Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 8, 2 avril 2021

— 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.

Correction. Le poly $X^3 - m$ est irréductible sur $\mathbb{Q}[X]$. Autrement il possède une racine a/b avec $a \wedge b = 1$; or, si p est un diviseur premier de b il suit de $b^3 m = a^3$ que $p \mid a$, ce qui est impossible. Donc $b = \pm 1$ et m serait un cube. Il suit que $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/(X^3 - m)$ et $1, \alpha, \alpha^2$ est une $\mathbb{Q}$-base.

Pour calculer la norme, on remarque que la matrice associée à la multiplication par $x + y\alpha + z\alpha^2$ est

$$\begin{pmatrix} x & mz & my \\ y & x & mz \\ z & y & x \end{pmatrix},$$

et

$$\boxed{\mathrm{N}_K = x^3 + my^3 + m^2 z^3 - 3m \cdot xyz}$$

est la forme cubique de la norme. □

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 4 de 2021.)

Correction. On a vu que dans ce cas $\mathfrak{O}_K = \mathbb{Z}[\alpha]$. Pour calculer Δ_K on fait appel à la formule $\Delta_K = -\mathrm{N}_K(3\alpha^2) = -27m^2$. □

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

Correction. La signature de K est $(1, 1)$. Comme vu à la séance du 24 mars 2021, le groupe de classes est engendré par les premiers $\mathfrak{p}$ (ou leurs classes) qui divisent les nombres premiers $p \leqslant \dfrac{4}{\pi} \cdot \dfrac{6}{27} \cdot 6 \cdot \sqrt{3} < 2,95$. Or, le premier 2 s'écrit comme $(\alpha)^3$ et (α) est bien évidemment un premier de $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(X^3 - 2)$. (Vérifier que vous pouvez justifier cet isomorphisme !) Donc, $\mathfrak{O}_K$ 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 $\mathrm{N}(g(\alpha)\mathfrak{O}_K)$.

Correction. En $\mathbb{F}_2[X]$, on a $X^3 - 3 = (X + 1)(X^2 + X + 1)$. Par conséquent, si $f \in \mathbb{Z}[X]$ se réduit sur $X + 1$ tandis que $g \in \mathbb{Z}[X]$ se réduit sur $X^2 + X + 1$, on a $2\mathfrak{O}_K = \mathfrak{p}\mathfrak{q}$ où $\mathfrak{p} = (2, f(\alpha))$ et $\mathfrak{q} = (2, g(\alpha))$.

Pour prouver que $\mathfrak{p}$ est principal—ce qui n'est pas évident—on note que $\deg \mathfrak{p} = 1$, d'où $\mathrm{N}\mathfrak{p} = 2$ (cela se lit sur $\deg f$). Or, en prenant $f = X - 1$, il suit du calcul de la norme fait avant que

$$\mathrm{N}_K(f(\alpha)) = 2.$$

Comme $\mathfrak{p} \mid f(\alpha)\mathfrak{O}_K$ et $\mathrm{N}\mathfrak{p} = 2 = \mathrm{N}(f(\alpha)\mathfrak{O}_K)$, on déduit que $\mathfrak{p} = f(\alpha)\mathfrak{O}_K$. (Plus de détails : on écrit $f(\alpha)\mathfrak{O}_K = \mathfrak{p}\mathfrak{m}$ et en prenant la norme, $\mathrm{N}(\mathfrak{m}) = 1$.)

Pour prouver que $\mathfrak{q}$ est principal, on note que $\mathrm{N}\mathfrak{q} = 2^2$. Or, si $g = X^2 + X + 1$, on déduit $\mathrm{N}(g(\alpha)) = 4$ et par le même argument que avant, $\mathfrak{q} = g(\alpha)\mathfrak{O}_K$. Donc, $\mathfrak{p}$ et $\mathfrak{q}$ sont principaux. □

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

Correction. Le groupe de classes est engendré par les premiers $\mathfrak{p}$ qui divisent les nombres premiers $p \leqslant \frac{4}{\pi} \cdot \frac{6}{27} \cdot 9 \cdot \sqrt{3} < 5$. Or, le premier 3 s'écrit comme $(\alpha)^3$ et (α) est bien évidemment un premier de $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(X^3-3)$. Dans la question précédente, on a montré que les premiers de $\mathscr{D}_2$ sont principaux, ce qui implique 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.

Correction. On note que $5\mathfrak{O}_K = \alpha^3\mathfrak{O}_K$ et come (α) est un idéal premier, on déduit que (α) est l'unique premier de K qui divise 5, et est principal.
Le poly $X^3 - 5$ est irréductible en $\mathbb{F}_7[X]$ car les cubes de $\mathbb{F}_7^*$ sont 1 et -1. Il suit que 7 est inerte, c'est-à-dire, $7\mathfrak{O}_K$ est premier. □

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.

Correction. Comme $5 = -1 = (-1)^3$ en $\mathbb{F}_3$, on déduit $X^3 - 5 = (X+1)^3$ en $\mathbb{F}_3[X]$. Par conséquent, $(3) = \mathfrak{p}_3^3$ avec $\mathfrak{p} = (3, f(\alpha))$, où $f \in \mathbb{Z}[X]$ est unitaire qui est $\equiv X + 1$ (3). Clairement, $\mathfrak{p}$ est un idéal de degré 1 et ainsi $\mathrm{N}\mathfrak{p} = 3$. En prenant $f = X + 1$ on trouve $\mathrm{N}_K(f(\alpha)) = 6$. Par contre, en prenant $f = X - 2$ on trouve $\mathrm{N}_K(f(\alpha)) = -3$. Comme $\mathfrak{p} \mid f(\alpha)\mathfrak{O}_K$ et $\mathrm{N}\mathfrak{p} = \mathrm{N}(f(\alpha)\mathfrak{O}_K)$, on déduit que $\mathfrak{p} = (f(\alpha))$. □

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 $(1 + \varepsilon_2)\alpha^2 + (1 + \varepsilon_1)\alpha + (1 + \varepsilon_0)$, où chaque ε_i est pair.

Correction. En $\mathbb{F}_2[X]$, on a $X^3 - 5 = (X+1)(X^2+X+1)$. (C'est le même calcul que pour $\mathbb{Q}(\sqrt[3]{3})$.) Il suit que $(2) = \mathfrak{p}\mathfrak{q}$ (dit autrement, $\mathscr{D}_2 = \{\mathfrak{p}, \mathfrak{q}\}$) avec $\mathfrak{p} = (2, \alpha + 1)$ et $\mathfrak{q} = (2, \alpha^2 + \alpha + 1)$. Puis, $\mathrm{N}\mathfrak{p} = 2$ et $\mathrm{N}\mathfrak{q} = 4$.
Pour prouver que $\mathfrak{p}$ est principal, on note que $\mathrm{N}((1 + \alpha)) = 6$. Dans ce cas, si $\mathfrak{r} \mid (1 + \alpha)$, alors $\mathfrak{r} \mid 6$. Il suit que

$$(1 + \alpha) = \underbrace{(\alpha - 2)}_{\text{l'idéal de } \mathscr{D}_3} \cdot \mathfrak{p}.$$

En particulier, $\alpha-2$ divise $\alpha+1$: $\dfrac{\alpha+1}{\alpha-2} = -3-2\alpha-\alpha^2$. Or, $\mathrm{N}((3+2\alpha+\alpha^2)) = 2$ et $(3+2\alpha+\alpha^2)$ est premier. Par unicité de la factorisation, on voit que

$$\mathfrak{p} = (3+2\alpha+\alpha^2).$$

(A posteriori, on obtient que $(\alpha+1)^2+2$ est un générateur de $\mathfrak{p}$.)

Pour étudier $\mathfrak{q}$. Si au lieu de prendre $1+\alpha+\alpha^2$ comme générateur de $\mathfrak{q}$, on choisit $-1-\alpha+\alpha^2$, on obtient $\mathfrak{q} = (-1-\alpha+\alpha^2)$ car $\mathrm{N}_K(\alpha^2-\alpha-1) = 4$.

□

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

Correction. C'est une conséquence des question précédentes et du fait que les idéaux de $\mathscr{D}_2 \cup \mathscr{D}_3 \cup \mathscr{D}_5 \cup \mathscr{D}_7$ engendrent Cl_K car $M_K < 8$. □

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 $\mathfrak{O}_{\mathbb{Q}(\sqrt{-14})} \simeq \mathbb{Z}[X]/(X^2+14)$.

Correction. On pose $\theta = \sqrt{-14}$. On a $M_K < 5$. Alors $\mathscr{D}_2$ et $\mathscr{D}_3$ engendrent Cl_K. Puisque $X^2+14 \equiv X^2$ (2), on voit que

$$(2) = \mathfrak{p}_2^2, \qquad \mathfrak{p}_2 = (2,\theta).$$

Clairement, $[\mathfrak{p}_2]^2 = [1]$. Car $X^2+14 \equiv X^2-1$ (3), on déduit

$$(3) = \mathfrak{p}_3\mathfrak{q}_3, \qquad \mathfrak{p}_3 = (3,\theta+1),\ \mathfrak{q}_3 = (3,\theta-1).$$

En particulier on déduit tout de suite que $[\mathfrak{p}_3]^{-1} = [\mathfrak{q}_3]$. Donc Cl_K est engendré par $[\mathfrak{p}_2]$ et $[\mathfrak{p}_3]$. On suit l'indication et on montre que $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$. Comme $[\mathfrak{p}_2]^2 = [1]$, il suffit de montrer que $\mathfrak{p}_2\mathfrak{p}_3^2$ est principal.

On note que $\mathrm{N}(\mathfrak{p}_2) = 2$ et $\mathrm{N}\mathfrak{p}_3 = 3 \Rightarrow \mathrm{N}(\mathfrak{p}_3^2) = 9$ et $\mathrm{N}(\mathfrak{p}_2\mathfrak{p}_3^2) = 18$. Par définition, $\mathfrak{p}_3^2 = (9, 3\theta+3, 2\theta-13)$ et donc

$$\begin{aligned}\mathfrak{O}_K/\mathfrak{p}_3^2 &\simeq \mathbb{Z}[X]/(9, 3X+3, 2X-13, X^2+14)\\ &\simeq (\mathbb{Z}_{/9})[X]/(X-2).\end{aligned}$$

(Ici, on a utilisé que pour un anneau arbitraire A, on peut dire que $P(X) \equiv P(a) \mod X-a$ et que $5\cdot(2X-13) = X-2$ en $\mathbb{Z}_{/9}[X]$.)

Il suit que $\mathfrak{p}_3^2 = (9, \theta-2)$. Ensuite,

$$\mathfrak{p}_2\mathfrak{p}_3^2 = (18, 9\theta, 2\theta-4, 2\theta+14)$$

et donc

$$\begin{aligned}\mathfrak{O}_K/\mathfrak{p}_2\mathfrak{p}_3^2 &\simeq \mathbb{Z}[X]/(18, 9X, 2X-4, 2X+14, X^2+14)\\ &= \mathbb{Z}[X]/(18, 9X, 2X-4, 2X+14, X^2+14, 11X-4)\\ &\simeq \mathbb{Z}/(18)[X]/(9X, 2X-4, 2X+14, X^2+14, 11X-4).\end{aligned}$$

Or, comme $11 \cdot 5 \equiv 1\ (18)$, il suit que $11X - 4 = 11(X-2)$ en $\mathbb{Z}_{/18}[X]$ et $\mathfrak{O}_K/\mathfrak{p}_2\mathfrak{p}_3^2 \simeq \mathbb{Z}_{/18}[X]/(X-2)$. Ceci implique que $\mathfrak{p}_2\mathfrak{p}_3^2 = (18, \theta - 2)$. Or, maintenant observe que $(\theta-2)(\theta+2) = -14-4$ et $(18, \theta-2) = (\theta-2)$. Conclusion : $\mathfrak{p}_2\mathfrak{p}_3^2 = (\theta-2)$. Donc $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$ et Cl_K est engendré par $[\mathfrak{p}_3]$. Puisque $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = [1]$, $\mathrm{ord}([\mathfrak{p}_3]) \mid 4$.

Pour terminer, on montre que l'ordre de $[\mathfrak{p}_3]$ est exactement 4. Autrement, $\mathfrak{p}_2 = (x + y\theta)$; on déduit que $(\mathrm{N}\mathfrak{p}_2) = (x^2 + 14y^2)\mathbb{Z} = 2\mathbb{Z}$ et $x^2 + 14y^2 = \pm 2$. Or, ceci est clairement impossible, donc $\mathfrak{p}_2$ n'est pas principal. □