

Réseaux et corps de nombres

— proposition de projets —

1 Corps de nombres

Ce projet est orienté vers la théorie algébrique des nombres. L'objectif est de comprendre et rédiger la preuve du *théorème des unités de Dirichlet* :

Théorème 1 *Soit K un corps de nombres de degré $n = r_1 + 2r_2$, où r_1 désigne le nombre de plongements réels et r_2 le nombre de paires de plongements complexes de K . Le groupe multiplicatif \mathcal{O}_K^\times des éléments inversibles de l'anneau d'entiers \mathcal{O}_K est isomorphe à $\mu_K \times \mathbb{Z}^{r_1+r_2-1}$, où μ_K est le groupe cyclique (fini) des racines de l'unité contenues dans K .*

La preuve du théorème utilise des outils d'algèbre et de théorie des nombres, notamment une variante du plongement canonique de K , appelée *plongement logarithmique*, ainsi que le théorème de Minkowski.

On pourra se baser sur le livre *Théorie algébrique des nombres* de Pierre Samuel, éd. Hermann (en particulier le chapitre IV).

2 Réseaux idéaux

Ce projet est orienté vers les réseaux idéaux et leur utilisation en théorie de l'information, pour construire des réseaux avec certaines propriétés, à partir d'idéaux de sous-corps totalement réels de corps cyclotomiques. Ce contexte arithmétique permet de calculer explicitement la *distance produit minimale* des réseaux considérés.

Il s'agit plus précisément d'étudier et de comprendre (au moins en partie) l'article « New algebraic constructions of rotated \mathbb{Z}^n -lattice constellations for the Rayleigh fading channel », Eva Bayer-Fluckiger, Frédérique Oggier, Emanuele Viterbo, *IEEE Trans. Inform. Theory* **50** (2004), no. 4, 702–714.

On retrouvera le même genre de calculs que ceux effectués en cours dans l'exemple de réseau idéal dans le corps cyclotomique engendré par une racine p -ième de l'unité.