Théorie algébrique des nombres (UM4MA234)

Exercice 1. Parmi les nombres suivants, lesquels sont des entiers algébriques ? Quel est leur degré ?

(1) $\frac{2}{3+\sqrt{13}}$

(2) $\frac{-2+\sqrt{2}+i\sqrt{2}}{2}$

(3) $\frac{\sqrt{a}+\sqrt{b}}{n}$, où a, b sont des entiers distincts sans facteur carré, et n un entier non nul.

Exercice 2.

(1) Soit $P(X) = a_n X^n + \ldots + a_0$ un polynôme à coefficients entiers de degré n. Supposons que la fraction irréductible u/v est une racine de P. Montrer que $u|a_0$ et $v|a_n$.

(2) Soit $x \in \mathbb{Q}$. Montrer que $2\cos(\pi x)$ est un entier algébrique.

(3) Soit $x \in [0,1] \cap \mathbb{Q}$ pour lequel $\cos(\pi x) \in \mathbb{Q}$. Montrer que $x \in \{0, 1/3, 1/2, 2/3, 1\}$.

Exercice 3. (Polynômes cyclotomiques)

Soit n un entier $\geqslant 1$. Le n–ième polynôme cyclotomique, noté Φ_n, est le polynôme unitaire dont les racines sont les racines primitives n–ièmes de l'unité, c'est-à-dire

$$\Phi_n(X) := \prod_{1 \leqslant a \leqslant n, a \wedge n = 1} (X - \mathrm{e}^{2ai\pi/n})$$

(1) Calculer $\Phi_1, \Phi_2, \Phi_3, \Phi_4$, et Φ_p pour p un nombre premier. On note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$. Quel est le degré de Φ_n ?

(2) Montrer que

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

En déduire que

$$n = \sum_{d|n} \varphi(d)$$

(3) Montrer que Φ_n est un polynôme à coefficients entiers.

(4) Montrer que si p est un nombre premier et $k \geqslant 1$ alors $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$.

(5) Démontrer que les polynômes cyclotomiques sont palindromiques.

(6) Soit $n \geqslant 3$. Soit ω une racine primitive n–ième de l'unité et soit P son polynôme minimal. Montrer que P est à coefficients entiers et qu'il existe $Q(X) \in \mathbb{Z}[X]$ unitaire tel que $\Phi_n(X) = P(X)Q(X)$.

(7) Soit p un nombre premier ne divisant pas n. Montrer que $\Phi_n(\omega^p) = 0$.

(8) Supposons que $Q(\omega^p) = 0$. Montrer que $P(X)$ divise le polynôme $Q(X^p)$. Démontrer que $\Phi_n(T)$ a un facteur carré modulo p et aboutir à une contradiction.

(9) Démontrer que $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 4. (Théorème de Kronecker)

Soit P un polynôme unitaire irréductible à coefficients entiers dont toutes les racines dans $\mathbb{C}$ ont un module $\leqslant 1$.

(1) Montrer que pour tout n, α^n est un entier algébrique de module $\leqslant 1$.

(2) Montrer qu'il existe deux entiers distincts n, m tels que $\alpha^n = \alpha^m$.

(3) Montrer que ou P est un polynôme cyclotomique ou $P(X) = X$.

Exercice 5.

Soit d un entier > 0 sans facteur carré.

(1) Calculer le groupe G_d formé par les unités de $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.

Exercice 6.

Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(1) Montrer que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une base du $\mathbb{Q}$–espace vectoriel K.

(2) Calculer dans cette base les matrices de multiplication par $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$.

(3) Déterminer les plongements de K dans $\mathbb{C}$.

(4) Factoriser le déterminant

$$\begin{vmatrix} a & 2b & 3c & 6d \\ b & a & 3d & 3c \\ c & 2d & a & 2b \\ d & c & b & a \end{vmatrix}$$

Exercice 7.

Soit $K = \mathbb{Q}(\alpha)$ où α est une racine de $P(T) = T^3 + T - 3$.

(1) Démontrer de deux façons que P est irréductible. Conclure que K est de degré 3.

(2) Calculer $\mathrm{N}_{K|\mathbb{Q}}(\alpha^2)$ et $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha^2)$.

(3) Montrer que pour tout $x \in K$, $P(x) = \mathrm{N}_{K|\mathbb{Q}}(x - \alpha)$.

Exercice 8.

Soit $n \geqslant 1$.

(1) Soit p un nombre premier. Montrer que $\Phi_n(X)$ admet une racine dans $\mathbb{F}_p$ si et seulement si $p = 1 \mod n$.

(2) Soit $N \geqslant 1$. Montrer que $\Phi_n(N) \wedge N = 1$.

(3) Montrer par l'absurde qu'il y a une infinité de nombres premiers p tels que $p = 1 \mod n$.

Exercice 9. (Discriminant) Soit P un polynôme unitaire de degré n à coefficients complexes et $\alpha_1, \ldots, \alpha_n$ ses racines comptées avec multiplicité.

(1) Obtenir la formule

$$\prod_{i=1}^{n} P'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}(P)$$

(2) Soient $a, b \in \mathbb{C}$ et $P(T) = T^n + aT + b$. Montrer que

$$\mathrm{disc}(P) = (-1)^{n(n-1)/2}(n^n b^{n-1} - (-1)^n a^n (n-1)^{n-1})$$

Désormais P est à coefficients rationnels, irréductible sur $\mathbb{Q}[X]$ et α en est une racine.

(3) Montrer que $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{disc}(P)$, où le discriminant de la famille est pris sur K.

(4) Montrer que

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} N_{K|\mathbb{Q}}(P'(\alpha))$$

Exercice 10. (Entiers cyclotomiques et apparentés)

Soient p un nombre premier et α une racine de P un polynôme p–Eisenstein, et enfin $K := \mathbb{Q}(\alpha)$.

(1) Montrer que si $u_0, \ldots, u_{n-1} \in \mathbb{Z}$ alors

$$N_{K|\mathbb{Q}}(u_0 + u_1\alpha + \ldots + u_{n-1}\alpha^{n-1}) = u_0^n \mod p$$

(2) Soit $\omega := u_0 + u_1\alpha + \ldots + u_{n-1}\alpha^{n-1}$ divisible par p dans $\mathcal{O}_K$. Montrer que pour tout $i \in \{0, \ldots, n-1\}$, $p | u_i$.

(3) En déduire que le cardinal de $\mathcal{O}_K/\mathbb{Z}[\alpha]$ n'est pas divisible par p.

(4) Soit $P(T) = T^3 - 5T - 5$. Montrer que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(5) Soit K_p le p–ième corps cyclotomique. Calculer $\mathrm{disc}(K_p)$ puis $\mathcal{O}_{K_p}$.

(6) Soient $\omega_p := 2\cos(2\pi/p)$ et $K_p^+ := \mathbb{Q}(\omega_p) \subset K_p$. Calculer $\mathcal{O}_{K_p^+}$.

(*Indication : faire usage des polynômes de Tchebychev* $T_n(X) \in \mathbb{Z}[X]$ *vérifiant* $T_n(2\cos\theta) = 2\cos(n\theta)$.)

(7) Montrer que si l est un entier et $K := \mathbb{Q}(p^{1/p^l})$ alors $\mathcal{O}_K = \mathbb{Z}[p^{1/p^l}]$.

Exercice 11. (Anneau d'entiers non monogène)

Soient $m, n \neq 0, 1$ deux entiers distincts sans facteur carré et tels que $m = n = 1 \mod 8$. Posons $K := \mathbb{Q}(\sqrt{m}, \sqrt{n})$ et

$$\alpha := \frac{1+\sqrt{m}}{2} \qquad \beta := \frac{1+\sqrt{n}}{2}$$

(1) Montrer que $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

(2) Monter que les anneaux $\mathcal{O}_K/2\mathcal{O}_K$ et $A = \mathbb{F}_2[X,Y]/(X^2-X, Y^2-Y)$ sont isomorphes.

(3) Montrer qu'il existe au moins 4 morphismes $A \longrightarrow \mathbb{F}_2$.

(4) En déduire que $\mathcal{O}_K$ n'est pas monogène.

Exercice 12. (Critères pour être une base)

Soient K un corps de nombres de degré n et $(\alpha_1, \ldots, \alpha_n)$ une famille d'éléments de $\mathcal{O}_K$.

(1,a) Supposons que le discriminant de $(\alpha_1, \ldots, \alpha_n)$ est sans facteur carré. Montrer que c'est une base de $\mathcal{O}_K$ en tant que $\mathbb{Z}$–module.

(1,b) Soient α une racine du polynôme $T^4 - T - 1$ et $K := \mathbb{Q}(\alpha)$. Montrer que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(2) Supposons maintenant que c'est une base de K et dont le discriminant est de valeur absolue minimale parmi les $\mathbb{Q}$–bases de K formées d'entiers algébriques.

(2,a) Soit $\omega \in \mathcal{O}_K$ tel que

$$\omega = x_1\alpha_1 + \ldots + x_n\alpha_n$$

où $0 \leqslant x_i < 1$. Montrer que $x_1 = 0$.

(2,b) En déduire que $(\alpha_1, \ldots, \alpha_n)$ est une base de $\mathcal{O}_K$ en tant que $\mathbb{Z}$–module.

(3) Soient α une racine du polynôme $T^3 - T - 4$ et $K := \mathbb{Q}(\alpha)$. On va montrer que $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$.

(3,a) Calculer le discriminant de $\mathbb{Z}[\alpha]$.

(3,b) Montrer que si $\omega = \frac{\alpha+\alpha^2}{2}$ alors $(1, \alpha, \omega)$ est une base de $\mathcal{O}_K$ en tant que $\mathbb{Z}$–module.

Exercice 13. (Théorème de Stickelberger)

Soit $K \subset \mathbb{C}$ un corps de nombres de degré n dont les plongements dans $\mathbb{C}$ sont notés $\varphi_1, \ldots, \varphi_n$. Il existe toujours un corps de nombres L contenant K et ayant la propriété d'être galoisien, c'est-à-dire que si $\psi : L \to \mathbb{C}$ est un plongement alors $\psi(L) = L$.

(1) Soit $z \in K$ tel que les $\varphi_i(z)$ sont égaux. Montrer que $z \in \mathbb{Q}$.

(1,bis) Montrer qu'un plongement $\psi : L \to \mathbb{C}$ induit une bijection de $\{\varphi_i\}$ par post-composition, i.e. $\varphi \mapsto \psi \circ \varphi$.

(2) Soient $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Posons

$$a := \sum_{\varepsilon(\sigma)=1} \prod_{i=1}^{n} \varphi_{\sigma(i)}(\alpha_i) \qquad b := \sum_{\varepsilon(\sigma)=-1} \prod_{i=1}^{n} \varphi_{\sigma(i)}(\alpha_i)$$

Montrer que $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = (a-b)^2$.

(3) Montrer que $a + b, ab \in \mathbb{Z}$.

(4) En déduire que $\mathrm{disc}(K) = 0, 1 \mod 4$.

Exercice 14.

Soient z_1, z_2, z_3 trois affixes dans le plan, et $j = \exp(2i\pi/3)$.

(1) Montrer que z_1, z_2, z_3 sont les sommets d'un triange équilatéral (ordonnés dans le sens trigonométrique) si et seulement si

$$z_1 + z_2 j + z_3 j^2 = 0$$

(2) En déduire qu'il n'y a pas de corps de nombres K tel que $K \cap \mathbb{Q}(j) = \mathbb{Q}$ contenant les sommets d'un triangle équilatéral (non trivial...).

Exercice 15.

Soient d, p deux entiers $\geqslant 1$ tels que $-d$ est un carré modulo p. Notons u un entier tel que $u^2 = -d[p]$ et L le réseau de $\mathbb{R}^2$ défini par

$$L := \{(a, b) \in \mathbb{Z}^2,\ \ a = ub\ \ [p]\}$$

(1) Montrer que L est de covolume p.

(2) Posons $C_d(r) := \{(x, y) \in \mathbb{R}^2, x^2 + dy^2 \leqslant r\}$. En utilisant le lemme du corps convexe, montrer que

$$L \cap C_d\left(\frac{4\sqrt{d}p}{\pi}\right) \neq \varnothing$$

(3) En déduire qu'au moins un des nombres $p, 2p, \ldots, hp$, où $h = \lfloor \frac{4\sqrt{d}}{\pi} \rfloor$, est de la forme $a^2 + db^2$.

(Informations)

Soit p premier $\neq 2$. Alors -2 est un carré modulo $p \iff p = 1, 3\ [8]$.

Soit p premier $\neq 3$. Alors -3 est un carré modulo $p \iff p = 1\ [3]$.

(4) Montrer qu'un nombre premier $p \neq 2$ est de la forme a^2+2b^2 si et seulement si $p = 1, 3\ [8]$.

(5) Montrer qu'un nombre premier $p \neq 3$ est de la forme a^2+3b^2 si et seulement si $p = 1\ [3]$.

Exercice 15.bis

Soit α un entier algébrique de polynôme minimal $P \in \mathbb{Z}[T]$ et $A := \mathbb{Z}[\alpha]$. Soit p un nombre premier et $R(T) \mapsto \overline{R}(T)$ la réduction modulo p.

(1) Soit $Q \in \mathbb{F}_p[T]$ un diviseur de $\overline{P}(T)$. Si $\widetilde{Q}(T)$ est un relevé de $Q(T)$ à $\mathbb{Z}[T]$ montrer que $pA + \widetilde{Q}(\alpha)A$ est un idéal de A indépendant du choix de $\widetilde{Q}(T)$, on le note $I(Q)$.

(2) Montrer que $Q \mapsto I(Q)$ induit une bijection entre les facteurs unitaires de $\overline{P}(T)$ et les idéaux de A contenant pA.

(3) Montrer que $A/I(Q)$ est isomorphe à $\mathbb{F}_p[T]/(Q(T))$. En déduire que $|A/I(Q)| = p^{\deg Q}$.

(4) Quels sont les idéaux de $\mathbb{Z}[\sqrt{-5}]$ qui contiennent 2 ? ceux qui contiennent 3 ?

Exercice 16.

Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$.

(1) Montrer que si $N(I)$ est un nombre premier alors I est maximal.

(2) Montrer que si I est maximal alors $N(I)$ est une puissance d'un nombre premier.

Exercice 17.

Soit $d > 1$ sans facteur carré. On pose $\omega := \frac{1+\sqrt{d}}{2}$ ou $\sqrt{d}$, de telle sorte à avoir $\mathcal{O}_K = \mathbb{Z}[\omega]$ pour $K = \mathbb{Q}(\sqrt{d})$, et P son polynôme minimal.

(1) Soit $\mathfrak{P}$ un idéal maximal de $\mathcal{O}_K$.

(1,a) Montrer que $\mathfrak{P}$ contient un unique nombre premier p et que $N = N_K(\mathfrak{P}) \in \{p, p^2\}$.

(1,b) Montrer que si $N = p^2$ alors $\mathfrak{P} = p\mathcal{O}_K$.

(1,c) Montrer que si $N = p$ alors P est réductible modulo p, il existe $c \in \{0, \dots, p-1\}$ tel que $\mathfrak{P} = (p, c - \omega)$ et si $\mathfrak{P}$ n'est pas principal alors pour tout n,

$$|N_{K|\mathbb{Q}}(\omega - (c + pn))| \geqslant 2p$$

(2) $d = 101$. Montrer que $\mathcal{O}_K$ est principal. *(Indication : montrer que $\mathcal{O}_K$ ne contient pas d'idéaux de norme 2, 3 ou 7.)*

Exercice 18.

Soient K le corps de nombres $\mathbb{Q}(\alpha)$, où $\alpha = \sqrt[3]{2}$, $A := \mathbb{Z}[\alpha]$ et $I = (2, \alpha)$.

(1) Montrer que A est de discriminant $-3^3 2^2$. En déduire que $\mathcal{O}_K = A$.

(2) Montrer que tout idéal de $\mathcal{O}_K$ est soit principal, soit équivalent à I ou à I^2.

(3) Montrer que I est principal et conclure que $\mathcal{O}_K$ est lui-même principal.

Exercice 19.

(1) Montrer que $\mathcal{O}_K$ est principal lorsque $K = \mathbb{Q}(\sqrt{d})$ et $d \in \{-19, -43, -67, -163\}$.

(2) Montrer que $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$ lorsque $K = \mathbb{Q}(\sqrt{-5})$.

(3) Montrer que $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/4\mathbb{Z}$ lorsque $K = \mathbb{Q}(\sqrt{-14})$.

Exercice 20.

Nous allons montrer que $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ lorsque $K = \mathbb{Q}(\sqrt{-30})$.

(1) Montrer qu'il y a des idéaux premiers $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$ contenant respectivement $2, 3$ et 5, et induisant une famille de classes d'idéaux génératrice.

(2) Montrer que $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = 1$ et que $[\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5] = 1$.

(3,a) Montrer que $\mathcal{O}_K^\times = \{\pm 1\}$.

(3,b) Montrer que $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$, et que $[\mathfrak{p}_2], [\mathfrak{p}_3] \neq 1$.

Exercice 21.

Soit K un corps de nombres de degré n. On dit que p y est **totalement ramifié** si $p\mathcal{O}_K = \mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier.

(1) On suppose que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et que le polynôme minimal de α soit p–Eisenstein. Montrer que p est totalement ramifié.

(1bis) Faire (1) avec l'hypothèse $K = \mathbb{Q}(\alpha)$.

(2) Supposons que p soit totalement ramifié.

(2,a) Montrer qu'il existe $\beta \in \mathfrak{p}\backslash\mathfrak{p}^2$.

(2,b) Montrer que $\beta\mathcal{O}_K = \mathfrak{p}\mathfrak{b}$, où $\mathfrak{b}$ est un idéal tel que $\mathfrak{b} + \mathfrak{p} = \mathcal{O}_K$.

(2,c) Soit $P(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0$ le polynôme caractéristique de β. Montrer que p divise b_0 et que p^2 ne divise pas b_0.

(2,d) Montrer par récurrence que p divise b_i, pour tout $i < n$.

(2,e) Conclure.

Exercice 22.

(1) Montrer que $\mathcal{O}_K = \mathbb{Z}[2^{1/m}]$, où $K = \mathbb{Q}(2^{1/m})$ et $m = 4$ ou 5.

(1bis) Trouver des informations sur $\mathrm{Cl}(\mathcal{O}_K)$.

Exercice 23. (Points entiers d'une famille de courbes elliptiques)

Soit d un entier > 0 sans facteur carré tel que $-d = 2, 3 \bmod 4$, et tel que $3 \nmid |\mathrm{Cl}(\mathcal{O}_K)|$, où $K = \mathbb{Q}(\sqrt{-d})$. Nous allons montrer que l'équation suivante a au plus deux solutions entières

$$y^2 = x^3 - d$$

(1) Supposons qu'une telle solution (x, y) existe.

(1,a) Montrer que x, y, d sont deux à deux premiers entre eux.

(1,b) Soient $\mathfrak{a}, \overline{\mathfrak{a}}$ les idéaux de $\mathcal{O}_K$ définis par

$$\mathfrak{a} = (y + \sqrt{-d})\mathcal{O}_K \qquad \overline{\mathfrak{a}} = (y - \sqrt{-d})\mathcal{O}_K$$

Montrer que $2 \in \mathfrak{a}+\overline{\mathfrak{a}}$. Après avoir décomposé $2\mathcal{O}_K$ montrer que $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont premiers entre eux.

(1,c) En déduire que $\mathfrak{a}$ est le cube d'un idéal principal.

(2) Conclure sur le nombre de solutions de l'équation.

Exercice 24. (Équation de Pell)

Soit $d > 0$ un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. Étudions l'équation en inconnues entières

$$x^2 - dy^2 = \pm 4$$

dont l'ensemble des solutions est noté $\mathscr{E}(d)$.

(0) Résoudre le cas $d = 1$.

Supposons que $d > 1$.

(1) Montrer que l'application $\mathcal{O}_K^\times \longrightarrow \mathbb{Z}^2$ définie par

$$n + m\sqrt{d} \mapsto (2n, 2m) \quad \text{si } d = 2, 3 \bmod 4$$

$$n + m\frac{1+\sqrt{d}}{2} \mapsto (2n + m, m) \quad \text{si } d = 1 \bmod 4$$

induit une bijection $\varphi : \mathcal{O}_K^\times \longrightarrow \mathscr{E}(d)$. En déduire que $\mathscr{E}(d)$ est infini.

(2) Montrer que φ^{-1} induit une bijection de $\mathscr{E}(d) \cap \mathbb{N} \times \mathbb{N}$ dans $\mathcal{O}_K^\times \cap [1, +\infty[$. Montrer que si x_1, x_2, y_1, y_2 sont $\geqslant 0$ et forment deux couples de solutions de l'équation telles que $y_1 < y_2$ alors

$$\varphi^{-1}(x_1, y_1) < \varphi^{-1}(x_2, y_2)$$

(3) Soit $u \in \mathcal{O}_K^\times$ tel que $u > 1$ et tel qu'il soit de norme minimale parmi les mêmes u. Montrer que u est une unité fondamentale de K. En déduire des unités fondamentales de $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt{10})$.

Exercice 25.

Montrer que $\mathbb{Q}(\zeta_3), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_7)$ ont des anneaux d'entiers principaux.

Problème I. (Théorème de Gross-Rohrlich)

Soient $p \neq 2$ un nombre premier et $K_p := \mathbb{Q}(\sqrt{1-2^{p+2}})$. Le théorème de Gross-Rohrlich affirme que $|\mathrm{Cl}(\mathcal{O}_{K_p})|$ est divisible par p. Montrons-le en supposant que $1-2^{p+2}$ est sans facteur carré.

(1) Trouver $x \in \mathcal{O}_{K_p}$ tel que $x\mathcal{O}_{K_p} + \overline{x}\mathcal{O}_{K_p} = \mathcal{O}_{K_p}$ et $2^p = |x|^2$.

(2) En déduire que p divise $|\mathrm{Cl}(\mathcal{O}_{K_p})|$.

(4) Calculer $|\mathrm{Cl}(\mathcal{O}_L)|$ pour $L = \mathbb{Q}(\sqrt{-31}), \mathbb{Q}(\sqrt{-127}), \mathbb{Q}(\sqrt{-511})$.

Problème II. (Unités de corps cubiques)

Soit $K \subset \mathbb{R}$ un corps de nombres de degré 3 avec un discriminant $\Delta < 0$, c'est-à-dire ayant un seul plongement réel.

(1) Montrer que $\mathcal{O}_K^\times = \{\pm u^n, n \in \mathbb{Z}\}$, où $u > 1$.

(2) Montrer que $u = t^2$, où $t^{-1}\exp(\pm i\theta)$ sont les deux autres conjugués de u.

(3) Soit Δ' le discriminant de $\mathbb{Z}[u]$. Montrer que si $\xi := \frac{t^3+t^{-3}}{2}$ alors

$$\sqrt{|\Delta'|} = 4(\xi - \cos\theta)\sin\theta$$

(4) Montrer que

$$4(\xi - \cos\theta)\sin\theta \leqslant 4(\xi - \cos\theta_0)\sin\theta_0$$

où θ_0 est défini par les relations $x_0 = \cos\theta_0$, $-1 < x_0 < -\frac{1}{2t^3}$ et

$$\xi x_0 - 2x_0^2 + 1 = 0$$

(5) En déduire que $|\Delta'| \leqslant 16(\xi^2 + 1 - x_0^2 - x_0^4)$ et que

$$|\Delta_K| < 4u^3 + 24$$

(6) Soit $K = \mathbb{Q}(\sqrt[3]{2})$. Montrer que $u > \sqrt[3]{21}$. En déduire que

$$u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

Problème III. (Formule du nombre de classes)

L'objectif est de calculer $h_K := |\mathrm{Cl}(\mathcal{O}_K)|$, où $K = \mathbb{Q}(\sqrt{-d})$ et $d > 0$ est un entier sans facteur carré. Richard Dedekind en a proposé une formule en 1830.

La fonction zêta de Dedekind ζ_K est définie par la série

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

où a_n est le nombre d'idéaux de $\mathcal{O}_K$ de norme n. On a deux autres expressions

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} (1 - N(\mathfrak{p})^{-s})^{-1}$$

où $\mathfrak{a}$ parcourt les idéaux de $\mathcal{O}_K$ et $\mathfrak{p}$ les idéaux premiers. Soient $a \in \mathbb{Z}$ et p est un nombre premier. Si a est un carré $\neq 0$ modulo p alors on pose

$$\left(\frac{a}{p}\right) = 1$$

et si ce n'est pas un carré

$$\left(\frac{a}{p}\right) = -1$$

et enfin $\left(\frac{a}{p}\right) = 0$ si $a|p$. On l'appelle symbole de Legendre de a modulo p.

On aura besoin du lemme suivant

Lemme 1. *Soient $A, C > 0$ et B des entiers tels que $D = B^2 - 4AC < 0$. Alors le nombre $\lambda(T)$ de vecteurs $(x, y) \in \mathbb{Z}^2$ tels que*

$$Ax^2 + Bxy + Cy^2 \leqslant T$$

vérifie quand $T \to \infty$

$$\lambda(T) = \frac{2\pi T}{\sqrt{-D}} + O(\sqrt{T})$$

(1) On note Δ le discriminant de K, i.e. $\Delta = d$ si $d = 3$ modulo 4 et $\Delta = 4d$ si $d = 1, 2$ modulo 4. Calculer $N(\mathfrak{p})$ en fonction de $\left(\frac{\Delta}{p}\right)$, où $\mathfrak{p}$ est un idéal premier divisant $p\mathcal{O}_K$.

(2) En déduire une factorisation de ζ_K par $\zeta_{\mathbb{Q}}$ la fonction zêta de Riemann.

(3) Exprimer le quotient $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$ sous la forme

$$L(s, \chi_\Delta) := \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s}$$

où la fonction $\chi_\Delta : \mathbb{N} \longrightarrow \mathbb{C}$ est multiplicative, c'est-à-dire $\chi_\Delta(nm) = \chi_\Delta(n)\chi_\Delta(m)$.

(4) Soit $F(T)$ le nombre d'idéaux de $\mathcal{O}_K$ de norme $\leqslant T$. On va montrer que

$$F(T) = \frac{2\pi h_K}{\omega_K \sqrt{-\Delta}} T + O(\sqrt{T})$$

où ω_K est le nombre de racines de l'unité dans K.

(4,a) Soit $\mathfrak{b}$ un idéal de $\mathcal{O}_K$. Estimer le nombre d'idéaux principaux inclus dans $\mathfrak{b}$ de norme $\leqslant T$ quand $T \to \infty$.

(4,b) En déduire l'estimation pour $F(T)$ quand $T \to \infty$.

(5) À partir de $a_n = F(n) - F(n-1)$, donner une expression de $L(s, \chi_\Delta)$ au voisinage de $s = 1$. En déduire que $L(1, \chi_\Delta)$ converge et que

$$L(1, \chi_\Delta) = \frac{2\pi h_K}{\omega_K \sqrt{-\Delta}}$$

(6) Retrouver deux expressions de π sous forme de somme infinie à partir des valeurs de $L(1, \chi_\Delta)$ pour $d = 1, 3$.

(7) On peut calculer h_K avec la formule qui découle de l'étude de $L(s, \chi_\Delta)$: si $\Delta \neq -3, -4$ alors

$$h_K = \frac{1}{2 - \chi_\Delta(2)} \left| \sum_{2 \leqslant 2k < |\Delta|} \chi_\Delta(k) \right|$$

Retrouver ainsi les nombres de classes des corps quadratiques imaginaires que vous chérissez.