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

Séance 5, 23 mars 2021

Notations et conventions.

- Pour chaque $n > 1$, μ_n, respectivement μ_n', note l'ensemble des racines de l'unité dans $\mathbb{C}$, respectivement les racines primitives.
- Si K est un corps de nombres, $\mathfrak{O}_K$ désigne son anneau d'entiers.
- Si K est un corps de nombres, Δ_K note *le* discriminant de K. Il s'agit d'un entier.
- Si K est un corps de nombres, un idéal premier de K est un idéal premier de $\mathfrak{O}_K$. Pour un tel premier $\mathfrak{p}$, le corps résiduel $\mathfrak{O}_K/\mathfrak{p}$ sera noté $\mathbb{F}_\mathfrak{p}$.

Calcul d'anneaux d'entiers

Exercice 1 (Une extension non-monogène)**.** Soient $0 < m < n$ des nombres naturels sans facteur carré et premiers entre eux, x le réel $\sqrt[3]{m^2n}$ et K le corps $\mathbb{Q}(x)$.

1/ Montrer que $y = \sqrt[3]{mn^2} \in \mathfrak{O}_K$ et que $\mathscr{B} = \{1, x, y\}$ est une base de K. Ensuite calculer $\Delta_K(\mathscr{B})$.

Correction. On note que m^2n ne peut pas être un cube et donc $X^3 - m^2n$ est irréductible sur $\mathbb{Q}[X] \Rightarrow [\mathbb{Q}(x) : \mathbb{Q}] = 3$. On note $x^2 = m\sqrt[3]{mn^2} = my$. Donc, y est entier et appartient à $\mathbb{Q}(x)$. Pour montrer que $\mathscr{B}$ est une base, on utilise $x^2 = my$ et $y^2 = \sqrt[3]{m^2n^4} = nx$ et on calcule directement $\Delta_K(\mathscr{B})$. On a

$$\mu_x = \begin{pmatrix} 0 & 0 & mn \\ 1 & 0 & 0 \\ 0 & m & 0 \end{pmatrix}, \quad \mu_y = \begin{pmatrix} 0 & mn & 0 \\ 0 & 0 & n \\ 1 & 0 & 0 \end{pmatrix}.$$

D'où

$$\begin{pmatrix} \mathrm{Tr}1 & \mathrm{Tr}(x) & \mathrm{Tr}(y) \\ \mathrm{Tr}(x) & \mathrm{Tr}(x^2) & \mathrm{Tr}(xy) \\ \mathrm{Tr}(y) & \mathrm{Tr}(xy) & \mathrm{Tr}(y^2) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3mn \\ 0 & 3mn & 0 \end{pmatrix},$$

et $\Delta_K(\mathscr{B}) = -27m^2n^2 \neq 0$. Ceci implique que $\mathscr{B}$ est une base. □

2/ Pour chaque $\alpha = a + bx + cy \in K$, calculer $\mathrm{N}_K(\alpha)$ et $\mathrm{Tr}_K(\alpha)$.

Correction. La matrice μ_α est

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 0 & bmn \\ b & 0 & 0 \\ 0 & bm & 0 \end{pmatrix} + \begin{pmatrix} 0 & cmn & 0 \\ 0 & 0 & cn \\ c & 0 & 0 \end{pmatrix} = \begin{pmatrix} a & cmn & bmn \\ b & a & cn \\ c & bm & a \end{pmatrix}.$$

Donc,

$$\boxed{\mathrm{N}_K(\alpha) = a^3 + m^2nb^3 + mn^2c^3 - 3mnabc, \quad \mathrm{Tr}_K(\alpha) = 3a.}$$

□

On suppose maintenant que mn n'est pas divisible par 3.

3/ Soit G le groupe quotient $\mathfrak{O}_K/\mathbb{Z} + \mathbb{Z}x + \mathbb{Z}y$. Montrer que son ordre est une puissance de 3.

Correction. On sait que $|G|^2 = \Delta_K(\mathscr{B})/\Delta_K$ et que $\Delta_K(\mathscr{B}) = -27m^2n^2$. Les facteurs premiers de $|G|$ sont parmi 3, et ceux de m et n. Si $p \mid m$ et p divise $|G|$ alors il existe un entier algébrique α ayant la forme

$$\frac{a + bx + cy}{p}, \quad a, b, c \in \{0, \ldots, p-1\}^3 \backslash \{(0,0,0)\}.$$

De

$$p\mathrm{Tr}(\alpha) = \mathrm{Tr}(a + bx + cy) = 3a$$

on obtient $p \mid a \Rightarrow a = 0$. Puis,

$$p^3 \cdot \mathrm{N}_K(\alpha) = m^2nb^3 + mn^2c^3$$

d'où

$$m^2nb^3 + mn^2c^3 \equiv 0 \mod p^3.$$

Comme $p^2 \mid m^2$, on a $c^3mn^2 \equiv 0 \mod p^2$. Parce que $p \nmid n$, on déduit que $p \mid c$, d'où $c = 0$. Ensuite $m^2nb^3 \equiv 0 \mod p^3 \Rightarrow p \mid b \Rightarrow b = 0$. Une contradiction avec le choix de (a, b, c).

Si q est facteur premier de n et divise $|G|$, alors il existe un entier algébrique α ayant la forme

$$\frac{a + bx + cy}{q}, \quad a, b, c \in \{0, \ldots, q-1\}^3 \backslash \{(0,0,0)\}.$$

Les mêmes arguments qu'avant conduisent à une contradiction, que voici. De $q\mathrm{Tr}(\alpha) = 3a$, il suit $q \mid a \Rightarrow a = 0$. On déduit que

$$mn^2c^3 + m^2nb^3 \equiv 0 \mod q^3.$$

Par conséquent, $m^2nb^3 \equiv 0 \mod q^2 \Rightarrow b \equiv 0 \mod q \Rightarrow b = 0$. Ensuite, $mn^2c^3 \equiv 0 \mod q^3 \Rightarrow q \mid c$ et $c = 0$. Une contradiction avec le choix de (a, b, c).

□

4/ En supposant $m = 5$ et $n = 7$, montrer que $\mathscr{B}$ est une base entière. (Il est possible de traiter des cas plus généraux que ceci.)

Correction. On sait que le groupe G est un 3-groupe. Ainsi, si $\#G > 1$, il existe un entier algébrique α ayant la forme

$$\frac{a + bx + cy}{3}, \quad a, b, c \in \{0, 1, 2\}^3 \backslash \{(0, 0, 0)\}.$$

On obtient $\mathrm{N}_K(a + bx + cy) \equiv 0 \mod 27$, c'est-à-dire,

$$\begin{aligned} a^3 + m^2nb^3 + mn^2c^3 - 3mnabc &\equiv a^3 + 13b^3 + 2c^3 + 3abc \\ &\equiv 0 \mod 27, \end{aligned}$$

car

$$m^2n = 175 \equiv 13 \mod 27, \quad mn^2 = 245 = 2 \mod 27,$$

et

$$-3mn \equiv 3 \mod 27.$$

On aura ainsi $26 = 3^3 - 1$ équations à vérifier, quitte à faire des manipulations pertinentes. On peut exclure les triplets $(a, b, c) \in \{0, 1\}^3$ car $1 + 2 + 13 + 3 < 27$. De même, si deux parmi $\{a, b, c\}$ sont nuls, on est conduit aux congruences

$$a^3 \equiv 0 \mod 27, \quad 13b^3 \equiv 0 \mod 27, \quad \text{et} \quad 2c^2 \equiv 0 \mod 27,$$

qui forcent respectivement

$$a \equiv 0 \mod 3, \quad b \equiv 0 \mod 3, \quad \text{et} \quad c \equiv 0 \mod 3,$$

qui sont exclues. On peut exclure ainsi $(0, 0, 1)$, $(0, 0, 2)$, $(0, 1, 0)$, $(0, 2, 0)$, $(1, 0, 0)$ et $(2, 0, 0)$. On étudie directement les cas manquants.

Cas $a = 0$. On teste directement les cas manquants : $(b, c) = (1, 2), (2, 1), (2, 2)$ et on n'obtient aucune solution.

Cas $a = 1$. On teste directement les cas manquants

$$(b, c) = (0, 2), (1, 2), (2, 0), (2, 1), (2, 2)$$

et on n'obtient aucune solution.

Cas $a = 2$. On teste directement les cas manquants

$$(b, c) = (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)$$

et on n'obtient aucune solution. □

5/ Soit $\theta = bx + cy$ avec $b, c \in \mathbb{Z}$. Calculer le quotient $\lambda := \dfrac{\Delta_K(1, \theta, \theta^2)}{\Delta_K(1, x, y)}$. En étudiant λ modulo 7, montrer que $\{1, \theta, \theta^2\}$ ne peut pas être une base entière de $\mathfrak{O}_K$.

Correction. On a $\theta^2 = b^2x^2 + c^2y^2 + 2abxy$. Comme $x^2 = my$, $y^2 = nx$ et $xy = mn$, on obtient $\theta^2 = 5yb^2 + 7xc^2 + 70bc$, d'où

$$\begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ y \end{pmatrix}.$$

Il suit que λ est

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{vmatrix}^2 = (5b^3 - 7c^3)^2.$$

Pour montrer que $\{1, \theta, \theta^2\}$ n'est pas base entière, il suffit de noter que $(5b^3 - 7c^3)^2$ n'est jamais 1. Si c'était le cas, en prenant modulo 7, on obtiendrai $25b^6 \equiv 1 \mod 7$. Il est facile de voir que ceci est impossible pour un entier b. □

6/ Soit $\theta = a + bx + cy$ avec $a, b, c \in \mathbb{Z}$. Montrer que si $\{1, \theta, \theta^2\}$ est base entière de $\mathfrak{O}_K$ et $\sigma = \theta - a$, alors $\{1, \sigma, \sigma^2\}$ est aussi base entière de $\mathfrak{O}_K$. Déduire que l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{175})$ n'est pas de la forme $\mathbb{Z}[\theta]$.

Correction. La matrice de $\{1, \theta, \theta^2\}$ dans la base $\{1, \sigma, \sigma^2\}$ est

$$\begin{pmatrix} 1 & a & a^2 \\ 0 & 1 & 2a \\ 0 & 0 & 1 \end{pmatrix}.$$

Son déterminant étant 1, l'affirmation en découle. □

Premiers décomposés, inertes et ramifiés

Exercice 2 (Vocabulaire)**.** Soit p un nombre premier et soient $K \subset L$ des corps de nombres. Montrer les implications suivantes :

1/ Si p se ramifie dans K alors il se ramifie dans L.

Correction. On note que p ramifie si et seulement si $p \in \mathfrak{p}^2$, où $\mathfrak{p}$ est un premier de K. Or, ceci étant vrai, on note que si $\mathfrak{P}$ est premier de $\mathfrak{O}_L$ au-dessus de $\mathfrak{p}$, c'est-à-dire, $\mathfrak{P}$ apparaît dans la décomposition de $\mathfrak{p}\mathfrak{O}_L$, alors $p \in \mathfrak{p}^2 \subset \mathfrak{P}^2$. □

2/ Si p se décompose totalement en L, alors il se décompose totalement en K.

Correction. Si p se décompose totalement en L, alors il ne se ramifie pas. Donc, il ne se ramifie pas dans K non plus, comme nous affirme la question précédente. On doit maintenant s'assurer que les extensions résiduelles sont toutes triviales. Soit ainsi $\mathfrak{P}$ un premier de L, au-dessus d'un premier $\mathfrak{p}$ de K, au-dessus de p. Alors $[\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_p] = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}] \cdot [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]$ et on obtient $[\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p] = 1$. □

3/ Si p est inerte en L alors il est inerte en K aussi.

Correction. On note que $p\mathfrak{O}_K = (p\mathfrak{O}_L) \cap \mathfrak{O}_K$. En effet, $p\mathfrak{O}_K \subset (p\mathfrak{O}_L) \cap \mathfrak{O}_K$ et si $x \in \mathfrak{O}_K$ est tel que $x = py$ avec $y \in \mathfrak{O}_L$, on déduit que $y \in \mathfrak{O}_K$ et $p \mid x$. □