FMA51052EP
Théorie Algébrique des Nombres

Examen - 18 décembre 2024 - 3 heures

Documents autorisés : *polycopié, notes de cours et de PC, dictionnaire papier.*
Vous pouvez écrire en anglais ou en français.

Le sujet est composé deux exercices courts et d'un long problème. Il n'est pas nécessaire de tout faire pour obtenir la note maximale.

Exercice 1 : Carré ou non ?

Déterminer si 34 est un carré modulo 1195. On remarquera que 239 est premier.

Exercice 2 : Inverse d'une fonction L

Soient $N \geqslant 1$ un entier et χ un caractère de Dirichlet modulo N. Trouver une fonction multiplicative $f : \mathbb{N}_{>0} \to \mathbb{C}$ bornée telle que, pour tout $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$:

$$\frac{1}{L(\chi, s)} = \sum_{n \geqslant 1} \frac{f(n)}{n^s}.$$

Problème : Un contre-exemple au principe de Hasse

On considère l'équation :

$$3x^3 + 4y^3 + 5z^3 = 0. \qquad (\star)$$

A) Dans cette question, on montre que l'équation $(\star)$ a des solutions non nulles dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$ avec p premier.

1) Montrer que l'équation $(\star)$ a des solutions non nulles dans $\mathbb{R}$.
2) Montrer que l'équation $(\star)$ a des solutions non nulles dans $\mathbb{Q}_3$. Pour ce faire, on pourra vérifier que $5/4$ admet une racine cubique dans $\mathbb{Q}_3$.
3) Soit p un nombre premier différent de 3 et tel que 3 est un cube modulo p. Montrer que l'équation $(\star)$ a des solutions non nulles dans $\mathbb{Q}_p$.
4) Soit p un nombre premier tel que 3 n'est pas un cube modulo p.
   a) Justifier pourquoi il existe $b \in \mathbb{Z}$ tel que l'une des congruences suivantes est satisfaite :
   $$b^3 \equiv 5 \mod p, \qquad 3b^3 \equiv 5 \mod p, \qquad 9b^3 \equiv 5 \mod p.$$
   b) Dans chacun des trois cas précédents, prouver que l'équation $(\star)$ admet une solution non nulle dans $\mathbb{Q}_p$. Dans le cas $9b^3 \equiv 5 \mod p$, on pourra chercher une solution avec $y = 5$ et $z = -7$ et remarquer que $5 \cdot 7^3 - 4 \cdot 5^3 = 1215 = 5 \cdot 3^5$.

B) Dans cette question, on s'intéresse au groupe de classes du corps de nombres $K = \mathbb{Q}(\alpha)$ avec $\alpha = \sqrt[3]{6}$.

1) Montrer que son anneau d'entiers est $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
2) Calculer le discriminant Δ_K.

3) En déduire que le groupe des classes Cl_K de K est engendré par l'ensemble S des idéaux premiers $\mathfrak{p}$ d'indice au plus 19 dans $\mathcal{O}_K$. On pourra utiliser l'**une** des valeurs approchées à 10^{-3} près suivantes au choix :

$$\sqrt{2} \approx 1,414, \quad \frac{\sqrt{2}}{\pi} \approx 0,450, \quad \frac{\sqrt{2}}{\pi^2} \approx 0,143, \quad \frac{\sqrt{2}}{\pi^3} \approx 0,046,$$
$$\sqrt{3} \approx 1,732 \quad \frac{\sqrt{3}}{\pi} \approx 0,551, \quad \frac{\sqrt{3}}{\pi^2} \approx 0,175, \quad \frac{\sqrt{3}}{\pi^3} \approx 0,056.$$

4) a) Justifier pourquoi les factorisations des idéaux (2), (3), (5) et (7) en produit d'idéaux premiers dans $\mathcal{O}_K$ sont de la forme :

$$(2) = \mathfrak{p}_2^3, \quad (3) = \mathfrak{p}_3^3, \quad (5) = \mathfrak{p}_5\mathfrak{p}_{25}, \quad (7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7'',$$

avec :

$$\begin{cases} \mathfrak{p}_2 \text{ idéal premier d'indice 2,} \\ \mathfrak{p}_3 \text{ idéal premier d'indice 3,} \\ \mathfrak{p}_5 \text{ idéal premier d'indice 5 et } \mathfrak{p}_{25} \text{ idéal premier d'indice 25,} \\ \mathfrak{p}_7, \mathfrak{p}_7' \text{ et } \mathfrak{p}_7'' \text{ trois idéaux premiers deux à deux distincts d'indice 7.} \end{cases}$$

b) Sans justification, décrire également les factorisations des idéaux (11), (13), (17) et (19) dans $\mathcal{O}_K$. On pourra remarquer que tous les éléments de $\mathbb{Z}/11\mathbb{Z}$ et de $\mathbb{Z}/17\mathbb{Z}$ sont des cubes, alors que les cubes dans $\mathbb{Z}/13\mathbb{Z}$ sont $0, \pm 1, \pm 5$, et ceux dans $\mathbb{Z}/19\mathbb{Z}$ sont $0, \pm 1, \pm 7, \pm 8$.

c) En déduire la liste des éléments de S. On vérifiera notamment que S est de cardinal 8.

5) a) Pour $k \in \mathbb{Z}$, calculer $N_{K/\mathbb{Q}}(k + \alpha)$ en fonction de k.

b) Montrer que :

$$\mathfrak{p}_2 = (\alpha - 2), \quad \mathfrak{p}_5 = (\alpha - 1).$$

c) Montrer que les idéaux $\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_7'$ et $\mathfrak{p}_7''$ sont tous principaux.

d) Montrer que tous les éléments de S sont principaux.

e) Conclure que le groupe Cl_K est trivial.

C) Dans cette question, on cherche à calculer le quotient $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 3}$, où $\mathcal{O}_K^{\times 3} := \{u^3 : u \in \mathcal{O}_K^\times\}$.

1) On note $\sigma : K \to \mathbb{C}$ le plongement de K dans $\mathbb{C}$ tel que $\sigma(\alpha) = e^{\frac{2i\pi}{3}}\alpha$. Vérifier que $\mathcal{O}_K^\times = \{z \in \mathcal{O}_K : z|\sigma(z)|^2 = \pm 1\}$.

2) On considère le morphisme :

$$\lambda : K^\times \to \mathbb{R}^2$$
$$z \mapsto (\log|z|, \log|\sigma(z)|).$$

Vérifier que $\ker(\lambda)$ est fini et en déduire que $\ker(\lambda) = \{\pm 1\}$.

3) On pose $\Gamma := \lambda(\mathcal{O}_K^\times)$. Montrer que Γ est un sous-réseau dans :

$$L := \{(x, y) \in \mathbb{R}^2 : x + 2y = 0\}.$$

4) Justifier que $u_0 := \frac{(\alpha-2)^3}{2} \in \mathcal{O}_K^\times$.

5) Vérifier que u_0 n'est pas un cube dans $\mathcal{O}_K$.

6) Déduire que :

$$\mathcal{O}_K^\times / {\mathcal{O}_K^\times}^3 = \{\pm 1, \pm\overline{u_0}, \pm\overline{u_0}^2\},$$

où $\overline{u_0}$ est la classe de u_0 dans $\mathcal{O}_K^\times / {\mathcal{O}_K^\times}^3$.

D) Dans cette question, on démontre que l'équation $(\star)$ n'a pas de solutions rationnelles non nulles. On suppose par l'absurde que l'on dispose bien d'une telle solution.

1) Montrer que l'on peut trouver trois entiers non nuls x, y, z, deux à deux premiers entre eux, tels que $x^3 + 6y^3 = 10z^3$.

2) Vérifier que x est pair, que y et z sont impairs, que x et z ne sont pas multiples de 3 et que x et y ne sont pas multiples de 5.

3) Montrer que l'on peut trouver des idéaux $\mathfrak{a}$ et $\mathfrak{a}'$ dans $\mathcal{O}_K$ tels que $(x + y\alpha) = \mathfrak{p}_2\mathfrak{a}$ et $(x^2 - xy\alpha + y^2\alpha^2) = \mathfrak{p}_2^2\mathfrak{a}'$.

4) Montrer que l'on peut trouver des idéaux $\mathfrak{b}$ et $\mathfrak{b}'$ dans $\mathcal{O}_K$ tels que $\mathfrak{a} = \mathfrak{p}_5\mathfrak{b}$ et $\mathfrak{a}' = \mathfrak{p}_{25}\mathfrak{b}'$.

5) Dans cette question, on cherche à prouver qu'il n'existe pas d'idéal premier divisant $\mathfrak{b}$ et $\mathfrak{b}'$ simultanément. Par l'absurde, on se donne un tel idéal premier $\mathfrak{p}$.

   a) Montrer que $3xy\alpha \in \mathfrak{p}$.

   b) Montrer que 2 et 3 ne sont pas dans $\mathfrak{p}$.

   c) Montrer que x et y ne sont pas dans $\mathfrak{p}$.

   d) Aboutir à une contradiction.

6) Montrer qu'il existe un idéal $\mathfrak{c}$ de $\mathcal{O}_K$ tel que $\mathfrak{c}^3 = \mathfrak{b}$.

7) Déduire qu'il existe $k \in \{0, 1, 2\}$ et $\gamma \in \mathcal{O}_K$ tel que :

$$2^k(x + y\alpha) = (\alpha - 2)(\alpha - 1)\gamma^3.$$

8) En écrivant $\gamma = A + B\alpha + C\alpha^2$ avec $A, B, C \in \mathbb{Z}$, montrer que 3 divise γ et aboutir à une contradiction. On pourra se convaincre que le coefficient de α^2 dans le développement de $(\alpha - 2)(\alpha - 1)(A + B\alpha + C\alpha^2)^3$ vaut :

$A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6AC^2 + 6B^2C) + 6(AB^2 + A^2C + 6BC^2)$.