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

Séance 7, 30 mars 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 $a \in \mathfrak{p}$.
— 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 $[\mathfrak{a}]$.

Autour des théorèmes de Minkowski

Exercice 1. 1/ Soit K un corps de nombres de signature (r, s), degré n et plongement canonique $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$. On choisit une base entière $\{\alpha_1, \ldots, \alpha_n\}$ de K. Rappeler pourquoi les vecteurs $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ sont $\mathbb{R}$-linéairement indépendants.

2/ Déterminer deux vecteurs $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$ qui sont $\mathbb{Q}$-linéairement indépendants, mais qui ne sont pas $\mathbb{R}$-linéairement indépendants. Le sous-groupe $A = \mathbb{Z}\boldsymbol{u} + \mathbb{Z}\boldsymbol{v}$ est-il discret ?

Correction. On choisit $\boldsymbol{u} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\boldsymbol{v} = \begin{pmatrix} \sqrt{2} \\ 0 \end{pmatrix}$. Clairement, $\boldsymbol{u}$ et $\boldsymbol{v}$ sont linéairement indépendants sur $\mathbb{Q}$. De plus, A est le sous-groupe de $\mathbb{R}^2$ formé par les vecteurs ${}^t(x + y\sqrt{2}, 0)$. Or, le sous-groupe $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ de $\mathbb{R}$ n'est pas cyclique : En effet, si $k(x_0+y_0\sqrt{2}) = 1$ on déduit $y_0 = 0$, et si $k(x_0 + y_0\sqrt{2}) = \sqrt{2}$ on déduit $x_0 = 0$. Il suit, par un exercice bien connu d'Analyse, que $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ est un sous-groupe *dense* de $\mathbb{R}$. □

Exercice 2. Soit $\alpha = \sqrt[3]{3}$ et soit $K = \mathbb{Q}(\alpha)$.

1/ Décrire explicitement le plongement canonique σ de K.

Correction. On définit $\zeta = e^{2\pi \mathrm{i}/3}$. Les racines du poly minimal de α sont $\alpha, \zeta\alpha, \zeta^2\alpha$. Donc,

$$\sigma(a + b\alpha + c\alpha^2) = (a + b\alpha + c\alpha^2, a + b\zeta\alpha + c\zeta^2\alpha^2) \in \mathbb{R} \times \mathbb{C}.$$

□

2/ Vérifiez directement que $\{\sigma(1), \sigma(\alpha), \sigma(\alpha^2)\}$ est une $\mathbb{R}$-base du $\mathbb{R}$-espace vectoriel $\mathbb{R}\times\mathbb{C}$ et que

$$\big[\det(\sigma(1), \sigma(\alpha), \sigma(\alpha^2))\big]^2 = \frac{|\Delta_K(1, \alpha, \alpha^2)|}{4}$$

Correction. On a

$$\sigma(1) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad \sigma(\alpha) = \alpha \begin{pmatrix} 1 \\ \cos(2\pi/3) \\ \sin(2\pi/3) \end{pmatrix}, \quad \sigma(\alpha^2) = \alpha^2 \begin{pmatrix} 1 \\ \cos(4\pi/3) \\ \sin(4\pi/3) \end{pmatrix}.$$

Or,

$$\begin{aligned} \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha\cos(2\pi/3) & \alpha^2\cos(4\pi/3) \\ 0 & \alpha\sin(2\pi/3) & \alpha^2\sin(4\pi/3) \end{vmatrix} &= 3 \begin{vmatrix} \cos(2\pi/3) & \cos(4\pi/3) \\ \sin(2\pi/3) & \sin(4\pi/3) \end{vmatrix} - 3 \begin{vmatrix} 1 & 1 \\ \sin(2\pi/3) & \sin(4\pi/3) \end{vmatrix} \\ &= 3\sin(2\pi/3) - 3(\sin(4\pi/3) - \sin(2\pi/3)) \\ &= \frac{3}{2}\sqrt{3} + 3\sqrt{3}. \end{aligned}$$

Donc de déterminant au carré vaut $3^5/4$. Ensuite, on note que $|\Delta(1, \alpha, \alpha^2)| = 3^5$ car $\Delta(1, \alpha, \alpha^2) = -27 \cdot 3^2$. □

Exercice 3. Quels sont les corps de nombres où chaque nombre premier est non-ramifié ?

Correction. On sait que $\mathbb{Q}$ est l'unique corps de nombres de discriminant égal à 1 par le Théorème de Minkowski. Soit ainsi $K \neq \mathbb{Q}$ un corps de nombres. Son discriminant possède un facteur premier p, d'où, par le théorème de Dedekind, p ramifie. □

Exercice 4. On fixe K un corps de nombres de degré n, signature (r, s) et constante de Minkowski $M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_K|}$. (Attention : La terminologie n'est pas universellement acceptée.)

1/ Montrer que Cl_K est engendré par (les classes des) idéaux premiers dont la norme est au plus M_K. (Note : On dira que l'ensemble $\varnothing$ engendre un groupe si et seulement si le groupe est trivial.)

Correction. Soit $\mathfrak{C}$ une classe de Cl_K. Il est possible de trouver $\mathfrak{a} \in \mathfrak{C}$ tel que $\mathrm{N}(\mathfrak{a}) \leqslant M_K$. Si $\mathfrak{a} \neq (1)$, ce qui équivaut à $\mathrm{N}(\mathfrak{a}) \neq 1$, on écrit $\mathfrak{a} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r$, où $\mathfrak{p}_i$ est premier. Alors $\mathrm{N}(\mathfrak{p}_i) \leqslant M_K$. Le resultat suis aussitôt. Si $\mathrm{N}(\mathfrak{a}) = 1$ alors $\mathfrak{a}$ est (1) et la seule classe est la classe triviale. □

2/ Pour chaque nombre premier p, on écrit

$$\mathscr{D}_p = \{\mathfrak{p} \text{ premier de } \mathfrak{O}_K \,:\, \mathfrak{p} \mid p\}.$$

Montrer que les (classes des) éléments de $\mathscr{M} = \bigcup_{p \leqslant M_K} \mathscr{D}_p$ engendrent Cl_K.

Correction. On sait que Cl_K est engendré par les classes des premiers dont la norme est $\leqslant M_K$. Soit $\mathfrak{p}$ un premier tel que $\mathrm{N}(\mathfrak{p}) \leqslant M_K$. Or, $\mathrm{N}(\mathfrak{p}) = p^f$, où p est le nombre premier tel que $(p) = \mathfrak{p} \cap \mathbb{Z}$; ceci étant, $p \leqslant M_K$ et $\mathfrak{p} \in \mathscr{M}$. □

3/ Soit K un corps de nombres parmi $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ et $\mathbb{Q}(\sqrt{-7})$. Montrer que l'ensemble $\mathscr{M}$ de la question précédente est vide et en déduire que $\mathfrak{O}_K$ est principal.

Correction. Si K a signature $(2,0)$ et $\sqrt{|\Delta_K|} < 4$, alors $\mathscr{M}$ est vide car $M_K < 2$. Les discriminants de $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(\sqrt{13})$ sont respectivement 8, 12, 5, 13.
Si K a signature $(0,1)$ et $|\Delta_K| < \pi^2$, alors $\mathscr{D}$ est vide. En particulier ceci se produit quand $|\Delta_K| < 9$. Les discriminants de $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ et $\mathbb{Q}(\sqrt{-7})$ sont respectivement -4, -8, -3, -7. □

4/ Pour chaque $d \in \{11, 19, 43, 67, 163\}$, soit $K = \mathbb{Q}(\sqrt{-d})$. Exprimer $\mathfrak{O}_K$ comme $\mathbb{Z}[\alpha]$; ensuite déterminer le polynôme minimal f de α ainsi que $\mathrm{disc}(f)$. Indication : Dans tous les cas, $d \equiv 3\ (4)$.

Correction. Clairement $-d \equiv 1\ (4)$. Il suit que $\mathfrak{O}_K = \mathbb{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-d}}{2}$. En particulier, le poly minimal de α est $f = X^2 - X + \dfrac{1+d}{4}$. Son discriminant est bien évidemment $-d$. □

5/ Montrer que les anneaux d'entiers des corps K de la question précédente sont tous principaux. (Gauss avait déjà conjecturé que $\mathfrak{O}_{\mathbb{Q}(\sqrt{-d})}$ était principal *seulement si*,

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Cette conjecture a été vérifiée au siècle XX.) Indication : Faire appel à une calculatrice et à $\frac{2}{\pi} < 0,637$.

Correction. Cas $d = 11$. On doit montrer que pour chaque $p < 0,637 \cdot \sqrt{11} < 3$ les idéaux de $\mathscr{D}_p$ sont principaux. Or, le poly minimal de α est $f = X^2 - X + 3$ et son image dans $\mathbb{F}_2[X]$ est irréductible. Il suit que 2 est inerte.
Cas $d = 19$. On doit montrer que pour chaque $p < 0,637 \cdot \sqrt{19} < 3$ les idéaux de $\mathscr{D}_p$ sont principaux. Or, le poly minimal de α est $f = X^2 - X + 5$ et son image dans $\mathbb{F}_2[X]$ est irréductible. Il suit que 2 est inerte.
Cas $d = 43$. On doit montrer que pour chaque $p < 0,637 \cdot \sqrt{43} < 5$ les idéaux de $\mathscr{D}_p$ sont principaux. Or, le poly minimal de α est $f = X^2 - X + 11$. L'image de f dans $\mathbb{F}_2[X]$ est irréductible et 2 est inerte. Puis, comme $-43 \equiv 2\ (3)$ n'est pas un carré modulo 3, on déduit que l'image de f dans $\mathbb{F}_3[X]$ est aussi irréductible et 3 est inerte.

Cas $d = 67$. On doit montrer que pour chaque $p < 0,637 \cdot \sqrt{67} \leqslant 6$, les idéaux de $\mathscr{D}_p$ sont principaux. Soit $f = X^2 - X + 17$ le poly minimal de α. On note que l'image de f en $\mathbb{F}_2[X]$ est irreductible. Puis, le discriminant -67 n'est pas un carré modulo 3 ou 5. Donc $2, 3, 5$ sont inertes en $\mathfrak{O}_K$.
Cas $d = 163$. On doit montrer que pour chaque $p < 0,637 \cdot \sqrt{163} \leqslant 9$, les idéaux de $\mathscr{D}_p$ sont principaux. Soit $f = X^2 - X + 41$ le poly minimal de α. On note que $f \equiv X^2 + X + 1\,(2)$ et donc f est irréductible modulo 2. Ensuite, $\left(\frac{-163}{3}\right) = -1$, $\left(\frac{-163}{5}\right) = -1$, $\left(\frac{-163}{7}\right) = -1$ et f ne possède aucune racine modulo $3, 5, 7$. Donc $2, 3, 5, 7$ sont inertes en $\mathfrak{O}_K$. □

Exercice 5. Déterminer la structure du groupe de classes des corps de nombres suivantes : $\mathbb{Q}(\sqrt{-6})$ et $\mathbb{Q}(\sqrt{-10})$ et $\mathbb{Q}(\sqrt{-13})$.

Correction. Cas $K = \mathbb{Q}(\sqrt{-6})$. On a $M_K < 4$. Alors $\mathscr{D}_2$ et $\mathscr{D}_3$ engendrent Cl_K. Puisque $X^2 + 6 \equiv X^2\ (2)$, on voit que $(2) = (2, \sqrt{-6})^2 = \mathfrak{p}_2^2$. Puisque $X^2 + 6 \equiv X^2\ (3)$, on voit que $(3) = (3, \sqrt{-6})^2 = \mathfrak{p}_3^2$. On note que $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = [1]$. Puis, $\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_2 \cap \mathfrak{p}_3 = (\sqrt{-6})$ et $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$. Donc, $\mathrm{Cl}_K \simeq \mathbb{Z}/2$.
Cas $K = \mathbb{Q}(\sqrt{-10})$. On a $M_K < 5$. Alors $\mathscr{D}_2$ et $\mathscr{D}_3$ engendrent Cl_K. Car $X^2 + 10 \equiv X^2\ (2)$, on voit que $(2) = (2, \sqrt{-10})^2 = \mathfrak{p}_2^2$. Car $X^2 + 10 \equiv X^2 + 1\ (3)$ et $\left(\frac{-1}{3}\right) = -1$, on voit que (3) est inerte. Clairement, $[\mathfrak{p}_2]^2 = [1]$ et $\mathrm{Cl}_K \simeq \mathbb{Z}/2$.
Cas $K = \mathbb{Q}(\sqrt{-13})$. On a $M_K < 5$: $\mathscr{D}_2$ et $\mathscr{D}_3$ engendrent Cl_K. Puisque $X^2 + 13 \equiv (X + 1)^2\ (2)$ on tire que $(2) = \mathfrak{p}_2^2$ avec $\mathfrak{p}_2 = (2, 1 + \sqrt{-13})$. Puisque $X^2 + 13 \equiv X^2 + 1\ (3)$ et -1 n'est pas carré modulo 3, on déduit que (3) est premier. Donc Cl_K est engendré par $[\mathfrak{p}_2]$. Pour calculer son ordre, on doit vérifier que il ne s'agit pas d'un idéal principal. Or, comme $\mathrm{N}\mathfrak{p}_2 = 2$ (car $(2) = \mathfrak{p}_2^2$), si $\mathfrak{p}_2$ était principal, il serait possible de trouver $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + 13y^2 = \pm 2$. Comme $x^2 + 13y^2 \geqslant 0$, on aurait $x^2 + 13y^2 = 2$, et ceci est évidemment impossible. □