TD 1 : Corps de nombres et entiers algébriques

Exercice 1. [Corps quadratiques]

Dans tout cet exercice, d est un entier relatif sans facteur carré, différent de 0 et 1.

(a) Pour tous $a, b \in \mathbb{Q}$, calculer la trace et la norme de $a + b\sqrt{d}$ dans $\mathbb{Q}(\sqrt{d})$, puis son polynôme minimal dans $\mathbb{Q}$.

(b) En déduire que l'ensemble des entiers algébriques de $\mathbb{Q}(\sqrt{d})$, noté $\mathcal{O}_d$, est $\mathbb{Z}[\sqrt{d}]$ si d est congru à 2 ou 3 modulo 4, et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si d est congru à 1 modulo 4.

(c) Déterminer $\mathcal{O}_d^*$ si $d < 0$. Sans preuve, que semble-t-il se passer pour $d > 0$? Étudier les premiers cas.

(d) Montrer que $\mathbb{Z}[i]$ est euclidien pour la norme usuelle, et calculer ses irréductibles.

(e) Montrer que $\mathcal{O}_{-5}$ n'est pas factoriel.

(f) Montrer que tout corps de nombres de degré 2 est égal à un $\mathbb{Q}(\sqrt{d})$ et que ceux-ci sont non-isomorphes deux à deux.

Exercice 2. [Norme sur un corps de nombres]

Soit K un corps de nombres quelconque, on note N la norme $N_{K/\mathbb{Q}}$ dans cet exercice.

(a) Pour tout $\alpha \in K$, montrer que $\alpha = 0 \iff N(\alpha) = 0$. Si $\alpha \in \mathcal{O}_K$, montrer que $N(\alpha) \in \mathbb{Z}$.

(b) Montrer que N est multiplicative et à valeurs entières sur $\mathcal{O}_K$, puis que les unités de $\mathcal{O}_K$ sont exactement les $\alpha \in \mathcal{O}_K$ tels que $N(\alpha) = \pm 1$.

(c) Montrer que pour $\alpha \in \mathcal{O}_K$, si $N(\alpha)$ est un nombre premier, alors α est irréductible dans l'anneau $\mathcal{O}_K$. La réciproque est-elle vraie ?

Exercice 3. [Discriminant]

(a) Avec les notations de l'exercice 1, calculer $\operatorname{disc}(1, \sqrt{d})$, puis $\operatorname{disc} \mathcal{O}_d$.

(b) Pour $X^3 + aX + b \in \mathbb{Q}[X]$ irréductible sur $\mathbb{Q}$ et α une racine de P, calculer $\operatorname{disc}(1, \alpha, \alpha^2)$.

(c) Pour $P \in \mathbb{Q}[X]$ irréductible de degré d, α une racine de P et $K = \mathbb{Q}(\alpha)$, montrer que

$$\operatorname{disc}(1, \alpha, \cdots, \alpha^{d-1}) = (-1)^{d(d-1)/2} N_{K/\mathbb{Q}}(P'(\alpha)).$$

Exercice 4. [Théorème de Taussky]

Soit K un corps de nombres de base $(\alpha_1, \cdots, \alpha_n)$ sur $\mathbb{Q}$, dont les plongements dans $\mathbb{C}$ sont notés $\sigma_1, \cdots, \sigma_n$, avec les r premiers réels et le reste venant par s paires de plongements complexes conjugués (soit $r + 2s = n$).

(a) Rappeler la preuve de l'égalité matricielle

$$(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j} = {}^tMM, \quad M = (\sigma_i(\alpha_j))_{i,j}.$$

(b) Montrer qu'il existe une matrice réelle inversible R telle que les $r+s$ premières lignes de RM sont réelles et les s dernières sont imaginaires pures.

(c) En posant $D = \mathrm{diag}(1, \cdots, 1, i, \cdots, i)$ avec $r+s$ valeurs égales à 1 et s valeurs égales à i, montrer que $M_1 = DRM$ est réelle. En déduire que ${}^tMM$ est congruente sur $\mathbb{R}$ à $D^{-1t}R^{-1}R^{-1}D^{-1}$.

(d) Prouver que $D^{-1t}R^{-1}R^{-1}D^{-1}$ est de la forme

$$\begin{pmatrix} B_1 & 0 \\ 0 & -B_2 \end{pmatrix}$$

avec B_1 et B_2 des matrices symétriques rélles définies positives de tailles respectives $r + s$ et s.

(e) En déduire que la signature de la forme trace sur K est $(r + s, s)$ avec r le nombre de plongements réels, et s le nombre de plongements complexes.

Exercice 5. [Approximation diophantienne]

(a) Soit $x \in \mathbb{R}$. Montrer que pour tout entier $M \geq 1$, il existe un couple d'entiers (p, q) avec $1 \leq q \leq M$ tel que $|qx - p| < 1/M$.

(b) En déduire le théorème d'approximation de Dirichlet : il existe une infinité de rationnels p/q tels que $|x - p/q| < 1/q^2$.

Le théorème de Hurwitz affirme en fait qu'on peut descendre à $\frac{1}{\sqrt{5}q^2}$. On note $\varphi = \frac{1+\sqrt{5}}{2}$ le nombre d'or, montrons que le théorème de Hurwitz est optimal pour celui-ci.

(c) Pour une fraction p/q, on note

$$\theta = \sqrt{5}q^2 \left|\varphi - \frac{p}{q}\right|.$$

Montrer que

$$\frac{\theta^2}{5q^2} - \theta = p^2 - pq - q^2.$$

En déduire que pour tout $c > 1$, il est impossible d'avoir $\theta < 1/c$ pour une infinité de rationnels. Conclure.

(d) Montrer que l'ensemble des nombres transcendants est de mesure totale dans $\mathbb{R}$, alors que celui des nombres de Liouville est de mesure nulle.