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 μ_n, respectivement μ_n', l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
- Le n-ème polynôme cyclotomique $\prod_{\zeta\in\mu_n'}(X - \zeta)$ 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 $\Delta_K(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_K(\alpha_i\alpha_j))$.

Correction. On a $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j)$. Soit $M_\alpha = (\sigma_i(\alpha_j))$. Alors $(\det M_\alpha)^2 = \det(M_\alpha^t \cdot M_\alpha) = \Delta_K(\alpha_1, \dots, \alpha_n)$. Or, il est facile de voir que l'entrée (i, j) de $M_\alpha^t \cdot M_\alpha$ est $\sum_{k=1}^n \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j)$, qui n'est autre que $\mathrm{Tr}_K(\alpha_i\alpha_j)$. □

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.

Correction. On note que

$$\Delta(1, \dots, x^{n-1}) = \begin{vmatrix} \sigma_1(1) & \cdots & \sigma_n(1) \\ \sigma_1(x) & \cdots & \sigma_n(x) \\ \sigma_1(x)^2 & \cdots & \sigma_n(x)^2 \\ \vdots & \vdots & \vdots \\ \sigma_1(x)^{n-1} & \cdots & \sigma_n(x)^{n-1} \end{vmatrix}^2 .$$

On voit que $\Delta(1, \dots, x^{n-1})$ est un déterminant de van der Monde et la formule cherchée est bien connue. $\square$

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

Correction. On écrit x_i au lieu de $\sigma_i x$. Comme $f(X) = \prod_{i=1}^n (X - x_i)$, on déduit que

$$f'(X) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ j \neq i}} (X - x_j)$$

et donc

$$f'(x_j) = \prod_{\substack{i=1 \\ j \neq i}} (x_j - x_i).$$

Or, il est clair que les conjugués de $f'(x)$ sont $\{f'(x_j)\}_{j=1}^n$ et par conséquent, en écrivant $Q = \{1, \dots, n\}^2$ et $D = \{(i,i) \,:\, 1 \leqslant i \leqslant n\}$, on déduit

$$\begin{aligned} \mathrm{N}_K(f'(x)) &= \prod_{j=1}^{n} f'(x_j) \\ &= \prod_{j=1}^{n} \prod_{\substack{i=1 \\ j \neq i}} (x_j - x_i) \\ &= \prod_{(i,j) \in Q \setminus D} (x_j - x_i). \end{aligned}$$

On obtient $Q \backslash D = Q^- \sqcup Q^+$, où Q^+ est la partie au-dessus de la diagonale et Q^- la partie en-dessous. Or, si $(i,j) \in Q^-$, alors $(j,i) \in Q^+$ et $\sigma_j(x) - \sigma_i(x) = -(\sigma_i(x) - \sigma_j(x))$. Donc,

$$\begin{aligned} \prod_{(i,j) \in Q^-} (x_j - x_i) &= \prod_{(i,j) \in Q^-} (-1) \cdot (x_i - x_j) \\ &= (-1)^{n(n-1)/2} \prod_{(i,j) \in Q^+} (x_j - x_i). \end{aligned}$$

En utilisant la formule de la première question, on a terminé. $\square$

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

Correction. On sait que $\Delta(1, \ldots, \zeta^{p-2}) = (-1)^{(p-1)(p-2)/2} \mathrm{N}_K(\Phi_p'(\zeta))$. Or,

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} \quad \Rightarrow \quad \Phi_p'(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1}.$$

On calcule maintenant la norme de $\Phi_p'(\zeta)$. Soit $\lambda = 1 - \zeta$. Il suit que $p = \Phi_p(1) = \prod_{j=1}^{p-1}(1 - \zeta^j) = \mathrm{N}_K(\lambda)$. En particulier, $\mathrm{N}_K(\zeta - 1) = (-1)^{p-1}p$. Or, $\mathrm{N}_K(\zeta) = 1 = \Phi_p(0)$ et

$$\mathrm{N}_K(\Phi_p'(\zeta)) = \frac{p^{p-1}}{(-1)^{p-1}p} = p^{p-2}.$$

Finalement,

$$\Delta = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

□

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

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

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

Correction. On a $\sigma_i(x_j) = \sum_{k=1}^n c_{kj}\sigma_i(\alpha_k)$ et $(\sigma_i(x_j)) = (\sigma_i(\alpha_j)) \cdot C$; d'où la formule puisque $\Delta_K = \det(\sigma_i(\alpha_j))^2$. Pour la deuxième question, on note simplement que la matrice C aura déterminant ± 1, et sera donc dans $\mathrm{GL}_n(\mathbb{Z})$. □

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 $\mathrm{disc}(g)$.

Correction. Si $\alpha_1, \ldots, \alpha_m$ sont les racines de f et $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n$ sont les racines de g, on introduit $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, qui est un corps de nombres. Comme $\mathrm{disc}(f) = \prod_{1 \leqslant i < j \leqslant m}(\alpha_i - \alpha_j)^2$ et $\mathrm{disc}(g) = \prod_{1 \leqslant i < j \leqslant n}(\alpha_i - \alpha_j)^2$ on déduit que

$$\frac{\mathrm{disc}(g)}{\mathrm{disc}(f)} \in \mathfrak{O}_K,$$

mais comme $\mathrm{disc}(f)$ et $\mathrm{disc}(g)$ sont des entiers, on a $\mathrm{disc}(f)/\mathrm{disc}(f) \in \mathbb{Q} \cap \mathfrak{O}_K = \mathbb{Z}$. □

3. Nous avons corrigé une erreur dans l'énoncé original.

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 $\mathfrak{O}_K$.

Correction. Par le théorème de la base adapté, il existe une base entière $\beta_1, \ldots, \beta_{md}$ de L et des entiers $d_1, \ldots, d_m$ tels que $d_1\beta_1, \ldots, d_m\beta_m$ est une base entière de $\mathfrak{O}_K$. Or, mais $d_i\beta_i \in K$ implique que $\beta_i \in K$ et comme β_i est entier, on voit que $\beta_i \in \mathfrak{O}_K$. Or, en écrivant $\beta_j = \sum_{i=1}^{m} c_{ij} \cdot (d_i\beta_i)$, avec $c_{ij} \in \mathbb{Z}$ et en utilisant que $\{\beta_i\}$ est une famille libre, on voit que chaque d_i divise 1 et donc $d_i = \pm 1$. Il suit que $\beta_1, \ldots, \beta_m$ est une base entière de $\mathfrak{O}_K$. $\square$

ii/ Soient $\sigma_1, \ldots, \sigma_m$ les plongements de K dans $\mathbb{C}$. Pour chaque $i \in \{1, \ldots, m\}$, 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,

$$\begin{tikzcd}[arrows=-] \tau_i \arrow[dr] & \tau_{i+m} \arrow[d] & \cdots \arrow[dl] & \tau_{i+(d-1)m} \arrow[dll] \\ & \sigma_i & & \end{tikzcd}$$

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.

Correction. Les plongements $\tau_1, \tau_{1+m} \ldots, \tau_{1+(d-1)m}$ prolongent σ_1, $\tau_2, \tau_{2+m}, \ldots, \tau_{2+(d-1)m}$ prolongent σ_2, etc. Dit autrement, τ_{i+mk} pour $k = 0, \ldots, d-1$ prolongent σ_i. Avec cette numérotation, on note que, pour chaque $i \in \{1, \ldots, m\}$, on a

$$(\tau_1\beta_i, \tau_2\beta_i, \ldots, \tau_n\beta_i) = (\sigma_*\beta_i, \ldots, \sigma_*\beta_i),$$

où $\sigma_*\beta_i = (\sigma_1\beta_i, \ldots, \sigma_m\beta_i)$. Donc,

$$B = \left(\begin{array}{c|c|c|c} A & A & \cdots & A \\ \hline * & * & \cdots & * \end{array}\right),$$

et en faisant des opérations colonne, on obtient

$$\det B = \det \left(\begin{array}{c|c|c|c} A & 0 & \cdots & 0 \\ \hline * & * & \cdots & * \end{array}\right),$$

d'où $\Delta_L = \det(A)^2 \cdot \mu$ avec $\mu \in \mathfrak{O}_L$. Or, mais $\det(A)^2 = \Delta_K$ et $\mu \in \mathbb{Q} \cap \mathfrak{O}_L = \mathbb{Z}$.

$\square$

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

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

Correction. On note que $\det \overline{X} = \overline{(\det X)}$. Donc, $\det X \cdot \det \overline{X} = |\det X|^2$ est un réel positif. Or, $\det X \cdot \det X = \det X \cdot (-1)^t \det \overline{X} = (-1)^t |\det X|^2$. $\square$

3/ Montrer que Δ_K a signe $(-1)^t$.