Calculs symboliques et preuves formelles en théorie algébrique des nombres

Laboratoire, institution, université :
Inria, Université de Nantes (LS2N),
en collaboration avec la Vrije Universiteit (VU) Amsterdam, Pays-Bas.

Lieu du stage :
LS2N - Laboratoire des Sciences du Numérique de Nantes
Université de Nantes – faculté des Sciences et Techniques (FST)
2 Chemin de la Houssinière, Bâtiment 34,
44322 Nantes.

Équipe : Gallinette.

Encadrants :
Assia Mahboubi, *Inria — VU Amsterdam (chaire à temps partiel)*
Sander Dahmen, *VU Amsterdam, département de Mathématiques.*

Contact : Assia.Mahboubi@inria.fr

Mots clefs : preuve formelle, calcul formel, théorie algébrique des nombres.

Contexte. La théorie des nombres explore les propriétés des nombres entiers. Ce domaine des mathématiques est connu pour le contraste saisissant entre la simplicité de ses énoncés et la sophistication des outils utilisés pour y répondre, qui convoquent par ailleurs une gamme très variée d'autres champs mathématiques.

L'utilisation de méthodes algébriques pour étudier les nombres entiers relève de la *théorie algébrique des nombres*. Elle trouve son origine dans l'étude des équations dites diophantiennes, c'est à dire les équations polynomiales, à une ou plusieurs inconnues et à coefficients entiers, et dont les solutions recherchées sont elles-mêmes entières (ou rationnelles). Le dernier théorème de Fermat, appelé aussi théorème de Fermat-Wiles, est un exemple de résultat emblématique de théorie algébrique des nombres :

Théorème 1 (A. Wiles, 1995). *L'équation $x^n + y^n = z^n$ ne possède pas de solution entière $x, y, z > 0$ lorsque $n \geq 3$.*

À partir des années 60, la puissance de calcul de l'ordinateur confère une place de premier plan aux aspects effectifs et algorithmiques de la théorie algébrique des nombres. Ces algorithmes jouent un rôle crucial dans plusieurs développements majeurs du domaine, mais aussi dans des applications à la cryptographie moderne. Leur conception et leur implantation constitue de fait un sujet de recherche très actif.

L'objectif de ce stage est de concevoir et de réaliser des bibliothèques de mathématiques formalisées en théorie algébrique des nombres, à l'aide de l'assistant de preuve Coq [4]. On s'intéressera en particulier à la vérification d'algorithmes de calcul symbolique (aussi appelé calcul formel). L'objectif à terme est de fournir des implantations de ces algorithmes dont la correction est vérifiée formellement, fournissant ainsi le plus haut niveau de garantie possible.

Les assistants de preuve sont des logiciels qui permettent de faire des mathématiques sur ordinateur. D'usage moins répandu que certains systèmes de calcul symbolique, numérique ou statistique, ils sont conçus pour aider leurs utilisateurs à représenter définitions, énoncés et démonstrations dans un formalisme logique précis et non ambigu. L'assistant de preuve Coq est doté d'un corpus de bibliothèques d'algèbre formalisée significatif, qui sera le point de départ de ce travail.

Mais les assistants de preuve peuvent également être utilisés pour écrire des programmes, les exécuter, les spécifier et vérifier formellement ces spécifications. Jusqu'il y a peu, c'est en fait l'usage majoritaire qui en a été fait, allant jusqu'à la vérification de programmes sophistiqués comme un compilateur ou un micro-noyau. Dans ce stage, on utilisera une approche similaire, mais pour des applications au calcul symbolique, en théorie des nombres.

Objectifs du stage. Dans le cadre de ce stage, on se propose d'étudier les algorithmes de calcul des nombres de classes des corps quadratiques.

Un corps de nombres algébriques, ou corps de nombres, est le plus petit corps obtenu en ajoutant au corps $\mathbb{Q}$ des rationnels la racine d'un polynôme à coefficient entiers. Un corps quadratique est engendré par la racine d'un polynôme de degré 2 : un tel corps de nombres est de la forme $\mathbb{Q}(\sqrt{d})$ pour d un nombre entier sans carré différent de 1.

Les corps de nombres apparaissent naturellement dans l'étude des équations diophantiennes. Par exemple, la classe d'équations qui fait l'objet du théorème 1 est liée à l'étude du corps $\mathbb{Q}(\zeta)$, où ζ est une racine primitive n-ème de l'unité. En effet, pour une ζ une racine primitive n-ème de l'unité, on peut écrire la forme

factorisée suivante :

$$x^n = z^n - y^n = (z-y)(z-\zeta y)(z-\zeta^2 y)\cdots(z-\zeta^{n-1}y).$$

Si K est un corps de nombres, on appelle anneau des entiers $\mathbb{Z}_K$ le sous-anneau de ce corps formé par les racines de polynômes unitaires à coefficients dans $\mathbb{Z}$. Par exemple, l'anneau des entiers du corps $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$. L'anneau $\mathbb{Z}_K$ joue de fait pour K un rôle analogue à celui que joue $\mathbb{Z}$ pour $\mathbb{Q}$.

Cette factorisation suggère que la solution puisse être obtenue par un analogue de la décomposition unique en produit de facteurs premiers, appliqué à chacun des membres de l'équation. Mais, contrairement à la situation dans l'anneau des entiers $\mathbb{Z}$, une telle propriété n'est en général pas disponible en dans l'anneau $\mathbb{Z}_K$. Le groupe des classes $Cl(K)$ associé à un corps de nombres K est un invariant important, qui mesure le "défaut" de factorisation unique de l'anneau $\mathbb{Z}_K$. Ce groupe est fini et son ordre, c'est à dire son cardinal, est appelé le nombre de classes de K.

Dans le cadre de ce stage, on se propose ainsi d'étudier le *calcul* de ce nombre de classes, pour le cas des corps quadratiques. Le cas très particulier des corps quadratiques est déjà associé à des problèmes ouverts importants. Par exemple, à la connaissance de l'auteur, on ne sait pas à ce jour s'il existe une infinité de corps de nombres quadratiques réels de nombre de classes égal à 1.

Néanmoins, le cas des corps quadratiques permet de considérer des méthodes élémentaires pour calculer ces invariants, qui ne font en fait pas appel à des résultats spécifiques de théorie algébrique des nombres, mais plutôt aux propriétés de réduction des formes quadratiques. Ce sera le point de départ du stage, qui pourra se prolonger selon le temps et l'envie du stagiaire par l'étude d'algorithmes plus complexes, et plus efficaces. Les algorithmes de calcul de nombres de classe que l'on se propose d'étudier sont ceux décrit par H. Cohen dans son livre de référence [2]. On pourra aussi consulter les notes de cours (en français) de K. Belabas [1] pour une introduction à l'algorithmique de la théorie algébrique des nombres.

L'objectif principal de ce travail est ultimement d'écrire des bibliothèques de mathématiques formalisées avec l'assistant de preuve Coq. Ces nouvelles bibliothèques compléteront un corpus existant avec des concepts élémentaires de théorie des nombres algébriques reliés aux corps de nombres. Il s'agira également d'implanter des versions vérifiées des algorithmes de calcul des nombres de classe, d'en évaluer l'efficacité, et d'avoir un aperçu de l'état de l'art, disponible par exemple dans le logiciel PARI/GP [5].

Ce travail de formalisation en Coq s'appuiera sur les bibliothèques Mathematical Components, et suivra la méthodologie de formalisation qu'elles mettent en œuvre [3]. Ces bibliothèques contiennent une base de vocabulaire en algèbre commutative, algèbre matricielle, etc. qui permettra de se concentrer sur les objets

mathématiques propres au sujet du stage. Les aspects calculatoires, eux, sont plus prospectifs.

Profil. Ce stage requiert un goût pour l'algèbre et pour ses aspects effectifs. Le programme de classes préparatoires en algèbre est suffisant pour aborder le contenu du stage. Aucune expérience préalable en preuve formelle n'est requise. Une culture en algèbre commutative ou en logique est un plus mais n'est pas du tout nécessaire.

Organisation du travail. Le stage se déroulera à Nantes, dans le laboratoire d'informatique (LS2N), au sein de l'équipe Inria Gallinette. Les thématiques de recherche de l'équipe sont la théorie de la démonstration, la théorie des types et leur application à la programmation et aux assistants de preuve. Des réunions hebdomadaires par visio-conférence sont prévues avec Sander Dahmen (VU Amsterdam). Une visite (financée) d'une semaine environ du ou de la stagiaire au département de mathématiques de la VU Amsterdam pendant le stage est envisagée.

Références

[1] Karim Belabas. L'algorithmique de la théorie algébrique des nombres, 2005. Disponible ici : `http://www.math.polytechnique.fr/xups/xups05-02.pdf`.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate texts in mathematics*. Springer, 1993.

[3] Assia Mahboubi and Enrico Tassi. *Mathematical Components*. 2019. Disponible ici :`https://math-comp.github.io/mcb/`.

[4] The Coq Development Team. 2019. Available from `http://coq.inria.fr`.

[5] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.11.0`, 2018. Available from `http://pari.math.u-bordeaux.fr/`.