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

Séance 3, 16 mars 2021

Notations et conventions.

- Le nombre algébrique α a “degré” n quand $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
- Pour chaque nombre algébrique α, on désigne par $\Pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal.
- Si K un corps de nombres de degré n, l'ensemble de plongements de K dans $\mathbb{C}$ est noté $\Sigma(K)$. Si $\alpha \in K$ est donné, les conjugués de α sont les complexes ayant la forme $\sigma(\alpha)$ pour $\sigma \in \Sigma(K)$. La K-norme $\mathrm{N}_K(\alpha)$ est $\prod_{\sigma\in\Sigma(K)} \sigma(\alpha)$ et la K-trace $\mathrm{Tr}_K(\alpha)$ est $\sum_{\sigma\in\Sigma(K)} \sigma(\alpha)$. (Une notation plus précise et plus encombrante serait $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.)
- Pour $n \geqslant 1$, on désigne par $\mu\!\!\mu_n$, respectivement $\mu\!\!\mu'_n$, l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
- Le n-ème polynôme cyclotomique $\prod_{\zeta\in\mu\!\!\mu'_n}(X - \zeta)$ sera désigné par Φ_n.
- L'anneau des entiers d'un corps de nombres K sera désigné par $\mathfrak{O}_K$.

Le discriminant

Exercice 1. Soit $\alpha_1, \dots, \alpha_n$ une $\mathbb{Q}$-base du corps de nombres K. Si $\Sigma(K) = \{\sigma_i : K \to \mathbb{C}\}_{i=1}^n$ sont les plongements, on rappelle que le discriminant $\Delta(\alpha_1, \dots, \alpha_n)$ est $\det(\sigma_i(\alpha_j))^2$. Montrer que $\Delta_K(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_K(\alpha_i\alpha_j))$.

Exercice 2. Soit $K = \mathbb{Q}(x)$ un corps de nombres algébriques de degré n et $f \in \mathbb{Q}[X]$ le polynôme minimal de x. On souhaite prouver la formule

$$\Delta(1, x, \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K/\mathbb{Q}}(f'(x)). \tag{d}$$

1/ Soit $\Sigma(K) = \{\sigma_i : K \to \mathbb{C}\}_{i=1}^n$ l'ensemble des plongements. Alors

$$\Delta(1, x, \dots, x^{n-1}) = \prod_{i<j}(\sigma_i(x) - \sigma_j(x))^2.$$

Justifier.

2/ Utiliser la question précédente pour montrer la formule (d).

3/ Soient $p > 2$ un premier, ζ une racine primitive p-ème de l'unité et $K = \mathbb{Q}(\zeta)$. Calculer $\Delta(1, \dots, \zeta^{p-1})$.

Exercice 3. Soit K un corps de nombres de degré n et $\{\alpha_1, \dots, \alpha_n\}$ une base entière de $\mathfrak{O}_K$. Soient $x_1, \dots, x_n$ sont des entiers algébriques de K. Montrer que

$$\Delta_K(x_1, \dots, x_n) = \det(C)^2 \cdot \Delta_K,$$

où $C = (c_{ij})$ est la matrice entière définie par $x_j = \sum_{i=1}^n c_{ij}\alpha_i$. En déduire que si $|\Delta_K(x_1, \dots, x_n)| = |\Delta_K|$ alors $\{x_1, \dots, x_n\}$ est une base entière de $\mathfrak{O}_K$.

Exercice 4. On étudie les propriétés de divisibilité des discriminants.

1/ Soient f et g dans $\mathbb{Z}[X]$ unitaires. Montrer que si f divise g, alors $\mathrm{disc}(f)$ divise $\mathrm{disc}(g)$.

2/ On souhaite démontrer un théorème de Kronecker sur le discriminant. *Soient $K \subset L$ des corps de nombres. Alors Δ_K divise Δ_L.*

Dans la suite, on écrit $m = [K : \mathbb{Q}]$ et $d = [L : K]$.

i/ Utiliser le théorème de la base adaptée pour trouver une base entière $\{\beta_i\}_{i=1}^{md}$ de $\mathfrak{O}_L$ telle que $\{\beta_i\}_{i=1}^{m}$ soit une base entière de $\mathfrak{O}_K$.

ii/ Soient $\sigma_1, \dots, \sigma_m$ les plongements de K dans $\mathbb{C}$. Pour chaque $i \in \{1, \dots, m\}$, on prolonge σ_i à L obtenant ainsi d plongements distincts $L \to \mathbb{C}$. En dénombrant les prolongements de chaque σ_i selon le schéma suivant,

$$\begin{tikzcd} \tau_i & \tau_{i+m} & \cdots & \tau_{i+(d-1)m} \\ & \sigma_i \arrow[ul, no head] \arrow[u, no head] \arrow[ur, no head] \arrow[urr, no head] & & \end{tikzcd}$$

exprimer la matrice $B = (\tau_j\beta_i)_{1 \leqslant i,j \leqslant md}$ en fonction de $A = (\sigma_j\beta_i)_{1 \leqslant i,j \leqslant m}$. Ensuite, prouver le théorème de Kronecker.

Exercice 5 (Le théorème de Brill)**.** Soit K un corps de nombres de degré n. On désigne par $\sigma_1, \dots, \sigma_s$ les plongements réels de K, et $\{\sigma_{s+1}, \dots, \sigma_{s+2t}\}$ les plongements complexes(=non-réels) où on suppose que $\sigma_{s+t+j} = \overline{\sigma}_{s+j}$ pour $j \in \{1, \dots, t\}$. Soient $x_1, \dots, x_n$ une $\mathbb{Q}$-base de K et

$$X_j := \begin{pmatrix} \sigma_j(x_1) \\ \vdots \\ \sigma_j(x_n) \end{pmatrix}.$$

1/ Soit X la matrice complexe $n \times n$ dont la j-ème colonne est X_j. Montrer que $\overline{X}$ est obtenue à partir de X en faisant les opérations colonne $X_{s+j} \leftrightarrow X_{s+t+j}$ pour chaque $j \in \{1, \dots, t\}$. En déduire que $\det \overline{X} = (-1)^t \det X$.

2/ En déduire que $(\det X)^2$ est un réel de signe $(-1)^t$.

3/ Montrer que Δ_K a signe $(-1)^t$.