

Tous les anneaux considérés sont supposés commutatifs et unitaires.

Exercice 1. Montrer que tout sous-anneau de $\mathbf{Q}$ est principal.

Exercice 2. Soit A un anneau. Montrer que A est un corps si et seulement si $A[X]$ est un anneau principal (pour $a \in A$, on pourra considérer l'idéal de $A[X]$ engendré par a et X).

Exercice 3. (1) Soient A un anneau intègre et $\pi \in A$ un élément premier. Montrer que π est irréductible.

(2) Soient A un anneau principal et π un élément irréductible. Montrer que l'idéal $\langle \pi \rangle$ est maximal.

Exercice 4. Montrer que $\mathbf{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}\}_{a,b \in \mathbf{Z}} \subset \mathbf{C}$ est un anneau non factoriel.

Exercice 5. (1) Soient A un anneau euclidien, et $\phi: A \setminus \{0\} \rightarrow \mathbf{N}$ un stathme euclidien. Supposons en outre que A n'est pas un corps.

(a) Justifier l'existence de $x \in E := A \setminus (\{0\} \cup A^\times)$ tel que $\phi(x) = \min_{y \in E} \phi(y)$.

(b) Notons $\pi: A \rightarrow A/\langle x \rangle$ la surjection canonique. Montrer que $\pi(\{0\} \cup A^\times) = A/\langle x \rangle$.

Posons $\theta = \frac{1+i\sqrt{19}}{2} \in \mathbf{C}$ et $A = \{a + b\theta\}_{a,b \in \mathbf{Z}}$.

(2) Calculer le polynôme minimal P de θ sur $\mathbf{Q}$.

(3) Construire un isomorphisme $\mathbf{Z}[X]/\langle P \rangle \xrightarrow{\sim} A$.

Si $z \in \mathbf{Q}(\theta)$, on pose $N(z) = |z|^2$ (où $|z|$ désigne le module du nombre complexe z).

(4) Montrer que l'application N est multiplicative, et que $N(A) \subset \mathbf{N}$.

(5) Montrer que $A^\times = \{\pm 1\}$.

(6) Supposons A euclidien.

(a) En utilisant la question (1), montrer qu'il existe $x \in A$ tel que $A/\langle x \rangle$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$.

(b) Montrer que cela implique que P a une racine dans $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$, et en déduire une contradiction.

(7) Montrer que l'idéal $2A$ est maximal dans A .

(8) Soient $a \in A$ et $b \in A \setminus \{0\}$. Posons $z = \frac{a}{b} \in \mathbf{Q}(\theta)$. Écrivons $z = x + y\theta$ avec $x, y \in \mathbf{Q}$, notons v l'entier le plus proche de y , et posons $y' = y - v$ (on a donc $|y'| \leq \frac{1}{2}$).

(a) Supposons $|y'| \leq \frac{1}{3}$ et notons u l'entier le plus proche de $x + \frac{y-v}{2}$. Montrer que $N(z - (u + v\theta)) < 1$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $a = bq + r$.

(b) Supposons $\frac{1}{3} < |y'| \leq \frac{1}{2}$. Montrer qu'il existe $v'' \in \mathbf{Z}$ tel que $|2y - v''| < \frac{1}{3}$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $2a = bq + r$.

(9) Montrer que A est principal [indication : si $I \subset A$ est un idéal non nul, on considérera un élément de norme minimale dans $I \setminus \{0\}$].

Exercice 6. (LEMME DE GAUSS) Soient A un anneau factoriel et $P, Q \in A[X]$. Démontrer que si P et Q sont primitifs, alors PQ est primitif.

Exercice 7. Soient A un anneau intègre, $K = \text{Frac}(A)$ et $P \in A[X]$ de degré $d \geq 1$.

- (1) Montrer que si P est premier dans $A[X]$, alors il est premier dans $K[X]$.
- (2) Supposons P primitif. Montrer que si P est irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.

Exercice 8. (1) Soient A un anneau factoriel, K son corps des fractions et $P(X) \in A[X]$ unitaire. Montrer que si $P(X) = P_1(X)P_2(X)$ avec $P_1, P_2 \in K[X]$ unitaires, alors on a $P_1, P_2 \in A[X]$.

- (2) En déduire que $\mathbf{Z}[2\sqrt{2}] = \{a + 2\sqrt{2}b\}_{a,b \in \mathbf{Z}}$ n'est pas factoriel.

Exercice 9. Montrer que l'anneau $\mathbf{R}[X, Y, Z]/\langle X^2 + Y^2 + Z^2 \rangle$ est intègre.

Exercice 10. Posons $A = \mathbf{Z}[i\sqrt{2}] = \{x + i\sqrt{2}y\}_{x,y \in \mathbf{Z}}$. C'est un sous-anneau de $\mathbf{C}$.

- (1) Montrer soigneusement que A , muni du stathme défini par $N(x + yi\sqrt{2}) = x^2 + 2y^2$ est un anneau euclidien [on pourra illustrer la preuve par un dessin].
- (2) Déterminer $A^\times$.
- (3) Montrer que $i\sqrt{2}$ est irréductible dans A .

Soit $(x, y) \in \mathbf{Z}^2$ tel que $x^3 = y^2 + 2$.

- (4) Soit $\pi \in A$ un élément irréductible divisant $y + i\sqrt{2}$ et $y - i\sqrt{2}$.
 - (a) Montrer qu'on a $\pi = \pm i\sqrt{2}$.
 - (b) En déduire que y est pair, et trouver une contradiction.
- (5) En déduire $\text{pgcd}(y + i\sqrt{2}, y - i\sqrt{2})$.
- (6) Montrer que $y + i\sqrt{2}$ est un cube dans A .
- (7) En déduire que les seules solutions de l'équation $x^3 = y^2 + 2$ sont $(3, \pm 5)$.

Exercice 11. Posons $A = \mathbf{R}[X]$ et $B = \mathbf{R}[X, Y]/\langle X^4 + Y^2 - 1 \rangle$. On note x et y les images de X et de Y dans B .

- (1) Montrer que B est intègre.
- (2) Montrer que l'unique morphisme $A \rightarrow B$ qui envoie X sur x est injectif. Il induit donc un isomorphisme $A \xrightarrow{\sim} \mathbf{R}[x] \subset B$.
- (3) Montrer que $B = \mathbf{R}[x] \oplus \mathbf{R}[x]y$. Tout élément de B s'écrit donc de façon unique sous la forme $P(x) + Q(x)y$ avec $P, Q \in \mathbf{R}[x]$.
- (4) Si $\alpha = P(x) + Q(x)y$, on pose $\bar{\alpha} = P(x) - Q(x)y$. Montrer que $\alpha \mapsto \bar{\alpha}$ est un automorphisme de l'anneau B .
- (5) Montrer que pour tout $\alpha \in A$, on a $N(\alpha) := \alpha\bar{\alpha} \in \mathbf{R}[x]$, puis que $N: B \rightarrow \mathbf{R}[x]$ est multiplicative (i.e. que $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$).
- (6) Déterminer $B^\times$.
- (7) Montrer que x est irréductible dans A .
- (8) L'anneau B est-il factoriel?

Exercice 12. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbf{Z}[X]$.

- (1) Démontrer que toutes ses racines rationnelles sont entières.
- (2) Démontrer que toute racine entière de $P(X)$ divise a_0 .
- (3) Soit a un entier. Le polynôme $X^3 - aX + 1$ est-il irréductible dans $\mathbf{Q}[X]$?
- (4) Déterminer la décomposition de $P(X) = 2X^5 - 7X^4 + 9X^3 - 9X^2 + 7X - 2$ en facteurs irréductibles dans $\mathbf{Z}[X]$.

Exercice 13. (CRITÈRE D'IRRÉDUCTIBILITÉ PAR RÉDUCTION). Soient A un anneau intègre, K son corps des fractions et $P(X) = a_d X^d + \dots + a_0 \in A[X]$ de degré $d > 0$. On suppose qu'il existe $\pi \in A$ premier ne divisant pas a_d et tel que $\bar{P}(X) = \bar{a}_d X^d + \dots + \bar{a}_0 \in (A/\pi A)[X]$ soit irréductible dans $(A/\pi A)[X]$.

- (1) Montrer que si P est primitif, alors P est irréductible dans $A[X]$.
- (2) Prouver que si A est factoriel, alors P est irréductible dans $K[X]$.
- (3) En déduire que $X^5 + X^2 - 2X - 1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 14. (CRITÈRE D'EISENSTEIN) Soient A un anneau intègre, K son corps des fractions et $P(X) = a_d X^d + \dots + a_0 \in A[X]$ de degré $d > 1$. On suppose qu'il existe $\pi \in A$ premier tel que :

- (i) π ne divise pas a_d ;
 - (ii) π divise a_i pour tout $i \in \{0, \dots, d-1\}$;
 - (iii) π^2 ne divise pas a_0 .
- (1) Montrer que si P est primitif, alors P est irréductible dans $A[X]$.
 - (2) Prouver que si A est factoriel, alors P est irréductible dans $K[X]$.
 - (3) En déduire que $X^4 - 10X^3 + 4X + 6$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 15. Soit $P(X) = X^5 + X^4 + 3X^2 + 1 \in \mathbf{Z}[X]$. En factorisant l'image $\bar{P}$ de P dans $\mathbf{F}_2[X]$, montrer que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 16. Montrer que si $a_1, \dots, a_n \in \mathbf{Z}$ sont deux à deux distincts, alors le polynôme $(X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbf{Z}[X]$.