ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°84

Exercice 1 (**)

Un idéal I d'un anneau commutatif A est dit *premier* si

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

1. Décrire les idéaux premiers de $\mathbb{Z}$.
2. Soit A un anneau commutatif, I idéal premier et J, K des idéaux. Montrer que

$$\mathrm{J} \cap \mathrm{K} = \mathrm{I} \quad \Longrightarrow \quad \mathrm{J} = \mathrm{I} \quad \text{ou} \quad \mathrm{K} = \mathrm{I}$$

Corrigé : 1. Soit I idéal premier de $\mathbb{Z}$. On suppose $\mathrm{I} \neq \{0\}$ sinon c'est immédiat par intégrité de $\mathbb{Z}$. Il existe p entier non 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 $p|ab$. Alors, on a $p|a$ ou $p|b$ ce qui prouve que I est un idéal premier. Ainsi

$$\boxed{\text{Les idéaux premiers de } \mathbb{Z} \text{ sont exactement les } p\mathbb{Z} \text{ avec } p \in \mathcal{P}.}$$

2. Supposons $\mathrm{J} \cap \mathrm{K} = \mathrm{I}$. Si $\mathrm{K} = \mathrm{I}$, il n'y a rien à faire. Supposons $\mathrm{K} \neq \mathrm{I}$. Soit $x \in \mathrm{J}$ et $y \in \mathrm{K} \setminus \mathrm{I}$. On a $xy \in \mathrm{J}$ et $xy \in \mathrm{K}$ par absorption d'où $xy \in \mathrm{I}$. Comme I est premier, il vient $x \in \mathrm{I}$ ou $y \in \mathrm{I}$ ce qui est exclu. On en déduit $x \in \mathrm{I}$ d'où $\mathrm{J} \subset \mathrm{I}$ et l'autre inclusion est immédiate par hypothèse. On conclut

$$\boxed{\mathrm{J} \cap \mathrm{K} = \mathrm{I} \Longrightarrow \mathrm{J} = \mathrm{I} \text{ ou } \mathrm{K} = \mathrm{I}}$$

Exercice 2 (***)

Un anneau A est dit *de Boole* si tout élément $x \in \mathrm{A}$ vérifie $x^2 = x$. On considère A un anneau de Boole.

1. Montrer que pour tout $x \in \mathrm{A}$, on a $x + x = 0_{\mathrm{A}}$ et que A est commutatif.
2. Soit $(x, y) \in \mathrm{A}^2$. Calculer $xy(x+y)$. En déduire que si A possède plus que deux éléments, il n'est pas intègre.

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

$$(-x + x)x = 0_{\mathrm{A}} = (-x)x + x^2 \quad \Longrightarrow (-x)x = -x^2$$

et $$(-x)(-x + x) = 0_{\mathrm{A}} = (-x)^2 + (-x)x = (-x)^2 - x^2 \quad \Longrightarrow \quad (-x)^2 = -x$$

On a $$x = x^2 = (-x)^2 = -x \quad \Longrightarrow \quad x + x = 0_{\mathrm{A}}$$

puis $$(x + y)^2 = x + y \iff x^2 + xy + yx + y^2 = x + y \iff xy + yx = 0_{\mathrm{A}}$$

d'où $$xy + yx - (xy + xy) = yx - xy = 0_{\mathrm{A}}$$

Ainsi $$\boxed{\text{On a } x + x = 0_{\mathrm{A}} \text{ pour tout } x \in \mathrm{A} \text{ et l'anneau A est commutatif.}}$$

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

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

D'où $$\boxed{\forall (x,y) \in \mathrm{A}^2 \qquad xy(x+y) = 0_\mathrm{A}}$$

Si A contient au moins trois éléments, on peut choisir $x = 1_\mathrm{A}$ et $y \notin \{0_\mathrm{A}, 1_\mathrm{A}\}$. Ainsi, on a

$$xy(x+y) = y(1_\mathrm{A} + y) = 0 \quad \text{et} \quad y \neq -1_\mathrm{A} = 1_\mathrm{A}$$

$$\boxed{\text{Si l'anneau A contient plus de deux éléments, alors il n'est pas intègre.}}$$

Exercice 3 (****)

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

1. Montrer que A est un anneau commutatif.
2. Justifier que pour $x \in \mathrm{A}$, l'écriture $x = a + b\sqrt{2}$ avec $(a,b) \in \mathbb{Z}^2$ est unique.
3. Pour $x = a + b\sqrt{2} \in \mathrm{A}$, on note $\mathrm{N}(x) = a^2 - 2b^2$. Vérifier que
$$\forall (x,y) \in \mathrm{A}^2 \qquad \mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$$
4. Montrer que $$x \in \mathrm{U}(\mathrm{A}) \iff \mathrm{N}(x) \in \{\pm 1\}$$
5. Montrer que $$\min \mathrm{U}(\mathrm{A}) \cap \,]\,1\,;+\infty\,[= 1 + \sqrt{2}$$
6. En déduire $\quad x \in \mathrm{U}(\mathrm{A}) \cap \,]\,0\,;+\infty\,[\quad \Longrightarrow \quad \exists n \in \mathbb{Z} \mid x = (1+\sqrt{2})^n$
7. Décrire U(A).

Corrigé : 1. Sans difficulté, on vérifie que A est un sous-anneau de $(\mathbb{R}, +, \times)$ d'où

$$\boxed{\text{L'ensemble A est un anneau commutatif.}}$$

2. Soit $(a,b) \in \mathbb{Z}^2$ et $(c,d) \in \mathbb{Z}^2$ tel que $a + b\sqrt{2} = c + d\sqrt{2}$. On a $a - c = (b-d)\sqrt{2}$. Si $b - d \neq 0$, alors $\sqrt{2}$ est rationnel ce qui est faux d'où $b = d$ puis $a = c$ et par conséquent

$$\boxed{\forall x \in \mathrm{A} \qquad \exists! (a,b) \in \mathbb{Z}^2 \quad \mid \quad x = a + b\sqrt{2}}$$

3. On pose $$\varphi \colon \begin{cases} \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{2}] \\ a + b\sqrt{2} \longmapsto a - b\sqrt{2} \end{cases}$$

L'application est bien définie puisque le couple $(a,b) \in \mathbb{Z}^2$ est unique pour $x = a + b\sqrt{2} \in \mathrm{A}$.

On a $$\forall x \in \mathrm{A} \qquad \mathrm{N}(x) = x\varphi(x)$$

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

et notant $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$, il vient

$$\varphi(xy) = ac + 2bd - (ad + bc)\sqrt{2} = ac + 2(-b)(-d) + (a(-d) + (-b)c)\sqrt{2} = \varphi(x)\varphi(y)$$

D'où $$\boxed{\forall (x,y) \in \mathrm{A}^2 \qquad \mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)}$$

4. Soit $x \in \mathrm{U}(\mathrm{A})$. Il existe $y \in \mathrm{A}$ tel que $xy = 1$ d'où $\mathrm{N}(x)\mathrm{N}(y) = \mathrm{N}(xy) = 1$. Or, les quantités $\mathrm{N}(x)$ et $\mathrm{N}(y)$ sont des entiers relatifs donc appartiennent à $\mathrm{U}(\mathbb{Z}) = \{\pm 1\}$. Réciproquement, si $\mathrm{N}(x) = \pm 1$, alors on a $x\varphi(x) = \pm 1$ d'où $x\mathrm{N}(x)\varphi(x) = 1$ autrement dit $x \in \mathrm{U}(\mathrm{A})$ avec $x^{-1} = \mathrm{N}(x)\varphi(x)$. On conclut

$$\boxed{x \in \mathrm{U}(\mathrm{A}) \iff \mathrm{N}(x) \in \{\pm 1\}}$$

5. On a clairement $$1+\sqrt{2} \in \mathrm{U(A)} \cap \left]1\,;+\infty\right[$$

Soit $x \in \mathrm{U(A)} \cap \left]1\,;+\infty\right[$. On suppose $x = a - b\sqrt{2}$ avec $(a,b) \in \mathbb{N}^2$. Alors, on a $\varphi(x) = a + b\sqrt{2} > x > 1$ d'où $\mathrm{N}(x) = x\varphi(x) > 1$ ce qui est faux. Si $x = -a + b\sqrt{2}$, alors $-\varphi(x) = a + b\sqrt{2} > x > 1$ d'où $-\mathrm{N}(x) > 1$ ce qui est encore faux. Il s'ensuit que $x = a + b\sqrt{2}$ avec $(a,b) \in \mathbb{N}^2$ et comme les cas $a = 0$ ou $b = 0$ sont exclus, il s'ensuit que $x \geqslant 1 + \sqrt{2}$ et on conclut

$$\boxed{\min \mathrm{U(A)} \cap \left]1\,;+\infty\right[= 1 + \sqrt{2}}$$

6. On a $$(1+\sqrt{2})^n \xrightarrow[n\to\infty]{} +\infty \quad \text{et} \quad (1+\sqrt{2})^n \xrightarrow[n\to-\infty]{} 0$$

On en déduit la partition de $\left]0\,;+\infty\right[$ donnée par $\left]0\,;+\infty\right[= \bigcup\limits_{n\in\mathbb{Z}} \left[(1+\sqrt{2})^n\,;(1+\sqrt{2})^{n+1}\right[$. Par suite, pour $x \in \mathrm{U(A)} \left]0\,;+\infty\right[$, il existe un unique $n \in \mathbb{Z}$ tel que

$$(1+\sqrt{2})^n \leqslant x < (1+\sqrt{2})^{n+1}$$

d'où $$1 \leqslant x(1+\sqrt{2})^{-n} < 1 + \sqrt{2}$$

Or, on a $x(1+\sqrt{2})^{-n} \in \mathrm{U(A)}$ puisque $\mathrm{U(A)}$ est un groupe multiplicatif. Si on avait $x(1+\sqrt{2})^{-n} > 1$, cela contredirait la minimalité de $1+\sqrt{2}$ dans $\mathrm{U(A)} \cap \left]0\,;+\infty\right[$. On en déduit que $x(1+\sqrt{2})^{-n} = 1$ autrement dit

$$\boxed{\forall x \in \mathrm{U(A)} \cap \left]0\,;+\infty\right[\qquad \exists n \in \mathbb{Z} \quad | \quad x = (1+\sqrt{2})^n}$$

7. On a clairement $0 \notin \mathrm{U(A)}$ et si $x \in \mathrm{U(A)} \cap \left]-\infty\,;0\right[$, alors $-x \in \mathrm{U(A)} \cap \left]0\,;+\infty\right[$ et le résultat précédent s'applique. On conclut

$$\boxed{\mathrm{U(A)} = \left\{\pm(1+\sqrt{2})^n, n \in \mathbb{Z}\right\}}$$

Exercice 4 (****)

Soient $\alpha > \beta$ les racines de $\mathrm{P} = \mathrm{X}^2 - \mathrm{X} - 1$. On pose $\mathrm{A} = \{x + \alpha y, (x,y) \in \mathbb{Z}^2\}$ et l'application $\sigma : \mathrm{A} \to \mathbb{R}, x + \alpha y \mapsto x + \beta y$.

1. Montrer que A est un anneau et que σ est un automorphisme de A. Expliciter σ^{-1}.
2. On note U l'ensemble des inversibles de A et $\mathrm{N} : \mathrm{A} \to \mathbb{R}, z \mapsto z\sigma(z)$.

   (a) Pour $z \in \mathrm{A}$, montrer $\qquad z \in \mathrm{U} \iff |\mathrm{N}(z)| = 1$

   (b) Soit $\mathrm{V} = \mathrm{U} \cap \left]1\,;+\infty\right[$, montrer que si $x + \alpha y \in \mathrm{V}$, alors $x \geqslant 0$ et $y \geqslant 1$.

   (c) En déduire $\qquad \mathrm{V} = \{\alpha^n, n \in \mathbb{N}^*\}$

Corrigé : 1. On trouve $\alpha = \dfrac{1+\sqrt{5}}{2}$ et $\beta = \dfrac{1-\sqrt{5}}{2}$. On a $1 \in \mathrm{A}$. Soit $(u,v) \in \mathrm{A}^2$ avec $u = x + \alpha y$, $v = z + \alpha t$ où x, y, z et t sont entiers relatifs. On trouve

$$\begin{aligned} uv &= (x+\alpha y)(z+\alpha t) = xz + \alpha(yz+xt) + \alpha^2 yt \\ &= xz + \alpha(yz+xt) + (1+\alpha)yt = xz + yt + \alpha(yz+xt+yt) \in \mathrm{A} \end{aligned}$$

et $$u + v = x + z + \alpha(y+t) \in \mathrm{A}$$

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

Vérifions que σ est bien défini. On a

$$u = v \iff x + \alpha y = z + \alpha t \iff x - z = \alpha(y - t)$$

On en déduit $$x = z \iff y \neq t$$

Si $y \neq t$, alors $\alpha = \dfrac{x - z}{y - t} \in \mathbb{Q}$ ce qui est absurde d'où $y = t$ et par suite $x = z$. L'écriture d'un élément de A est donc unique ce qui prouve que l'application σ est bien définie. Puis, on a

$$\sigma(u + v) = x + z + \beta(y + t) = x + \beta y + z + \beta t = \sigma(u) + \sigma(v)$$

et

$$\sigma(uv) = xz + yt + \beta(yz + xt + yt) \quad \text{et} \quad \sigma(u)\sigma(v) = (x + \beta y)(z + \beta t) = xz + yz + \beta(yz + xt + yt)$$

Avec $\alpha\beta = -1$, il vient

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = -1$$

d'où $$\sigma(\beta) = -\frac{1}{\beta} = \alpha$$

Ainsi $$\sigma^2(x + \alpha y) = \sigma(x + \beta y) = x + \alpha y$$

On conclut $\boxed{\text{L'application est un automorphisme d'anneau avec } \sigma^{-1} = \sigma.}$

2.(a) Soit $u \in \mathrm{U}$ avec $u = x + \alpha y$, x et y entiers relatifs. Avec $\alpha\beta = -1$ et $\alpha + \beta = 1$, il vient

$$\mathrm{N}(u) = u\sigma(u) = (x + \alpha y)(x + \beta y) = x^2 - y^2 + xy \in \mathbb{Z}$$

S'il existe $v \in \mathrm{U}$ tel que $uv = 1$, alors

$$\mathrm{N}(uv) = uv\sigma(uv) = u\sigma(u)v\sigma(v) = \mathrm{N}(u)\mathrm{N}(v) \quad \text{et} \quad \mathrm{N}(uv) = \mathrm{N}(1) = 1$$

On en déduit que $\mathrm{N}(u) \in \mathrm{U}(\mathbb{Z}) = \{-1, 1\}$. Réciproquement, on a

$$\mathrm{N}(u) = \pm 1 \iff (x + \alpha y)(x + \beta y) = \pm 1 \iff u(\pm\sigma(u)) = 1$$

ce qui prouve que $u \in \mathrm{U}$. On conclut

$$\boxed{\mathrm{U} = \{u \in \mathrm{A} \;:\; |\mathrm{N}(u)| = 1\}}$$

2.(b) Soit $u \in \mathrm{V}$. Supposons que $u = x - \alpha y$ avec $(x, y) \in \mathbb{N}^2$. Comme $-\alpha < 0$ et $-\beta > 0$, on a clairement $x - \beta y \geqslant x - \alpha y > 1$ puis

$$\mathrm{N}(u) = (x - \alpha y)(x - \beta y) > 1$$

ce qui contredit $u \in \mathrm{U}$. Supposons que $u = -x + \alpha y$ avec $(x, y) \in \mathbb{N}^2$. Comme $-x + \alpha y > 1$, on a nécessairement $y \geqslant 1$. Si $x \geqslant 1$, alors $-x + \beta y \leqslant -1 + \beta$ et on a

$$\mathrm{N}(u) = \underbrace{(-x + \alpha y)}_{>1}\underbrace{(-x + \beta y)}_{\leqslant -1+\beta} < -1$$

ce qui contredit $u \in \mathrm{U}$. On conclut

$$\boxed{\text{Pour } (x, y) \in \mathbb{Z}^2, \text{ si } x + \alpha y \in \mathrm{V}, \text{ alors } x \geqslant 0 \text{ et } y \geqslant 1.}$$

2.(c) D'après le résultat précédent, on a $\alpha = \operatorname{Min} \mathrm{V}$. On en déduit $\{\alpha^n, n \in \mathbb{N}^*\} \subset \mathrm{V}$. Réciproquement, soit $x \in \mathrm{V}$. On observe que $\alpha^n \xrightarrow[n\to\infty]{} +\infty$ d'où $\mathrm{V} \subset [\,\alpha\,;+\infty\,[\; = \bigcup_{n\in\mathbb{N}^*} [\,\alpha^n\,;\alpha^{n+1}\,[$. Par conséquent, il existe n entier non nul tel que $x \in [\,\alpha^n\,;\alpha^{n+1}\,[$ d'où $1 \leqslant x(-\beta)^n < \alpha$. Comme U est un groupe multiplicatif, on a $x(-\beta)^n \in \mathrm{U}$. Si $x(-\beta)^n > 1$, alors on aurait $x(-\beta)^n \geqslant \operatorname{Min} \mathrm{V} = \alpha$ ce qui est faux. On en déduit $x(-\beta)^n = 1$ d'où $x = \alpha^n$. On conclut

$$\boxed{\mathrm{V} = \{\alpha^n, n \in \mathbb{N}^*\}}$$