Entiers algèbriques

Exercice 1 Montrer que les nombres suivants sont des entiers algébriques :

$$\sqrt[4]{5},\quad j+\sqrt{2},\quad \sqrt{3}-\sqrt[3]{5},\quad \frac{2}{3+\sqrt{13}},\quad \frac{-2+\sqrt{2}+i\sqrt{2}}{2},\quad e^{\frac{2i\pi}{n}}.$$

Pour chacun d'eux, on trouvera un polynôme unitaire de $\mathbf{Z}[X]$ l'annulant.
Montrer que $\frac{1}{2}$ n'est pas un entier algébrique.

Exercice 2 Soit k un corps et K une extension finie de k de degré n. On peut voir K comme un k-espace vectoriel de dimension n. Pour tout $b \in K$ on a une application k-linéaire :

$$\begin{array}{rccc} \mu_b : & K & \longrightarrow & K \\ & x & \to & bx. \end{array}$$

On appelle *norme* de b (resp. *trace* et polynôme caractéristique de b) le déterminant (resp. la trace et le polynôme caractéristique) de μ_b. On les notera $N_{K/k}(b)$, $Tr_{K/k}(b)$ et $P_{car_{K/k}}(b)$.

1. (a) Remarquer que $N_{K/k}(b)$ et $Tr_{K/k}(b)$ sont dans k et que $P_{car_{K/k}}(b)$ est à coefficients dans k.
   (b) Montrer que pour tout polynôme P et tout $b \in K$, on a $\mu_{P(b)} = P(\mu_b)$. En déduire que le polynôme minimal de μ_b est égal au polynôme minimal de b.
   (c) Montrer que l'application $b \to Tr(b)$ est k-linéaire et l'on a $Tr(a) = na$ pour $a \in k$.
   Montrer que l'application $b \to N(b)$ est multiplicative et l'on a $N(a) = a^n$ pour $a \in k$.
   (d) Soit L une extension finie de K de degré m et soit $b \in K$. Montrer que $N_{L/k}(b) = N_{K/k}(b)^m$, $Tr_{L/k}(b) = mTr_{K/k}(b)$ et $P_{car_{L/k}}(b) = P_{car_{K/k}}(b)^m$.
2. (a) Pour $k = \mathbf{Q}$ et $K = \mathbf{Q}[\sqrt{d}]$ un corps quadratique, montrer que $N_{K/k}$ est la norme définie en cours.
   (b) Soit $x \in \mathbf{C}$ un entier algébrique et soit f son polynôme minimal sur $\mathbf{Q}$. Sur $\mathbf{C}$, f se factorise sous la forme $f = \prod_{i=1}^{n}(X - x_i)$.
   Montrer que chacun des x_i est un entier algébrique. En déduire que f est un polynôme de $\mathbf{Q}[X]$ dont les coefficients sont tous des entiers algébriques.
   (c) En déduire que le polynôme minimal d'un entier algébrique est unitaire à coefficients dans $\mathbf{Z}$.
   (d) En déduire que pour tout entier algébrique x et pour $K = \mathbf{Q}(x)$, on a $Tr_{K/\mathbf{Q}}(x) \in \mathbf{Z}$, $N_{K/\mathbf{Q}}(x) \in \mathbf{Z}$ et $P_{car_{K/Q}}(x) = f(x) \in \mathbf{Z}[X]$.

Exercice 3 Soit $x = \sqrt[3]{2}$ et $K = \mathbf{Q}(\sqrt[3]{2})$. Soient $A = \mathbf{Z}[x]$ et B l'anneau des entiers de K. On se propose de montrer que $A = B$.

1. Montrer que $A \subset B$, et donner une base du $\mathbf{Z}$-module A.
2. Soit $z = a + bx + cx^2 \in K$, avec $a, b, c \in \mathbf{Q}$. Calculer le polynôme caractéristique de z. Calculer $Tr_{K/\mathbf{Q}}(z), Tr_{K/\mathbf{Q}}(xz)$ et $Tr_{K/\mathbf{Q}}(x^2z)$. En déduire que $6B \subset A$.

Exercice 4

1. Montrer qu'un nombre complexe x est un entier algébrique si et seulement si x est valeur propre d'une matrice à coefficients entiers. (On pourra écrire la matrice de μ_x dans la $\mathbf{Q}$-base $(1, x, x^2, \ldots, x^{n-1})$ où n est le degré algébrique de x.)
2. Retrouver que si x et y sont des entiers algébriques, alors $x+y$ et xy sont des entiers algébriques en donnant explicitement des matrices à coefficients entiers les ayant pour valeurs propres.
3. En appliquant cette méthode, trouver des polynômes annulateurs de $i+j$ et ij.

Exercice 5 Soit A un anneau et

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X].$$

1. Montrer qu'il existe une A-algèbre C vérifiant :
   (i) C est un A-module de rang $n!$
   (ii) Il existe $\lambda_1, \ldots, \lambda_n \in C$ tels que $f = \prod_{i=1}^{n}(x - \lambda_i)$
   (Indication : procéder par récurrence sur n en s'inspirant de la preuve de l'existence d'un corps de décomposition pour un polynôme à coefficients dans un corps)
2. Soit $B = A[X]/(f)$, et soit $z \in B$. En utilisant (1), justifier la méthode suivante pour calculer (par exemple) la norme $N_{B/A}(z)$:
   - On écrit $z - h(x) = h(X) \bmod f$ (avec x= classe de X dans B, et $h \in A[X]$)
   - On calcule le polynôme $S = \prod_{i=1}^{n} h(L_i) \in A[L_1, \ldots, L_n]$ où les L_i sont des indéterminées
   - On écrit $S = T(\sigma_1, \ldots, \sigma_n)$ où les σ_i sont les polynômes symétriques élémentaires en les L_i et où T est à coefficients dans A.
   - On renvoie $-N_{B/A}(z) = T(-a_{n-1}, a_{n-2}, \ldots, (-1)^n a_0)$.

Exercice 6 Soient A un anneau intégralement clos, K son corps de fractions et $f \in A[X]$ un polynôme unitaire. On suppose que $f = gh$ avec g et h unitaires dans $K[X]$. Montrer que g et h sont dans $A[X]$. (Indication : considérer les racines de f dans la clôture algébrique de K.)

Exercice 7 Soient A un anneau et R une A-algèbre. Soit $P \in R[X]$.
Montrer que P est entier sur $A[X]$ si et seulement si ses coefficients sont entiers sur A.
(Indication : supposons P racine de $Q(Y) = Y^m + F_1Y^{m-1} + \cdots + F_m$, avec les F_i dans $A[X]$. On pose $P_1 = P - X^r$ avec r assez grand. Alors P_1 est racine de $Q(Y+X^r) = Y^m + G_1Y^{m-1} + \cdots + G_m$. On en déduit que $(-P_1)(P_1^{m-1} + \cdots + G_{m-1)} = G_m$ dans $R[X]$. Pour r convenable, $G_m = Q(X^r)$ est unitaire, ainsi que $-P_1$. On en déduit que le facteur $P_1^{m-1} + \cdots + G_{m-1}$ est aussi unitaire, puis que P est à coefficients dans A.)

Exercice 8 Soient A un anneau, R une A-algèbre, n un entier naturel, A' la clôture intégrale de A dans R. Déduire de l'exercice précedent que la clôture intégrale de $A[X_1 + \cdots + X_n]$ dans $R[X_1 + \cdots + X_n]$ est $A'[X_1 + \cdots + X_n]$, en déduire que si A est intégralement clos, $A[X_1 + \cdots + X_n]$ également.

Exercice 9 Soient A un anneau et B une A-algèbre de type fini. Montrer l'équivalence :

$$B \text{ est entière sur } A \Leftrightarrow B \text{ est un } A - \text{module de type fini.}$$

Fractions continues et Pell-Fermat

On appelle développement en fraction continue d'un nombre réel x, l'écriture de x sous la forme

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

où $a_0 \in \mathbf{Z}$ et les autres a_i sont des entiers strictement positifs. On note alors $x = [a_0, a_1, a_2, \ldots]$. Tout nombre réel admet un unique développement en fraction continue. Si x est rationnel, ce développement est fini et se note $x = [a_0, a_1, \ldots, a_n]$.
Exemple : $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots] = [2, \overline{1, 2k, 1}]_{k\geq 1}$.

Exercice 10 **Propriétés des fractions continues**
Soit α un réel. On note $[a_0, a_1, a_2, \cdots]$ son développement en fraction continue.

1. Montrer que ce développement s'obtient récursivement ainsi :
$$\alpha_0 = \alpha \quad \text{et pour tout } n \geq 0 \quad a_n = [\alpha_n], \qquad \alpha_{n+1} = \frac{1}{\alpha_n - a_n},$$
où $[y]$ désigne la partie entière de y.
2. Pour $n \geq 0$, on note $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ avec $p_n \wedge q_n = 1$. Montrer que p_n et q_n vérifient les relations
$$p_n = a_n p_{n-1} + p_{n-2} \qquad p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \tag{1}$$
$$q_n = a_n q_{n-1} + q_{n-2} \qquad p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n. \tag{2}$$
3. Montrer que pour $n \geq 0$, $\alpha_n = [a_n, a_{n+1}, \ldots]$ et justifier l'écriture $\alpha = [a_0, \ldots, a_{n-1}, \alpha_n]$. Montrer que pour tout n,
$$\alpha = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}. \tag{3}$$
4. Montrer que
$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$
Remarque : $\frac{p_n}{q_n}$ est appelée n-ième réduite de α. Ces fractions sont en un certain sens les meilleures approximations de α par des rationnels.

Exercice 11

1. Soit $\alpha = \frac{1}{2}(\sqrt{5} - 1)$. Montrer que α est un entier algébrique et trouver le polynôme minimal de $\frac{1}{\alpha}$. En déduire le développement en fraction continue de α.
2. Écrire le développement en fraction continue de $3 + \sqrt{2}$, $2 + \sqrt{6}$ et $2 + \frac{\sqrt{15}}{5}$ $(\sqrt{15} \approx 3,8)$.

Exercice 12 Montrer que pour $a, b \in \mathbf{N}$, $a \neq 0$, on a

$$\sqrt{a^2 + b} = a + \cfrac{b}{2a + \cfrac{b}{2a + \cfrac{b}{\ddots}}}.$$

En déduire le développement en fraction continue de $\sqrt{5}$, $\sqrt{10}$, $\sqrt{17}$, $\sqrt{26}$, $\sqrt{37}$.

Exercice 13 **Équation de Pell-Fermat**

1. Soit α un nombre irrationnel tel que son développement en fraction continue soit finalement périodique, *i.e*

   $\alpha = [a_0, a_1, \ldots, a_N, a_{N+1}, \ldots, a_{N+T}, a_{N+1}, \cdots, a_{N+T}, a_{N+1}, \ldots] = [a_0, \ldots, a_N, \overline{a_{N+1}, \ldots, a_{N+T}}]$.

   Nous allons montrer que α est un nombre algébrique de degré 2.

   - Soit $\beta = [\overline{a_{N+1}, \ldots, a_{N+T}}]$. Montrer que $\beta = [a_{N+1}, \ldots, a_{N+T}, \beta]$.
   - En déduire que β est solution d'une équation de degré 2 à coefficients rationnels.
   - Montrer que $\alpha \in \mathbf{Q}(\beta)$ et en déduire que α est un nombre algébrique de degré 2.

   La réciproque de ce résultat est vraie, c'est le théorème de Lagrange. Dans le cas où $\alpha = \sqrt{d}$ avec d un entier sans facteur carré, on peut montrer que le développement de α est de la forme $[a_0, \overline{a_1, \ldots, a_n}]$, où n est le plus petit indice tel que $a_n = 2a_0$.

2. Soit d un entier sans facteur carré. Considérons l'équation de Pell-Fermat : $x^2 - dy^2 = 1$.

   Soit (x_1, y_1) une solution de l'équation. Dans $\mathbf{Q}(\sqrt{d})$ considérons la matrice M de la multiplication par $x_1 + y_1\sqrt{d}$ dans la base $(1, \sqrt{d})$.

   Après avoir remarqué que pour tout entier n, $(x_1^2 - dy_1^2)^n = 1$, montrer que $\binom{x_n}{y_n} = M^n \binom{x_1}{y_1}$ est une solution de l'équation de Pell-Fermat pour tout n.

   On peut montrer qu'il existe une solution (x_1, y_1) "minimale" et que toutes les autres solutions s'en déduisent à l'aide de l'expression ci-dessus.

3. Cherchons maintenant une solution minimale (x_1, y_1) de l'équation.

   (a) Montrer que si (p, q) est solution de l'équation, alors $|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$.

   La fraction $\frac{p}{q}$ est donc une bonne approximation de $\sqrt{d}$. On peut déduire de cela que $\frac{p}{q}$ est nécessairement une réduite du développement de $\sqrt{d}$.

   (b) Soit T la période du développement de $\sqrt{d}$. Soit n un entier impair tel que $n+1$ est un multiple de T. Nous allons montrer que la réduite $\frac{p_n}{q_n}$ de $\sqrt{d}$ fournit une solution (p_n, q_n) de l'équation de Pell-Fermat.

   Si on prend un tel n minimal, on peut montrer que la solution obtenue est minimale.

   - On pose $\alpha = \sqrt{d}$ et on reprend les notations de l'exercice **1**.
     Remarquer que $\frac{1}{\alpha_{n+2}} = \frac{1}{\alpha_1} = \alpha - a_0$.
   - En utilisant (3), montrer que $(q_{n+1} - a_0 q_n)\sqrt{d} + dq_n = p_n\sqrt{d} + (p_{n+1} - a_0 p_n)$.
   - En déduire avec (1) que $p_n^2 - dq_n^2 = (-1)^{n+1}$ et conclure.

Conclusion : pour trouver les solutions de l'équation de Pell-Fermat, on commence par chercher le développement en fraction continue de $\sqrt{d}$: $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_T}]$. Si la période T est paire, on calcule la réduite $\frac{p_{T-1}}{q_{T-1}} = [a_0, \ldots, a_{T-1}]$; si T est impaire, on calcule $\frac{p_{2T-1}}{q_{2T-1}} = [a_0, \ldots, a_{2T-1}]$. Dans les deux cas, le couple (p_k, q_k) est une solution minimale de l'équation. Toutes les autres solutions se déduisent à l'aide de la matrice M de la question (2).

Application : trouver les solutions de l'équation de Pell-Fermat pour $d = 3, 5, 6, 13, 17, 19, 34, 37, 53$.
(indication : $\sqrt{34} = [5, \overline{1, 4, 1, 10}]$, $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$)

(Pour la preuve complète de ces résultats, on pourra aller voir
http ://agreg-maths.univ-rennes1.fr/documentation/docs/fraccont.pdf)