ANNEAUX, ARITHMÉTIQUE

# Anneaux et corps

### Exercice 1 ★★ — Entiers de Gauss

On note $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.
2. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

### Exercice 2 ★★ — Éléments nilpotents

Soit $(\mathrm{A}, +, \times)$ un anneau. Un élément $a$ de A est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0_\mathrm{A}$.

1. Soit $(x, y) \in \mathrm{A}^2$. Montrer que si $x \times y$ est nilpotent, alors $y \times x$ est nilpotent.
2. Soit $(x, y) \in \mathrm{A}^2$. Montrer que si $x$ et $y$ commutent et que l'un des deux est nilpotent, alors $x \times y$ est nilpotent.
3. Soit $(x, y) \in \mathrm{A}^2$. Montrer que si $x$ et $y$ sont nilpotents et commutent, alors $x + y$ est nilpotent.
4. Soit $x \in \mathrm{A}$. Montrer que si $x$ est nilpotent, alors $1_\mathrm{A} - x$ est inversible et calculer son inverse.

### Exercice 3 ★

Soit A un anneau tel que $\forall x \in \mathrm{A}, x^2 = x$ (on dit que les éléments de A sont idempotents).

1. Montrer que $\forall x \in \mathrm{A}, 2x = 0$.
2. Montrer que A est commutatif.

### Exercice 4 ★★ — Endomorphismes de corps de $\mathbb{R}$

Soit $f$ un endomorphisme de corps de $\mathbb{R}$.

1. Montrer que $f_{|\mathbb{Q}} = \mathrm{Id}_\mathbb{Q}$.
2. Montrer que $f$ est croissant.
3. Montrer que $f = \mathrm{Id}_\mathbb{R}$.

### Exercice 5 ★★ — Différence symétrique

Soit E un ensemble non vide. Pour $\mathrm{A}, \mathrm{B} \in \mathcal{P}(\mathrm{E})$, on définit la différence de A et B par $\mathrm{A}\Delta\mathrm{B} = (\mathrm{A} \setminus \mathrm{B}) \cup (\mathrm{B} \setminus \mathrm{A})$.

1. Montrer que $(\mathcal{P}(\mathrm{E}), \Delta, \cap)$ est un anneau commutatif. Préciser les éléments neutres pour $\Delta$ et $\cap$.
2. Quels sont les éléments de $\mathcal{P}(\mathrm{E})$ inversibles pour $\cap$ ?
3. L'anneau $(\mathcal{P}(\mathrm{E}), \Delta, \cap)$ est-il intègre ?

### Exercice 6 ★ — Corps quadratique

On note $\mathbb{Q}[\sqrt{3}]$ l'ensemble des réels de la forme $a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Q}^2$. Montrer que $\mathbb{Q}[\sqrt{3}]$ est un corps.

### Exercice 7 ★

Soit A un anneau intègre commutatif fini.

1. Soit $a$ un élément non nul de A. Montrer que l'application $\phi : \left\{ \begin{array}{ccc} \mathrm{A} & \longrightarrow & \mathrm{A} \\ x & \longmapsto & ax \end{array} \right.$ est bijective.
2. En déduire que A est un corps.

**Exercice 8** ★

On note $\mathbb{Z}[\sqrt{3}]$ l'ensemble des réels de la forme $a+b\sqrt{3}$ avec $a,b\in\mathbb{Z}$.

**1.** Montrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $(\mathbb{R},+,\times)$.

**2.** **a.** Montrer que $\sqrt{3}$ est irrationnel. On pourra raisonner par l'absurde en écrivant $\sqrt{3}$ sous la forme d'une fraction irréductible $\frac{p}{q}$ i.e. avec $(p,q)\in\mathbb{Z}\times\mathbb{Z}^*$ tel que $p\wedge q=1$.

**b.** Montrer que $f:\left\{\begin{array}{ccc}\mathbb{Z}^2 & \longrightarrow & \mathbb{Z}[\sqrt{3}]\\ (a,b) & \longmapsto & a+b\sqrt{3}\end{array}\right.$ est un isomorphisme du groupe $(\mathbb{Z}^2,+)$ sur le groupe $(\mathbb{Z}[\sqrt{3}],+)$.

**3.** Pour tout $x\in\mathbb{Z}[\sqrt{3}]$, il existe donc un unique couple $(a,b)\in\mathbb{Z}^2$ tel que $x=a+b\sqrt{3}$.

**a.** Pour tout réel $x=a+b\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$ avec $(a,b)\in\mathbb{Z}^2$, on appelle *conjugué* de $x$, noté $\tilde{x}$, le réel $a-b\sqrt{3}$.
Montrer que $g:\left\{\begin{array}{ccc}\mathbb{Z}[\sqrt{3}] & \longrightarrow & \mathbb{Z}[\sqrt{3}]\\ x & \longmapsto & \tilde{x}\end{array}\right.$ est un automorphisme d'anneau.

**b.** Pour tout réel $x=a+b\sqrt{3}\in\mathbb{Z}[\sqrt{3}]$ avec $(a,b)\in\mathbb{Z}^2$, on pose $\mathrm{N}(x)=x\tilde{x}$. Vérifier que pour tout $(x,y)\in\left(\mathbb{Z}[\sqrt{3}]\right)^2$, $\mathrm{N}(xy)=\mathrm{N}(x)\mathrm{N}(y)$.

**c.** Montrer que $x\in\mathbb{Z}[\sqrt{3}]$ est inversible si et seulement si $\mathrm{N}(x)=1$ ou $\mathrm{N}(x)=-1$.
Que vaut alors son inverse ? On distinguera les cas $\mathrm{N}(x)=1$ et $\mathrm{N}(x)=-1$.

# Idéaux

**Exercice 9** ★★★ **Radical d'un idéal**

Soit A un anneau commutatif. Pour tout idéal I de A, on note

$$\mathrm{R(I)}=\{x\in\mathrm{A},\ \exists n\in\mathbb{N},\ x^n\in\mathrm{I}\}$$

L'ensemble R(I) est appelé *radical* de I.

**1.** Soit I un idéal de A. Montrer que R(I) est un idéal de A contenant I.

**2.** Soit I un idéal de A. Montrer que $\mathrm{R(R(I))}=\mathrm{R(I)}$.

**3.** Soient I et J deux idéaux de A. Montrer que $\mathrm{R(I\cap J)}=\mathrm{R(I)}\cap\mathrm{R(J)}$.

**Exercice 10** ★★ **$\mathbb{Q}$ est un anneau principal**

Montrer que $(\mathbb{Q},+,\times$ = est un anneau principal, c'est-à-dire que tous ses idéaux sont principaux i.e. de la forme $a\mathbb{Q}$ avec $a\in\mathbb{Q}$.

**Exercice 11** ★★ **$\mathbb{D}$ est un anneau principal**

Montrer que $(\mathbb{D},+,\times)$ est un anneau principal, c'est-à-dire que tous ses idéaux sont principaux i.e. de la forme $a\mathbb{D}$ avec $a\in\mathbb{D}$.

**Exercice 12** ★★ **CCINP (ou CCP) MP 2015**

Soit $(\mathrm{A},+,\times)$ un anneau commutatif.

**1.** Rappeler la définition d'un anneau et d'un idéal.

**2.** Soit I un idéal de A. Montrer que si $1_\mathrm{A}\in\mathrm{I}$, alors $\mathrm{I}=\mathrm{A}$.

**3.** On pose $\mathrm{I}_a=\{ax,\ x\in\mathrm{A}\}$. Montrer que $\mathrm{I}_a$ est bien un idéal de A.

**4.** On suppose que A n'est pas l'anneau nul. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0_\mathrm{A}\}$ et A.

# Arithmétique de $\mathbb{Z}$

**Exercice 13 ★★★**

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$.

1. Montrer que le quotient de la division euclidienne de $a$ par $b$ est $\left\lfloor \frac{a}{b} \right\rfloor$.
   A partir de maintenant, on suppose $a \wedge b = 1$.
2. Montrer que l'application $\left\{ \begin{array}{ccc} \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/b\mathbb{Z} \\ \overline{k} & \longmapsto & \overline{ak} \end{array} \right.$ est bijective.
3. En déduire que $\displaystyle\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \frac{(a-1)(b-1)}{2}$.

**Exercice 14 ★★★★**

Soit $a$ et N des entiers naturels non nuls. On définit $u_n$ par $u_0 = 1$ et $u_{n+1} = a^{u_n}$ pour $n \in \mathbb{N}$. Montrer que la suite de terme général $u_n \mod \mathrm{N}$ est stationnaire (on note $a \mod b$ le reste de la division euclidienne de $a$ par $b$).

**Exercice 15 ★★** **Mines-Télécom (hors Mines-Ponts) MP 2021**

1. Résoudre $x^2 = x$ dans $\mathbb{Z}/p\mathbb{Z}$, $p$ premier.
2. Résoudre $x^2 = x$ dans $\mathbb{Z}/34\mathbb{Z}$.

**Exercice 16 ★★** **Nombres de Mersenne**

Pour $n \in \mathbb{N}^*$, on appelle $n^{\text{ème}}$ nombre de Mersenne l'entier $\mathrm{M}_n = 2^n - 1$.

1. **a.** Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{N}^*$ un diviseur positif de $n$. Montrer que $2^a - 1$ divise $\mathrm{M}_n$.
   **b.** En déduire que si $\mathrm{M}_n$ est un nombre premier, alors $n$ est un nombre premier.
2. Soient $p$ et $q$ des nombres premiers avec $p$ impair. On suppose que $q$ divise $\mathrm{M}_p$.
   **a.** Montrer que $q$ est impair. En déduire que $2^{q-1} \equiv 1[q]$.
   **b.** En considérant l'ordre de $\overline{2}$ dans $(\mathbb{Z}/q\mathbb{Z})^*$, montrer que $q \equiv 1[p]$ puis que $q \equiv 1[2p]$.
3. Soient $p$ un nombre premier impair et $n \in \mathbb{N}^*$ divisant $\mathrm{M}_p$. En utilisant la décomposition en facteurs premiers de $n$ et la question précédente, montrer que $n \equiv 1[2p]$.

**Exercice 17 ★★★** **Navale MP 2017**

On note $\varphi$ l'indicatrice d'Euler. Soit $n \in \mathbb{N}^*$.

1. Soit $d$ un diviseur positif de $n$. Montrer qu'il y a $\varphi(d)$ éléments du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre $d$.
2. Montrer que $n = \displaystyle\sum_{d|n} \varphi(d)$.
3. En déduire un programme Python permettant de calculer $\varphi(n)$.

**Exercice 18 ★★★** **Magistère MP 2018**

1. Soit $n_1, \dots, n_k$ des entiers deux à deux distincts supérieurs ou égaux à 2. Montrer que
$$\prod_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) \geq \frac{1}{k+1}$$
2. On note $\varphi$ l'indicatrice d'Euler. Montrer que
$$\forall n \in \mathbb{N}^*,\ \varphi(n) \geq \frac{n\ln(2)}{\ln(n) + \ln(2)}$$

**Exercice 19 ★★★** **Indicatrice d'Euler et fonction de Möbius**

On note $\mu$ la fonction de Möbius définie sur $\mathbb{N}^*$ par

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers } \textit{distincts} \end{cases}$$

Montrer que pour tout $n \in \mathbb{N}^*$,

$$\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d)$$

où la somme porte sur les diviseurs positifs de $n$.

# Arithmétique de $\mathbb{K}[\mathrm{X}]$

**Exercice 20** ★★

Pour quelles valeurs de $m \in \mathbb{N}$ le polynôme $P_m = (X+1)^m - X^m - 1$ est il divisible par $Q = X^2 + X + 1$ ?

**Exercice 21** ★★

1. Le polynôme $(X+1)^{2009} + X^{2009} + 1$ est-il divisible par le polynôme $X^2 + X + 1$ ?
2. Pour quelles valeurs de $n \in \mathbb{N}$ le polynôme $X^2 + X + 1$ divise-t-il le polynôme $(X+1)^n + X^n + 1$ ?

**Exercice 22** ★ **Banque CCP**

On considère les polynômes $P = 3X^4 - 9X^3 + 7X^2 - 3X + 2$ et $Q = X^4 - 3X^3 + 3X^2 - 3X + 2$.

1. Décomposez P et Q en facteurs irréductibles sur $\mathbb{R}[X]$, puis sur $\mathbb{C}[X]$ (on pourra calculer les valeurs de P et Q en 1 et 2).
2. Déterminer le PPCM et le PGCD des polynômes P et Q.

**Exercice 23** ★★ **Banque CCP**

Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Décomposez en produit de polynômes irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$ le polynôme :

$$P = X^{2n} - 2X^n \cos(n\theta) + 1$$

**Exercice 24** ★★

Soient $n, p \in \mathbb{N}^*$. Déterminer le pgcd de $X^n - 1$ et $X^p - 1$.

**Exercice 25** ★★★

Soit $(P, Q) \in \mathbb{Z}[X]^2$ tel que $P \wedge Q = 1$. Pour $n \in \mathbb{N}$, on pose $u_n = P(n) \wedge Q(n)$. Montrer que la suite $(u_n)$ est périodique.

**Exercice 26** ★★

Soit $P \in \mathbb{K}[X]$ un polynôme scindé. Exprimer $P \wedge P'$ à l'aide des racines de P et de leurs multiplicités.