Géométrie des nombres et théorème des classes

Exercice 1 Soit p un nombre premier congru à 1 modulo 4. On rappelle que, dans ce cas, il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv 1 \mod p$.

1) On pose :
$$L := \{(a,b) \in \mathbb{Z}^2 : a \equiv ub \mod p\}.$$
Montrer que L intersecte le disque ouvert de centre 0 et de rayon $\sqrt{2p}$ ailleurs qu'en 0.
2) Conclure qu'il existe $(a,b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.

Exercice 2 Soit n un entier naturel. On cherche à montrer que n est somme de quatre carrés.

1) Expliquer pourquoi on peut supposer que n est sans facteurs carrés. On fera cette hypothèse dans toute la suite de l'exercice.
2) Montrer qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \mod n$.
3) On pose :
$$L := \{(a,b,c,d) \in \mathbb{Z}^4 : c \equiv au + bv \mod n, d \equiv av - bu \mod n\}.$$
Montrer que L intersecte la boule ouverte de centre 0 et de rayon $\sqrt{2n}$ dans $\mathbb{R}^4$ ailleurs qu'en 0.
4) Conclure.

Exercice 3 Soit $K = \mathbb{Q}(\sqrt{-5})$.

1) Montrer que $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$.
2) Trouver toutes les solutions entières de l'équation $x^2 + 5 = y^3$.

Exercice 4 Soit K un corps de nombres.

1) Soit I un idéal non nul de $\mathcal{O}_K$. Soient $m \geqslant 1$ et $a \in \mathcal{O}_K$ tels que $I^m = (a)$. En posant $L := K(\sqrt[m]{a})$, montrer que l'idéal $I\mathcal{O}_L$ est principal.
2) Montrer qu'il existe une extension finie L de K telle que, pour tout idéal I de $\mathcal{O}_K$, l'idéal $I\mathcal{O}_L$ de $\mathcal{O}_L$ est principal.

Exercice 5 Soit p un nombre premier tel que $p \equiv -1 \mod 12$. On pose $K := \mathbb{Q}(\sqrt{p})$.

1) Montrer qu'il existe deux idéaux premiers distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de $\mathcal{O}_K$ tels que :
$$3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2.$$
2) Montrer que l'ordre de $\mathfrak{p}_1$ dans Cl_K est au moins $\lfloor \log_3(p) \rfloor$.

Exercice 6 Montrer que l'anneau des entiers de $K := \mathbb{Q}(\sqrt{-19})$ est principal.

Exercice 7 L'anneau des entiers de $K := \mathbb{Q}(\sqrt{14})$ est-il principal ?

Exercice 8 Soit $z \in \mathbb{C}$ une racine de $P(T) := T^5 - T + 1$. L'anneau des entiers de $K := \mathbb{Q}(z)$ est-il principal ?

Exercice 9

1) Soient r et s deux entiers naturels. Soit $t > 0$. On pose :

$$X_t := \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |x_1| + \cdots + |x_r| + 2|z_1| + \cdots + 2|z_s| < t\}.$$

Montrer que X_t est une partie convexe centralement symétrique de $\mathbb{R}^r \times \mathbb{C}^s$ et calculer son volume.

2) Soit K un corps de nombres de degré n. Soit s le nombre de plongements complexes non réels de K à conjugaison près. Montrer que toute classe $c \in \mathrm{Cl}_K$ admet un représentant I qui est un idéal de $\mathscr{O}_K$ avec :

$$[\mathscr{O}_K : I] \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

3) a) Montrer que $|\Delta_K| > 1$ pour tout corps de nombres $K \neq \mathbb{Q}$.

b) Montrer que $|\Delta_K|$ tend vers l'infini lorsque K décrit des corps de nombres dont le degré tend vers l'infini.

4) Dans cette question, il est utile de connaître un peu de théorie de Galois. Soit $\Delta > 0$.

a) Montrer qu'il existe une constante $C_0(\Delta) > 0$ telle que, pour tout corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$, on a $|\Delta_{K(i)}| < C_0(\Delta)$.

b) Montrer qu'il existe une constante $C_1(\Delta) > 0$ telle que, pour tout corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$, il existe un plongement $\tau_0 : K(i) \to \mathbb{C}$ et un élément $x \in \mathscr{O}_{K(i)}$ vérifiant les propriétés suivantes :

$$|\mathrm{Im}(\tau_0(x))| < C(\Delta), \quad |\mathrm{Re}(\tau_0(x))| < 1, \quad \forall \tau \in \mathrm{Hom}_{\mathbb{Q}}(K(i), \mathbb{C}) \smallsetminus \{\tau_0, \overline{\tau}_0\},\ |\tau(x)| < 1.$$

c) Dans le contexte de la question précédente, montrer que $K(i) = \mathbb{Q}(x)$.

d) En déduire qu'il existe un nombre fini de corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$. Ce résultat s'appelle le **théorème d'Hermite**.

Exercice 10 Soit K un corps de nombres de degré n. Soient $r = |\Sigma_{\mathbb{R}}|$ et $s = |\Sigma_{\mathbb{C}}|$, de sorte que $n = r + 2s$. On cherche à comprendre le groupe $\mathscr{O}_K^\times$.

1) Justifier que $\mathscr{O}_K^\times = \{z \in \mathscr{O}_K : N_{K/\mathbb{Q}}(z) = \pm 1\}$.

2) On considère le morphisme :

$$\begin{aligned}\lambda : K^\times &\to \mathbb{R}^{\Sigma_\mathbb{R}} \times \mathbb{R}^{\Sigma_\mathbb{C}} \\ z &\mapsto ((\log|\sigma(z)|)_{\sigma\in\Sigma_\mathbb{R}}, (2\log|\sigma(z)|)_{\sigma\in\Sigma_\mathbb{C}}).\end{aligned}$$

Vérifier que l'image de λ est contenue dans :

$$V := \{(x_\sigma)_{\sigma\in\Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}} \in \mathbb{R}^{\Sigma_\mathbb{R}} \times \mathbb{R}^{\Sigma_\mathbb{C}} : \sum_{\sigma\in\Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}} x_\sigma = 0\}$$

et que $\mathrm{Ker}(\lambda)$ est un groupe fini égal au groupe $\mu(K)$ des racines de l'unité dans K.

3) On pose $\Gamma := \lambda(\mathscr{O}_K^\times)$. Montrer que Γ est un sous-réseau dans V. En déduire que $\mathscr{O}_K^\times$ est un groupe abélien de type fini.

4) a) Construire une famille de constantes $(c_\sigma)_{\sigma\in\Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}} \in \mathbb{R}_{>0}^{\Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}}$ de sorte que l'ensemble $X := \{(x_\sigma)_{\sigma\in\Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}} \in \mathbb{R}^{\Sigma_\mathbb{R}} \times \mathbb{R}^{\Sigma_\mathbb{C}} : \forall\sigma \in \Sigma_\mathbb{R}\cup\Sigma_\mathbb{C}, |x_\sigma| < c_\sigma\}$ vérifie la propriété suivante : pour tout $z \in K$ tel que $N_{K/\mathbb{Q}}(z) = \pm 1$, il existe $a_z \in \mathscr{O}_K$ non nul tel que $\lambda(a_z) \in X + \lambda(z)$.

b) Montrer que, pour toute constante $C > 0$, il existe une partie finie $\Theta(C) \subset \mathscr{O}_K \smallsetminus \{0\}$ telle que tout élément non nul de $\mathscr{O}_K$ de norme au plus C est associé à un élément de $\Theta(C)$.

c) A l'aide des deux questions précédentes, construire une partie finie $\Theta \subset \mathscr{O}_K \smallsetminus \{0\}$ telle que :

$$V = \bigcup_{\gamma\in\Gamma} (\gamma + T)$$

avec $T := V \cap \bigcup_{\theta\in\Theta}(X - \lambda(\theta))$.

d) Conclure que Γ est un réseau de V.

5) A l'aide des questions précédentes, montrer que $\mathscr{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$.