ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°82

Exercice 1 (*)

Soit $(\mathrm{A}, +, \times)$ un anneau tel que

$$\forall (x, y) \in \mathrm{A}^2 \qquad (x+y)^2 = x^2 + y^2$$

Montrer que l'anneau est commutatif

Corrigé : Soit $(x, y) \in \mathrm{A}^2$. On a

$$(x+y)^2 - (x^2+y^2) = xy + yx = 0$$

d'où $xy = -yx$. En particulier, pour $x = 1$, on trouve $y = -y$. Ainsi, il vient

$$\forall (x, y) \in \mathrm{A}^2 \qquad xy = -yx = yx$$

On conclut $\boxed{\text{L'anneau } (\mathrm{A}, +, \times) \text{ est commutatif.}}$

Exercice 2 (*)

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

1. Montrer que le triple $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un anneau commutatif.
2. Déterminer $\mathrm{U}(\mathbb{Z}[\mathrm{i}])$. On pourra considérer l'application $\mathrm{N} : \mathbb{C} \to \mathbb{R}, z \mapsto z\bar{z}$.
3. Déterminer le *corps des fractions* de $\mathbb{Z}[\mathrm{i}]$, c'est-à-dire l'ensemble

$$\left\{\frac{u}{v}, (u, v) \in \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}] \setminus \{0\}\right\}$$

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

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

et loi $\times$ est commutative. Ainsi

$$\boxed{\text{Le triplet } (\mathbb{Z}[\mathrm{i}], +, \times) \text{ est un anneau commutatif.}}$$

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

$$\forall (a, b) \in \mathbb{Z}^2 \qquad \mathrm{N}(a + \mathrm{i}b) = a^2 + b^2 \in \mathbb{N}$$

Soit $(a, b) \in \mathbb{Z}^2$ tel que $a + \mathrm{i}b \in \mathrm{U}(\mathbb{Z}[\mathrm{i}])$. Il existe $(c, d) \in \mathbb{Z}^2$ tel que $(a + \mathrm{i}b)(c + \mathrm{i}d) = 1$ et

$$\mathrm{N}((a + \mathrm{i}b)(c + \mathrm{i}d)) = \mathrm{N}(a + \mathrm{i}b)\mathrm{N}(c + \mathrm{i}d) = \mathrm{N}(1) = 1 \quad \Longrightarrow \quad (a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$$

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

L'inclusion réciproque est immédiate et on conclut

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

3. On vérifie sans difficulté que le corps des fractions $\mathbb{K}$ de $\mathbb{Z}[\mathrm{i}]$ est bien un corps en tant que sous-corps de $(\mathbb{C}, +, \times)$. On pose

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

Soit (a,b), (c,d) dans $\mathbb{Z}^2$ avec c ou d non nuls ce qui équivaut à dire $c + \mathrm{i}d \neq 0$. On a

$$\frac{a+\mathrm{i}b}{c+\mathrm{i}d} = \frac{(a+\mathrm{i}b)(c-\mathrm{i}d)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \mathrm{i}\frac{bc-ad}{c^2+d^2} \in \mathbb{Q}[i]$$

Réciproquement, un élément de $\mathbb{Q}[i]$ s'écrit $\dfrac{p_1}{q_1} + \mathrm{i}\dfrac{p_2}{q_2}$ avec (p_1,p_2) dans $\mathbb{Z}^2$ et (q_1,q_2) dans $(\mathbb{N}^*)^2$.

Il vient
$$\frac{p_1}{q_1} + \mathrm{i}\frac{p_2}{q_2} = \frac{p_1q_2 + \mathrm{i}p_2q_1}{q_1q_2} \in \mathbb{K}$$

On conclut
$$\boxed{\mathbb{K} = \mathbb{Q}[\mathrm{i}]}$$

Exercice 3 (*)

Décrire les morphismes d'anneaux $f : \mathbb{C} \to \mathbb{C}$ tels que $f(x) = x$ pour tout $x \in \mathbb{R}$.

Corrigé : Soit f un tel morphisme. On a $f(\mathrm{i})^2 = f(\mathrm{i}^2) = f(-1) = -1$ d'où $f(\mathrm{i}) \in \{\mathrm{i}, -\mathrm{i}\}$. Il s'ensuit

$$\forall (x,y) \in \mathbb{R}^2 \qquad f(x+\mathrm{i}y) = f(x) + f(\mathrm{i})f(y) = x \pm \mathrm{i}y$$

ce qui prouve que f est l'identité ou la conjugaison. La réciproque est immédiate. On conclut

$$\boxed{f = \mathrm{id} \text{ ou } f = z \mapsto \bar{z}}$$

Exercice 4 (*)

Un corps $(\mathbb{K}, \times, +)$ est dit *algébriquement clos* si tout polynôme à coefficients dans $\mathbb{K}$ de degré supérieur ou égal à un admet une racine dans $\mathbb{K}$.

1. Déterminer parmi $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ les corps algébriquement clos.
2. Un corps fini peut-il être algébriquement clos ?

Corrigé : Le corps $\mathbb{Q}$ n'est pas algébriquement clos puisque le polynôme $\mathrm{X}^2 - 2$ n'admet pas de racine dans $\mathbb{Q}$. Le corps $\mathbb{R}$ n'est pas algébriquement clos puisque le polynôme $\mathrm{X}^2 + 1$ n'admet pas de racine réelle. En revanche, d'après le théorème de d'Alembert-Gauss, tout polynôme non constant de $\mathbb{C}[\mathrm{X}]$ admet une racine complexe ce qui prouve que le corps $\mathbb{C}$ est algébriquement clos.

2. Soit $\mathbb{K}$ un corps fini. On considère $\mathrm{P} = 1 + \prod_{\alpha \in \mathbb{K}} (\mathrm{X} - \alpha)$. Le polynôme P ne s'annule en aucun point de $\mathbb{K}$ et par conséquent

$$\boxed{\text{Un corps fini ne peut être algébriquement clos.}}$$

Exercice 5 (*)

Un *morphisme de corps* est un morphisme d'anneaux entre deux corps (commutatifs, conformément au programme). Montrer qu'un tel morphisme est injectif.

Corrigé : Soit $\varphi : \mathbb{K} \to \mathbb{K}'$ un morphisme de corps. Le noyau $\mathrm{Ker}\ \varphi$ est un idéal de $\mathbb{K}$ distinct de $\mathbb{K}$ puisque $\varphi(1) = 1 \neq 0$ car un corps est, par définition, un anneau non nul. Comme les idéaux d'un corps sont triviaux, on conclut que $\mathrm{Ker}\ \varphi = \{0\}$ d'où

$$\boxed{\text{Un morphisme de corps est injectif.}}$$

Exercice 6 (**)

On note $\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3},\ (a,b) \in \mathbb{Z}^2\right\}$ muni des opérations $+$ et $\times$.

1. Montrer que $(\mathbb{Z}[\sqrt{3}], +, \times)$ est un anneau commutatif.
2. Déterminer le plus petit corps inclus dans $\mathbb{R}$ contenant $\mathbb{Z}[\sqrt{3}]$.

Corrigé : 1. On a $1 = 1 + 0\sqrt{n} \in \mathbb{Z}[\sqrt{3}]$. Pour (a,b) et (c,d) dans $\mathbb{Z}^2$, il vient

$$a + b\sqrt{3} - (c + d\sqrt{3}) = a - c + (b-d)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

et

$$(a + b\sqrt{3})(c + d\sqrt{3}) = ac + 3bd + (bd + ac)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

ce qui prouve que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de l'anneau commutatif $(\mathbb{R}, +, \times)$. Ainsi

$$\boxed{\text{Le triplet } (\mathbb{Z}[\sqrt{3}], +, \times) \text{ est un anneau commutatif.}}$$

2. On pose

$$\mathbb{Q}[\sqrt{3}] = \left\{a + b\sqrt{3},\ (a,b) \in \mathbb{Q}^2\right\}$$

L'ensemble $\mathbb{Q}[\sqrt{3}]$ est clairement un sous-groupe de $(\mathbb{R}, +)$ et contient 1. Soient (a,b) et (c,d) dans $\mathbb{Q}^2$. On a

$$(a + b\sqrt{3})(c + d\sqrt{3}) = ac + 3bd + (ad + bc)\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$

ce qui prouve que $\mathbb{Q}[\sqrt{3}]$ est un sous-anneau du corps $(\mathbb{R}, +, \times)$ et est par conséquent un anneau commutatif. Soit $(a,b) \in \mathbb{Q}^2$ tel que $a + b\sqrt{3} \neq 0$. En multipliant par la quantité conjuguée, on trouve

$$(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$$

Supposons $a^2 - 3b^2 = 0$. Si $b = 0$, alors $a = 0$ ce qui est exclu car $a + b\sqrt{3} \neq 0$. Ainsi, on a $b \neq 0$ et $a \pm b\sqrt{3} = 0$ ce qui prouve que $\sqrt{3}$ est rationnel, ce qui est faux. On a donc $a^2 - 3b^2 \neq 0$ puis

$$(a + b\sqrt{3})\left(\frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}\right) = 1$$

ce qui prouve que tout élément non nul de $\mathbb{Q}[\sqrt{3}]$ est inversible. Ainsi, l'ensemble $\mathbb{Q}[\sqrt{3}]$ est un corps contenant clairement $\mathbb{Z}[\sqrt{3}]$. Enfin, soit $(\mathbb{K}, +, \times)$ un corps avec $\mathbb{Z}[\sqrt{3}] \subset \mathbb{K}$. Pour a, b entiers relatifs et c, d entiers non nuls, le produit cd est un entier non nul qui admet donc un inverse dans $\mathbb{K}$ et

$$\frac{a}{c} + \frac{b}{d}\sqrt{3} = \frac{ad + bc\sqrt{3}}{cd} \in \mathbb{K}$$

ce qui prouve $\mathbb{Q}[\sqrt{3}] \subset \mathbb{K}$. On conclut

$$\boxed{\text{Le triplet } (\mathbb{Q}[\sqrt{3}], +, \times) \text{ est le plus petit sous-corps de } (\mathbb{R}, +, \times) \text{ contenant } \mathbb{Z}[\sqrt{3}].}$$

Exercice 7 (**)

Montrer que tout anneau intègre fini est un corps.

Corrigé : Soit $(\mathrm{A}, +, \times)$ un anneau intègre fini et $a \in \mathrm{A} \setminus \{0\}$. On pose $\varphi : \mathrm{A} \to \mathrm{A},\ x \mapsto ax$. L'application φ est un morphisme de groupes additifs puisque par distributivité

$$\forall (x,y) \in \mathrm{A}^2 \qquad \varphi(x+y) = \varphi(x) + \varphi(y)$$

Soit $x \in \text{Ker } \varphi$. Par intégrité, comme $ax = 0$ et $a \neq 0$, il vient $x = 0$ d'où $\text{Ker } \varphi = \{0\}$ ce qui prouve l'injectivité de φ. Le morphisme φ est donc une application injective de A fini dans lui-même. Par conséquent, l'application φ est bijective et donc surjective ce qui prouve l'existence de $b \in \text{A}$ tel que $\varphi(b) = 1$, autrement dit $ab = 1$. L'élément b est un inverse à droite et donc également à gauche par commutativité de $\times$ ce qui prouve l'inversibilité de a. On conclut

Tout anneau intègre fini est un corps.

Variante : Soit $a \in \text{A} \setminus \{0\}$. La suite $(a^n)_n$ est à valeurs dans A fini d'où l'existence d'entiers m et n avec $m < n$ tels que $a^m = a^n$ et par suite $a^m(a^{n-m} - 1) = 0$ d'où par intégrité $aa^{n-m-1} = 1$ et le résultat suit.

Exercice 8 (**)

Soit $(\mathbb{K}, +, \times)$ un corps. Montrons qu'un polynôme de $\mathbb{K}[\text{X}]$ de degré n entier admet au plus n racines distinctes.

Corrigé : On procède par récurrence sur le degré de n. L'initialisation pour $n = 0$ est immédiate. Soit $\text{P} = \sum_{k=0}^{n} a_k \text{X}^k$ avec n entier non nul et $a_n \in \mathbb{K}^*$. Soit $\alpha \in \mathbb{K}$ tel que $\text{P}(\alpha) = 0$. Il vient pour $x \in \mathbb{K}$

$$\text{P}(x) = 0 \iff \text{P}(x) - \text{P}(\alpha) = 0 \iff \sum_{k=1}^{n} a_k(x^k - \alpha^k) = 0 \iff (x - \alpha)\sum_{k=1}^{n} a_k \sum_{\ell=0}^{k-1} x^\ell \alpha^{k-1-\ell} = 0$$

Ainsi, pour x racine de P avec $x \neq \alpha$, il vient par intégrité

$$\text{P}(x) = 0 \iff \text{Q}(x) = 0 \quad \text{avec} \quad \text{Q} = \sum_{k=1}^{n} a_k \sum_{\ell=0}^{k-1} \text{X}^\ell \alpha^{k-1-\ell}$$

et le polynôme Q admet au plus $n - 1$ racines distinctes par hypothèse de récurrence. Ainsi

Un polynôme de $\mathbb{K}[\text{X}]$ de degré n admet au plus n racines distinctes.

Remarque : La preuve classique est également une preuve par récurrence qui utilise le fait suivant : pour $\text{P} \in \mathbb{K}[\text{X}]$ et $\alpha \in \mathbb{K}$, on a $\text{P}(\alpha) = 0$ si et seulement si $\text{X} - \alpha$ divise P. Le sens indirect est immédiat mais le sens direct requiert le théorème de la division euclidienne. Ce théorème existe dans l'anneau de polynômes $(\mathbb{K}[\text{X}], +, \times)$ avec $\mathbb{K}$ un corps (commutatif, conformément au programme) qui n'est pas forcément $\mathbb{R}$ ou $\mathbb{C}$, par exemple $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Mais si on veut l'invoquer, il faudrait en toute rigueur savoir réécrire sa preuve ce qui n'est pas trivial.

Exercice 9 (**)

Montrer que les anneaux $(\mathbb{Z}^n, +, \times)$ avec n entier non nul sont deux à deux non isomorphes.

Corrigé : Soit $(m, n) \in (\mathbb{N}^*)^2$. Supposons qu'il existe $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ isomorphisme d'anneaux.

On a $$\text{U}(\mathbb{Z}^n) = \{-1, 1\}^n$$

Comme l'application φ est un morphisme d'anneaux, on a $\varphi(\text{U}(\mathbb{Z}^n)) \subset \text{U}(\mathbb{Z}^m)$ et $\varphi^{-1}(\text{U}(\mathbb{Z}^m)) \subset \text{U}(\mathbb{Z}^n)$ avec l'isomorphisme réciproque. Ceci prouve que φ réalise une bijection de $\text{U}(\mathbb{Z}^n)$ sur $\text{U}(\mathbb{Z}^m)$. Ces deux ensembles finis ont donc même cardinal d'où $2^n = 2^m$ et par suite $n = m$. On conclut

Les anneaux $(\mathbb{Z}^n, +, \times)$ avec n entier non nul sont deux à deux non isomorphes.

Exercice 10 (**)

Soit $(\mathrm{A}, +, \times)$ un anneau non commutatif et $a \in \mathrm{A}$ qui possède un inverse à droite et un seul. Montrer que a possède un inverse à gauche.

Corrigé : Soit $b \in \mathrm{A}$ tel que $ab = 1$. Il vient $aba = a$ puis $a(ba - 1) = 0$ d'où $a(ba - 1) + ab = 1$ autrement dit $a(ba - 1 + b) = 1$. Par unicité de l'inverse à droite, on trouve $ba - 1 + b = b$ d'où $ba = 1$ ce qui prouve

Dans un anneau non commutatif, l'inversibilité à droite avec unicité implique l'inversibilité à gauche.