

Anneaux et corps

Exercice 1 ★

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

- Montrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
- 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 $p \wedge q = 1$.
 - Montrer que $f : \begin{cases} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}[\sqrt{3}] \\ (a, b) & \longmapsto & a + b\sqrt{3} \end{cases}$ est un isomorphisme du groupe $(\mathbb{Z}^2, +)$ sur le groupe $(\mathbb{Z}[\sqrt{3}], +)$.
- Pour tout $x \in \mathbb{Z}[\sqrt{3}]$, il existe donc un unique couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{3}$.
 - 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 $g : \begin{cases} \mathbb{Z}[\sqrt{3}] & \longrightarrow & \mathbb{Z}[\sqrt{3}] \\ x & \longmapsto & \tilde{x} \end{cases}$ est un automorphisme d'anneau.
 - Pour tout réel $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ avec $(a, b) \in \mathbb{Z}^2$, on pose $N(x) = x\tilde{x}$. Vérifier que pour tout $(x, y) \in (\mathbb{Z}[\sqrt{3}])^2$, $N(xy) = N(x)N(y)$.
 - Montrer que $x \in \mathbb{Z}[\sqrt{3}]$ est inversible si et seulement si $N(x) = 1$ ou $N(x) = -1$.
Que vaut alors son inverse ? On distinguera les cas $N(x) = 1$ et $N(x) = -1$.

Exercice 2 ★★★★★

Centrale-Supélec MP 2019

On dit qu'un anneau A est régulier si, et seulement si, pour tout x appartenant à A , il existe un u appartenant à A tel que $xux = x$.

- L'anneau $(\mathbb{Z}, +, \times)$ est-il régulier ?
 - Si A est un corps, A est-il régulier ?
 - Montrer que $(\mathcal{L}(E), +, \circ)$ est un anneau régulier.
- Soit A la matrice n'ayant que des 0, sauf sur la sur-diagonale où il n'y a que des 1. Exhiber U telle que $AUA = A$.
- Donner une condition nécessaire et suffisante pour que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ soit un anneau régulier.

Exercice 3 ★★★

Soit $(A, +, \times)$ un anneau tel que $\forall x \in A, x^3 = x$.

- Montrer que $\forall x \in A, 3(x^2 + x) = 0_A$.
- Montrer que $\forall x \in A, 6x = 0_A$.
- Montrer que $\forall (x, y) \in A^2, 3(xy + yx) = 0_A$ puis que $3(xy - yx) = 0_A$.
- Montrer que $\forall (x, y) \in A^2, 2(xy - yx) = 0_A$. On pourra commencer par développer $(x + y)^3 + (x - y)^3$.
- En déduire que A est un anneau commutatif.

Exercice 4 ★★

Entiers de Gauss

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

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

Exercice 5 ★★**Éléments nilpotents**

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

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

Exercice 6 ★

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

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

Exercice 7 ★★**Endomorphismes de corps de \mathbb{R}**

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

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

Exercice 8 ★★**Différence symétrique**

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

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

Exercice 9 ★**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 10 ★

Soit A un anneau intègre commutatif fini.

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

Idéaux**Exercice 11 ★★★****Radical d'un idéal**

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

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

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

Exercice 12 ★★ **\mathbb{Q} est un anneau principal**

Montrer que les idéaux de $(\mathbb{Q}, +, \times)$ sont les ensembles de la forme $a\mathbb{Q}$ avec $a \in \mathbb{Z}$.

Exercice 13 ★★ **\mathbb{D} est un anneau principal**

On note \mathbb{D} l'ensemble des nombres décimaux. Vérifier que $(\mathbb{D}, +, \times)$ est un anneau puis montrer que les idéaux $(\mathbb{D}, +, \times)$ sont les ensembles de la forme $a\mathbb{D}$ avec $a \in \mathbb{Z}$.

Exercice 14 ★★**CCINP (ou CCP) MP 2015**

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

1. Rappeler la définition d'un anneau et d'un idéal.
2. Soit I un idéal de A . Montrer que si $1_A \in I$, alors $I = A$.
3. On pose $I_a = \{ax, x \in A\}$. Montrer que 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 $\{0_A\}$ et A .

Exercice 15**Mines-Télécom (hors Mines-Ponts) MP 2022**

Pour un anneau A , on dit qu'un idéal I de A est premier si et seulement si :

$$\forall (x, y) \in A^2, xy \in I \implies x \in I \text{ ou } y \in I$$

Soit A un anneau abélien dont tous les idéaux sont premiers. Montrer que A est un anneau intègre, puis que A est un corps.

Arithmétique de \mathbb{Z} **Exercice 16 ★★★**

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 $\begin{cases} \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/b\mathbb{Z} \\ \bar{k} & \longmapsto & \overline{ak} \end{cases}$ est bijective.
3. En déduire que $\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \frac{(a-1)(b-1)}{2}$.

Exercice 17 ★★★★★

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 $u_n \bmod N$ est stationnaire (on note $a \bmod b$ le reste de la division euclidienne de a par b).

Exercice 18 ★★**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 19 ★★**Nombres de Mersenne**

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

1. a. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{N}^*$ un diviseur positif de n . Montrer que $2^a - 1$ divise M_n .
b. En déduire que si 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 M_p .
a. Montrer que q est impair. En déduire que $2^{q-1} \equiv 1[q]$.
b. En considérant l'ordre de $\bar{2}$ 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 M_p . En utilisant la décomposition en facteurs premiers de n et la question précédente, montrer que $n \equiv 1[2p]$.

Exercice 20 ★★★★★**Centrale-Supélec MP 2019**

On pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec p premier et impair, $\mathcal{C} = \{x^2, x \in \mathbb{F}_p \setminus \{\bar{0}\}\}$.

1. Que dire de la structure algébrique de \mathbb{F}_p et de \mathcal{C} ?
2. Expliciter \mathcal{C} pour $p = 11$.
3. Soit P un polynôme de degré strictement inférieur à d et à coefficients entiers, avec $d \in \mathbb{N}^*$. Soient $(a_1, \dots, a_d) \in \mathbb{Z}^d$ tel que les a_i soient distincts modulo p et tel que p divise les $P(a_i)$. Montrer que pour tout $n \in \mathbb{Z}$, p divise $P(n)$.
4. Montrer que $\mathcal{C} = \left\{x \in \mathbb{F}_p, x^{\frac{p-1}{2}} = \bar{1}\right\}$.

Exercice 21 ★★★

Résoudre dans $\mathbb{Z}/65\mathbb{Z}$ l'équation $x^2 - 2x + 2 = 0$.

Exercice 22 ★★★**Critère d'Euler**

Soit p un nombre premier distinct de 2. On pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

1. On pose $\mathcal{C} = \{x^2, x \in \mathbb{F}_p^*\}$. Montrer que $\text{card } \mathcal{C} = \frac{p-1}{2}$.
2. Soit $a \in \mathbb{F}_p^*$. Montrer que $a^{\frac{p-1}{2}} = \pm 1$.
3. Montrer plus précisément que

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \in \mathcal{C} \\ -1 & \text{sinon} \end{cases}$$

On admettra qu'un polynôme à coefficients dans \mathbb{F}_p admet moins de racines dans \mathbb{F}_p que son degré.

Exercice 23 ★★★**Navale MP 2017**

On note φ 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 d'ordre d dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. Montrer que $n = \sum_{d|n} \varphi(d)$.
3. En déduire un programme Python permettant de calculer $\varphi(n)$.

Exercice 24 ★★★**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 φ l'indicatrice d'Euler. Montrer que

$$\forall n \in \mathbb{N}^*, \varphi(n) \geq \frac{n \ln(2)}{\ln(n) + \ln(2)}$$

Exercice 25 ★★★**Indicatrice d'Euler et fonction de Möbius**

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

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

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 .

Exercice 26 ★★★**Déterminant de Smith**

1. Pour $(i, j) \in (\mathbb{N}^*)^2$, on pose $a_{i,j} = 1$ si j divise i et $a_{i,j} = 0$ sinon. Que vaut le déterminant de la matrice $A = (a_{i,j})_{1 \leq i, j \leq n}$?
2. Pour $(i, j) \in (\mathbb{N}^*)^2$, on note $d_{i,j}$ le nombre de diviseurs positifs communs à i et j . Que vaut le déterminant de la matrice $D = (d_{i,j})_{1 \leq i, j \leq n}$?
3. On pose enfin $S = (i \wedge j)_{1 \leq i, j \leq n}$. Montrer que $\det S = \prod_{k=1}^n \varphi(k)$. On admettra la formule classique $\sum_{d|n} \varphi(d) = n$.

Exercice 27 ★★

Soient un entier $n \in \mathbb{N}^*$ et un entier impair $a \in \mathbb{Z}$. Montrer que $a^{2^{n-1}} \equiv 1[2^n]$.

Arithmétique de $\mathbb{K}[X]$ **Exercice 28 ★★**

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 29 ★★

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 30 ★**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 31 ★★**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 32 ★

Déterminer la décomposition en produit de facteurs irréductibles sur \mathbb{R} du polynôme $P = (X+1)^7 - X^7 - 1$ sachant que j est une racine multiple de P .

Exercice 33 ★★**D'après CCP PC 2007**

Pour tout $n \in \mathbb{N}$, on note $Q_n = (X^2 - 1)^n$ et $P_n = \frac{1}{2^n n!} Q_n^{(n)}$. On pourra confondre polynôme et fonction polynomiale associée.

1. Calculer P_0, P_1, P_2 et P_3 .
2. Quel est le degré de P_n ?
3. Montrer que P_n a la parité de n . En déduire $P_n(0)$ pour n impair et $P'_n(0)$ pour n pair.
4. En utilisant la formule du binôme de Newton, calculer $P_n(0)$ pour n pair et $P'_n(0)$ pour n impair. On exprimera les résultats à l'aide de factorielles.
5. a. Vérifier que

$$\forall n \in \mathbb{N}, (X^2 - 1)Q'_n = 2nXQ_n$$

- b. En dérivant $n+1$ fois cette relation, montrer que

$$\forall n \in \mathbb{N}, (X^2 - 1)P''_n + 2XP'_n = n(n+1)P_n$$

6. a. Montrer que $Q_n^{(k)}(-1) = Q_n^{(k)}(1) = 0$ pour tout $k \in \llbracket 0, n-1 \rrbracket$.
b. En appliquant le théorème de Rolle et à l'aide d'une récurrence, montrer que P_n admet exactement n racines réelles distinctes dans $] -1, 1[$.

Exercice 34 ★★

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

Exercice 35 ★★

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 36 ★★

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

Exercice 37 ★★

Pour tout entier $n \geq 2$, on pose $P_n = (X + i)^n - (X - i)^n$.

1. Déterminer les racines complexes de P_n .
2. En déduire les valeurs de

$$A_n = \sum_{k=1}^{n-1} \cotan\left(\frac{k\pi}{n}\right) \quad \text{et} \quad B_n = \prod_{k=1}^{n-1} \cotan\left(\frac{k\pi}{n}\right)$$

Algèbres**Exercice 38 ★★★★★****Centrale-Supélec MP 2021**

Soit \mathbb{K} une \mathbb{R} -algèbre commutative intègre de dimension finie $n \geq 2$.

1. Soit $a \in \mathbb{K} \setminus \{0\}$, montrer que $f : x \mapsto ax$ est un automorphisme. En déduire que a est inversible.
2. Soit $a \in \mathbb{K} \setminus \mathbb{R}$. Montrer que $(1, a)$ est libre et $(1, a, a^2)$ est liée.
3. Montrer l'existence de $i \in \mathbb{K}$ tel que $i^2 = -1$, puis que \mathbb{K} est isomorphe à \mathbb{C} en tant que \mathbb{R} -algèbre.

Exercice 39 ★

Montrer que l'application $\begin{cases} \mathbb{C} & \longrightarrow \mathcal{M}_2(\mathbb{R}) \\ z & \longmapsto M(z) \end{cases}$ où $M(z) = \begin{pmatrix} \operatorname{Re}(z) & -\operatorname{Im}(z) \\ \operatorname{Im}(z) & \operatorname{Re}(z) \end{pmatrix}$ est un morphisme injectif de \mathbb{R} -algèbres.

Exercice 40 ★

Déterminer les morphismes d'algèbres de $\mathbb{K}[X]$ dans \mathbb{K} .

Exercice 41 ★★

1. Montrer que l'application $\Phi : \begin{cases} \mathbb{C} & \longrightarrow \mathcal{M}_2(\mathbb{R}) \\ z & \longmapsto \begin{pmatrix} \operatorname{Re}(z) & -\operatorname{Im}(z) \\ \operatorname{Im}(z) & \operatorname{Re}(z) \end{pmatrix} \end{cases}$ est un morphisme injectif d'algèbres.
2. On pose $A_\theta = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$ pour $\theta \in \mathbb{R}$. Calculer $\exp(A_\theta)$.