Corps de nombres et anneaux d'entiers

1 Entiers algébriques

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 un nombre algébrique. Montrer qu'il existe un entier $n \geqslant 1$ tel que nz est un entier algébrique.

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

Exercice 4 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 5 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 $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\alpha\beta$ 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.

Exercice 6 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 il n'existe pas d'élément $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$.

1) Exhiber un idéal I de $\mathbb{Z}[X, Y]$ tel que $\mathcal{O}_K \cong \mathbb{Z}[X, Y]/I$.
2) Faire la liste des idéaux $\mathfrak{m}$ de $\mathcal{O}_K$ tels que $\mathcal{O}_K/\mathfrak{m} \cong \mathbb{Z}/2\mathbb{Z}$.
3) Conclure.

Exercice 7 Soit K un corps de nombres. Montrer que :

$$\mathcal{O}_K^\times = \{x \in \mathcal{O}_K : N_{K/\mathbb{Q}}(x) = \pm 1\}.$$

Exercice 8 Soit K un corps de nombres de degré n.

1) Soit $\mathbf{x} = (x_1, \ldots, x_n)$ une $\mathbb{Q}$-base de K et soit $\Gamma_\mathbf{x} := \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$. Soit Γ un sous-groupe de K contenant $\Gamma_\mathbf{x}$ tel que $[\Gamma : \Gamma_\mathbf{x}] < \infty$. Montrer que K admet une base $\mathbf{y} = (y_1, \ldots, y_n)$ telle que :
$$\Gamma = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n.$$
Vérifier que le discriminant $d(\mathbf{y})$ est indépendant de $\mathbf{y}$ et que $d(\mathbf{x}) = [\Gamma : \Gamma_\mathbf{x}]^2 \cdot d(\mathbf{y})$.
2) Montrer que K admet une base $\mathbf{z} = (z_1, \ldots, z_n)$ telle que :
$$\mathcal{O}_K = \mathbb{Z}z_1 \oplus \cdots \oplus \mathbb{Z}z_n,$$
que le discriminant $\Delta_K := d(\mathbf{z})$ est indépendant de $\mathbf{z}$ et que $d(\mathbf{w}) = [\mathcal{O}_K : \Gamma_\mathbf{w}]^2 \cdot \Delta_K$ pour toute $\mathbb{Q}$-base $\mathbf{w}$ de K contenue dans $\mathcal{O}_K$. Le discriminant Δ_K est généralement appelé le *discriminant de* K.

Exercice 9 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 10 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 $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0 + \ldots + b_{n-1}u^{n-1}}{p}$.
   b) Notons r le plus petit entier tel que b_r n'est pas divisible par p. Montrer que $y = \frac{b_r u^r + \ldots + b_{n-1}u^{n-1}}{p}$ 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 11 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 $\mathscr{O}_{p^k}$ l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$. Nous allons établir par une méthode différente de celle de l'exercice 10 que $\mathscr{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

1) Montrer l'identité $p = \prod_{\substack{r=1 \\ p \nmid r}}^{p^k} (1-\zeta^r)$.
2) En déduire que $(\zeta-1)\mathscr{O}_{p^k} \cap \mathbb{Z} = p\mathbb{Z}$.

Supposons $k = 1$.

3) En utilisant la trace, montrer que l'anneau $\mathscr{O}_p$ est égal à $\mathbb{Z}[\zeta]$.

Revenons au cas général $k \geqslant 1$.

4) Montrer que l'on a $\mathscr{O}_{p^k} = \mathbb{Z}[\zeta] + p^m \mathscr{O}_{p^k}$ pour tout $m \geqslant 0$.
5) 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).
6) En déduire que l'anneau $\mathscr{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

Exercice 12 *Attention, pour cet exercice, il convient d'être un peu familier avec la théorie de Galois!* Soient K et L des extensions finies galoisiennes de $\mathbb{Q}$ de degrés respectifs m et n. On suppose que K et L sont linéairement disjointes, c'est-à-dire que $K \cap L = \mathbb{Q}$

1) Montrer que l'extension composée KL de $\mathbb{Q}$ est galoisienne finie.
2) Montrer que la restriction induit un isomorphisme de groupes $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/\mathbb{Q})$.
3) Montrer que l'application canonique $\mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ est un isomorphisme de groupes.

Soit maintenant $(x_1, \ldots, x_m)$ (resp. $(y_1, \ldots, y_n)$) une base de K (resp. L) telle que :

$$\mathscr{O}_K = \bigoplus_{i=1}^{m} \mathbb{Z} x_i \quad (\text{resp. } \mathscr{O}_L = \bigoplus_{i=1}^{n} \mathbb{Z} y_i).$$

On pose $\Delta_K := d(x_1, \ldots, x_m)$ et $\Delta_L := d(y_1, \ldots, y_n)$ et on suppose que $\Delta_K \wedge \Delta_L = 1$.

4) Montrer que $\Delta_K \mathscr{O}_{KL} \subset \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathbb{Z} x_i y_j$.
5) Montrer que $\mathscr{O}_{KL} = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{m} \mathbb{Z} x_i y_j$.
6) Calculer $d((x_i y_j)_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n})$.
7) 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 10.

Exercice 13 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 $\mathscr{O}_K$ 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 $\mathcal{O}_K$. On note Δ_K le discriminant de 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 14 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 15 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

Exercice 16 Soient $d \in \mathbb{Z} \smallsetminus \{0,1\}$ sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. Soit p un nombre premier.

1) Déterminer en fonction de p et d la factorisation de $p\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$.
2) Vérifier que $p\mathcal{O}_K$ est le carré d'un idéal premier si, et seulement si, p divise le discriminant de K. Dans ce cas, on dit que l'extension $K/\mathbb{Q}$ *ramifie* en p.

Exercice 17 Cet exercice vise à généraliser le calcul de l'exercice précédent. Soit K un corps de nombres. On suppose qu'il existe $\theta \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\theta]$. Soient μ le polynôme minimal de θ et p un nombre premier. On écrit la décomposition en produit d'irréductibles de la réduction $\overline{\mu}$ de μ modulo p :

$$\overline{\mu} = \overline{\mu}_1^{e_1} \dots \overline{\mu}_r^{e_g},$$

où les $\overline{\mu}_i \in \mathbb{F}_p[X]$ sont des polynômes irréductibles non associés deux à deux. Pour chaque $1 \leqslant i \leqslant g$, on introduit un relèvement μ_i de $\overline{\mu}_i$ à $\mathbb{Z}[X]$ et on pose $\mathfrak{p}_i := (p, \mu_i(\theta))$.

1) Montrer que $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont des idéaux premiers deux à deux distincts de $\mathcal{O}_K$ tels que $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_1}$.
2) Vérifier qu'il existe $i \in \{1, 2, \dots, g\}$ tel que $e_i \geqslant 2$ si, et seulement si, p divise le discriminant de K. On dit alors que l'extension $K/\mathbb{Q}$ *ramifie* en p.

Exercice 18 Soit K un corps de nombres. Soit $(x_1, \dots, x_n)$ une base de K telle que $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z} x_i$. 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 $(x_1^*, \dots, x_n^*)$ 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 $(x_1^*, \dots, x_n^*)$ vers la base $(x_1, \dots, x_n)$. 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 $\mathscr{O}_K$. Soit $e \geqslant 0$ tel que $p\mathscr{O}_K = \mathfrak{p}^e\mathfrak{a}$ pour un certain idéal $\mathfrak{a}$ premier avec $\mathfrak{p}$. On suppose que $e \geqslant 2$. On dit alors que l'extension $K/\mathbb{Q}$ *ramifie* en p.

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

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

c) Conclure que p divise Δ_K.

Il est possible de montrer une réciproque à cet énoncé : si p divise Δ_K, alors l'extension $K/\mathbb{Q}$ ramifie en p. Mais ce résultat est plus difficile à établir.

Exercice 19 Soient K un corps de nombres et p un nombre premier. On écrit :

$$p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

avec $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ des idéaux premiers deux à deux distincts de $\mathscr{O}_K$ et $e_1, \dots, e_g \geqslant 1$.

1) Montrer que, pour chaque i, l'indice $[\mathscr{O}_K : \mathfrak{p}_i^{e_i}]$ est une puissance de p. Soit $f_i \geqslant 1$ tel que $[\mathscr{O}_K : \mathfrak{p}_i^{e_i}] = p^{f_i}$.
2) Montrer que $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$.

Exercice 20 Soient $n \geqslant 3$ et $K = \mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité. Soient p un nombre premier et f_p l'ordre de la classe de p modulo $\frac{n}{p^{v_p(n)}}$. Montrer qu'il existe $r := \frac{\varphi(n)}{f_p \varphi(p^{v_p(n)})}$ idéaux premiers deux à deux distincts de $\mathscr{O}_K$ tels que :

$$p\mathscr{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^{\varphi(p^{v_p(n)})}.$$

Exercice 21 Montrer qu'un anneau de Dedekind qui a un nombre fini d'idéaux premiers est principal.

Exercice 22 Soient A un anneau de Dedekind et I un idéal non nul. Montrer que I est engendré par deux éléments.