Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 8, 27 mars 2020

- Un premier de K est un idéal premier de $\mathfrak{O}_K$.
- On dit qu'un premier $\mathfrak{p}$ de K divise un $a \in \mathfrak{O}_K$ si $a \in \mathfrak{p}$. O désigne par $\mathscr{D}_a$ (les diviseurs) l'ensemble des premiers de K qui contiennent a.
- Le groupe des classes de $\mathfrak{O}_K$ est noté Cl_K. La classe d'un idéal fractionnaire $\mathfrak{a}$ dans Cl_K sera désignée par $[\mathfrak{a}]$.
- Si K est un corps de nombres de degré n et signature (r, s), la constante de Minkowski de K est $M_K = \dfrac{4^s}{\pi^s}\dfrac{n!}{n^n}\sqrt{|\Delta_K|}$. (Cette terminologie n'est pas universelle.)

Groupes de classes

Exercice 1. Soient $m > 0$ un entier qui n'est pas un cube, α la racine $\sqrt[3]{m}$ et K le corps de nombres $\mathbb{Q}(\alpha)$. On étudie, dans des cas spécifiques, le groupe de classes de l'anneau d'entiers $\mathfrak{O}_K$. (Une technique utile qui est présentée dans la suite est une méthode pour *trouver des générateurs d'un idéal.*)

1/ Justifier brièvement pourquoi $\{1, \alpha, \alpha^2\}$ est une $\mathbb{Q}$-base de K. Ensuite, exprimer $\mathrm{N}_K(x + y\alpha + z\alpha^2)$ en fonction de x, y et z.

2/ En supposant que m n'a pas de facteur carré et que $m \not\equiv \pm 1$ (9), déterminer une base entière de $\mathfrak{O}_K$ et le discriminant Δ_K. (Vous pouvez consulter les Exercices de la séance du 13 mars 2020.)

3/ Montrer que si $m = 2$, alors $\mathfrak{O}_K$ est principal.

4/ On se concentre sur le cas $m = 3$.

a/ Montrer que
$$2\mathfrak{O}_K = \mathfrak{p}\mathfrak{q},$$
où $\mathfrak{p} = (2, f(\alpha))$ et $\mathfrak{q} = (2, g(\alpha))$ avec f et g dans $\mathbb{Z}[X]$ tels que $f \equiv X + 1$ (2) et $g \equiv X^2 + X + 1$ (2). Par un choix judicieux de f et g, déduire que $\mathfrak{p}$ et $\mathfrak{q}$ sont principaux. Indication : Considérer $\mathrm{N}(f(\alpha)\mathfrak{O}_K)$ et $\mathrm{N}(g(\alpha)\mathfrak{O}_K)$.

b/ En déduire que $\mathfrak{O}_K$ est principal.

5/ On se concentre sur le cas $m = 5$.

a/ Montrer que chaque premier de $\mathscr{D}_5$ et de $\mathscr{D}_7$ est principal.

b/ Montrer que $\mathscr{D}_3$ possède un unique élément et que cet élément, $\mathfrak{p}$ disons, est de la forme $(3, f(\alpha))$, où $f \in \mathbb{Z}[X]$ est tel que $f \equiv X+1$ (3). Prouver que $\mathfrak{p}$ est principal en choisissant judicieusement f.

c/ Montrer que $(2) = \mathfrak{p}\mathfrak{q}$ avec $\mathfrak{p} = (2, \alpha+1)$ et $\mathfrak{q} = (2, \alpha^2+\alpha+1)$. Montrer que $\mathfrak{p}$ et $\mathfrak{q}$ sont principaux. Indication : Pour trouver un générateur de $\mathfrak{p}$, on montrera que *l'unique* idéal de $\mathscr{D}_3$ (trouvé dans la question précédente) divise $(\alpha+1)$, et pour $\mathfrak{q}$ on remplacera $\alpha^2+\alpha+1$ par $\varepsilon_2\alpha^2+\varepsilon_1\alpha+\varepsilon_0$ où ε_i est pair.

d/ En déduire que $\mathfrak{O}_K$ est principal.

Exercice 2. Montrer que le groupe de classes de $\mathbb{Q}(\sqrt{-14})$ est $\mathbb{Z}_{/4}$. Indications : (a) On considère un diviseur $\mathfrak{p}_2$ de 2 et un diviseur $\mathfrak{p}_3$ de 3 et on montre que $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$. (b) Pour déterminer des générateurs d'un idéal $\mathfrak{a}$, on travaillera avec l'isomorphisme $\mathfrak{O}_{\mathbb{Q}(\sqrt{-14})} \simeq \mathbb{Z}[X]/(X^2+14)$.