Anneaux d'entiers et anneaux de Dedekind

1 Entiers algébriques at anneaux d'entiers

Exercice 1 Parmi les nombres suivants, lesquels sont des entiers algébriques ?

$$\frac{8+2\sqrt{13}}{1+\sqrt{13}}, \quad \frac{6+3\sqrt{7}}{5+\sqrt{7}}, \quad \sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}, \quad \frac{-23+2\sqrt[3]{6}-2\sqrt[3]{36}}{1+2\sqrt[3]{6}}, \quad \frac{1+\sqrt[3]{5}+\sqrt[3]{25}}{2}.$$

Exercice 2 Soit $z \in \mathbb{C}$ tel que $z^3 - z + 1 = 0$. Soit $K := \mathbb{Q}(z)$. Montrer que $\mathcal{O}_K = \mathbb{Z}[z]$.

Exercice 3 Soit $z \in \mathbb{C}$ tel que $z^3 - z - 4 = 0$. Soit $K := \mathbb{Q}(z)$. Montrer que $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}z \oplus \mathbb{Z}\frac{z+z^2}{2}$.

Exercice 4 Soient $m, n \in \mathbb{Z} \smallsetminus \{0,1\}$ des entiers distincts, sans facteur carré, et tels que $m \equiv n \equiv 1 \mod 4$. On se propose de montrer que, si $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, alors $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ avec $\alpha = \frac{1+\sqrt{n}}{2}$ et $\beta = \frac{1+\sqrt{m}}{2}$.

1) Montrer que $[K : \mathbb{Q}] = 4$ et déterminer l'ensemble des plongements de K dans $\mathbb{C}$.
2) Vérifier que $d(1, \alpha, \beta, \alpha\beta) = m^2 n^2$.
3) Montrer que :

$$\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\alpha\beta \subset \mathcal{O}_K \subset \frac{1}{4}\left(\mathbb{Z} \oplus \mathbb{Z}\sqrt{n} \oplus \mathbb{Z}\sqrt{m} \oplus \mathbb{Z}\sqrt{mn}\right).$$

   On pourra utiliser les traces sur $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ et $\mathbb{Q}(\sqrt{mn})$.
4) Conclure que $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.
5) Écrire la factorisation de l'idéal $2\mathcal{O}_K$ dans $\mathcal{O}_K$. Quels sont les indices de ramification et les degrés résiduels des idéaux premiers de $\mathcal{O}_K$ qui sont au-dessus de 2 ?
6) Déduire qu'il n'existe pas d'élément $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$.

Exercice 5 Soient $n \geqslant 3$ et $a, b \in \mathbb{Q}$ tels que $P := X^n + aX + b$ est irréductible dans $\mathbb{Q}[X]$. Soient $z \in \mathbb{C}$ une racine de P et $K = \mathbb{Q}(z)$. Calculer $d(1, z, z^2, \ldots, z^{n-1})$.

Exercice 6 Soit K un corps de nombres de degré n, et soit $u \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(u)$. Soit p un nombre premier tel que le polynôme minimal de u sur $\mathbb{Q}$ soit d'Eisenstein en p. L'objectif de l'exercice est de montrer que p ne divise pas l'indice de $\mathbb{Z}[u]$ dans $\mathcal{O}_K$.

1) Montrer que $\frac{u^n}{p} \in \mathcal{O}_K$ et que p^2 ne divise pas $N_{K/\mathbb{Q}}(u)$.
2) Supposons que $p | [\mathcal{O}_K : \mathbb{Z}[u]]$.

a) Montrer qu'il existe $x \in \mathcal{O}_K \smallsetminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. En déduire qu'il existe $b_0, ..., b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0 + ... + b_{n-1}u^{n-1}}{p}$.

b) Notons r le plus petit entier tel que b_r n'est pas divisible par p. Montrer que $y = \frac{b_r u^r + ... + b_{n-1}u^{n-1}}{p}$ est dans $\mathcal{O}_K$.

c) Montrer que $z = \frac{b_r u^{n-1}}{p} \in \mathcal{O}_K$.

d) Obtenir une contradiction en calculant la norme de z.

3) Soit q est une puissance de p.

a) Montrer que, si $K = \mathbb{Q}(\sqrt[q]{p})$, alors $\mathcal{O}_K = \mathbb{Z}[\sqrt[q]{p}]$.

b) Soit ζ une racine primitive q-ième de l'unité. Montrer que, si $K = \mathbb{Q}(\zeta)$, alors $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

4) Montrer que, si $K = \mathbb{Q}(\sqrt[3]{2})$, alors $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

Exercice 7 Soient p un nombre premier et $k \geqslant 1$ un entier. Soit $\zeta \in \mathbb{C}$ une racine primitive p^k-ème de l'unité. Soit $\mathcal{O}_{p^k}$ l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$. Nous allons établir par une méthode différente de celle de l'exercice 6 que $\mathcal{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

1) On pose $\mathfrak{q} = (1-\zeta)\mathcal{O}_{p^k}$. Montrer que la factorisation de $p\mathcal{O}_{p^k}$ s'écrit $\mathfrak{q}^{\varphi(p^k)}$. Quel est le degré résiduel $f(\mathfrak{q}/\mathfrak{p})$?

2) En déduire que l'on a $\mathcal{O}_{p^k} = \mathbb{Z}[\zeta] + p^m\mathcal{O}_{p^k}$ pour tout $m \geqslant 0$.

3) Montrer que le discriminant de $(1, \zeta, \ldots, \zeta^{\varphi(p^k)-1})$ est, au signe près, une puissance de p (que l'on explicitera).

4) En déduire que l'anneau $\mathcal{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

Exercice 8 Soient K et L des extensions finies galoisiennes de $\mathbb{Q}$ de degrés respectifs m et n. On suppose que qu'elles sont linéairement disjointes. Soit $(x_1, \ldots, x_m)$ (resp. $(y_1, \ldots, y_n)$) une base entière de $\mathcal{O}_K$ (resp. $\mathcal{O}_L$). On suppose que $\Delta_K \wedge \Delta_L = 1$.

1. Montrer que $\Delta_K\mathcal{O}_{KL} \subset \bigoplus_{i=1}^m \bigoplus_{j=1}^n \mathbb{Z}x_i y_j$.
2. Montrer que $\mathcal{O}_{KL} = \bigoplus_{i=1}^m \bigoplus_{j=1}^m \mathbb{Z}x_i y_j$.
3. Calculer $d((x_i y_j)_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n})$.
4. Soient $n \geqslant 3$ un entier et $\zeta \in \mathbb{C}$ une racine primitive n-ième de l'unité. Calculer l'anneau des entiers de $\mathbb{Q}(\zeta)$. On pourra pour cela utiliser le résultat de l'exercice 6 ou de l'exercice 7.

Exercice 9 Soit $d \in \mathbb{Z}$, $d > 1$ sans facteur cubique. Notons $\theta = \sqrt[3]{d}$ et $K = \mathbb{Q}(\theta)$. On cherche à déterminer l'anneau des entiers $\mathcal{O}_K$ de K.

1) Montrer que la base $(1, \theta, \theta^2)$ est de discriminant $\Delta = -27d^2$.

2) On écrit $d = ab^2$, avec $a, b \in \mathbb{N}$ sans facteur carré. On pose $\theta' = \sqrt[3]{a^2 b}$. Montrer que $K = \mathbb{Q}(\theta')$ et calculer le discriminant Δ' de la base $(1, \theta', \theta'^2)$.

3) Montrer que $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K et calculer son discriminant Δ''.

4) On note f, f' et f'' les indices respectifs de $\mathbb{Z}[\theta]$, $\mathbb{Z}[\theta']$ et $\mathbb{Z}\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\theta'$ dans $\mathcal{O}_K$.
   a) Montrer que $f^2=\frac{\Delta}{\Delta_K}$, $f'^2=\frac{\Delta'}{\Delta_K}$ et $f''^2=\frac{\Delta''}{\Delta_K}$.
   b) Montrer que $a\wedge f=1$ et que $b\wedge f'=1$.
   c) En déduire les assertions suivantes :
      i) $\Delta_K<0$;
      (ii) $a^2b^2|\Delta_K|27a^2b^2$;
      (iii) si $3|a$, alors $27a^2|\Delta_K$;
      (iv) si $3|b$, alors $27b^2|\Delta_K$.
5) Montrer que si $3|d$, alors $\Delta_K=-27a^2b^2$ et $\mathcal{O}_K=\mathbb{Z}\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\theta'$.
6) Supposons que 3 ne divise pas d et que $d\pm1$ n'est pas multiple de 9. Montrer que le polynôme minimal de $\theta-d$ est 3-Eisenstein. En procédant comme dans les questions précédentes, en déduire que $\Delta_K=-27a^2b^2$ et $\mathcal{O}_K=\mathbb{Z}\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\theta'$.
7) On suppose $d\equiv 1 \mod 9$. On pose $\alpha=\frac{1+\theta+\theta^2}{3}$.
      i) Montrer que $\alpha\in\mathcal{O}_K$ et calculer son polynôme minimal.
      ii) En déduire que $3|f''$, puis que $\Delta_K=-3a^2b^2$.
      iii) Montrer que $\mathcal{O}_K=\mathbb{Z}\alpha\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\theta'$.
8) Supposons $d\equiv -1 \mod 9$. On pose $\alpha'=\frac{1-\theta+\theta^2}{3}$. Montrer que $\mathcal{O}_K=\mathbb{Z}\alpha'\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\theta'$.

Exercice 10 Pour $n\in\mathbb{N}$, on note $\mathbb{Q}_n[X]$ le $\mathbb{Q}$-espace vectoriel des polynômes de degré strictement plus petit que n. On appellera base canonique de $\mathbb{Q}_n[X]$ la base $(X^{n-1},X^{n-2},...,1)$. Pour $(P,Q)\in\mathbb{Q}[X]\times\mathbb{Q}[X]$ avec $\deg P=n$ et $\deg Q=m$, on note $\mathrm{Res}(P,Q)$ le déterminant dans les bases canoniques de l'application $\mathbb{Q}$-linéaire $\mathbb{Q}_m[X]\times\mathbb{Q}_n[X]\to\mathbb{Q}_{m+n}[X]$ qui envoie (U,V) sur $PU+QV$.

1) Écrire $\mathrm{Res}(P,Q)$ comme déterminant d'une matrice.
2) Comparer $\mathrm{Res}(P,Q)$ et $\mathrm{Res}(Q,P)$.
3) On suppose que P est un polynôme unitaire.
   a) Montrer que $\mathrm{Res}(P,Q)$ est égal au déterminant de la multiplication par Q sur l'anneau $A[X]/(P)$ dans la base $(X^{n-1},X^{n-2},...,1)$.
   b) Considérons $Q_1\in A[X]$ et $Q_2\in A[X]$ de degrés respectifs m_1 et m_2. Calculer $\mathrm{Res}(P,Q_1Q_2)$ en fonction de $\mathrm{Res}(P,Q_1)$ et $\mathrm{Res}(P,Q_2)$.
   c) Exprimer $\mathrm{Res}(P,(X-\lambda_1)...(X-\lambda_m))$ en fonction de $P(\lambda_1)...P(\lambda_m)$.
   d) Soit x un nombre algébrique de degré n. On pose $K=\mathbb{Q}(x)$. Exprimer $d(1,x,x^2,\dots,x^{n-1})$ en fonction des coefficients du polynôme minimal μ_x de x.

Exercice 11 Soit K un corps de nombres. Soit Δ_K son discriminant. Les deux questions suivantes sont indépendantes.

1) Montrer le signe de Δ_K est $(-1)^s$ où s est le nombre d'éléments dans $\Sigma_{\mathbb{C}}$ (c'est-à-dire la moitié du nombre de plongements de K dans $\mathbb{C}$ dont l'image n'est pas contenue dans $\mathbb{R}$).
2) Montrer que Δ_K est congru à 0 ou 1 modulo 4.

2 Anneaux de Dedekind et ramification

Exercice 12 Soit A un anneau de Dedekind. Montrer que pour tous idéaux fractionnaires I, J, on a $I \cap J = I \cdot J \cdot (I+J)^{-1}$.

Exercice 13 Montrer qu'un anneau de Dedekind est principal si et seulement il est factoriel.

Exercice 14 Montrer qu'un anneau de Dedekind qui a un nombre fini d'idéaux premiers est principal.

Exercice 15 Soient A un anneau de Dedekind et I un idéal non nul. Montrer que tout idéal de A/I est principal. En déduire que tout idéal de A est engendré par deux éléments.

Exercice 16 Soient A un anneau de Dedekind de corps des fractions K et I un idéal non nul de A. Montrer qu'il existe $a \in K^\times$ tel que aI est un idéal de A premier avec I.

Exercice 17 Soient A un anneau intègre qui n'est pas un corps. Montrer que les assertions suivantes sont équivalentes :

(i) A est un anneau de Dedekind.
(ii) Tout idéal non nul de A admet une factorisation unique en produit d'idéaux premiers
(iii) A est noethérien et pour tout idéal maximal $\mathfrak{m}$ de A le localisé $A_\mathfrak{m}$ est un anneau principal.
(iv) Tout idéal fractionnaire non nul de A est inversible.
(v) Pour I et J idéaux de A, on a $I \subset J$ si, et seulement si, J divise I.

Exercice 18 Soit A un anneau de Dedekind, K son corps des fractions et $\mathfrak{p}$ un idéal premier de A.

1. Soit $x \in \mathfrak{p}$. Montrer qu'il existe $y \notin xA$ tel que $y\mathfrak{p} \subseteq xA$.
2. Montrer qu'avec ces conditions on a $\mathfrak{p}^{-1} = A + (\frac{y}{x})A$.
3. Soit I un idéal entier et $k \geqslant 0$. Montrer que $I \subseteq \mathfrak{p}^k$ si et seulement si $\left(\frac{y}{x}\right)^k I \subseteq A$.
4. Soit $\alpha = \sqrt[3]{5}$. Justifier que $\mathbb{Z}[\alpha]$ est de Dedekind. Calculer l'inverse de l'idéal $(3, 1+\alpha)$.

Exercice 19 Prenons $K_1 = \mathbb{Q}(\sqrt{5})$ et $K_2 = \mathbb{Q}(\sqrt{5})$.

1) Quels nombres premiers ramifient dans K_1 et dans K_2 ?
2) Selon la valeur du nombre premier p, écrire la factorisation des idéaux $p\mathcal{O}_{K_1}$ et $p\mathcal{O}_{K_2}$. On pourra utiliser la loi de réciprocité quadratique.

Prenons maintenant $d \in \mathbb{Z} \smallsetminus \{0,1\}$ sans facteurs carrés et posons $K = \mathbb{Q}(\sqrt{d})$. Soit S l'ensemble des diviseurs premiers de Δ_K.

3) Décrire D en fonction de d.
4) Montrer qu'il

Exercice 20 On prend $K = \mathbb{Q}(\sqrt[3]{2})$. Soit p un nombre premier. Quelles sont les factorisations possibles de l'idéal $p\mathcal{O}_K$? Donner un exemple concret pour chaque possibilité.

Exercice 21 Soient $n \geqslant 3$, p un nombre premier et $K = \mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité. Comment se factorise l'idéal $p\mathcal{O}_K$? On pourra faire apparaître l'ordre f_p de la classe de p modulo $\frac{n}{p^{v_p(n)}}$.

Exercice 22 On va montrer que $\mathbb{Z}[\zeta_{23}]$ n'est pas principal. On note dans la suite $\zeta = \exp(2i\pi/23)$ et $K = \mathbb{Q}(\zeta)$.

1. Remarquer que $2^{23} - 1$ est divisible par 47 mais pas par 47^2, et calculer $N_{K/\mathbb{Q}}(\zeta - 2)$.
2. On note $I = 47\mathcal{O}_K + (\zeta - 2)\mathcal{O}_K$. Montrer que pour tout $\alpha \in I$, on a $47 \mid N_{K/\mathbb{Q}}(\alpha)$.
3. On suppose désormais que $I = (\alpha)$ est principal. Montrer que la norme de α divise 47^{22} et $N_{K/\mathbb{Q}}(\zeta - 2)$. Calculer $N_{K/\mathbb{Q}}(\alpha)$.
4. Montrer que K contient un unique corps quadratique F, et qu'il s'agit de $\mathbb{Q}(\sqrt{-23})$. Montrer que F est le seul sous-corps quadratique de K.
5. Montrer que $N_{K/F}(\alpha)$ est un entier algébrique de norme 47 et en déduire que I n'est pas principal.

Exercice 23 Soient $n \geqslant 3$, p un nombre premier et $K = \mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité.

1. Comment se factorise l'idéal $p\mathcal{O}_K$? On pourra faire apparaître l'ordre f_p de la classe de p modulo $\frac{n}{p^{v_p(n)}}$.

On suppose désormais que p est impair et que $n = \ell$ est un autre premier impair.

2) Justifier que $\sqrt{(-1)^{\frac{\ell-1}{2}}\ell} \in \mathbb{Q}(\zeta_\ell)$. On pourra pour cela utiliser le discriminant $\Delta_{\mathbb{Q}(\zeta_\ell)}$.
3) On suppose que p est totalement décomposé dans $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$. Montrer que $g_{\mathbb{Q}(\zeta_\ell)}(p)$ est pair.
4) Réciproquement, on suppose que $g_{\mathbb{Q}(\zeta_\ell)}(p)$ est pair.
   (a) Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbb{Q}(\zeta_\ell)}$ au-dessus de p. Montrer que le corps de décomposition de $\mathfrak{p}$ contient $\sqrt{(-1)^{\frac{\ell-1}{2}}\ell}$.
   (b) En déduire que p est totalement décomposé dans $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$.
5) Déduire la loi de réciprocité quadratique des questions précédentes : $(-1)^{\frac{\ell-1}{2}}\ell$ est un carré modulo p si, et seulement si, p est un carré modulo ℓ.

Exercice 24 Soit L/K une extension de corps de nombres. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$ et soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$.

1. A l'aide du lemme de Nakayama, montrer qu'il existe $\alpha_\mathfrak{q} \in \mathcal{O}_L$ tel que $\mathcal{O}_{L,\mathfrak{q}} = \mathcal{O}_{K,\mathfrak{p}}[\alpha_\mathfrak{q} + \beta]$ pour tout $\beta \in \mathcal{O}_L$ tel que $v_\mathfrak{q}(\beta) \geqslant 2$.
2. Montrer qu'il une élément primitif α de L/K tel que $\mathfrak{p}\mathcal{O}_L$ et le conducteur $\mathfrak{f}(\mathcal{O}_L/\mathcal{O}_K[\alpha])$ sont premiers entre eux.
3. Soit maintenant L' une extension finie de K. On suppose que $\mathfrak{p}$ est totalement décomposé dans L et dans L'. Montrer que $\mathfrak{p}$ est totalement décomposé dans LL'.
4. Montrer que $\mathfrak{p}$ est totalement décomposé dans L si, et seulement si, il l'est dans la clôture galoisienne de L.

Exercice 25 Soit L/K une extension galoisienne non cyclique de corps de nombres. Montrer qu'il existe un nombre fini d'idéaux de $\mathcal{O}_K$ qui ne sont pas décomposés dans L.

Exercice 26 Soit K un corps de nombres. Soit $(x_1, \ldots, x_n)$ une base entière de $\mathcal{O}_K$. On définit :

$$I := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}.$$

1) a) Montrer qu'il existe une base $(x_1^*, \ldots, x_n^*)$ de K telle que, pour $1 \leqslant i, j \leqslant n$:

$$\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j^*) = \delta_{ij}.$$

b) Montrer que $I = \bigoplus_{i=1}^n \mathbb{Z} x_i^*$.

c) Déduire que I est un idéal fractionnaire.

2) Soit $\mathcal{D} := I^{-1}$. On dit que $\mathcal{D}$ est la *différente* de K. Montrer que $\mathcal{D}$ est un idéal de $\mathcal{O}_K$.

3) a) Soit $B = (b_{ij})_{1 \leqslant i,j \leqslant n}$ la matrice de passage de la base $(x_1^*, \ldots, x_n^*)$ vers la base $(x_1, \ldots, x_n)$. Montrer que $\det(B)$ est le discriminant Δ_K de K.

b) Déduire que $[\mathcal{O}_K : \mathcal{D}] = |\Delta_K|$.

c) Soient p un nombre premier et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au-dessus de p. On suppose que $\mathfrak{p}$ ramifie dans l'extension $K/\mathbb{Q}$.

a) Montrer que $\frac{1}{p} \cdot \mathfrak{p}\mathfrak{a} \subset I$.

b) Déduire que $\mathfrak{p}^{e-1}$ divise $\mathcal{D}$.

c) Conclure que p divise Δ_K.

3 Géométrie des nombres et applications

Exercice 27 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 28 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 29

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 $\mathcal{O}_K$ avec :

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

Exercice 30 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 31 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 32 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 33 Montrer que l'anneau des entiers de $K := \mathbb{Q}(\sqrt{-19})$ est principal.

Exercice 34 L'anneau des entiers de $K := \mathbb{Q}(\sqrt{14})$ est-il principal ?

Exercice 35 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 36 On considère le corps $K = \mathbb{Q}(\sqrt{-43})$.

1. Montrer que $\mathcal{O}_K$ est principal.
2. Soit $\alpha \in \mathcal{O}_K \smallsetminus \mathbb{Z}$ qui engendre un idéal premier. Montrer que $N_{K/\mathbb{Q}}(\alpha)$ est un nombre premier.
3. Montrer que si $\alpha \in \mathcal{O}_K \smallsetminus \mathbb{Z}$ alors $N_{K/\mathbb{Q}}(\alpha) \geqslant 11$.
4. Soient x et $y \neq 0$ deux entiers premiers entre eux tels que $x^2 + xy + 11y^2 < 121$. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

Remarque : On en déduit en particulier que $x^2 + x + 11$ est un nombre premier pour x compris entre 0 et 9. Le même raisonnement avec $\mathbb{Q}(\sqrt{-163})$ montre que $x^2 + x + 41$ est premier pour x allant de 0 à 39.

Exercice 37 Soit $d > 1$ un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{-d})$. Soit p un nombre premier décomposé dans K, et $\mathfrak{p}$ un idéal au dessus de p.

1. Montrer que pour tout $i > 1$ tel que $p^i < \frac{|\Delta_K|}{4}$, $\mathfrak{p}^i$ n'est pas principal.
2. En déduire que $|\mathrm{Cl}_K| > 1 + \left\lfloor \frac{\log|\Delta_K|}{\log p} \right\rfloor$.

Exercice 38 Soit K un corps de nombres, et $m > 1$ un entier. On pose $\mathrm{Cl}_K[m] = \{a \in \mathrm{Cl}_K,\ a^m = 1\}$ le groupe de m-torsion.

1. Montrer que si $|\mathrm{Cl}_K|$ est premier à m, alors $\mathrm{Cl}_K[m] = \{1\}$. On définit $G_m(K) = \{x^m,\ x \in K^*\}$ et $L_m(K)$ l'ensemble des éléments $x \in K^*$ tels que dans la factorisation en idéaux premiers de (x) tous les exposants sont multiples de m. On pose $S_m(K) = L_m(K)/G_m(K)$.
2. Montrer qu'on a un morphisme de groupes $\phi\colon S_m(K) \to \mathrm{Cl}_K[m]$ défini par $\phi(x) = a_x$, où a_x est l'unique idéal fractionnaire tel que $a_x^m = (x)$.
3. Montrer que ϕ est surjectif et déterminer son noyau. On suppose désormais que $K = \mathbb{Q}(\sqrt{-d})$ est un corps quadratique imaginaire, avec $d > 0$ sans facteur carré.

4. Soit $x = a + b\sqrt{-d} \in K$ tel que $N_{K/\mathbb{Q}}(x) = 1$. Montrer qu'il existe $y \in K^*$ tel que $x = \frac{y}{\overline{y}}$, où $\overline{y}$ désigne le conjugué complexe de y (on pourra considérer l'application $\psi : K \to K$ définie par $\psi(y) = \overline{y} - xy$).
5. Soit $\mathfrak{a} \in \mathrm{Cl}_K[2]$, on pose $a = N_{K/\mathbb{Q}}(\mathfrak{a})$. Montrer qu'il existe $y \in K^*$ tel que $\mathfrak{a}^2 = \left(\frac{a\overline{y}}{y}\right)$.
6. On pose $\mathfrak{b} = y\mathfrak{a}$, montrer qu'il existe $b \in \mathbb{Q}^*$ tel que $\mathfrak{b}^2 = (b)$.
7. Montrer que $\mathfrak{a} \in \mathrm{Cl}_K[2]$ est dans la classe d'un produit d'idéaux ramifiés.
8. On note $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ les premiers ramifiés de K. Soit une famille $0 \leqslant e_i \leqslant 1$, montrer que si $\prod_{i=1}^t \mathfrak{p}_i^{e_i}$ est principal, ce produit vaut (1) ou $(\sqrt{d})$.
9. Montrer que $\mathrm{Cl}_K[2] \cong \mathbb{F}_2^{t-1}$.

Exercice 39 Donner des unités fondamentales pour $\mathbb{Q}(\sqrt{d})$ lorsque $d = 2, 3, 5, 6$.

Exercice 40 Soit $\omega = \sqrt[3]{2}$ et $K = \mathbb{Q}(\omega)$.

1. Montrer que le rang de $\mathcal{O}_K^\times$ est égal à 1 et que, si on note $N_1 \subset \mathcal{O}_K^\times$ le sous-groupe des unités de norme 1, le groupe N_1 est isomorphe à $\mathbb{Z}$ et $\mathcal{O}_K^\times = \{\pm 1\} \cdot N_1$.
2. Soit $\varepsilon = \omega - 1$, vérifier que ε est une unité et qu'elle engendre N_1.
3. Montrer que $\mathcal{O}_K = \mathbb{Z}[\omega]$ est principal.

Exercice 41 Soit K un corps de nombres cubique, tel que $\Delta_K < 0$.

1. Montrer qu'il y a un seul plongement de K dans $\mathbb{R}$. Désormais, on utilise ce plongement pour voir K comme un sous-corps de $\mathbb{R}$.
2. Montrer qu'il existe $\varepsilon > 1$ tel que $\mathcal{O}_K^\times = \{\pm\varepsilon^k, k \in \mathbb{Z}\}$.
3. Montrer que $K = \mathbb{Q}(\varepsilon)$, et que le polynôme minimal de ε est de la forme $g(x) = (x - \varepsilon)(x - \sqrt{\varepsilon^{-1}}e^{it})(x - \sqrt{\varepsilon^{-1}}e^{-it})$ pour $t \in \mathbb{R}$.
4. Montrer l'inégalité d'Artin : $\left|d(1, \varepsilon, \varepsilon^2)\right| < 4(\varepsilon^3 + 6)$ (utiliser sans preuve l'inégalité magique $\left(\frac{u^3+u^{-3}}{2} - \cos t\right)^2 \sin^2 t < \frac{u^6+6}{4}$, valable pour tous réels u, t).
5. Montrer que si $u > 1$ est une unité qui vérifie $4(u^{3/2} + 6) < |\Delta_K|$, alors $u = \varepsilon$.
6. Soit $K = \mathbb{Q}(\alpha)$ où $\alpha^3 + \alpha = 1$. Déterminer une unité fondamentale de K (on donne $\alpha \approx 0.6823$ dans $\mathbb{R}$).

Exercice 42 Soit $K = \mathbb{Q}(\alpha)$, où α est une racine de $x^3 + 6x + 6$.

1. Déterminer le discriminant Δ_K de K et son anneau d'entiers.
2. Montrer que Cl_K est engendré par 3 idéaux premiers $\mathfrak{p}_2$, $\mathfrak{p}_3$ et $\mathfrak{p}_7$ qui sont au-dessus de 2, 3 et 7 respectivement.
3. Calculer $N_{K/\mathbb{Q}}(\alpha)$ et $N_{K/\mathbb{Q}}(\alpha + 2)$ et en déduire que Cl_K est cyclique.
4. Montrer que $u = \alpha + 1$ est une unité fondamentale dans $\mathcal{O}_K^\times$ et en déduire que u est non triviale dans $\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^3$. On utilisera l'inégalité d'Artin avec une calculatrice : $\alpha \approx -0.884$.

5. Montrer que 2, $2u$ et $2u^2$ ne sont pas des cubes dans $\mathcal{O}_K$. On pourra travailler modulo $\mathfrak{p}_7$.
6. En déduire Cl_K.

Exercice 43

1. 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.
2. 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 $x \in \mathcal{O}_{K(i)}$ 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**.