Méthodes explicites pour les groupes arithmétiques

Aurel Page

15 juillet 2014

Résumé

Les algèbres centrales simples ont de nombreuses applications en théorie des nombres, mais leur algorithmique est encore peu développée. Dans cette thèse, j'apporte une contribution dans deux directions. Premièrement, je présente des algorithmes de complexité prouvée, ce qui est nouveau dans la plupart des cas. D'autre part, je développe des algorithmes heuristiques mais très efficaces en pratique pour les exemples qui nous intéressent le plus, comme en témoignent mes implantations. Les algorithmes sont à la fois plus rapides et plus généraux que les algorithmes existants.

Précisément, je m'intéresse aux problèmes suivants : calcul du groupe des unités d'un ordre et problème de l'idéal principal. Je commence par étudier le diamètre du domaine fondamental de certains groupes d'unités grâce à la théorie des représentations. Je décris ensuite un algorithme prouvé pour calculer des générateurs et une présentation du groupe des unités d'un ordre maximal dans une algèbre à division, puis un algorithme efficace qui calcule également un domaine fondamental dans le cas où le groupe des unités est un groupe kleinéen. De même, je donne un algorithme de complexité prouvée qui détermine si un idéal d'un tel ordre est principal et qui en calcule un générateur le cas échéant, puis je décris un algorithme heuristiquement sous-exponentiel pour résoudre le même problème dans le cas d'une algèbre de quaternions indéfinie.

Abstract

Central simple algebras have many applications in number theory, but their algorithmic theory is not fully developped yet. In this thesis, I am contributing in two directions. First, I present algorithms with proved complexity, which is new in most cases. On the other hand, I develop heuristic algorithms that are very efficient in practice for the most interesting examples, as witnessed by my implementations. The algorithms are both faster and more general than the existing ones.

Precisely, I consider the following problems: computation of the unit group of an order and principal ideal problem. I start by studying the diameter of fundamental domains of some unit groups using representation theory. Then I describe an algorithm with proved complexity for computing generators and a presentation of the unit group of a maximal order in a division algebra, and then an efficient algorithm that also computes a fundamental domain in the case where the unit group is a Kleinian group. Similarly, I present an algorithm with proved complexity that decides whether an ideal of such an order is principal and that computes a generator when it is the case, then I describe a heuristically subexponential algorithm that solves the same problem in indefinite quaternion algebras.