UE Théorie des nombres. Examen du 30 avril 2018, 9h-12h

Tous documents interdits.

Qing Liu

Exercice 1 Rappeler les propriétés générales de la fonction zêta $\zeta(s)$ de Riemann, les zéros connus et les pôles, les valeurs aux entiers strictement positifs pairs si possible.

Exercice 2 (Corps de nombres de petits discriminants) Soit L un corps de nombre de degré $n = [L : \mathbb{Q}]$. Rappelons (Minkowski) que tout idéal fractionnaire de L est équivalent à un idéal J de norme $N(J) \leq C_L\sqrt{|d_L|}$, où $C_L = (4/\pi)^{r_2} n!/n^n$, r_2 est le nombre de plongements imaginaires et d_L est le discriminant de L. On sait aussi que $|d_L| \geq \pi^n/4$.

Trouver tous les L avec $|d_L| \leq 5$.

Exercice 3 (Bases et localisation) Soit L un corps de nombres. Considérons $b_1, \ldots, b_n \in \mathcal{O}_L$ qui forment une base de L comme $\mathbb{Q}$-espace vectoriel. En général ce n'est pas une base de $\mathcal{O}_L$ comme $\mathbb{Z}$-module. Cependant, posons

$$\delta = D_{L/\mathbb{Q}}(b_1, \ldots, b_n).$$

On va montrer que $\delta \in \mathbb{Z} \setminus \{0\}$ et que tout $b \in \mathcal{O}_L$ s'écrit comme

$$b = \sum_{1 \leq j \leq n} \frac{a_j}{\delta} b_j, \quad a_j \in \mathbb{Z}.$$

Soit M la matrice $(\mathrm{Tr}_{L/\mathbb{Q}}(b_j b_k))_{1 \leq j,k \leq n}$.

(1) Est-ce que $\{b_1, \ldots, b_n\}$ est une famille libre du $\mathbb{Z}$-module $\mathcal{O}_L$?

(2) Montrer que $M \in M_n(\mathbb{Z})$ et que $\delta \in \mathbb{Z}$, $\delta \neq 0$.

(3) Soit $b \in \mathcal{O}_L$. On écrit $b = \sum_{1 \leq k \leq n} x_k b_k$ avec $x_k \in \mathbb{Q}$. Posons $a_k = \mathrm{Tr}_{L/\mathbb{Q}}(b_k b)$ pour tout $k \leq n$. Montrer que $M \cdot {}^t(x_1, \ldots, x_n) = {}^t(a_1, \ldots, a_n)$.

(4) En utilisant la comatrice de M, montrer que $\delta x_k \in \mathbb{Z}$ pour tout $k \leq n$. Conclure.

Exercice 4 (Étude détaillée d'une extension cubique) Soit $\alpha \in \mathbb{C}$ une racine du polynôme

$$m(X) = X^3 - 3X + 1 \in \mathbb{Z}[X].$$

Soit $L = \mathbb{Q}[\alpha]$ l'extension de $\mathbb{Q}$ engendrée α.

(1) Montrer que $m(X)$ est irréductible dans $\mathbb{Q}[X]$ et que $[L : \mathbb{Q}] = 3$.

(2) Montrer que le discriminant $D_{L/\mathbb{Q}}(\{1, \alpha, \alpha^2\}) = 3^4$. En déduire que L possède trois plongements réels et que les racines de $m(X)$ sont des nombres réels.

(3) Montrons maintenant que l'anneau des entiers $\mathcal{O}_L$ est égal à $\mathbb{Z}[\alpha]$.

(a) Soit $\theta = \alpha + 1$. Montrer que

$$\theta^3 - 3\theta + 3 = 0$$

et que $L = \mathbb{Q}[\theta]$, $\mathbb{Z}[\alpha] = \mathbb{Z}[\theta]$.

(b) Calculer $\mathrm{Tr}_{L/\mathbb{Q}}(\theta)$ et $\mathrm{N}_{L/\mathbb{Q}}(\theta)$.

(c) Montrer que $\theta^n \in 3\mathcal{O}_L$ pour tout entier $n \geq 3$.

(d) Soit $b \in \mathcal{O}_L$. Montrer qu'il existe $a_0, a_1, a_2 \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que

$$b = \frac{a_0}{3^r} + \frac{a_1}{3^r}\theta + \frac{a_2}{3^r}\theta^2$$

et que 3 ne divise pas $\mathrm{pgcd}(a_0, a_1, a_2)$. On va montrer que $r = 0$. Ce qui impliquera que $b \in \mathbb{Z}[\theta]$ et donc que $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

(e) Supposons $r \geq 1$. Montrer que $3^{-1}a_0\theta^2 \in \mathcal{O}_L$ (considérer $3^{r-1}b\theta^2$). Utiliser la norme pour en déduire que $3 \mid a_0$.

(f) Montrer que $3^{-1}a_1\theta + 3^{-1}a_2\theta^2 \in \mathcal{O}_L$ et que $3^{-1}a_1\theta^2 \in \mathcal{O}_L$.

(g) Montrer que $3 \mid \mathrm{pgcd}(a_0, a_1, a_2)$. Conclure.

(4) (Groupe des classes de L). On va montrer que $\mathcal{O}_L$ est principal.

(a) Quel est le discriminant d_L de L ?

(b) Montrer que tout idéal fractionnaire de $\mathcal{O}_L$ est équivalent à un idéal $J \subseteq \mathcal{O}_L$ de norme $N(J) \leq 2$.

(c) Donner la décomposition de l'idéal $2\mathcal{O}_L$.

(d) Montrer que $\mathcal{O}_L$ est principal.

(e) Donner la décomposition des idéaux $3\mathcal{O}_L, 5\mathcal{O}_L$.

(5) (Groupe des unités) On sait que $b \in \mathcal{O}_L$ est une unité (i.e. inversible pour la multiplication) si et seulement si $\mathrm{N}_{L/\mathbb{Q}}(b) = \pm 1$. Notons U le groupes des unités de $\mathcal{O}_L$.

(a) Rappeler la preuve de l'implication $b \in U \Longrightarrow \mathrm{N}_{L/\mathbb{Q}}(b) = \pm 1$.

(b) Soit $b \in U_{\mathrm{tors}}$ un élément d'ordre fini $n \geq 2$ (donc une racine primitive n-ième de 1). Montrer que $\phi(n) \mid 3$, où ϕ est la fonction indicatrice d'Euler. En déduire que $n = 2$ et que

$$U/\{\pm 1\} \simeq \mathbb{Z}^2$$

comme groupe.

(c) Montrer que $\alpha \in U$.

(d) Vérifier que $\alpha^2 - 2$ est aussi racine de $m(X)$ et est donc une unité. Remarque : on peut montrer que les images de $\alpha, \alpha^2 - 2$ dans $U/\{\pm 1\}$ forment une base.

(6) (Propriétés galoisiennes) Montrer que $L/\mathbb{Q}$ est une extension galoisienne. Vérifier que $2\cos(2\pi/9) \in \mathbb{R}$ est racine de $m(X)$. En déduire que L est une (la) sous-extension d'indice 2 de l'extension cyclotomique $\mathbb{Q}[e^{2i\pi/9}]$.

Exercice 5 Soit A un anneau de Dedekind de corps de fractions K. Soit B la clôture intégrale de A dans une extension finie séparable L/K. En général B n'est pas monogène sur A (i.e. de la forme $A[\alpha]$ pour un $\alpha \in B$ convenable). Nous allons montrer que quitte à localiser A convenablement, B devient alors monogène sur A.

(1) Pourquoi existe-il $\alpha \in L$ tel que $L = K[\alpha]$?

(2) Soit $b_1, \ldots, b_m$ une famille génératrice de B comme A-module. Soit $m(X) \in K[X]$ le polynôme minimal de α sur K et soit $\delta = \mathrm{disc}(m(X)) \in K$ le discriminant de $m(X)$. Montrer qu'il existe $f \in A$ non nul tel que

$$b_1, \ldots, b_m \in A_f[\alpha], \quad m(X) \in A_f[X], \quad \delta \in (A_f)^*.$$

(3) On sait que B_f est la clôture intégrale de A_f dans L. Montrer que $B_f = A_f[\alpha]$, que B_f est libre sur A_f, que le discriminant

$$D_{B_f/A_f}(\{1, \alpha, \ldots, \alpha^{n-1}\}) \in (A_f)^*$$

et que B_f est non-ramifié sur A_f (pour cette dernière assertion, on supposera pour simplifier que les corps $A/\mathfrak{p}$ sont parfaits pour tous les idéaux maximaux $\mathfrak{p}$ de A).

(4) Quelle relation existe-il entre l'ensemble des idéaux maximaux de A et ceux de A_f ?

◇◇ Fin ◇◇