ est équipé du produit scalaire euclidien défini pour tout $x, y \in K_{\mathbb{R}}^n$ par

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

où $\rho_\sigma := 1$ si σ est un plongement réel et $\rho_\sigma := 1/2$ sinon.

Ce produit scalaire provient essentiellement d'une version tordue de la trace de $K_{\mathbb{R}}$ sur $\mathbb{R}$ (qui prolonge la trace de K sur $\mathbb{Q}$).

☞ Les identifications entre $K_{\mathbb{R}}^n$, $\mathbb{R}^{nr} \times \mathbb{C}^{ns}$ et $\mathbb{R}^{nd}$ deviennent des isométries de $\mathbb{R}$-espaces vectoriels (en considérant la structure euclidienne classique de $\mathbb{R}^{nd}$).

Automorphismes orthogonaux

Un élément $A \in \mathrm{GL}_n(K_{\mathbb{R}})$ est dit orthogonal si $\langle Ax \,|\, Ay \rangle = \langle x \,|\, y \rangle$ pour tout $x, y \in K_{\mathbb{R}}^n$. On note $\mathrm{O}_n(K_{\mathbb{R}})$ le sous-groupe des éléments orthogonaux de $\mathrm{GL}_n(K_{\mathbb{R}})$.

Il y a un isomorphisme de groupes

$$\mathrm{O}_n(K_{\mathbb{R}}) \cong \mathrm{O}_n(\mathbb{R})^r \times \mathrm{U}_n(\mathbb{C})^s \hookrightarrow \mathrm{O}_{nd}(\mathbb{R}).$$

☞ Il est possible de construire φ une involution $\mathbb{R}$-linéaire sur $K_{\mathbb{R}}^n$ telle que une matrice $A \in \mathrm{GL}_n(K_{\mathbb{R}})$ est orthogonale si et seulement si $\varphi(A)^{\mathsf{T}} \cdot A = I_n$.

Plan

Réseaux algébriques

Définition

Un sous-groupe Λ de $K_{\mathbb{R}}^n$ est appelé un réseau algébrique de rang n si :

- Λ est un $\mathbb{Z}$-réseau de $K_{\mathbb{R}}^n$, c'est-à-dire un sous-groupe discret de $K_{\mathbb{R}}^n$ de rang nd.
- Λ est un sous-$\mathcal{O}_K$-module de $K_{\mathbb{R}}^n$.

Exemples fondamentaux : les sous-$\mathcal{O}_K$-modules de rang n de K^n.

L'ensemble des réseaux algébriques de $K_{\mathbb{R}}^n$

Théorème

Soit Λ un réseau algébrique de $K_{\mathbb{R}}^n$.

- Il existe une $K_{\mathbb{R}}$-base $(b_1, \ldots, b_n)$ de $K_{\mathbb{R}}^n$ et des idéaux fractionnaires $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ de K tels que

$$\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n.$$

- La classe de l'idéal $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ caractérise complètement Λ modulo $\mathrm{GL}_n(K_{\mathbb{R}})$.

☞ Construction explicite des systèmes de représentants de l'ensemble des réseaux de $K_{\mathbb{R}}^n$ modulo $\mathrm{GL}_n(K_{\mathbb{R}})$.

Automorphismes et isométries de réseaux algébriques

Deux groupes d'automorphismes sont associés à un réseau algébrique Λ de $K_{\mathbb{R}}^n$:

Définition

- Le groupe $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ des $\mathbb{R}$-automorphismes (orthogonaux) de Λ des $\mathbb{R}$-automorphismes de Λ est le groupe d'automorphismes de Λ vu comme $\mathbb{Z}$-réseau euclidien de $\mathbb{R}^{nd}$.
- Les éléments $K_{\mathbb{R}}$-linéaires de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ forment le sous-groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ des $K_{\mathbb{R}}$-automorphismes de Λ.

On a les identifications :

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

On définit de manière analogue les notions d'isométries pour les réseaux algébriques.

Plan

Calcul des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique

Questions

1. Comment déterminer le groupe des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique ?
2. Comment décider si deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques ?

☞ Le cas des $\mathbb{Z}$-réseaux est traité par l'algorithme de Plesken et Souvignier (1997).

Automorphisme partiel

On fixe $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \mathfrak{a}_n b_n$ un réseau algébrique de K^n et $(\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base de K.

Un $K_{\mathbb{R}}$-endomorphisme f est orthogonal si et seulement si pour tout $1 \leqslant i, j \leqslant n$ et $1 \leqslant k, l \leqslant d$

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

Définition

Soit $1 \leqslant m \leqslant n$. Un m-automorphisme partiel de Λ est un m-uplet $(v_1, \ldots, v_m)$ d'éléments de Λ tel que pour tout $1 \leqslant i, j \leqslant m$ et $1 \leqslant k, l \leqslant d$

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

Construction récursive d'un $K_{\mathbb{R}}$-automorphisme

Idée

Compléter récursivement un 1-automorphisme partiel de Λ en un $K_{\mathbb{R}}$-automorphisme, en choisissant à chaque étape un élément $v_i \in \Lambda$ convenable.

Problème

Un automorphisme partiel n'est pas toujours prolongeable en un $K_{\mathbb{R}}$-automorphisme de Λ.

☞ Importance d'avoir des invariants permettant de tester si un automorphisme partiel est un bon candidat pour fournir un $K_{\mathbb{R}}$-automorphisme de Λ.

Empreinte d'une $K_{\mathbb{R}}$-base

Proposition

Soit v un m-automorphisme partiel. Si v se prolonge en un automorphisme de Λ, le nombre de prolongements de v en un $(m+1)$-automorphisme partiel est égal au nombre de prolongements de $(b_1, \ldots, b_m)$ en un $(m+1)$-automorphisme partiel.

En pratique

- On précalcule le nombre de prolongements possible de $(b_1, \ldots, b_m)$ en un $(m+1)$-automorphisme partiel de Λ pour tout $1 \leqslant m < n$.
- On détermine aussi une permutation de la base initiale permettant de minimiser ces valeurs.

Sommes de vecteurs

Soient $s = (s_{k,l,j})_{\substack{1 \leqslant k,l \leqslant d \\ 1 \leqslant j \leqslant m}} \in \mathbb{R}^{md^2}$ et v un m-automorphisme partiel de Λ. On pose :

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

$$\overline{X}_s(v) := \sum_{x \in X_s(v)} x.$$

Les $K_{\mathbb{R}}$-automorphismes préservent ces données :

Proposition

Soit $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. On a

$$f(\overline{X}_s(b_1, \ldots, b_m)) = \overline{X}_s(f(b_1), \ldots, f(b_m)).$$

Précalcul des sommes de vecteurs

Les sommes de vecteurs associées à $(b_1, \ldots, b_m)$ sont précalculées sous la forme suivante pour tout $1 \leqslant m \leqslant n$:

1. On extrait une K-base X de l'ensemble des $\overline{X}_s(b_1, \ldots, b_m)$, donnée par des indices $(x_1, \ldots, x_h)$, de telle façon que $X_i = \overline{X}_{x_i}(b_1, \ldots, b_m)$ pour tout $1 \leqslant i \leqslant h$.

2. On calcule l'ensemble $\{\langle \omega_k X_i \,|\, \omega_l X_j \rangle \quad i, j, k, l \text{ convenables}\}$.

3. On détermine les K-coordonnées des $\overline{X}_s(b_1, \ldots, b_m)$ dans la base X.

Test d'un candidat : étape 1

Soient v un m-automorphisme partiel de Λ et C l'ensemble des éléments $x \in S$ tels que (v, x) soit un $(m+1)$-automorphisme partiel.

Étape 1

On vérifie si le cardinal de C est égal au nombre de prolongements de $(b_1, \ldots, b_m)$ en un $(m+1)$-automorphisme partiel à l'aide des données de l'empreinte.

Test d'un candidat : étape 2

On calcule les sommes de vecteurs $\overline{X}_s(v)$ associées à v. On pose ensuite $\tilde{X}_i := \overline{X}_{x_i}(v)$, où les x_i sont les indices de la base des sommes de vecteurs associées à $(b_1, \ldots, b_m)$.

Étape 2

1. On vérifie que $\langle \omega_k \tilde{X}_i \,|\, \omega_l \tilde{X}_j \rangle = \langle \omega_k X_i \,|\, \omega_l X_j \rangle$ pour tout i, j, k, l.

2. On teste si $\overline{X}_s(v) = \sum_{i=1}^{h} \lambda_{s,i} \tilde{X}_i$ pour tout $s \in \mathbb{R}^{nd^2}$, où les $(\lambda_{s,i})_i$ sont les K-coordonnées de $\overline{X}_s(b_1, \ldots, b_m)$ dans la base X.

Recherche d'un $K_{\mathbb{R}}$-automorphisme

1. On calcule l'ensemble C_1 des 1-automorphismes de Λ et on choisit un élément v_1 de C_1.

2. Supposons déterminé v un m-automorphisme partiel de Λ (avec $m < n$). On calcule C_{n+1} des éléments $x \in S$ tels que (v, x) soit un $(n+1)$-automorphisme partiel et on choisit $x \in C_{n+1}$.
   - Si (v, x) est un « bon » candidat pour fournir un $K_{\mathbb{R}}$-automorphisme, on passe au rang $m+1$.
   - Sinon, un autre $x \in C_{n+1}$ est choisit. Si toutes les possibilités sont épuisées, on retourne au rang $m-1$.

Passage au groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$

Nous disposons maintenant d'un algorithme permettant de prolonger les automorphismes partiels de Λ.

Question

Comment déterminer le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ tout entier ?

Il est inenvisageable de donner $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ comme une liste exhaustive d'éléments, même en petite dimension :

- Le réseau $\mathbf{E}_8$, plongé dans $\mathbb{Q}(i\sqrt{5})^8$, possède plus de 10^7 $K_{\mathbb{R}}$-symétries.
- Le réseau de Leech, plongé dans $\mathbb{Q}(i)^{24}$, possède plus de 10^{38} $K_{\mathbb{R}}$-symétries.

Passage au groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$

Le groupe $G := \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ peut être identifié à un groupe de permutations ➢ Adaptation de l'algorithme de Schreier et Sims (1970).

On cherche à déterminer $\mathcal{G}$ une famille génératrice de G telle que

$$\langle\, \mathcal{G} \cap \mathrm{Stab}_G(b_1, \ldots, b_i) \,\rangle = \mathrm{Stab}_G(b_1, \ldots, b_i) \quad \forall\, 1 \leqslant i \leqslant n.$$

☞ Connaître une telle famille génératrice apporte de nombreuses informations sur le groupe et facilite les manipulations algorithmiques.

Conclusions et perspectives

- ✓ Algorithme théorique pour tout corps de nombres et tout réseau algébrique.
- ✓ Code C utilisant la librairie PARI/GP (env. 2000 lignes).
  - ✓ Fonctionnel pour les réseaux algébriques de $\mathbb{Q}(\sqrt{d})^n$.
  - ✗ Passage à tout corps de nombres ?
  - ✗ Passage aux réseaux algébriques de $K_{\mathbb{R}}^n$?
- ✗ Analyse de complexité manquante (même dans le cas euclidien classique).
- ✗ La certification des résultats est partiellement effective.