

Feuille d'exercices n°83

Exercice 1 (**)

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

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

1. Montrer que $R(I)$ est un idéal de A contenant I .

2. On suppose $A = \mathbb{Z}$. Déterminer l'ensemble des entiers n non nuls tels que $R(n\mathbb{Z}) = n\mathbb{Z}$.

Corrigé : 1. On a $0 \in R(I)$ puisque $0^1 = 0 \in I$. Soit $(x, y) \in R(I)^2$. Il existe des entiers non nuls n et m tels que $x^n \in I$ et $y^m \in I$. 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 $k \geq n$, on a

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

et pour $k < n$

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

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

Le radical $R(I)$ est un idéal de $(A, +, \times)$ contenant I .

2. On a clairement $R(\mathbb{Z}) = \mathbb{Z}$. Soit n entier avec $n \geq 2$ tel que $R(n\mathbb{Z}) = n\mathbb{Z}$. 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 $\alpha_1 \geq 2$, on pose $x = p_1^{\alpha_1-1} \prod_{i=2}^r p_i^{\alpha_i}$. On a $n \nmid x$ mais $n \mid x^2$ puisque

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

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

Les entiers n non nuls tels que $R(n\mathbb{Z}) = n\mathbb{Z}$ 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 $R(n\mathbb{Z}) = \left(\prod_{i=1}^r p_i \right) \mathbb{Z}$. Soit $x \in R(n\mathbb{Z})$. On dispose de k entier non nul tel que $n \mid x^k$. 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 $k = \max_{i \in \llbracket 1; r \rrbracket} \alpha_i$ 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, ils 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 $1 = \frac{1}{10^0} \in \mathbb{D}$. Pour $(x, y) \in \mathbb{D}^2$, on a $x = \frac{p}{10^n}$ et $y = \frac{q}{10^m}$ 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

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

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

Exercice 3 (***)

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

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

Le triplet $(A, +, \times)$ est un corps.

Exercice 4 (***)

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

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

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

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

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

et

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

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

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

On a clairement $C \subset D$. 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 $\sqrt{n} = \pm \frac{c}{d}$, on aurait $nd^2 = c^2$ d'où $v_p(n) + 2v_p(d) = 2v_p(c)$ pour p un nombre premier présent dans la décomposition de n avec une valuation impaire. Ainsi

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

On conclut

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

2. Soit $\varphi : C \rightarrow C$ 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

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

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

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

et

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

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

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

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 $\alpha + \beta\sqrt{n} \mapsto \alpha - \beta\sqrt{n}$.

Remarque : On note habituellement $C = \mathbb{Q}[\sqrt{n}]$. On a déterminé ici le *groupe de Galois* $\text{Gal}(\mathbb{Q}[\sqrt{n}]/\mathbb{Q})$, ensemble des automorphismes du corps $\mathbb{Q}[\sqrt{n}]$ qui stabilisent le corps $\mathbb{Q}$. Dans ce cas très simple, on a obtenu $\text{Gal}(\mathbb{Q}[\sqrt{n}]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 5 (***)

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

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

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

Corrigé : 1. Soit I idéal premier de $(\mathbb{Z}, +, \times)$. On suppose $I \neq \{0\}$ sinon c'est immédiat par intégrité de $\mathbb{Z}$. Il existe p entier non nul tel que $I = p\mathbb{Z}$. 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 $(A, +, \times)$. Soit $x \in A \setminus \{0\}$. L'idéal x^2A est premier et $x^2 \in x^2A$ d'où $x \in x^2A$ ce qui prouve qu'il existe $y \in A$ 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 (***)

Soit $(A, +, \times)$ un anneau commutatif. On dit que l'anneau $(A, +, \times)$ est *local* si l'ensemble $V(A)$ de ses éléments non inversibles est un idéal de l'anneau. Soit n entier ≥ 2 . Établir

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ local} \iff \exists (p, \alpha) \in \mathcal{P} \times \mathbb{N}^* \mid n = p^\alpha$$

Corrigé : On suppose $n = p^\alpha$ avec p nombre premier et α entier non nul. Soit $k \in \mathbb{Z}$. On a

$$\bar{k} \in U(\mathbb{Z}/n\mathbb{Z}) \iff k \wedge n = 1 \iff k \wedge p^\alpha = 1 \iff k \wedge p = 1$$

d'où
$$\bar{k} \notin U(\mathbb{Z}/n\mathbb{Z}) \iff k \wedge p \neq 1 \iff p|k$$

Ainsi
$$V(\mathbb{Z}/n\mathbb{Z}) = \langle \bar{p} \rangle$$

C'est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ qui vérifie la propriété d'absorption sans difficulté. On procède par l'absurde pour la réciproque. Supposons qu'il existe p et q nombres premiers distincts diviseurs de n . On a $n \wedge p = p \neq 1$ et $n \wedge q = q \neq 1$ d'où $\bar{p}$ et $\bar{q}$ non inversibles. D'après la relation de Bézout, comme $p \wedge q = 1$, il existe u, v entiers relatifs tels que $pu + qv = 1$ d'où

$$\bar{1} = u\bar{p} + v\bar{q} \in V(\mathbb{Z}/n\mathbb{Z})$$

d'après la structure de groupe de $(V(\mathbb{Z}/n\mathbb{Z}), +)$. Or, l'élément $\bar{1}$ est clairement inversible et on a donc une contradiction. On conclut

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ local} \iff \exists (p, \alpha) \in \mathcal{P} \times \mathbb{N}^* \mid n = p^\alpha$$

Exercice 7 (****)

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

Corrigé : Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ 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
$$\forall r \in \mathbb{Q} \quad f(r) = r$$

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

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

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

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 $a \leq x \leq b$ et $b - a \leq \varepsilon$. Ainsi, par croissance de f , il vient

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

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

Ainsi
$$\forall \varepsilon > 0 \quad |f(x) - x| \leq \varepsilon$$

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

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