ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°82

Exercice 1 (*)

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

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

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

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

$$\forall a \in \mathrm{A} \qquad a(x - y) = ax - ay = xa - ya = (x - y)a$$

d'où $x - y \in \mathrm{Z(A)}$ et

$$\forall a \in \mathrm{A} \qquad a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$$

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

Exercice 2 (*)

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 3 (*)

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 $\operatorname{Ker} \varphi$ 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 $\operatorname{Ker} \varphi = \{0\}$ d'où

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

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

2. Soit $\mathbb{K}$ un corps fini. On considère $P = 1 + \prod_{\alpha \in \mathbb{K}} (X - \alpha)$. 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 (**)

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

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

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

$$a + b\sqrt{2} - (c + d\sqrt{2}) = a - c + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

et
$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + bdn + (bd + ac)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

ce qui prouve que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de l'anneau commutatif $(\mathbb{R}, +, \times)$. Ainsi

$$\boxed{\text{Le triplet } (\mathbb{Z}[\sqrt{2}], +, \times) \text{ est un anneau commutatif.}}$$

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

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

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

ce qui prouve que $\mathbb{Q}[\sqrt{2}]$ 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 $a + b\sqrt{2} \neq 0$. En multipliant par la quantité conjuguée, on trouve

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

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

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

ce qui prouve que tout élément non nul de $\mathbb{Q}[\sqrt{2}]$ est inversible. Ainsi, l'ensemble $\mathbb{Q}[\sqrt{2}]$ est un corps contenant clairement $\mathbb{Z}[\sqrt{2}]$. Enfin, soit $(\mathbb{K}, +, \times)$ un corps avec $\mathbb{Z}[\sqrt{2}] \subset \mathbb{K}$. Pour a, b entiers relatifs et c, d entiers non nuls, le ppcm $c \vee d$ est un entier non nul qui admet donc un inverse dans $\mathbb{K}$ et

$$\frac{a}{c} + \frac{b}{d}\sqrt{2} = \frac{a(c \vee d) + b(c \vee d)\sqrt{2}}{c \vee d} \in \mathbb{K}$$

ce qui prouve $\mathbb{Q}[\sqrt{2}] \subset \mathbb{K}$. On conclut

$$\boxed{\text{Le triplet } (\mathbb{Q}[\sqrt{2}], +, \times) \text{ est le plus petit sous-corps de } (\mathbb{R}, +, \times) \text{ contenant } \mathbb{Z}[\sqrt{2}].}$$

Exercice 6 (**)

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 $x \in \operatorname{Ker} \varphi$. Par intégrité, comme $ax = 0$ et $a \neq 0$, il vient $x = 0$ d'où $\operatorname{Ker} \varphi = \{0\}$ 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 $b \in \mathrm{A}$ 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

$$\boxed{\text{Tout anneau intègre fini est un corps.}}$$

Exercice 7 (**)

Soit $(\mathbb{K}, +, \times)$ un corps. Montrons qu'un polynôme de $\mathbb{K}[\mathrm{X}]$ 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 $\mathrm{P} = \sum\limits_{k=0}^{n} a_k \mathrm{X}^k$ avec n entier non nul et $a_n \in \mathbb{K}^*$. Soit $\alpha \in \mathbb{K}$ tel que $\mathrm{P}(\alpha) = 0$. Il vient pour $x \in \mathbb{K}$

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

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

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

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

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

Remarque : La preuve classique est également une preuve par récurrence qui utilise le fait suivant : pour $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ et $\alpha \in \mathbb{K}$, on a $\mathrm{P}(\alpha) = 0$ si et seulement si $\mathrm{X} - \alpha$ 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 $(\mathbb{K}[\mathrm{X}], +, \times)$ 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 8 (**)

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
$$\mathrm{U}(\mathbb{Z}^n) = \{-1, 1\}^n$$

Comme l'application φ est un morphisme d'anneaux, on a $\varphi(\mathrm{U}(\mathbb{Z}^n)) \subset \mathrm{U}(\mathbb{Z}^m)$ et $\varphi^{-1}(\mathrm{U}(\mathbb{Z}^m)) \subset \mathrm{U}(\mathbb{Z}^n)$ avec l'isomorphisme réciproque. Ceci prouve que φ réalise une bijection de $\mathrm{U}(\mathbb{Z}^n)$ sur

$\mathrm{U}(\mathbb{Z}^m)$. Ces deux ensembles finis ont donc même cardinal d'où $2^n = 2^m$ et par suite $n = m$. On conclut

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

Exercice 9 (**)

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

$$\boxed{\text{Dans un anneau non commutatif, l'inversibilité à droite avec unicité implique l'inversibilité à gauche.}}$$

Exercice 10 (**)

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

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

1. Établir $\qquad \forall (x, y) \in \mathrm{A}^2 \qquad xyx = x^2 y = yx^2$
2. En déduire que l'anneau $(\mathrm{A}, +, \times)$ est commutatif.

Corrigé : 1. Soit $(x, y) \in \mathrm{A}^2$. On a

$$\big(x(y+1)\big)^2 = x^2 (y+1)^2 = x^2 y^2 + 2x^2 y + x^2$$

et
$$\big(x(y+1)\big)^2 = (xy + x)^2 = (xy)^2 + xyx + x^2 y + x^2$$

d'où par soustraction
$$x^2 y = xyx$$

Puis
$$\big((y+1)x\big)^2 = (y+1)^2 x^2 = (y^2 + 2y + 1)x^2 = y^2 x^2 + 2yx^2 + x^2$$

et
$$\big((y+1)x\big)^2 = (yx + x)^2 = (yx)^2 + yx^2 + xyx + x^2$$

d'où par soustraction
$$yx^2 = xyx$$

On conclut
$$\boxed{\forall (x, y) \in \mathrm{A}^2 \qquad xyx = x^2 y = yx^2}$$

2. Soit $(x, y) \in \mathrm{A}^2$. Il vient

$$(x+1)y(x+1) = (xy + y)(x+1) = xyx + xy + yx + y$$

et
$$(x+1)^2 y = (x^2 + 2x + 1)y = x^2 y + 2xy + y$$

d'où
$$xy + yx - 2xy = yx - xy = 0$$

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

Remarque : Finalement, une seule des égalités de la première question permet de conclure avec des rôles dissymétriques en x et y, ce qui est un peu déroutant ...