

Feuille d'exercices n°13

Exercice 1 (*)

Soit $G = \mathbb{R}_+^* \times \mathbb{R}$ muni de la loi $\star$ définie par $(x, y) \star (a, b) = (xa, xb + ya)$. Montrer $(G, \star)$ est un groupe.

Corrigé : L'ensemble G n'est pas le sous-groupe d'un groupe connu. On vérifie sans difficultés les différentes propriétés d'un groupe. Le neutre est $(1, 0)$, on a

$$((x, y) \star (a, b)) \star (u, v) = (xau, xav + uxb + uya) = (x, y) \star ((a, b) \star (u, v))$$

et
$$(x, y) \star (1/x, -y/x^2) = (1/x, -y/x^2) \star (x, y) = (1, 0)$$

Ainsi

$$\boxed{(G, \star) \text{ est un groupe.}}$$

Exercice 2 (**)

Soit φ un morphisme non constant d'un groupe fini $(G, \star)$ vers $(\mathbb{C}^*, \times)$. Calculer

$$\sum_{x \in G} \varphi(x)$$

On pourra considérer l'application $x \mapsto a \star x$ avec $a \in G$ bien choisi.

Corrigé : Soit $a \in G$ tel que $\varphi(a) \neq 1$. L'application $x \mapsto a \star x$ est une permutation de G dont la réciproque est donnée par $x \mapsto a^{-1} \star x$. Ainsi, on a

$$\sum_{x \in G} \varphi(x) = \sum_{x \in G} \varphi(a \star x) = \sum_{x \in G} \varphi(a) \varphi(x) = \varphi(a) \sum_{x \in G} \varphi(x)$$

Compte-tenu du choix de a , on conclut

$$\boxed{\sum_{x \in G} \varphi(x) = 0}$$

Exercice 3 (*)

Soit A un anneau. On définit le *centre* de A noté $Z(A)$ par

$$Z(A) = \{x \in A \mid \forall a \in A \quad ax = xa\}$$

Montrer que $Z(A)$ est un sous-anneau de $(A, +, \times)$.

Corrigé : On a $1_A \in Z(A)$, $0_A \in Z(A)$ $((0_A + 0_A)a = 0_A a$ d'où $0_A a = 0_A$ pour $a \in A$) Soit $(x, y) \in Z(A)^2$. On a

$$\forall a \in A \quad a(x - y) = ax - ay = xa - ya = (x - y)a$$

d'où $x - y \in Z(A)$ et

$$\forall a \in A \quad a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$$

Ainsi

$$\boxed{\text{L'ensemble } Z(A) \text{ est un sous-anneau de } (A, +, \times).}$$

Exercice 4 (*)

On pose

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

Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif puis déterminer $U(\mathbb{Z}[i])$. On pourra considérer l'application $N : \mathbb{C} \rightarrow \mathbb{R}, z \mapsto z\bar{z}$.

Corrigé : On a $\mathbb{Z}[i]$ sous-groupe de $(\mathbb{C}, +)$ et contenant 1. Puis, soit $(a, b), (c, d)$ dans $\mathbb{Z}^2$. On a

$$(a + ib)(c + id) = ac - bd + i(ad + bc) \in \mathbb{Z}[i]$$

et loi $\times$ est commutative. Ainsi

L'ensemble $\mathbb{Z}[i]$ est un anneau commutatif.

Notons $N(z) = z\bar{z}$ pour $z \in \mathbb{C}$. On a $N(zz') = N(z)N(z')$ pour tout $(z, z') \in \mathbb{C}^2$ et

$$\forall (a, b) \in \mathbb{Z}^2 \quad N(a + ib) = a^2 + b^2 \in \mathbb{N}$$

Soit $a + ib \in U(\mathbb{Z}[i])$. Il existe $c + id \in \mathbb{Z}[i]$ tel que $(a + ib)(c + id) = 1$ et

$$N((a + ib)(c + id)) = N(a + ib)N(c + id) = N(1) = 1 \implies (a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$$

Autrement dit

$$U(\mathbb{Z}[i]) \subset \{\pm 1, \pm i\}$$

L'inclusion réciproque est immédiate et on conclut

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

Remarque : L'anneau $\mathbb{Z}[i]$ est appelé *anneau des entiers de Gauss*.

Exercice 5 (**)

Soit $(A, +, \times)$ un anneau commutatif. Un élément $x \in A$ est dit *nilpotent* s'il existe n entier non nul tel que $x^n = 0_A$. On note

$$\mathcal{N}(A) = \{x \in A \mid x \text{ nilpotent}\}$$

1. Montrer que $\mathcal{N}(A)$ est un idéal de A .
2. Soit $a \in \mathcal{N}(A)$. Montrer que $1_A - a$ est inversible.
3. Soit $a \in \mathcal{N}(A)$ et b inversible. Montrer que $a + b$ est inversible.

Corrigé : 1. On a $0 \in \mathcal{N}(A)$. Soit $(x, y) \in \mathcal{N}(A)^2$ et n, m entiers non nuls tels que $x^n = y^m = 0$. On a $(-x)^n = ((-1)x)^n = (-1)^n x^n = 0$ d'où $-x \in \mathcal{N}(A)$. Puis

$$(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$$

Pour $k \in \llbracket 0; n+m \rrbracket$, on a un des deux exposants k ou $n+m-k$ suffisamment grand (on peut le voir comme une utilisation du principe des tiroirs : on doit placer $n+m$ chaussettes dans les deux tiroirs que constituent les exposants sur x et y dans la somme). Soit on a $k \geq n$, soit on a $k < n$ d'où $n+m-k > m$. Par suite, il vient $(x + y)^{n+m} = 0$ d'où $\mathcal{N}(A)$ sous-groupe de $(A, +)$. Enfin, pour $(a, x) \in A \times \mathcal{N}(A)$, avec n entier tel que $x^n = 0$, on a $(ax)^n = a^n x^n = 0$ et ainsi

L'ensemble $\mathcal{N}(A)$ est un idéal de l'anneau A .

Remarque : L'idéal $\mathcal{N}(A)$ est appelé *nilradical* de l'anneau A .

2. Il existe n entier tel que $a^n = 0$. D'après l'identité de Bernoulli, on a

$$1 = 1 - a^n = (1 - a) \sum_{k=0}^{n-1} a^{n-1-k}$$

Ainsi

$$\boxed{\forall a \in \mathcal{N}(A) \quad 1 - a \in U(A)}$$

3. On a $a + b = b(1 - c)$ avec $c = -b^{-1}a$ nilpotent puisque $\mathcal{N}(A)$ est un idéal. Ainsi, on a $1 - c \in U(A)$ et comme $U(A)$ est un groupe, on conclut

$$\forall (a, b) \in \mathcal{N}(A) \times U(A) \quad a + b = b(1 + b^{-1}a) \in U(A)$$

Exercice 6 (**)

Un idéal I d'un anneau commutatif $(A, +, \times)$ est dit *premier* si

$$\forall x, y \in A \quad xy \in I \implies x \in I \text{ ou } y \in I$$

Décrire les idéaux premiers de $(\mathbb{K}[X], +, \times)$.

Corrigé : Soit I idéal premier de $\mathbb{K}[X]$. On suppose $I \neq \{0\}$ sinon c'est immédiat par intégrité de $\mathbb{K}[X]$. Il existe P unitaire tel que $I = P \cdot \mathbb{K}[X]$. Si $P = AB$ avec A et B non constants, alors $AB \in I$ et $A \notin I$, $B \notin I$. On a donc nécessairement P irréductible. Supposons P irréductible qui divise AB . On a $P \wedge A$ diviseur de P donc $P \wedge A = 1$ ou P (car constant ou associé à P). Si $P \wedge A = P$, comme $P \wedge A | A$, c'est fini. Sinon, si $P \wedge A = 1$ d'après le lemme de Gauss, on a $P | B$. Ainsi

$$\boxed{\text{Les idéaux premiers de } \mathbb{K}[X] \text{ sont exactement les } P \cdot \mathbb{K}[X] \text{ avec } P \text{ irréductible.}}$$

Exercice 7 (**)

Soit n entier. Déterminer le reste de la division euclidienne X^n par $(X - a)(X - b)$ avec a, b dans $\mathbb{K}$.

Corrigé : D'après le théorème de la division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tel que

$$X^n = (X - a)(X - b)Q + R \tag{*}$$

avec $\deg R < 2$, autrement dit $R = \alpha X + \beta$ avec α, β scalaires.

Supposons $a \neq b$. En substituant X par a puis par b dans $(*)$, on obtient

$$\begin{cases} a^n = \alpha a + \beta \\ b^n = \alpha b + \beta \end{cases} \iff \begin{cases} \alpha = \frac{a^n - b^n}{a - b} \\ \beta = \frac{ab^n - ba^n}{a - b} \end{cases}$$

Ainsi

$$\boxed{\text{Si } a \neq b, \text{ on a } R = \frac{1}{a - b} ((a^n - b^n)X + ab^n - ba^n)}$$

Supposons $a = b$. Notant $S = (X - a)^2 Q$, on observe que S admet a pour racine double d'où $S(a) = S'(a) = 0$. En substituant X par a dans $(*)$ puis dans la relation obtenue par dérivation de $(*)$, on obtient

$$\begin{cases} a^n = \alpha a + \beta \\ na^{n-1} = \alpha \end{cases} \iff \begin{cases} \alpha = na^{n-1} \\ \beta = (1 - n)a^n \end{cases}$$

Ainsi

$$\boxed{\text{Si } a = b, \text{ on a } R = na^{n-1}X + (1 - n)a^n}$$

Variantes : 1. Avec la formule de Taylor, on a

$$P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(a)}{n!} (X-a)^n = R + (X-a)^2 Q \quad \text{et} \quad R = P(a) + P'(a)(X-a)$$

2. On peut aussi considérer la base des polynômes de Lagrange $L_a = \frac{X-b}{X-a}$ et $L_b = \frac{X-a}{b-a}$. On a instantanément

$$R = a^n L_a + b^n L_b$$

Exercice 8 (*)

Soit $P \in \mathbb{C}[X]$ avec $\deg P \geq 1$. Déterminer r le nombre de racines de P en fonction de P et $P \wedge P'$.

Corrigé : Notons $P = \lambda \prod_{i=1}^r (X - \alpha_i)^{m_i}$ avec λ, α_i des complexes, λ non nul et m_i des entiers non nuls. Comme α_i racine de P' de multiplicité $m_i - 1$, on a

$$P \wedge P' = \prod_{i=1}^r (X - \alpha_i)^{m_i - 1}$$

puis
$$\deg(P \wedge P') = \sum_{i=1}^r (m_i - 1) = \deg P - r$$

Ainsi

$$\boxed{r = \deg P - \deg(P \wedge P')}$$

Exercice 9 (**)

Soit $(P_n)_n$ suite de polynômes de $\mathbb{R}[X]$ définie par

$$P_0 = 2, \quad P_1 = X \quad \forall n \in \mathbb{N} \quad P_{n+2} = X P_{n+1} - P_n$$

1. Calculer P_2, P_3 .
2. Déterminer le degré et le coefficient dominant de P_n .
3. Montrer que pour tout $(n, z) \in \mathbb{N} \times \mathbb{C}^*$ $P_n(z + 1/z) = z^n + 1/z^n$.
4. En déduire une expression simple de $P_n(2 \cos(\theta))$ pour $\theta \in \mathbb{R}$.
5. Déterminer les racines de P_n .

Corrigé :

1. Le calcul donne $\boxed{P_2 = X^2 - 2 \quad \text{et} \quad P_3 = X^3 - 3X}$

2. On peut aisément conjecturer

$$\forall n \in \mathbb{N}^* \quad P_n = X^n + Q_n \quad \text{avec} \quad Q_n \in \mathbb{R}_{n-1}[X]$$

Montrons cette propriété par récurrence double. Notons :

$$\mathcal{P}(n) : \quad P_n = X^n + Q_n \quad \text{avec} \quad Q_n \in \mathbb{R}_{n-1}[X]$$

- Les propriétés $\mathcal{P}(1)$ et $\mathcal{P}(2)$ sont clairement vraies.
- $\mathcal{P}(n)$ et $\mathcal{P}(n+1) \implies \mathcal{P}(n+2)$: On suppose $\mathcal{P}(n)$ et $\mathcal{P}(n+1)$ vraies pour n entier non nul fixé. On a

$$\begin{aligned} P_{n+2} &= X P_{n+1} - P_n = X(X^{n+1} + Q_{n+1}) - P_n \\ &= X^{n+2} + Q_{n+2} \end{aligned}$$

avec

$$Q_{n+2} = XQ_{n+1} - P_n \in \mathbb{R}_{n+1}[X]$$

ce qui clôt la récurrence. Ainsi

$$\boxed{\forall n \in \mathbb{N}^* \quad P_n = X^n + Q_n \quad \text{avec} \quad Q_n \in \mathbb{R}_{n-1}[X]}$$

3. On procède là encore par récurrence double. Notons

$$\mathcal{P}(n) : \quad \forall z \in \mathbb{C}^* \quad P_n(z + 1/z) = z^n + 1/z^n$$

- La vérification de $\mathcal{P}(0)$ et $\mathcal{P}(1)$ est immédiate.
- $\mathcal{P}(n)$ et $\mathcal{P}(n+1) \implies \mathcal{P}(n+2)$: On suppose $\mathcal{P}(n)$ et $\mathcal{P}(n+1)$ vraies pour n entier fixé. On a

$$\begin{aligned} P_{n+2}(z + 1/z) &= (z + 1/z)P_{n+1}(z + 1/z) - P_n(z + 1/z) \\ &= (z + 1/z)(z^{n+1} + 1/z^{n+1}) - (z^n + 1/z^n) = z^{n+2} + 1/z^{n+2} \end{aligned}$$

ce qui clôt la récurrence. Par conséquent

$$\boxed{\forall (n, z) \in \mathbb{N} \times \mathbb{C}^* \quad P_n(z + 1/z) = z^n + 1/z^n}$$

4. Soit $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$. D'après l'identité d'Euler, on a $2 \cos(\theta) = e^{i\theta} + e^{-i\theta}$. Par suite, il vient

$$P_n(2 \cos(\theta)) = P_n(e^{i\theta} + e^{-i\theta}) = e^{in\theta} + e^{-in\theta}$$

On en déduit

$$\boxed{\forall \theta \in \mathbb{R} \quad P_n(2 \cos(\theta)) = 2 \cos(n\theta)}$$

5. A l'aide de la question précédente, déterminons les racines de P_n . Pour $\theta \in \mathbb{R}$, on a

$$P_n(2 \cos(\theta)) = 0 \iff 2 \cos(n\theta) = 0 \iff n\theta \equiv \frac{\pi}{2} [\pi] \iff \theta \in \left\{ \frac{\pi}{2n} + \frac{k\pi}{n}, k \in \mathbb{Z} \right\}$$

L'application $\theta \mapsto 2 \cos(\theta)$ est strictement décroissante sur $[0; \pi]$ donc injective sur cet intervalle.

Comme on a
$$0 < \frac{\pi}{2n} \quad \text{et} \quad \frac{\pi}{2n} + \frac{(n-1)\pi}{n} = \pi - \frac{\pi}{2n} < \pi$$

on en déduit
$$\text{Card} \left\{ 2 \cos \left\{ \frac{\pi}{2n} + \frac{k\pi}{n} \right\}, k \in \llbracket 0; n-1 \rrbracket \right\} = n$$

Comme P_n est un polynôme de degré n , il admet au plus n racines et on a donc déterminé exactement toutes ses racines. Le coefficient dominant de P_n étant égal à 1, on en déduit la forme factorisée

$$\boxed{\forall n \in \mathbb{N}^* \quad P_n(X) = \prod_{k=1}^n \left(X - 2 \cos \left[\pi \left(\frac{2k-1}{2n} \right) \right] \right)}$$

Exercice 10 (*)

Soit
$$\varphi : \begin{cases} \mathbb{K}_{2n-1}[X] & \longrightarrow \mathbb{K}^{2n} \\ P & \longmapsto (P(0), P'(0), \dots, P^{(n-1)}(0), P(1), P'(1), \dots, P^{(n-1)}(1)) \end{cases}$$

Montrer que φ est bijective.

Corrigé : On a $\varphi \in \mathcal{L}(\mathbb{K}_{2n-1}[X], \mathbb{K}^{2n})$, la linéarité résultant simplement de la linéarité de la dérivation. On remarque l'égalité des dimensions

$$\dim \mathbb{K}_{2n-1}[X] = \dim \mathbb{K}^{2n}$$

On a donc φ isomorphisme si et seulement si φ injective (si et seulement si φ surjective). Soit $P \in \text{Ker } \varphi$. On a 0 et 1 qui sont racines de P de multiplicité n donc X^n et $(X - 1)^n$ divisent P . Comme ces polynômes sont premiers entre eux, on a $X^n(X - 1)^n$ divise P mais $\deg P \leq 2n - 1$. Il s'ensuit que P est le polynôme nul et par suite

L'application φ est un isomorphisme de $\mathbb{K}_{2n-1}[X]$ sur $\mathbb{K}^{2n}$.

Exercice 11 (**)

Soit $X \subset \mathbb{R}$ un ensemble fini non vide. Montrer qu'il existe $P \in \mathbb{R}[X]$ tel que

$$\forall x \in X \quad P(x) = \sqrt[3]{x}$$

Corrigé : Notons $X = \{x_1, \dots, x_n\}$ et $(L_i)_{1 \leq i \leq n}$ la famille des polynômes interpolateurs de Lagrange associés à X . On a $L_i(x_j) = \delta_{i,j}$ pour tout $(i, j) \in \llbracket 1; n \rrbracket^2$. On choisit alors $P = \sum_{i=1}^n \sqrt[3]{x_i} L_i$. On a

$$\forall j \in \llbracket 1; n \rrbracket \quad P(x_j) = \sum_{i=1}^n \sqrt[3]{x_i} L_i(x_j) = \sum_{i=1}^n \sqrt[3]{x_i} \delta_{i,j} = \sqrt[3]{x_j}$$

Exercice 12 (**)

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Établir $P(X + a) = \sum_{k=0}^{+\infty} a^k \frac{P^{(k)}}{k!}$

Corrigé : D'après la formule de Taylor, on a

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (X - a)^k$$

d'où $P(X + a) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} X^k$

et par conséquent $\forall (x, a) \in \mathbb{K}^2 \quad P(x + a) = \sum_{k=0}^{+\infty} x^k \frac{P^{(k)}(a)}{k!}$

d'où, en échangeant les rôles

$$\forall (a, x) \in \mathbb{K}^2 \quad P(a + x) = \sum_{k=0}^{+\infty} a^k \frac{P^{(k)}(x)}{k!}$$

Ainsi, pour $a \in \mathbb{K}$, le polynôme $P(X + a) - \sum_{k=0}^{+\infty} a^k \frac{P^{(k)}}{k!}$ admet une infinité de racines et par conséquent

$$P(X + a) = \sum_{k=0}^{+\infty} a^k \frac{P^{(k)}}{k!}$$

Exercice 13 (*)

On pose $E = \left\{ M(a, b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, (a, b) \in \mathbb{R}^2 \right\}$

Montrer que E est un algèbre réelle commutative pour les lois usuelles.

Corrigé : Notons $K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On a clairement $E = \text{Vect}(I_n, K)$ d'où $I_n \in E$, E est un sev de $\mathcal{M}_2(\mathbb{R})$ et pour $(a, b), (c, d)$ dans $\mathbb{R}^2$, on a

$$M(a, b)M(c, d) = M(ac - bd, ad + bc) = M(c, d)M(a, b)$$

Ceci prouve que E est une sous-algèbre commutative de $(\mathcal{M}_2(\mathbb{R}), +, \times, \cdot)$ d'où

L'ensemble E est une $\mathbb{R}$ -algèbre commutative.

Exercice 14 (*)

Déterminer les morphismes de $\mathbb{R}$ -algèbres de $\mathbb{C}$ dans $\mathbb{C}$.

Corrigé : Soit $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ un morphisme de $\mathbb{R}$ -algèbres. On a $\varphi(1) = 1$ puis, pour $(x, y, \lambda) \in \mathbb{C}^2 \times \mathbb{R}$

$$\varphi(\lambda x + y) = \lambda \varphi(x) + \varphi(y) \quad \varphi(xy) = \varphi(x)\varphi(y)$$

Ainsi

$$\varphi(i^2) = \varphi(-1) = -\varphi(1) = -1 = \varphi(i)^2$$

d'où $\varphi(i) = \pm i$. On en déduit que φ est l'identité ou la conjugaison. Réciproquement, on vérifie que ces applications sont bien des morphismes de $\mathbb{R}$ -algèbres de $\mathbb{C}$ dans $\mathbb{C}$ et on conclut

Les morphismes de $\mathbb{R}$ -algèbres de $\mathbb{C}$ dans $\mathbb{C}$ sont l'identité et la conjugaison.