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

Séance 4, 19 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 $\mathbb{F}_\mathfrak{p}$.

Détermination des anneaux d'entiers

Exercice 1. Soient p un nombre premier, $q = p^m$ et K le corps de nombres $\mathbb{Q}(\theta)$ où $\theta = \sqrt[q]{p}$. Montrer que $\mathfrak{O}_K = \mathbb{Z}[\theta]$.

Correction. Le polynôme minimal de θ est $X^q - p$, qui est p-Eisenstein. Il suit que p ne divise pas $[\mathfrak{O}_K : \mathbb{Z}[\theta]]$, d'après un résultat vu en cours. Or, mais $\Delta_K(1, \theta, \dots, \theta^{q-1})$ est, au signe près, $\mathrm{N}_K(q\theta^{q-1}) = \pm q^q p^{q-1}$. (La norme de θ est $-(-1)^q p$.) Ensuite, comme vu en cours,

$$[\mathfrak{O}_K : \mathbb{Z}[\theta]]^2 = \frac{\Delta_K(1, \theta, \dots, \theta^{q-1})}{\Delta_K},$$

et donc p ne divise pas $\dfrac{q^q p^{q-1}}{\Delta_K}$. Ce quotient vaut 1. □

Exercice 2. Soient p un nombre premier, $q > 1$ une puissance de p, ζ une racine primitive q-ème de l'unité et K le corps de nombres $\mathbb{Q}(\zeta)$. Montrer que $\mathscr{B} = \{1, \zeta, \dots, \zeta^{\varphi(q)-1}\}$ est une base entière de $\mathfrak{O}_K$ et calculer ensuite, à signe près, Δ_K.

Correction. Si $\lambda + 1 = \zeta$, on voit que Π_λ est $\Phi_q(X+1)$. Or, on sait que $\Phi_q(X)(X^{q/p} - 1) = X^q - 1$ et par conséquent, puisque q/p est puissance de p, on déduit que $\Phi_q(X+1)X^{q/p} \equiv X^q \bmod p$, ce qui implique que $\Phi_p(X+1)$ est p-Eisenstein. (Clairement $\Phi_q(0+1) = p$.) Ceci nous permet d'affirmer que $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\lambda]]$.

On sait, d'après le cours, que

$$[\mathfrak{O}_K : \mathbb{Z}[\zeta]]^2 = \frac{\Delta_K(\mathscr{B})}{\Delta_K}.$$

On prouvera que $\dfrac{\Delta_K(\mathscr{B})}{\Delta_K}$ est, à signe près, une puissance de p, ce qui montrera que $[\mathfrak{O}_K : \mathbb{Z}[\zeta]]$ est 1. Pour y arriver, on montre que $\Delta_K(\mathscr{B})$ est, à signe près, une puissance de p.

Il suffit de calculer

$$\Delta_K(\mathscr{B}) = \pm \mathrm{N}_K(\Phi_q'(\zeta)).$$

En dérivant la formule $\Phi_q(X) = \dfrac{X^q - 1}{X^{q/p} - 1}$, on arrive à

$$\Phi_q'(\zeta) = \frac{q\zeta^{q-1}}{\zeta^{q/p} - 1},$$

d'où

$$\mathrm{N}_K(\Phi_q'(\zeta)) = q^{\varphi(q)} \frac{\mathrm{N}_K(\zeta)^{q-1}}{\mathrm{N}_K(\zeta^{q/p} - 1)}.$$

Or, $\mathrm{N}_K(\zeta) = \pm 1$, car $\zeta \in \mathfrak{O}_K^\times$. Ensuite, $\zeta^{q/p} \in \boldsymbol{\mu}_p'$ et

$$\mathrm{N}_K(\zeta^{q/p} - 1) = \left[\mathrm{N}_{\mathbb{Q}(\boldsymbol{\mu}_p)}(\zeta^{q/p} - 1)\right]^{\frac{\varphi(q)}{p-1}} = \left[\mathrm{N}_{\mathbb{Q}(\boldsymbol{\mu}_p)}(\zeta^{q/p} - 1)\right]^{q/p}.$$

Le calcul de $\mathrm{N}_{\mathbb{Q}(\boldsymbol{\mu}_p)}(\zeta^{q/p} - 1)$ a déjà été fait :

$$\mathrm{N}_{\mathbb{Q}(\boldsymbol{\mu}_p)}(1 - \zeta^{q/p}) = \prod_{\xi \in \boldsymbol{\mu}_p'} (1 - \xi) = \Phi_q(1) = p.$$

Donc, $\mathrm{N}_K(\zeta^{q/p} - 1) = \pm p^{q/p}$. Finalement,

$$\mathrm{N}_K(\Phi_q'(\zeta)) = \pm \frac{q^{\varphi(q)}}{p^{q/p}}.$$

De ce fait, on voit que $\mathscr{B}$ est base entière et que Δ_K est, à signe près, $\dfrac{q^{\varphi(q)}}{p^{q/p}}$ □

Exercice 3. Soit $K = \mathbb{Q}(\mathrm{i}, \sqrt{2})$. En utilisant un corps cyclotomique et l'exercice 2, déterminer le discriminant de K. Ensuite, montrer que $\mathscr{B} = \left\{1, \mathrm{i}, \sqrt{2}, \dfrac{\sqrt{2} + \mathrm{i}\sqrt{2}}{2}\right\}$ est base entière de $\mathfrak{O}_K$.

Correction. On note que $K = \mathbb{Q}(\boldsymbol{\mu}_8)$. Par conséquent, si $\zeta = e^{2\pi \mathrm{i}/8}$, $\mathscr{C} = \{1, \zeta, \zeta^3, \zeta^5, \zeta^7\}$ est $\mathbb{Z}$-base de $\mathfrak{O}_K$. En plus, le discriminant est $\pm 2^{3\cdot 4} \cdot 2^{-4} = \pm 2^8$ d'après l'exercice 2. Il y a plusieurs façons de prouver que $\mathscr{B}$ est une base entière, et on calcule le discriminant. Pour prouver que $\mathscr{B}$ est $\mathbb{Z}$-base, on calcule $\Delta_K(\mathscr{B})$. On pose $\alpha = \sqrt{2}$ et $\beta = \dfrac{\sqrt{2} + \mathrm{i}\sqrt{2}}{2}$.

Or, $\mathrm{Tr}_{\mathbb{Q}(\mathrm{i})}(\mathrm{i}) = 0$, $\mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha) = 0$ et $\mathrm{Tr}_{\mathbb{Q}(\mathrm{i}\alpha)} = 0$. Donc, $\mathrm{Tr}_K(\mathrm{i}) = \mathrm{Tr}_K(\alpha) = \mathrm{Tr}_K(\mathrm{i}\alpha) = 0$, et $\mathrm{Tr}_K(\beta) = 0$. Il suit que

$$\Delta_K(\mathscr{B}) = \begin{vmatrix} 4 & & & \\ & -4 & & \\ & & 8 & 4 \\ & & 4 & 0 \end{vmatrix} = 4^4,$$

et $\Delta_K(\mathscr{B})$ est le discriminant. □

Exercice 4 (Extensions monogènes cubiques)**.** Soient $m > 0$ un entier qui n'est pas un cube, $\theta = \sqrt[3]{m}$ et $K = \mathbb{Q}(\theta)$.

1/ Soit $\mathscr{B} = \{1, \theta, \theta^2\}$. Calculer $\Delta_K(\mathscr{B})$.

Correction. On affirme que $X^3 - m$ est irréductible sur $\mathbb{Q}$. Autrement, il possède une racine a/b avec $\mathrm{pgcd}(a, b) = 1$. On suppose que $b \neq \pm 1$. Soit p un diviseur premier de b (et donc $p \nmid a$). De $b^3 m = a^3$ on déduit $p \mid a^3 \Rightarrow p \mid a$, un absurde. Donc, $b = \pm 1$ et dans ce cas, m est un cube, ce qui est exclu.

Par conséquent, $[K : \mathbb{Q}] = 3$ et $1, \theta, \theta^2$ est une $\mathbb{Q}$-base de K. On a

$$\mu_\theta = \begin{pmatrix} 0 & 0 & m \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mu_{\theta^2} = \begin{pmatrix} 0 & m & 0 \\ 0 & 0 & m \\ 1 & 0 & 0 \end{pmatrix}.$$

Donc,

$$\Delta(\mathscr{B}) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(m) \\ \mathrm{Tr}(\theta^2) & \mathrm{Tr}(m) & \mathrm{Tr}(m\theta) \end{vmatrix} = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3m \\ 0 & 3m & 0 \end{vmatrix} = -27m^2.$$

□

2/ On suppose désormais que m *n'a pas de facteur carré et* $m \not\equiv \pm 1 \mod 9$. Montrer que $\mathscr{B}$ est une base entière de $\mathfrak{O}_K$ et en particulier $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Indication : Si $3 \nmid m$, on considère $\mathbb{Z}[\sigma]$, où $\sigma = \theta - m$.

Correction. On sait que $\Delta_K(\mathscr{B}) = -27m^2$. L'égalité $[\mathfrak{O}_K : \mathbb{Z}[\theta]]^2 = \Delta_K(\mathscr{B})/\Delta_K$ garantit que les diviseurs premiers de $[\mathfrak{O}_K : \mathbb{Z}[\theta]]$ sont aussi des diviseurs premiers de $\Delta_K(\mathscr{B})$ et par conséquent, les possibles diviseurs premiers de $[\mathfrak{O}_K : \mathbb{Z}[\theta]]$ sont les diviseurs premiers de m et de 3.

Soit maintenant $p \neq 3$ un facteur premier de m. Le poly $X^3 - m$ est p-Eisenstein, et donc $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$. Si $3 \mid m$, alors $X^3 - m$ est 3-Eisenstein et $3 \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$ et l'entier $[\mathfrak{O}_K : \mathbb{Z}[\theta]]$ ne possède aucun facteur premier, ce qui signifie que $\mathbb{Z}[\theta] = \mathfrak{O}_K$.

Si $3 \nmid m$, alors on ne peut pas directement déterminer que $[\mathfrak{O}_K : \mathbb{Z}[\theta]] = 1$ car il est possible que $3 \mid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$. On considère ainsi σ comme dans l'énoncé. Dans ce cas, le polynôme minimal de σ est $(X+m)^3 - m = X^3 + 3mX^2 + 3m^2X + m^3 - m$, qui est 3-Eisenstein. (Un calcul simple montre que $m^3 - m \not\equiv 0 \mod 9$ si $m \equiv 2, 4, 5, 7 \mod 9$.) On déduit que l'indice de $\mathbb{Z}[\theta] = \mathbb{Z}[\sigma]$ en $\mathfrak{O}_K$ est aussi premier à 3. $\square$