Théorie des Nombres 2024-2025

Semestre 3

- Théorie algébrique des nombres 1 (Éric Gaudron)
- Courbes elliptiques (Francesco Campagna)

Semestre 4

- Théorie algébrique des nombres 2 (Francesco Campagna)
- Introduction aux méthodes de transcendance (Éric Gaudron)

Ce cours d'introduction à la théorie des nombres se déroule sur deux semestres avec un thème par semestre comprenant deux parties. L'objectif est de passer en revue quelques notions de base de la théorie des nombres contemporaine. Cette discipline aux multiples facettes sera abordée ici à travers le prisme de l'algèbre, de la géométrie et de l'analyse. Les notions évoquées permettront d'étudier un texte mathématique récent en stage de M2.

La théorie algébrique des nombres utilise les notions développées dans les cours d'algèbre des années précédentes (anneaux, idéaux, extensions de corps, théorie de Galois ...) pour résoudre des questions d'arithmétique telles que : « Si d est un entier (sans facteur carré), quels sont les entiers x et y vérifiant x^2-dy^2=1 ? » ou «Quels sont les nombres entiers qui peuvent s'écrire comme la somme de deux carrés? ».

Une courbe elliptique (sur le corps des rationnels) est une courbe algébrique plane qui peut être décrit avec une équation de la forme y^2=P(x) où P est un polynôme de degré 3, à coefficients rationnels et sans racine multiple. En ajoutant un point « à l'infini », l'ensemble des solutions rationnelles d'une telle équation acquiert une structure de groupe. Cette combinaison de géométrie et de théorie des groupes a des conséquences arithmétiques importantes et fait des courbes elliptiques l'un des objets les plus riches et les plus utilisés de la théorie des nombres. La théorie algébrique des nombres est un outil essentiel pour comprendre les nombreuses propriétés de ces courbes. On remarque que les courbes elliptiques ont également des applications importantes dans la vie réelle, notamment en cryptographie.

Le cours de transcendance permettra d'utiliser les notions ci-dessus pour obtenir la transcendance de nombres tels que e, π ainsi que d'autres énoncés plus généraux.

Les deux cours d'un semestre ne sont pas indépendants. En fonction du nombre d'inscrits, une partie de l'apprentissage pourra se faire par le biais de lectures guidées, d'exposés, etc.

Semestre 3

a) **Théorie algébrique des nombres 1** (par Éric **Gaudron**)

Un nombre complexe est dit algébrique s'il est racine d'un polynôme unitaire à

coefficients entiers. L'ensemble des nombres algébriques forme un sous-corps du corps des nombres complexes. La théorie algébrique des nombres est l'étude de ce corps et, plus généralement, des extensions algébriques d'un corps commutatif. Les *corps de nombres,* qui sont les extensions (finies) de Q engendrées par un nombre algébrique, entrent dans cette catégorie et ils représentent une des notions de base de la théorie des nombres. L'objectif de ce cours est d'étudier ces corps de nombres et leurs anneaux d'entiers. Les principaux théorèmes de la théorie « élémentaire » seront abordés.

Bibliographie :

- Pierre Samuel. Théorie algébrique des Nombres. Hermann (1997).
- (pour approfondir) Jürgen Neukirch. Algebraic number theory. Grundlehren der Mathematischen Wissenschaften 322. Springer (1999).

b) **Courbes elliptiques** (par Francesco **Campagna**)

Ce cours est une introduction à la théorie géométrique et arithmétique des courbes elliptiques. De telles courbes apparaissent naturellement dans l'étude des équations diophantiennes. C'est le premier exemple de courbes auxquelles on ne peut pas appliquer systématiquement le principe de Hasse, contrairement à ce qui se passe pour les coniques. La richesse des courbes elliptiques vient notamment du fait que la méthode dite *de la corde et de la tangente* permet de définir sur ses points une loi de groupe.
Les structures arithmétiques et géométriques des courbes elliptiques et leur lien, *via* les fonctions L, à des objets de nature algébrique (représentations de Galois) ou analytique (formes modulaires) sont au cœur de nombreux résultats et questions de géométrie arithmétique actuels. Parmi ces résultats se trouve le célèbre *Dernier Théorème de Fermat* énoncé au 17è siècle et démontré en 1995 par Wiles et Breuil, Conrad, Diamond, Taylor.
Dans ce cours nous étudierons les notions classiques suivantes sur les courbes elliptiques : définitions et propriétés géométriques, loi de groupe, morphismes et isogénies, points rationnels, réduction des courbes elliptiques, points de torsion, théorème de Mordell Weil. Nous tenterons également d'aborder les aspects computationnels du sujet, en illustrant le fonctionnement de la base de données LMFDB et l'utilisation du langage de programmation SageMath pour effectuer des calculs explicites avec les courbes elliptiques.

Bibliographie :

- Knapp. *Elliptic curves*, vol 40. Mathematical Notes. Princeton Univ. Press (1992).
- Milne. *Elliptic curves* BookSurge Publishers, Charleston, SC (2006).
- Silverman. *The arithmetic of elliptic curves*, vol 106, Graduate Texts in Mathematics, Springer Verlag (2009).
- Silverman-Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer Verlag (1994).
- Washington. *Elliptic curves : number theory and cryptography*, Chapman and Hall, CRC (2008).

Semestre 4

a) **Théorie algébrique des nombres 2** (par Francesco **Campagna**)

De nombreux problèmes sur les corps de nombres vus au cours du premier semestre (comme la détermination de la décomposition des idéaux premiers dans une extension fixée des corps de nombres) deviennent plus naturels lorsqu'ils sont considérés « localement ». L'idée est que chaque idéal premier p d'un corps de nombres K induit une topologie par rapport à laquelle K peut être complété, de la même manière que l'on passe du corps Q des rationnels au corps R des nombres réels. Le corps K_p ainsi obtenu contient encore beaucoup d'informations arithmétiques sur K, mais il est plus simple à étudier.
Dans ce cours, nous définirons la notion de corps local et étudierons les différentes propriétés arithmétiques de ces corps (lemme de Hensel, ramification, etc.) en mettant l'accent sur leurs applications dans l'étude des corps de nombres. Nous suivrons principalement le chapitre 2 de Neukirch et les parties 1 et 2 de Serre (voir références). Si le temps le permet, nous donnerons une introduction à la théorie du corps de classe local.

Bibliographie :

- James Milne. *Class field theory.* Course Notes, disponible en ligne (1997).
- Jürgen Neukirch. *Algebraic Number Theory*. Springer (1999).
- Jean-Pierre Serre. *Corps locaux*. Hermann (1997).

b) **Introduction aux méthodes de transcendance** (par Éric **Gaudron**)

Dans ce cours, nous passerons en revue quelques théorèmes classiques de la théorie des nombres transcendants (théorème des six exponentielles, théorème de Schneider-Lang, Gel'fond-Baker etc.) grâce auxquels on obtient la transcendance de e, π ou de certaines valeurs des fonctions elliptiques de Weierstraß associées aux courbes elliptiques. Cela sera l'occasion de faire quelques incursions en géométrie des nombres (*lemme de Siegel*) et théorie des hauteurs.

Bibliographie :

- Serge Lang *Introduction to transcendental numbers* . Addison-Wesley publishing company (1966)
- Michel Waldschmidt. *Nombres transcendants.* LNM 402, Springer (1974)
- Michel Waldschmidt. *Diophantine approximation on linear algebraic groups.* Springer (2000)