ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°83

Exercice 1 (**)

Soit I un idéal d'un anneau commutatif $(\mathrm{A}, +, \times)$. On définit le *radical* de I noté R(I) par

$$\mathrm{R(I)} = \left\{ x \in \mathrm{A} \mid \exists k \in \mathbb{N}^* \ : \ x^k \in \mathrm{I} \right\}$$

1. Montrer que R(I) est un idéal de A contenant I.
2. On suppose $\mathrm{A} = \mathbb{Z}$. Déterminer l'ensemble des entiers n non nuls tels que $\mathrm{R}(n\mathbb{Z}) = n\mathbb{Z}$.

Corrigé : 1. On a $0 \in \mathrm{R(I)}$ puisque $0^1 = 0 \in \mathrm{I}$. Soit $(x, y) \in \mathrm{R(I)}^2$. Il existe des entiers non nuls n et m tels que $x^n \in \mathrm{I}$ et $y^m \in \mathrm{I}$. On rappelle que dans un anneau, on a $(-y)^k = (-1)^k y^k$ pour tout k entier. Puis

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} (-1)^{n+m-k} x^k y^{n+m-k}$$

Pour $k \geqslant n$, on a $$x^k y^{n+m-k} = \underbrace{x^n}_{\in \mathrm{I}} \underbrace{x^{k-n} y^{n+m-k}}_{\in \mathrm{A}} \in \mathrm{I}$$

et pour $k < n$ $$x^k y^{n+m-k} = \underbrace{y^m}_{\in \mathrm{I}} \underbrace{x^k y^{n-k}}_{\in \mathrm{A}} \in \mathrm{I}$$

par absorption, les expressions précédentes ayant du sens puisque $k - n \geqslant 0$ pour $k \geqslant n$ et $n - k \geqslant 0$ pour $k < n$. Comme l'idéal I est sous-groupe de $(\mathrm{A}, +)$, on en déduit $(x-y)^{n+m} \in \mathrm{I}$ d'où $x - y \in \mathrm{R(I)}$. Enfin, pour $(x, a) \in \mathrm{R(I)} \times \mathrm{A}$ et n entier non nul tel que $x^n \in \mathrm{I}$, on a $(xa)^n = x^n a^n \in \mathrm{I}$ par absorption et pour $y \in \mathrm{I}$, on a $y^1 = y \in \mathrm{I}$ d'où

$$\boxed{\text{Le radical R(I) est un idéal de } (\mathrm{A}, +, \times) \text{ contenant I.}}$$

2. On a clairement $\mathrm{R}(\mathbb{Z}) = \mathbb{Z}$. Soit n entier avec $n \geqslant 2$ tel que $\mathrm{R}(n\mathbb{Z}) = n\mathbb{Z}$. On note $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. S'il existe un $\alpha_i > 1$, par exemple $\alpha_1 \geqslant 2$, on pose $x = p_1^{\alpha_1 - 1} \prod_{i=2}^{r} p_i^{\alpha_i}$. On a $n \nmid x$ mais $n | x^2$ puisque

$$\alpha_1 \leqslant 2(\alpha_1 - 1) \iff 2 \leqslant \alpha_1$$

Par conséquent, on aurait $\mathrm{R}(n\mathbb{Z}) \neq n\mathbb{Z}$. L'égalité supposée implique donc que n est sans facteur carré. Supposons $n = \prod_{i=1}^{r} p_i$. Soit $x \in \mathrm{R}(n\mathbb{Z})$ et k entier non nul tel que $n | x^k$. Il s'ensuit $p_i | x^k$ puis $p_i | x$ pour tout $i \in [\![1 \,;\, r]\!]$ d'où $\prod_{i=1}^{r} p_i | x$. On conclut

$$\boxed{\text{Les entiers } n \text{ non nuls tels que } \mathrm{R}(n\mathbb{Z}) = n\mathbb{Z} \text{ sont ceux sans facteur carré.}}$$

Variante : Notant $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls, on peut aussi établir $\mathrm{R}(n\mathbb{Z}) = \left(\prod_{i=1}^{r} p_i \right) \mathbb{Z}$. Soit $x \in \mathrm{R}(n\mathbb{Z})$. On dispose de k entier non nul tel que $n | x^k$. Comme les p_i divisent n et qu'ils sont premiers entre eux, alors $\prod_{i=1}^{r} p_i$ divise n

d'où une première inclusion. Réciproquement, si $x = m\prod_{i=1}^{r} p_i$ avec m entier, alors $x^k \in n\mathbb{Z}$ avec $k = \underset{i\in[\![1\,;r]\!]}{\text{Max}}\ \alpha_i$ ce qui prouve l'autre inclusion. Enfin, si on a $a\mathbb{Z} = b\mathbb{Z}$ avec a, b entiers naturels, alors a et b sont associés et comme ce sont des entiers naturels, il sont égaux. On a donc l'unicité d'un générateur entier naturel d'un idéal de $\mathbb{Z}$. On retrouve le résultat précédent.

Exercice 2 (***)

On note $$\mathbb{D} = \left\{\frac{p}{10^n},\ (p,n) \in \mathbb{Z}\times\mathbb{N}\right\}$$ l'ensemble des nombres décimaux.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q},+,\times)$.
2. Montrer que les idéaux de $(\mathbb{D},+,\times)$ sont de la forme $a\mathbb{D}$ avec $a \in \mathbb{D}$.

Corrigé : 1. On a $1 = \dfrac{1}{10^0} \in \mathbb{D}$. Pour $(x,y) \in \mathbb{D}^2$, on a $x = \dfrac{p}{10^n}$ et $y = \dfrac{q}{10^m}$ avec $(p,q,n,m) \in \mathbb{Z}^2\times\mathbb{N}^2$ puis

$$x+y = \frac{p}{10^n} + \frac{q}{10^m} = \frac{10^m p + 10^n q}{10^{n+m}} \in \mathbb{D} \quad \text{et} \quad xy = \frac{p}{10^n}\frac{q}{10^m} = \frac{pq}{10^{n+m}} \in \mathbb{D}$$

Ainsi $$\boxed{\text{L'ensemble } \mathbb{D} \text{ est un sous-anneau de } (\mathbb{Q},+,\times).}$$

2. Soit I un idéal de $(\mathbb{D},+,\times)$. Comme I et $\mathbb{Z}$ sont des sous-groupes de $(\mathbb{D},+)$, alors $\mathrm{I}\cap\mathbb{Z}$ a une structure de groupe donc est un sous-groupe de de $(\mathbb{Z},+)$. Ainsi, il existe $a \in \mathbb{N}$ tel que $\mathrm{I}\cap\mathbb{Z} = a\mathbb{Z}$. Comme $a \in \mathrm{I}$, on a par absorption $a\mathbb{D} \subset \mathrm{I}$. Réciproquement, soit $x \in \mathrm{I}$, il existe n entier tel que $10^n x \in \mathbb{Z}$ et par absorption $10^n x \in \mathrm{I}\cap\mathbb{Z} = a\mathbb{Z}$ d'où $10^n x = ap$ avec $p \in \mathbb{Z}$ et donc $x \in a\mathbb{D}$. On conclut

$$\boxed{\text{Pour tout idéal I de } (\mathbb{D},+,\times), \text{ il existe } a \in \mathbb{D} \text{ tel que } \mathrm{I} = a\mathbb{D}.}$$

Exercice 3 (***)

Soit $(\mathrm{A},+,\times)$ un anneau intègre. On suppose que cet anneau n'a qu'un nombre fini d'idéaux. Montrer que $(\mathrm{A},+,\times)$ est un corps.

Corrigé : Soit $x \in \mathrm{A}\setminus\{0_\mathrm{A}\}$. La famille d'idéaux $(x^n\mathrm{I})_n$ est finie donc il existe des entiers $p<q$ tel que $x^p\mathrm{A} = x^q\mathrm{A}$. Par suite, il existe $a \in \mathrm{A}$ tel que $x^p = x^q a$ d'où $x^p(1_\mathrm{A} - x^{q-p}a) = 0_\mathrm{A}$. Par récurrence, comme $x \neq 0_\mathrm{A}$, on montre $x^p \neq 0_\mathrm{A}$ par intégrité puis on trouve $x^{q-p}a = 1_\mathrm{A}$ d'où $xx^{q-p-1}a = 1_\mathrm{A}$. Ainsi, tout élément non nul de A est inversible et on conclut

$$\boxed{\text{Le triplet } (\mathrm{A},+,\times) \text{ est un corps.}}$$

Exercice 4 (***)

Soit $n \in \mathbb{N}$ qui n'est pas un carré. On pose

$$\mathrm{A} = \{a+b\sqrt{n}, (a,b) \in \mathbb{Z}^2\} \quad \text{et} \quad \mathrm{C} = \{\alpha+\beta\sqrt{n}, (\alpha,\beta) \in \mathbb{Q}^2\}$$

1. Montrer que $(\mathrm{A},+,\times)$ est un anneau et que C est son corps des fractions.
2. Déterminer tous les automorphismes du corps $(\mathrm{C},+,\times)$.

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

$$a + b\sqrt{n} - (c + d\sqrt{n}) = a - c + (b - d)\sqrt{n} \in \mathrm{A}$$

et

$$(a + b\sqrt{n})(c + d\sqrt{n}) = ac + bdn + (bd + ac)\sqrt{n} \in \mathrm{A}$$

ce qui prouve que A est un sous-anneau de $(\mathbb{R}, +, \times)$. Le corps des fractions de A est défini par

$$\mathrm{D} = \left\{ \frac{u}{v}, (u, v) \in \mathrm{A} \times \mathrm{A} \setminus \{0\} \right\}$$

On a clairement $\mathrm{C} \subset \mathrm{D}$. Soit $u = a + b\sqrt{n}$ et $v = c + d\sqrt{n}$ avec (a, b), (c, d) dans $\mathbb{Z}^2$ et $v \neq 0$. En multipliant par la quantité conjuguée, on trouve

$$(c + d\sqrt{n})\,(c - d\sqrt{n}) = c^2 - nd^2$$

Supposons $c^2 - nd^2 = 0$. Si $d = 0$, alors $c = 0$ ce qui est exclu car $c + d\sqrt{n} \neq 0$. ainsi, on a $d \neq 0$ et $c \pm d\sqrt{n} = 0$ ce qui prouve que $\sqrt{n}$ est rationnel ce qui est faux puisque n n'est pas un carré. En effet, si on a avait $\sqrt{n} = \pm \dfrac{c}{d}$, on aurait $nd^2 = c^2$ d'où $1 + 2v_p(d) = 2v_p(c)$ pour p un nombre premier présent dans la décomposition de n. Ainsi

$$\frac{u}{v} = \frac{a + b\sqrt{n}}{c + d\sqrt{n}} = \frac{(a + b\sqrt{n})(c - d\sqrt{n})}{c^2 - nd^2} = \frac{ac - bdn}{c^2 - nd^2} + \frac{bc - ad}{c^2 - nd^2}\sqrt{n} \in \mathrm{C}$$

On conclut

Le triplet $(\mathrm{A}, +, \times)$ est un anneau et C son corps des fractions.

2. Soit $\varphi : \mathrm{C} \to \mathrm{C}$ un morphisme de corps. On a tout d'abord $\varphi(1) = 1$. Par morphisme, il vient $\varphi(k) = k\varphi(1) = k$ pour tout $k \in \mathbb{Z}$. Pour $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a

$$\varphi\left(q\frac{p}{q}\right) = \varphi(p) = p = q\varphi\left(\frac{p}{q}\right)$$

d'où

$$\forall r \in \mathbb{Q} \qquad \varphi(r) = r$$

Ainsi, pour $(\alpha, \beta) \in \mathbb{Q}^2$, il vient

$$\varphi(\alpha + \beta\sqrt{n}) = \alpha + \beta\varphi(\sqrt{n})$$

et

$$n = \varphi(n) = \varphi\left(\sqrt{n}^2\right) = \left(\varphi\left(\sqrt{n}\right)\right)^2 \quad \Longrightarrow \quad \varphi\left(\sqrt{n}\right) \in \{-\sqrt{n}, \sqrt{n}\}$$

Soient (α, β) et (λ, μ) dans $\mathbb{Q}^2$ tels que $\alpha + \beta\sqrt{n} = \lambda + \mu\sqrt{n}$. On a $\alpha - \lambda = (\mu - \beta)\sqrt{n}$. Si $\mu - \beta \neq 0$, alors $\sqrt{n}$ est rationnel ce qui est faux d'où $\beta = \mu$ et $\alpha = \lambda$. Par conséquent, l'écriture d'un élément de C est unique. Pour $\varepsilon \in \{-1, 1\}$, on peut donc définir

$$\varphi : \begin{cases} \mathrm{C} & \longrightarrow \mathrm{C} \\ \alpha + \beta\sqrt{n} & \longmapsto \alpha + \varepsilon\beta\sqrt{n} \end{cases}$$

Sans difficulté, on vérifie que φ est un morphisme de corps et même un automorphisme de corps. On conclut

Les automorphismes du corps $\mathbb{C}$ sont l'identité et la conjugaison $\alpha + \beta\sqrt{n} \mapsto \alpha - \beta\sqrt{n}$.

Exercice 5 (***)

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

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

1. Décrire les idéaux premiers de $(\mathbb{Z}, +, \times)$.

2. Montrer que si l'anneau $(\mathrm{A}, +, \times)$ est commutatif et si tous ses idéaux sont premiers, alors $(\mathrm{A}, +, \times)$ est un corps.

Corrigé : 1. Soit I idéal premier de $(\mathbb{Z}, +, \times)$. On suppose $\mathrm{I} \neq \{0\}$ sinon c'est immédiat par intégrité de $\mathbb{Z}$. Il existe p entier non nul tel que $\mathrm{I} = p\mathbb{Z}$. Si $p = ab$ avec a et $b > 1$, alors $ab \in p\mathbb{Z}$ et $a \notin p\mathbb{Z}$, $b \notin p\mathbb{Z}$. On a donc nécessairement p premier. Supposons p premier. Soient a et b dans $\mathbb{Z}$ tels que $p|ab$. D'après le lemme d'Euclide, on a $p|a$ ou $p|b$ ce qui prouve que I est un idéal premier. Ainsi

Les idéaux premiers de $(\mathbb{Z}, +, \times)$ sont exactement les $p\mathbb{Z}$ avec $p \in \mathcal{P}$.

2. L'idéal trivial $\{0\}$ est premier d'où l'intégrité de $(\mathrm{A}, +, \times)$. Soit $x \in \mathrm{A} \setminus \{0\}$. L'idéal $x^2\mathrm{A}$ est premier et $x^2 \in x^2\mathrm{A}$ d'où $x \in x^2\mathrm{A}$ ce qui prouve qu'il existe $y \in \mathrm{A}$ tel que $x = x^2y$, *i.e.* $x(xy - 1) = 0$ et par intégrité $xy = 1$ puisque $x \neq 0$. Tout élément non nul de A est inversible et on conclut

Un anneau commutatif dont tous les idéaux sont premiers est un corps.

Exercice 6 (****)

Déterminer les endomorphismes du corps $(\mathbb{R}, +, \times)$.

Corrigé : Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps. On a tout d'abord $f(1) = 1$. Par morphisme, il vient $f(k) = k$ pour tout $k \in \mathbb{Z}$. Pour $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a

$$f\left(q\frac{p}{q}\right) = f(p) = p = qf\left(\frac{p}{q}\right)$$

d'où $$\forall r \in \mathbb{Q} \qquad f(r) = r$$

Pour $x \geqslant 0$, on trouve $$f(x) = f\left(\left(\sqrt{x}\right)^2\right) = \left(f\left(\sqrt{x}\right)\right)^2 \geqslant 0$$

Ainsi, pour $(x, y) \in \mathbb{R}^2$ avec $x \leqslant y$, il vient

$$f(y) - f(x) = f(y - x) \geqslant 0$$

ce qui prouve que l'application f est croissante. Enfin pour x réel et $\varepsilon > 0$, par densité de $\mathbb{Q}$ dans $\mathbb{R}$, on peut trouver des rationnels a et b tels que $a \leqslant x \leqslant b$ et $b - a \leqslant \varepsilon$. Ainsi, par croissance de f, il vient

$$a = f(a) \leqslant f(x) \leqslant f(b) = b$$

d'où $$-(b - a) \leqslant f(x) - x \leqslant b - a$$

Ainsi $$\forall \varepsilon > 0 \qquad |f(x) - x| \leqslant \varepsilon$$

ce qui prouve $f(x) = x$. On conclut

L'unique endomorphisme du corps $(\mathbb{R}, +, \times)$ est l'identité.

Exercice 7 (***)

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

1. Montrer que $f_\mathrm{A} : \mathbb{Z} \to \mathrm{A}, k \mapsto k1_\mathrm{A}$ est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A. Montrer qu'il existe $k_\mathrm{A} \in \mathbb{N}$ tel que $\mathrm{Ker}\ f_\mathrm{A} = k_\mathrm{A}\mathbb{Z}$.

2. On suppose que A est un corps. Montrer que $k_A = 0$ ou que k_A est premier. Étudier la réciproque.
   On suppose que A est un corps fini et on admet que $|A| = p^n$ avec p premier et $n \in \mathbb{N}^*$.
3. Soit $\varphi : A \to A, x \mapsto x^p$. Montrer que φ est un automorphisme de A. Déterminer l'ordre de φ dans $(\mathrm{Aut}(A), \circ)$.

Corrigé : 1. Soit $f : \mathbb{Z} \to A$ un morphisme d'anneaux. On a $f(1) = 1_A$ puis $f(k) = kf(1) = k1_A$ (résultat de cours qu'on redémontre au besoin avec une récurrence pour $k \in \mathbb{N}$ et pour $-k \in \mathbb{N}$). Ainsi, on a $f = f_A$ et on vérifie sans difficulté qu'il s'agit bien d'un morphisme d'anneaux. Par conséquent

$$\boxed{\text{L'application } f_A \text{ est l'unique morphisme d'anneaux de } \mathbb{Z} \text{ dans A.}}$$

En particulier, le morphisme d'anneaux f_A est un morphisme de groupes additifs. Par conséquent, les notions de noyaux de morphismes d'anneaux et de groupes coïncidant, le noyau $\mathrm{Ker}\, f_A$ est un sous-groupe de $(\mathbb{Z}, +)$ et on conclut

$$\boxed{\text{Il existe } k_A \text{ entier tel que } \mathrm{Ker}\, f_A = k_A\mathbb{Z}}$$

Remarque : L'entier k_A est appelé *caractéristique de l'anneau* A.

2. Supposons $k_A \notin \{0\} \cup \mathcal{P}$. Si $k_A = 1$, alors $1_A = 0_A$ et l'anneau A serait nul, ce qui est absurde. Sinon, on dispose alors de a et b entiers non nuls diviseurs stricts de $ab = k_A$ et qui ne sont donc pas dans $\mathrm{Ker}\, f_A = k_A\mathbb{Z}$. Par suite

$$f_A(a)f_A(b) = f_A(ab) = f_A(k_A) = 0_A \quad \text{avec} \quad f_A(a) \neq 0_A \quad \text{et} \quad f_A(b) \neq 0_A$$

ce qui contredit l'intégrité du corps A. On conclut

$$\boxed{\text{Si A est un corps, alors } k_A \in \{0\} \cup \mathcal{P}.}$$

Avec $A = \mathbb{Z}$, on a $k_A = 0$ mais l'anneau $\mathbb{Z}$ n'est pas un corps. Avec $A = (\mathbb{Z}/2\mathbb{Z})^2$, on a $k_A = 2$ mais l'anneau $(\mathbb{Z}/2\mathbb{Z})^2$ n'est pas intègre en observant par exemple

$$(\bar{1}, \bar{0}) \times (\bar{0}, \bar{1}) = (\bar{0}, \bar{0})$$

On conclut $\boxed{\text{La réciproque est fausse.}}$

3. En considérant f_A comme morphisme de groupes, on a $\mathrm{Im}\, f_A = \langle 1_A \rangle$. Si $k_A = 0$, alors on a $\langle 1_A \rangle \simeq \mathbb{Z}$ qui est donc infini ce qui absurde. On en déduit $k_A \in \mathcal{P}$ et $\langle 1_A \rangle \simeq \mathbb{Z}/k_A\mathbb{Z}$. L'ordre de 1_A dans le groupe $(A, +)$ divise l'ordre de ce groupe, autrement dit k_A divise p^n d'où $k_A \in \{1, p\}$ et par conséquent $k_A = p$. Soit $(x, y) \in A^2$. Le corps A étant commutatif conformément aux consignes du programme de CPGE, il vient

$$\varphi(x + y) = (x + y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + y^p$$

La formule des chefs assure que

$$\forall k \in [\![1\,;\, p-1]\!] \qquad k\binom{p}{k} = p\binom{p-1}{k-1}$$

et comme $k \wedge p = 1$ pour $k \in [\![1\,;\, p-1]\!]$, le lemme de Gauss assure que p divise $\binom{p}{k}$ d'où $\binom{p}{k} \in \mathrm{Ker}\, f_A$ pour tout $k \in [\![1\,;\, p-1]\!]$. Par conséquent

$$\varphi(x + y) = x^p + y^p = \varphi(x) + \varphi(y)$$

et on a clairement $\varphi(1) = 1_A$ et $\varphi(xy) = \varphi(x)\varphi(y)$. Soit $x \in \mathrm{Ker}\, \varphi$, c'est-à-dire $x^p = 0$. Par intégrité de A, il vient $x = 0_A$ ou $x^{p-1} = 0_A$ et une récurrence donne alors $x = 0_E$. Ainsi,

l'application φ est injectif de A dans lui-même avec A ensemble fini d'où la bijectivité de φ et on conclut

$$\boxed{\text{L'application } \varphi \text{ est un automorphisme de A.}}$$

On observe $\qquad \forall x \in \mathrm{A} \qquad \varphi^2(x) = \varphi(x^p) = x^{p^2}$

d'où par récurrence $\qquad \forall (k,x) \in \mathbb{N} \times \mathrm{A} \qquad \varphi^k(x) = x^{p^k}$

Comme l'anneau A est un corps, on a $\mathrm{U(A)} = \mathrm{A} \setminus \{0_\mathrm{A}\}$ et par conséquent Card $\mathrm{U(A)} = p^n - 1$. Dans le groupe multiplicatif $(\mathrm{U(A)}, \times)$, l'ordre d'un élément divisant l'ordre du groupe, on a $x^{p^n-1} = 1_\mathrm{A}$ pour $x \in \mathrm{A} \setminus \{0_\mathrm{A}\}$ d'où $x^{p^n} = x$ et cette égalité vaut aussi pour $x = 0_\mathrm{A}$. On a donc établi $\varphi^n = \mathrm{id}$. Supposons que l'ordre de φ soit $r < n$. On aurait alors

$$\forall x \in \mathrm{A} \qquad \varphi^r(x) = x^{p^r} = x$$

Par conséquent, tout élément de A serait racine du polynôme $\mathrm{X}^{p^r} - \mathrm{X}$ de degré $p^r < p^n$. Or, un polynôme n'admet pas plus de racines distinctes que son degré ce qui contredit l'inégalité précédente. Il s'ensuit $\varphi^r \neq \mathrm{id}$ pour tout $r < n$ et on conclut

$$\boxed{\text{L'ordre de } \varphi \text{ est égal à } n.}$$