

Calcul des isométries de réseaux algébriques

Thomas Camus*

Institut Fourier, UMR 5582 (CNRS-Université Grenoble Alpes),
100 rue des Mathématiques, 38402 Saint Martin d'Hères, France.

`thomas.camus@ujf-grenoble.fr`

Les réseaux sur un anneau d'entiers algébriques (ou réseaux algébriques) sont une spécialisation de la notion classique de réseau euclidien. Ce sont des objets qui apparaissent naturellement dans des domaines variés tels que la géométrie algorithmique des nombres et la cryptographie. Bien que la théorie englobant les réseaux algébriques soit aujourd'hui mieux comprise, son versant algorithmique demeure encore incomplet.

Nous considérons ici deux des problèmes majeurs en algorithmique des réseaux algébriques :

1. Comment décider si deux réseaux algébriques sont isométriques ?
2. Comment déterminer le groupe des automorphismes d'un réseau algébrique ?

La première question revient à se demander s'il possible de vérifier si deux objets algébriques partagent les mêmes propriétés géométriques. Quant à la seconde, elle concerne la faisabilité du calcul des symétries d'un réseau algébrique.

L'algorithme de Plesken et Souvignier [1] permet aujourd'hui de répondre à ces questions dans le cadre euclidien. On dispose notamment d'implantations effectives de cet algorithme (par exemple dans la librairie PARI/GP [2]).

L'objectif de ce travail est de présenter une adaptation de l'algorithme de Plesken et Souvignier pour les réseaux algébriques. Nous expliquerons notamment comment s'affranchir de l'identification d'un réseau algébrique à un réseau euclidien en travaillant directement sur l'anneau d'entiers algébriques

*Partiellement supporté par le LabEx PERSYVAL-Lab (ANR-11-LABX-0025).

considéré. Ce travail mélange des techniques de calcul exact et de le calcul approché. Cet algorithme a été implantée et testée avec succès en utilisant la librairie PARI/GP.

Ces travaux rentrent dans le cadre de ma thèse dirigée par Ph. Elbaz-Vincent (Institut Fourier) et J.-G. Dumas (Laboratoire Jean Kuntzmann).

Bibliographie

- [1] W. PLESKEN ET B. SOUVIGNIER, *Computing isometries of lattices*, Journal of Symbolic Computation, 24 (1997), pp. 327–334.
<http://www.sciencedirect.com/science/article/pii/S0747717196901303>
- [2] THE PARI GROUP, *PARI/GP version 2.7.3*, Bordeaux, 2014.
<http://pari.math.u-bordeaux.fr/>.
- [3] K. OKUDA ET S. YANO, *A generalization of Voronoi's Theorem to algebraic lattices*, Journal de Théorie des Nombres de Bordeaux, 22 (2010), pp. 727–740.
<https://eudml.org/doc/116430>
- [4] T. WATANABE, S. YANO ET T. HAYASHI, *Voronoi's reduction theory of GL_n over a totally real number field*, Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, 587 (2013). p. 213
<http://www.math.sci.osaka-u.ac.jp/~twatanabe/voronoioreduction.pdf>
- [5] J. MARTINET, *Perfect lattices in Euclidean spaces*, vol. 327, Springer, 2003.
- [6] Y. GAN, C. LING ET W.-H. WAI, *Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection*, Signal Processing, IEEE Transactions on, 57-7 (2009), pp. 2701–2710.