

TD N°1

Structures algébriques usuelles (correction)

1 Groupes

Corrigé de l'exercice 1. 1. On a $1 \in H$ et si $(z_1, z_2) \in H^2$, alors $(z_1 z_2^{-1})^n = z_1^n z_2^{-n} = 1$ donc $z_1 z_2^{-1} \in H$. Ainsi H est un sous-groupe de G .

2. On vérifie d'abord que $H \subset G$. Pour $a + b\sqrt{3} \in H$, on a $a^2 - 3b^2 = 1 > 0$ et $a \in \mathbb{N}$ donc $a > \sqrt{3}|b|$ et par suite $a + b\sqrt{3} > \sqrt{3}(|b| + b) \geq 0$. Ainsi $H \subset G$.

- On a $1 = 1 + 0\sqrt{3}$ donc $1 \in H$.
- Soient $a + b\sqrt{3}$ et $a' + b'\sqrt{3}$ deux éléments de H . On a

$$(a + b\sqrt{3})(a' + b'\sqrt{3}) = \underbrace{(aa' + 3bb')}_{\in \mathbb{N}} + \sqrt{3} \underbrace{(ab' + ba')}_{\in \mathbb{Z}}.$$

Car $a \geq \sqrt{3}|b|$ et $a' \geq \sqrt{3}|b'|$ donc $aa' + 3bb' \geq 3(|b||b'| + bb') \geq 0$ donc $aa' + 3bb' \in \mathbb{N}$. Ainsi $(a + b\sqrt{3})(a' + b'\sqrt{3}) \in H$.

- Il reste à montrer que H est stable par passage à l'inverse. Soit $a + b\sqrt{3} \in H$, on a

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = a - b\sqrt{3} \in H \text{ puisque } a^2 - 3b^2 = 1$$

D'où, H est bien un sous-groupe de G .

3. Il est clair que $I_3 \in H$. Soient $A = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}$ deux éléments de H . On a

$$AB = \begin{pmatrix} 1 & x + x' & z + z' + xy' \\ 0 & 1 & y + y' \\ 0 & 0 & 1 \end{pmatrix} \in H.$$

De plus, le calcul précédent montre que $A^{-1} = \begin{pmatrix} 1 & -x & -z + xy \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}$ qui est, bien un élément de H .

Corrigé de l'exercice 2. Soit $x \in G$. On a $x^2 = e$ donc $x = x^{-1}$. Si $(x, y) \in G^2$ alors, $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$. Ainsi G est un groupe abélien.

Corrigé de l'exercice 3. 1.

$\sigma \circ \sigma'$	$\sigma = \text{Id}$	$\sigma = (12)$	$\sigma = (13)$	$\sigma = (23)$	$\sigma = (123)$	$\sigma = (132)$
$\sigma' = \text{Id}$	Id	(12)	(13)	(23)	(123)	(132)
$\sigma' = (12)$	(12)	Id	(123)	(132)	(13)	(23)
$\sigma' = (13)$	(13)	(132)	Id	(123)	(23)	(12)
$\sigma' = (23)$	(23)	(123)	(132)	Id	(12)	(13)
$\sigma' = (123)$	(123)	(23)	(12)	(13)	(132)	Id
$\sigma' = (132)$	(132)	(13)	(23)	(12)	Id	(123)

2. On a $(12)^{-1} = (12)$, $(13)^{-1} = (13)$, $(23)^{-1} = (23)$ et $(123)^{-1} = (132)$, $(132)^{-1} = (123)$.

3. Le groupe $(\mathcal{S}_3, \circ)$ n'est pas abélien car $(12)(13) \neq (13)(12)$. Les sous-groupes du groupe $(\mathcal{S}_3, \circ)$ sont $H_1 = \{\text{Id}, (12)\}$, $H_2 = \{\text{Id}, (13)\}$, $H_3 = \{\text{Id}, (23)\}$, et $H_4 = \{\text{Id}, (123), (132)\}$.

Corrigé de l'exercice 4. 1. Soit $(\bar{k}, \bar{\ell}) \in (\mathbb{Z}/n\mathbb{Z})^2$. On a : $\varphi(\bar{k} + \bar{\ell}) = \varphi(\overline{k + \ell}) = e^{2i(k+\ell)\pi/n} = e^{2ik\pi/n} e^{2i\ell\pi/n} = \varphi(\bar{k})\varphi(\bar{\ell})$.
Donc φ est un morphisme de groupes. De plus,

$$\bar{k} \in \ker \varphi \iff \varphi(\bar{k}) = 1 \iff e^{2ik\pi/n} = 1 \iff 2k\pi/n \in 2\pi\mathbb{Z} \iff \bar{k} = \bar{0}.$$

Donc $\ker \varphi = \{\bar{0}\}$ et φ est injectif. Comme $\text{Card } \mathbb{Z}/n\mathbb{Z} = \text{Card } \mathbb{U}_n$, alors φ est un isomorphisme de groupes.

2. Soit $(\theta, \theta') \in \mathbb{R}^2$. On a

$$\begin{aligned} \varphi(\theta)\varphi(\theta') &= \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \theta' & -\sin \theta' \\ \sin \theta' & \cos \theta' \end{pmatrix} \\ &= \begin{pmatrix} \cos \theta \cos \theta' - \sin \theta \sin \theta' & -\cos \theta \sin \theta' - \sin \theta \cos \theta' \\ \cos \theta \sin \theta' + \sin \theta \cos \theta' & \cos \theta \cos \theta' - \sin \theta \sin \theta' \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta + \theta') & -\sin(\theta + \theta') \\ \sin(\theta + \theta') & \cos(\theta + \theta') \end{pmatrix} = \varphi(\theta + \theta'). \end{aligned}$$

Donc φ est un morphisme de groupes. De plus,

$$\theta \in \ker \varphi \iff \varphi(\theta) = I_2 \iff \cos \theta = 1 \text{ et } \sin \theta = 0 \iff \theta \in 2\pi\mathbb{Z}.$$

Donc $\ker \varphi = 2\pi\mathbb{Z}$.

Corrigé de l'exercice 5. 1. Soit $(m, n) \in \mathbb{N}^* \times \mathbb{N}$. On a $f(n) = f(\underbrace{1 + \dots + 1}_{n \text{ termes}}) = \underbrace{f(1) + \dots + f(1)}_{n \text{ termes}} = nf(1)$ et

$$f(1) = f\left(\frac{m}{m}\right) = f\left(\frac{1}{m} + \dots + \frac{1}{m}\right) = mf\left(\frac{1}{m}\right) \text{ donc } f\left(\frac{1}{m}\right) = \frac{1}{m}f(1).$$

2. De la relation $mf\left(\frac{1}{m}\right) = f(1)$ on a m divise $f(1)$ pour tout $m \in \mathbb{N}^*$ donc nécessairement $f(1) = 0$ et par suite $f(n) = 0$ pour tout $n \in \mathbb{Z}$. Si $r = \frac{p}{q} \in \mathbb{Q}$ alors, $f(r) = f\left(\frac{p}{q}\right) = pf\left(\frac{1}{q}\right) = rf(1) = 0$. Ainsi f est le morphisme nul.

Corrigé de l'exercice 6. On a $\{-1, 1\} \times \{-1, 1\} = \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}$ qui est un groupe multiplicatif et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$ qui est un groupe additif.

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	et	$\times$	$(1, 1)$	$(-1, 1)$	$(1, -1)$	$(-1, -1)$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$		$(1, 1)$	$(1, 1)$	$(-1, 1)$	$(1, -1)$	$(-1, -1)$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$		$(-1, 1)$	$(-1, 1)$	$(1, 1)$	$(-1, -1)$	$(1, -1)$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$		$(1, -1)$	$(1, -1)$	$(-1, -1)$	$(1, 1)$	$(-1, 1)$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$		$(-1, -1)$	$(-1, -1)$	$(1, -1)$	$(-1, 1)$	$(1, 1)$

On remarque que les tables sont « identiques », donc les groupes $(\{-1, 1\} \times \{-1, 1\}, \times)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ sont isomorphes. Plus précisément, l'application $\varphi : (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +) \longrightarrow (\{-1, 1\} \times \{-1, 1\}, \times)$ est un isomorphisme de groupes.

Corrigé de l'exercice 7. 1. D'abord, H est un sous-groupe de G . En effet :

- On a $e = a^0 b^0 \in H$.
- Si $x = a^{i_1} b^{j_1} a^{i_2} b^{j_2} \dots a^{i_n} b^{j_n} \in H$ et $y = a^{k_1} b^{\ell_1} a^{k_2} b^{\ell_2} \dots a^{k_m} b^{\ell_m} \in H$ alors, $xy = a^{p_1} b^{q_1} a^{p_2} b^{q_2} \dots a^{p_r} b^{q_r} \in H$.
- Si $x = a^{i_1} b^{j_1} a^{i_2} b^{j_2} \dots a^{i_n} b^{j_n} \in H$ alors, $x^{-1} = b^{-j_n} a^{-i_n} \dots b^{-j_2} a^{-i_2} b^{-j_1} a^{-i_1} = a^0 b^{-j_n} a^{-i_n} \dots b^{-j_2} a^{-i_2} b^{-j_1} a^{-i_1} b^0 \in H$.

Soit $K = \langle a, b \rangle$ le groupe engendré par a et b . On a $a = a^1 b^0 \in H$ et $b = a^0 b^1 \in H$ donc $K \subset H$.

Inversement, On a $a^i \in K$ et $b^j \in K$ pour tout $(i, j) \in \mathbb{Z}^2$ donc $a^i b^j \in K$ et par suite, $H \subset K$ d'où $K = H$.

2. Lorsque $ab = ba$, alors $H = \{a^i b^j, (i, j) \in \mathbb{Z}^2\}$.

3. Soit $G = \langle A, B \rangle$ le groupe engendré par A et B . On a $A^2 = I_3$ donc $A^{-1} = A$ et $B^3 = I_3$ donc $B^{-1} = B^2$. On en déduit que $A^i \in \{I_2, A\}$ et $B^j \in \{I_3, B, B^2\}$ pour tout $(i, j) \in \mathbb{Z}^2$. De plus, $BA = AB^2$ donc

$$G = \left\{ A^{i_1} B^{j_1} A^{i_2} B^{j_2} \dots A^{i_n} B^{j_n}, \quad n \in \mathbb{N}^*, i_1, j_1, i_2, j_2, \dots, i_n, j_n \in \mathbb{Z} \right\} = \left\{ A^i B^j, \quad i, j \in \mathbb{Z} \right\} = \left\{ I_3, A, B, AB, AB^2 \right\}.$$

Corrigé de l'exercice 8. Il est clair que $\frac{1}{3}\mathbb{Z}$ et $\frac{3}{5}\mathbb{Z}$ sont deux sous-groupes additifs de $\mathbb{Q}$ donc $\frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$. Par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $1 = 5u + 9v$ donc $\frac{1}{15} = \frac{1}{3}u + \frac{3}{5}v \in \frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z}$, donc $\frac{1}{15} \in \frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z}$. Inversement, on a $\frac{1}{3}\mathbb{Z} \subset \frac{1}{15}\mathbb{Z}$ et $\frac{3}{5}\mathbb{Z} \subset \frac{1}{15}\mathbb{Z}$ donc $\frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z} \subset \frac{1}{15}\mathbb{Z}$. D'où $\frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z} = \frac{1}{15}\mathbb{Z}$.

Corrigé de l'exercice 9. Supposons $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle (\bar{a}, \bar{b}) \rangle$. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de cardinal 4. Le générateur $(\bar{a}, \bar{b})$ vérifie $2 \times (\bar{a}, \bar{b}) = (\bar{0}, \bar{0})$ donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{a}, \bar{b})\}$ et par suite, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de cardinal 2, ce qui est absurde. Ainsi, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique.

Corrigé de l'exercice 10. 1. On pose $E = \{1, \dots, n\}$ et $\sigma' = (\tau(x_1) \tau(x_2) \dots \tau(x_r))$.

- Si $x \in E \setminus \{x_1, \dots, x_r\}$, on a $\sigma(x) = x$ et $\tau(x) \in E \setminus \{\tau(x_1), \dots, \tau(x_r)\}$, ce qui donne $\tau \circ \sigma(x) = \tau(x) = \sigma'(\tau(x)) = \sigma' \circ \tau(x)$, i-e : $\tau \circ \sigma \circ \tau^{-1}(x) = \sigma'(x)$.
- Si $x = x_k$ où $k \in \{1, \dots, r\}$, alors $\tau \circ \sigma(x) = \tau(\sigma(x_k)) = \tau(x_{k+1})$ en notant $x_{r+1} = x_1$ donc $\sigma' \circ \tau(x) = \sigma'(\tau(x_k)) = \tau(x_{k+1})$ i-e : $\tau \circ \sigma \circ \tau^{-1}(x) = \sigma'(x)$.

Ainsi, $\tau \circ \sigma \circ \tau^{-1}(x) = \sigma'(x)$ pour tout $x \in E$. D'où $\tau \circ \sigma \circ \tau^{-1} = \sigma'$.

2. a. Soit $(i j)$ une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à montrer car $(i j) = (j i)$. Supposons $i \neq 1$ et $j \neq 1$, on a d'après la première question :

$$(i j) = (1 i)(1 j)(1 i)^{-1} = (1 i)(1 j)(1 i).$$

Comme $\mathcal{S}_n$ est engendré par les transpositions, on déduit que $\mathcal{S}_n$ est engendré par les $n - 1$ transpositions $(1 k)$ avec $2 \leq k \leq n$.

- b. D'après la première question, $\mathcal{S}_n$ est engendré par les transpositions $(1 k)$ avec $2 \leq k \leq n$, il suffit de décomposer chaque transposition $(1 k)$ en produit de transpositions de type $(i i + 1)$.

Si $k = 2$, alors $(1 k) = (1 2) = (1 1 + 1)$ est de la forme souhaitée.

Si $3 \leq k \leq n$, alors d'après la première question :

$$(1 k) = (k - 1 k)(1 k - 1)(k - 1 k)^{-1} = (k - 1 k)(1 k - 1)(k - 1 k).$$

D'autre part : $(1 k - 1) = (k - 2 k - 1)(1 k - 2)(k - 2 k - 1)$ et on continue la décomposition ainsi de suite si nécessaire.

- c. D'après la deuxième question, $\mathcal{S}_n$ est engendré par les transpositions $(k k + 1)$ avec $1 \leq k \leq n - 1$, il suffit de montrer que chaque transposition $(k k + 1)$ est dans G où $G \stackrel{\text{déf}}{=} \langle \tau, \gamma \rangle$ avec $\tau = (1 2)$ et $\gamma = (1 2 \dots n)$ le sous groupe de $\mathcal{S}_n$ engendré par τ et γ . Pour $n \geq 3$, on a d'après la première question :

$$\begin{aligned} \gamma(1 2)\gamma^{-1} &= (\gamma(1) \gamma(2)) = (2 3) \\ \gamma(2 3)\gamma^{-1} &= (\gamma(2) \gamma(3)) = (3 4) \\ &\vdots \\ \gamma(n - 2 \ n - 1)\gamma^{-1} &= (\gamma(n - 2) \gamma(n - 1)) = (n - 1 \ n) \end{aligned}$$

Donc $(k k + 1) = \gamma^{k-1}(1 2)(\gamma^{k-1})^{-1}$ pour $1 \leq k \leq n - 1$.

Corrigé de l'exercice 11. 1. Supposons G abélien et soit $(x, y) \in H^2$, donc $x = \varphi(a)$ et $y = \varphi(b)$ avec $(a, b) \in G^2$.

On a $x \top y = \varphi(a) \top \varphi(b) = \varphi(a \star b) = \varphi(b \star a) = \varphi(b) \top \varphi(a) = y \top x$. Donc H est abélien.

Supposons H abélien, on a $\varphi^{-1} : (H, \top) \longrightarrow (G, \star)$ est un isomorphisme de groupes, donc d'après ce qui précède, G est abélien.

2. Supposons $G = \langle a \rangle$. On a $\varphi(a) \in H$ donc $\langle \varphi(a) \rangle \subset H$. Soit $h \in H$, donc $h = \varphi(g)$ avec $g \in G$, donc $g = a^k$ avec $k \in \mathbb{Z}$, i.e $h = \varphi(a^k) = (\varphi(a))^k$ donc $h \in \langle \varphi(a) \rangle$ donc $H \subset \langle \varphi(a) \rangle$, d'où l'égalité : $H = \langle \varphi(a) \rangle$. Pour la réciproque, on considère φ^{-1} au lieu de φ .

3. Fixons $(k, b) \in \mathbb{Z} \times G$ et considérons les ensembles $I = \{x \in G, x^k = b\}$ et $J = \{x \in H, x^k = \varphi(b)\}$. On va montrer que φ réalise une bijection entre I et J .

Soit $y \in J$, il existe $x \in G$ unique tel que $y = \varphi(x)$. Or $(\varphi(x))^k = \varphi(b)$ i.e $\varphi(x^k) = \varphi(b)$ donc $x^k = b$ car φ est injectif donc $x \in I$. D'où : $\forall y \in J, \exists! x \in I, y = \varphi(x)$. En particulier, les ensembles I et J ont même cardinal.

4. Le groupe $\mathbb{Z}/4\mathbb{Z}$ est cyclique mais $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique, donc $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/4\mathbb{Z}, +)$ ne sont pas isomorphes.

Le groupe $\mathbb{Z}/6\mathbb{Z}$ est abélien mais $\mathcal{S}_3$ n'est pas abélien, donc $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathcal{S}_3, \circ)$ ne sont pas isomorphes.

Les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ne sont pas isomorphes car l'équation $x^4 = 1$ a deux solutions dans $\mathbb{R}^*$ et quatre solutions dans $\mathbb{C}^*$.

2 Ordre d'un élément dans un groupe

Corrigé de l'exercice 12. 1. On a $4 \times \bar{3} = \bar{12} = \bar{0}$ et $k \times \bar{3} \neq \bar{0}$ pour $1 \leq k \leq 3$ donc l'ordre de $\bar{3}$ est 4.

2. Soit $D = \text{diag}(1, j, j^2)$. On a $D^3 = \text{diag}(1, j^3, j^6) = I_3$ et $D^2 = \text{diag}(1, j^2, j) \neq I_3$ donc l'ordre de D est 3.

Corrigé de l'exercice 13. 1. Soit $k \in \mathbb{N}$. On a

$$(aba^{-1})^k = \underbrace{(aba^{-1})(aba^{-1}) \dots (aba^{-1})(aba^{-1})}_{k \text{ termes}} = ab(a^{-1}a)a \dots (a^{-1}a)ba^{-1} = ab^ka^{-1}$$

donc $(aba^{-1})^k = e \iff ab^ka^{-1} = e \iff b^ka^{-1} = e \iff b^k = e$. On en déduit que b et aba^{-1} ont le même ordre (fini ou infini).

Soit $k \in \mathbb{N}$. On a $a^k = e \iff (a^k)^{-1} = e \iff (a^{-1})^k = e$ donc a et a^{-1} ont le même ordre (fini ou infini).

2. Supposons $(ab)^n = e$. On a $b(ab)^n = b$ soit encore $(ba)^nb = b$ donc $(ba)^n = e$. Ainsi, ba est d'ordre fini au plus égal à n . Un raisonnement symétrique établit que ab est d'ordre inférieur à celui de ba et donc ab et ba ont le même ordre.

Corrigé de l'exercice 14. 1. Pour tout $k \in \mathbb{N}$, on a $R_\theta^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} = R_{k\theta}$ (récurrence sur k), donc

$$\begin{aligned} R_\theta \text{ est d'ordre fini} &\iff \exists k \in \mathbb{N}^* \text{ tel que } R_\theta^k = I_2 \\ &\iff R_{k\theta} = I_2 \\ &\iff \cos k\theta = 1 \text{ et } \sin k\theta = 0 \\ &\iff k\theta \in 2\pi\mathbb{Z} \iff \frac{\theta}{2\pi} \in \mathbb{Q}. \end{aligned}$$

2. Supposons $\frac{\theta}{2\pi} = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $p \wedge q = 1$. D'après la question précédente, R_θ est d'ordre fini. Soit n l'ordre de R_θ , on a

$$R_\theta^n = I_2 \iff n\theta \in 2\pi\mathbb{Z} \iff \frac{np}{q} \in \mathbb{Z} \iff q \text{ divise } np \xrightarrow{\text{Bézout}} q \text{ divise } n \implies n \in \{q, 2q, 3q, \dots\}.$$

Or $R_\theta^q = I_2$ donc l'ordre de R_θ égal à q .

Corrigé de l'exercice 15. 1. a. Soit $d = m \wedge n$. On a $n = n'd$, $m = m'd$ avec $n' \wedge m' = 1$. Pour tout $k \in \mathbb{Z}$, on a

$$(a^m)^k = e \iff a^{mk} = e \iff n \mid mk \iff n' \mid m'k \xrightarrow{\text{Bézout}} n' \mid k \iff \frac{n}{d} \text{ divise } k.$$

Donc l'ordre de a^m est égal à $\frac{n}{m \wedge n}$.

- b. On a $\overline{m} = m.\overline{1}$ et $\overline{1}$ est d'ordre n , par suite, l'ordre de $\overline{m}$ est égal à $\frac{n}{m \wedge n}$.
2. a. On a $p \mid p \vee q$ et $q \mid p \vee q$ donc $a^{p \vee q} = e_G$ et $b^{p \vee q} = e_H$ donc $(a, b)^{p \vee q} = (a^{p \vee q}, b^{p \vee q}) = (e_G, e_H)$. De plus, pour tout $k \in \mathbb{Z}$ on a

$$(a, b)^k = (e_G, e_H) \iff a^k = e_G \text{ et } b^k = e_H \iff p \mid k \text{ et } q \mid k \iff p \vee q \mid k.$$

Donc l'ordre de (a, b) est égale à $p \vee q$.

- b. Soit $(\overline{a}, \overline{b})$ un élément de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ d'ordre 3. Notons p l'ordre de $\overline{a}$ et q l'ordre de $\overline{b}$. D'après la question précédente, $p \vee q = 3$. Mais, l'ordre d'un élément divise l'ordre du groupe, donc p divise 3 et q divise 6. Ainsi, $(p, q) = (1, 3), (3, 1)$ ou $(3, 3)$. D'où $(\overline{a}, \overline{b}) \in \{(\overline{0}, \overline{2}), (\overline{0}, \overline{4}), (\overline{1}, \overline{0}), (\overline{2}, \overline{0}), (\overline{1}, \overline{2}), (\overline{1}, \overline{4}), (\overline{2}, \overline{2}), (\overline{2}, \overline{4})\}$.

Corrigé de l'exercice 16. Soit p l'ordre de G et q l'ordre de H .

- Supposons $p \wedge q = 1$. Soit a un générateur de G (donc d'ordre p) et b un générateur de H (donc d'ordre q). Le couple (a, b) est d'ordre $p \vee q = pq$. Puisque $G \times H$ est de cardinal pq , on en déduit que $G \times H$ est cyclique.
- Supposons $G \times H$ est cyclique. Soit (a, b) un générateur de $G \times H$, donc a est un générateur de G et b est un générateur de H donc l'ordre de a est p et l'ordre de b est q . Or (a, b) est d'ordre $p \vee q$, donc $p \vee q$ divise pq et par suite, $p \vee q = pq$ ce, qui implique que $p \wedge q = 1$.

Corrigé de l'exercice 17. 1. On a $\sigma = (i_1 i_2 \dots i_r) = (i_1 i_2)(i_2 i_3) \dots (i_{r-1} i_r)$ donc

$$\varepsilon(\sigma) = \varepsilon((i_1 i_2)(i_2 i_3) \dots (i_{r-1} i_r)) = \underbrace{\varepsilon(i_1 i_2) \dots \varepsilon(i_{r-1} i_r)}_{(r-1) \text{ termes}} = \underbrace{(-1) \dots (-1)}_{(r-1) \text{ termes}} = (-1)^{r-1}.$$

2. Pour $1 \leq k \leq r-1$, on a $\sigma^k(i_1) = i_{k+1}$ donc $\sigma^r(i_1) = i_1$. De même, $\sigma^r(i_2) = i_2, \dots, \sigma^p(i_r) = i_r$ et $\sigma^p(j) = j$ pour $j \notin \{i_1, \dots, i_r\}$ donc $\sigma^r = \text{Id}$ c'est-à-dire, σ est d'ordre r .

Corrigé de l'exercice 18. 1. Soit p l'ordre de a . On a $(f(a))^p = (a^p) = f(e_G) = e_H$, donc l'ordre de $f(a)$ divise p . Supposons f injectif et soit $1 \leq k \leq p-1$. On a $a^k \neq e_G \implies f(a^k) \neq f(e_G) \implies f(a^k) \neq e_H \implies (f(a))^k \neq e_H$. Ainsi, a et $f(a)$ ont même ordre.

2. Supposons G fini donc H est fini. Pour $n \in \mathbb{N}^*$, considérons les ensembles

$$A_n = \{a \in G, a \text{ est d'ordre } n\} \quad \text{et} \quad B_n = \{b \in H, b \text{ est d'ordre } n\}.$$

A_n et B_n sont finis, la question revient donc à montrer que A_n et B_n ont même cardinal. Pour cela, on va montrer que f réalise une bijection entre A_n et B_n .

Soit alors $b \in B_n$, donc il existe $a \in G$ tel que $f(a) = b$ et, d'après la question précédente, a et b ont même ordre, donc $a \in A_n$. D'où les ensembles A_n et B_n ont même cardinal.

3. Dans le groupe $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, les éléments $(\overline{3}, \overline{0})$ et $(\overline{0}, \overline{1})$ sont d'ordre 2 et, dans le groupe $\mathbb{Z}/12\mathbb{Z}$, seul $\overline{6}$ qui est d'ordre 2. Ainsi, $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

Corrigé de l'exercice 19. 1. On a

$$\begin{aligned} (ab)^{p \vee q} &= a^{p \vee q} \cdot b^{p \vee q} \quad \text{car } a \text{ et } b \text{ commutent} \\ &= e \cdot e = e \quad \text{car } p \mid p \vee q \text{ et } q \mid p \vee q \end{aligned}$$

donc ab est d'ordre fini et divise $p \vee q$. Le résultat n'est pas vrai si a et b ne commutent pas. En effet : dans

$(\mathcal{GL}_2(\mathbb{R}), \times)$, les matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ sont d'ordre fini : $A^4 = I_2$, $B^3 = I_2$, mais le produit AB

ne l'est pas : $(AB)^k = \begin{pmatrix} (-1)^k & (-1)^k k \\ 0 & (-1)^k \end{pmatrix} \neq I_2$ pour tout $k \in \mathbb{N}^*$.

2. Soit $k \in \mathbb{Z}$. On a

$$(ab)^k = e \implies a^k b^k = e \implies (a^k b^k)^p = e \implies a^{kp} b^{kp} = e \implies b^{kp} = e \implies q \text{ divise } kp \xrightarrow{\text{Gauss}} q \text{ divise } k.$$

De même, on obtient p divise k et par suite, $p \vee q$ divise k . De plus, $(ab)^{p \vee q} = e$ d'où ab est d'ordre $p \vee q$.

Le résultat n'est pas vrai si p et q ne sont pas premiers entre eux. En effet : dans le groupe (abélien) $\mathbb{Z}/12\mathbb{Z}$, on a $\bar{2}$ est d'ordre 6 et $\bar{3}$ est d'ordre 4 ($4 \wedge 6 \neq 1$) mais, le produit $\bar{2} \times \bar{3} = \bar{6}$ est d'ordre $2 \neq 4 \vee 6$.

3. Soit $k \geq 3$ un entier fixé. Soit r_i , $1 \leq i \leq k$ l'ordre de a_i avec $r_i \wedge r_j = 1$ pour $i \neq j$. Notons $c = \prod_{i=1}^k a_i$ avec $a_i a_j = a_j a_i$ pour tout $i \neq j$ et $r = r_1 \vee \dots \vee r_k$. On veut montrer le résultat suivant : l'ordre de c est égal à r .

On a :

$$\begin{aligned} c^r &= a_1^r \dots a_k^r \quad \text{car } a_i a_j = a_j a_i \text{ pour tout } i \neq j \\ &= e \dots e = e \quad \text{car chaque } r_i \text{ divise } r \text{ pour } 1 \leq i \leq k \end{aligned}$$

donc c est d'ordre fini et divise r .

Soit $m \in \mathbb{Z}$ tel que $c^m = e$. Posons, pour $1 \leq i \leq k$, $r'_i = r_1 \vee \dots \vee r_{i-1} \vee r_{i+1} \vee \dots \vee r_k$. On a

$$c^m = e \implies a_1^m \dots a_k^m = e \implies (a_1^m \dots a_k^m)^{r'_i} = e \implies a_1^{mr'_i} \dots a_k^{mr'_i} = e \implies a_i^{mr'_i} = e$$

donc r_i divise mr'_i . Or les r_i sont premiers entre eux deux à deux donc $r'_i = \prod_{\substack{j=1 \\ j \neq i}}^k r_j$. Par le lemme de Gauss, puisque $r_i \wedge r'_i = 1$, on a r_i divise m pour tout $1 \leq i \leq k$ et par suite, r divise m . D'où c est d'ordre r .

4. On a $\sigma = \underbrace{(1 \ 2 \ 7)}_{=\sigma_1} \underbrace{(3 \ 4 \ 6 \ 8)}_{=\sigma_2} \underbrace{(9 \ 13 \ 11 \ 12 \ 10)}_{=\sigma_3}$. Les cycles σ_1 , σ_2 et σ_3 sont à supports disjoints, donc commutent deux à deux. De plus, l'ordre de σ_1 égal à 3, l'ordre de σ_2 égal à 4 et l'ordre de σ_3 égal à 5. D'où l'ordre de σ est égal à $3 \vee 4 \vee 5 = 60$.

Corrigé de l'exercice 20. 1. Soit $a \in G$ tel que $a \neq e$. On a l'ordre de a divise p donc l'ordre de a égal à 1 ou p . Comme $a \neq e$, alors l'ordre de a égal à p . Par ailleurs, $\langle a \rangle \subset G$ et les groupes $\langle a \rangle$ et G ont même cardinal, donc $G = \langle a \rangle$. Par suite, G est cyclique.

2. a. $\langle a \rangle$ est un sous-groupe de H différent de $\{e\}$, donc nécessairement $H = \langle a \rangle$.
- b. Si a est d'ordre infini alors on a de même pour H . D'après le théorème de classification des groupes monogènes, H est isomorphe à $\mathbb{Z}$ qui contient des sous-groupes non triviaux (on a vu dans le cours que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$, donc si $f : \mathbb{Z} \rightarrow H$ est un isomorphisme de groupes, alors $f(2\mathbb{Z})$ est un sous-groupe non trivial de H) ce qui est absurde donc H est cyclique isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ contient des sous-groupes non triviaux, donc (même raisonnement) H contient des sous-groupes non triviaux ce qui est absurde. Ainsi, H est cyclique d'ordre un nombre premier.

3 Anneaux, corps et algèbres

Corrigé de l'exercice 21. 1. On a $1 = 1 + \sqrt{2} \times 0 \in \mathbb{Z}[\sqrt{2}]$.

Soit $(x, x') \in (\mathbb{Z}[\sqrt{2}])^2$ tel que $x = a + \sqrt{2}b$ et $x' = a' + \sqrt{2}b'$ avec $(a, a', b, b') \in \mathbb{Z}^4$. On a

$$x - x' = \underbrace{a - a'}_{\in \mathbb{Z}} + \sqrt{2} \underbrace{(b - b')}_{\in \mathbb{Z}} \in \mathbb{Z}[\sqrt{2}] \quad \text{et} \quad xx' = \underbrace{aa'}_{\in \mathbb{Z}} + \sqrt{2} \underbrace{(ab' + ba')}_{\in \mathbb{Z}} \in \mathbb{Z}[\sqrt{2}].$$

Donc $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

2. Soit $f : (\mathbb{C}, +, \times) \rightarrow (\mathcal{M}_2(\mathbb{R}), +, \times)$. Vérifiant que f est un morphisme d'anneaux.

$$a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

On a $f(1) = f(1 + i \times 0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. Soit $(a, a', b, b') \in \mathbb{R}^4$. On a

$$f((a+ib) + (a'+ib')) = \begin{pmatrix} a+a' & -(b+b') \\ b+b' & a+a' \end{pmatrix} = f(a+ib)f(a'+ib')$$

et

$$f(a+ib)f(a'+ib') = \begin{pmatrix} aa'-bb' & -(ab'+ba') \\ ab'+ba' & aa'-bb' \end{pmatrix} = f(aa'-bb'+i(ab'+ba')) = f((a+ib)(a'+ib')).$$

Donc f est un morphisme d'anneaux. De plus, $\mathcal{A} = \text{Im } f$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$ donc un anneau.

Soit $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{A}$ non nul, donc a ou b est non nul. Mais $\det M = a^2 + b^2 \neq 0$ et par suite, M est inversible.

D'où $\mathcal{A}$ est un corps.

Il est clair que f est injectif, donc $f: \mathbb{C} \rightarrow \mathcal{A}$ est un isomorphisme de corps.

Corrigé de l'exercice 22. • On a $1 = 1 + i \times 0 \in \mathbb{Z}[i]$.

Soit $(x, x') \in (\mathbb{Z}[i])^2$ tel que $x = a + ib$ et $x' = a' + ib'$ avec $(a, a', b, b') \in \mathbb{Z}^4$. On a

$$x - x' = \underbrace{a - a'}_{\in \mathbb{Z}} + i \underbrace{(b - b')}_{\in \mathbb{Z}} \in \mathbb{Z}[i] \quad \text{et} \quad xx' = \underbrace{aa' - bb'}_{\in \mathbb{Z}} + i \underbrace{(ab' + ba')}_{\in \mathbb{Z}} \in \mathbb{Z}[i].$$

Donc $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

- Soit $z \in \mathbb{U}(\mathbb{Z}[i])$ (groupe des éléments inversibles de l'anneau $\mathbb{Z}[i]$). Il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. On écrit $z = a + ib$ et $z' = a' + ib'$ avec $(a, a', b, b') \in \mathbb{Z}^4$, on a

$$zz' = 1 \implies |z||z'| = 1 \implies \underbrace{(a^2 + b^2)}_{\in \mathbb{N}} \underbrace{(a'^2 + b'^2)}_{\in \mathbb{N}} = 1 \implies a^2 + b^2 = 1$$

donc $(a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}$ et $z \in \{1, i, -1, -i\}$. Inversement, les éléments $1, i, -1$ et $-i$ sont bien inversibles et par suite, $\mathbb{U}(\mathbb{Z}[i]) = \mathbb{U}_4 = \{1, i, -1, -i\}$ groupe des racines 4-ème de l'unité.

Corrigé de l'exercice 23. 1. a. On a

$$\begin{aligned} a \sum_{k=0}^{p-1} (1-a)^k &= (a-1+1) \sum_{k=0}^{p-1} (1-a)^k \\ &= -(1-a) \sum_{k=0}^{p-1} (1-a)^k + \sum_{k=0}^{p-1} (1-a)^k \\ &= -\sum_{k=0}^{p-1} (1-a)^{k+1} + \sum_{k=0}^{p-1} (1-a)^k \\ &= -\sum_{k=1}^p (1-a)^k + \sum_{k=0}^{p-1} (1-a)^k = -(1-a)^p + 1 = 1. \end{aligned}$$

De même, $\left(\sum_{k=0}^{p-1} (1-a)^k\right)a = 1$, donc a est inversible et $a^{-1} = \sum_{k=0}^{p-1} (1-a)^k$.

- b. On a $(1-a)^p = (-a(1-a^{-1}))^p = (-a)^p(1-a^{-1})^p$ car $-a$ et $(1-a^{-1})$ commutent. Par suite, $(1-a^{-1})^p = 0$ car a est inversible.

2. On écrit $M = I_3 - N$ avec $N = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$. On a $N^3 = (I_3 - M)^3 = O_3$ donc d'après la question précédente,

$$\text{la matrice } M \text{ est inversible et } M^{-1} = \sum_{k=0}^2 (I_3 - M)^k = I_3 + I_3 - M + (I_3 - M)^2 = I_3 + N + N^2 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

3. a. • On a $\mathcal{N} \neq \emptyset$ car $0 \in \mathcal{N}$. Si $x \in \mathcal{N}$ et $a \in A$, alors $ax \in \mathcal{N}$. Soit $(x, y) \in \mathcal{N}^2$ donc, il existe $(n, p) \in \mathbb{N}^{*2}$ tel que $x^n = y^p = 0$. Par la formule du binôme, on a

$$(x+y)^{n+p} = \sum_{k=0}^{n+p} \binom{n+p}{k} x^{n+p-k} y^k = \underbrace{x^n \sum_{k=0}^p \binom{n+p}{k} x^{p-k} y^k}_{=0 \text{ car } x^n=0} + \underbrace{y^p \sum_{k=p+1}^{n+p} \binom{n+p}{k} x^{n+p-k} y^{k-p}}_{=0 \text{ car } y^p=0} = 0$$

donc $x+y \in \mathcal{N}$ ce qui permet de conclure que $\mathcal{N}$ est un idéal de A .

- Le résultat n'est pas vrai si A n'est pas commutatif. En effet : si on prend $A = \mathcal{M}_2(\mathbb{R})$ alors les matrices $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$ sont nilpotentes d'ordre 2 mais $A+B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'est pas nilpotente car inversible (matrice de rotation d'angle π).
4. Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers ($n \geq 2$).

- Soit $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ un élément nilpotent. Il existe $\alpha \in \mathbb{N}^*$ tel que $\bar{k}^\alpha = \bar{0}$ donc p_i divise k^α pour tout $1 \leq i \leq r$ et par suite p_i divise k pour tout $1 \leq i \leq r$. Comme les p_i sont premiers entre eux, $\prod_{i=1}^r p_i$ divise k .

- Inversement, si $k = \prod_{i=1}^r p_i \times b$ avec $b \in \mathbb{N}$ alors, en posant $\alpha = \max_{1 \leq i \leq r} p_i$ on a $k^\alpha = nb^\alpha p_1^{\alpha-\alpha_1} \dots p_r^{\alpha-\alpha_r}$ donc $\bar{k}^\alpha = \bar{0}$.

D'où $\mathcal{N} = \left\{ \bar{k} \in \mathbb{Z}/n\mathbb{Z}, \prod_{i=1}^r p_i \text{ divise } k \right\}$.

Corrigé de l'exercice 24. 1. Soit $n \in \mathbb{N}$. On a $f(1) = 1$, $0 = f(0) = f(n-n) = f(n) + f(-n)$ donc $f(-n) = -f(n)$ et

$$f(n) = f(\underbrace{1 + \dots + 1}_n) = \underbrace{f(1) + \dots + f(1)}_n = nf(1) = n.$$

Ainsi, $f(n) = n$ pour tout $n \in \mathbb{Z}$. De plus, pour $m \in \mathbb{N}^*$, on a :

$$1 = f(1) = f\left(\frac{m}{m}\right) = f\left(\frac{1}{m} + \dots + \frac{1}{m}\right) = mf\left(\frac{1}{m}\right) \text{ donc } f\left(\frac{1}{m}\right) = \frac{1}{m}.$$

Si $r = \frac{p}{q} \in \mathbb{Q}$ alors, $f(r) = f\left(\frac{p}{q}\right) = pf\left(\frac{1}{q}\right) = r$. D'où $f(r) = r$ pour tout $r \in \mathbb{Q}$.

2. Soit $x \geq 0$. Il existe $y \in \mathbb{R}$ tel que $x = y^2$ donc $f(x) = f(y^2) = (f(y))^2 \geq 0$.

Si maintenant a et b sont des réels tels que $a \geq b$ alors $a-b \geq 0$, donc $f(a) - f(b) = f(a-b) \geq 0$. Ainsi, f est croissante.

3. Soit $x \in \mathbb{R}$. On a $a_n \leq x < b_n$ avec $a_n = \frac{\lfloor x \cdot 10^n \rfloor}{10^n}$ et $b_n = \frac{\lfloor x \cdot 10^n \rfloor + 1}{10^n}$. D'après la question précédente, on a

$$f(a_n) = a_n \text{ et } f(b_n) = b_n, \text{ donc } a_n \leq f(x) \leq b_n.$$

Comme $a_n \xrightarrow{n \rightarrow +\infty} 0$ et $b_n \xrightarrow{n \rightarrow +\infty} 0$, on en déduit que $f(x) = x$ pour tout $x \in \mathbb{R}$. Ainsi, $f = \text{Id}_{\mathbb{R}}$.

Corrigé de l'exercice 25. 1. On a $\mathbb{U}(\mathbb{Z}/8\mathbb{Z}) = \{\bar{k} \in \mathbb{Z}/8\mathbb{Z}, k \wedge 8 = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

$\bar{k}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
Ordre de $\bar{k}$	1	3	5	7

Aucun élément n'étant d'ordre 4 = Card $\mathbb{U}(\mathbb{Z}/8\mathbb{Z})$. Ainsi, la groupe $\mathbb{U}(\mathbb{Z}/8\mathbb{Z})$ n'est pas cyclique.

2. On a $\mathbb{U}(\mathbb{Z}/11\mathbb{Z}) = \{\bar{k} \in \mathbb{Z}/11\mathbb{Z}, k \wedge 11 = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\}$. Cherchons le sous-groupe de $\mathbb{U}(\mathbb{Z}/11\mathbb{Z})$ engendré par $\bar{2}$. On a $\bar{2}^0 = \bar{1}$, $\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^4 = \bar{16} = \bar{5}$, $\bar{2}^5 = \bar{10}$, $\bar{2}^6 = \bar{9}$, $\bar{2}^7 = \bar{7}$, $\bar{2}^8 = \bar{3}$, $\bar{2}^9 = \bar{6}$. On obtient ainsi tous les éléments de $\mathbb{U}(\mathbb{Z}/11\mathbb{Z})$. Ainsi, $\mathbb{U}(\mathbb{Z}/11\mathbb{Z})$ est cyclique.

Corrigé de l'exercice 26. 1. Soit $a \in I \cap \mathbb{U}(A)$. Si $x \in A$ alors, $x = \underbrace{a^{-1}}_{\in A} \cdot \underbrace{ax}_{\in I} \in I$ car I est un idéal, donc $I = A$.

2. On a A est un anneau commutatif. Soit $x \in A \setminus \{0\}$. L'idéal engendré par x ne peut pas être l'idéal $\{0\}$, donc c'est A tout entier. En particulier, il existe $y \in A$ tel que $xy = yx = 1$. Ainsi, tout élément non nul de A est inversible et par suite, A est un corps.

3. Soit $x \in A \setminus \{0\}$. Considérons, pour $m \in \mathbb{N}$, $I_m = x^m A$, l'idéal engendré par x^m . Puisque A admet un nombre fini d'idéaux, il existe $n < m$ tel que $x^m A = x^n A$. En particulier, il existe $a \in A$ tel que $x^n = x^m a$ donc $x^n(1 - x^{m-n}a) = 0$. L'anneau A étant intègre (et étant non nul), ceci entraîne que $x^{m-n}a = 1$. Ainsi, x est inversible (d'inverse $x^{m-n-1}a$) et par suite, A est un corps.

4. Soit I un idéal non nul de K et soit $x \in I \setminus \{0\}$ alors, x est inversible et d'après la première question, $I = K$.

Corrigé de l'exercice 27. On va montrer que $\mathcal{C}_A$ est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$. On a :

- $I_3 \in \mathcal{C}_A$.
- Si $\lambda \in \mathbb{R}$ et $M, N \in \mathcal{C}_A$, alors $A(M + \lambda N) = AM + \lambda AN = MA + \lambda NA = (M + \lambda N)A$, donc $M + \lambda N \in \mathcal{C}_A$.
- Si $M, N \in \mathcal{C}_A$, alors $AMN = MAN = MNA$, donc $MN \in \mathcal{C}_A$.

D'où $\mathcal{C}_A$ est une algèbre.

Corrigé de l'exercice 28. Il suffit de montrer que $\mathcal{A}$ est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$.

- Si $M = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in \mathcal{A}$, alors $M = \underbrace{a I_3}_{\in \mathcal{A}} + \underbrace{b \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{=M \in \mathcal{A}} + \underbrace{c \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{=N \in \mathcal{A}}$ donc $\mathcal{A} = \text{Vect}(I_3, M, N)$. Ainsi, $\mathcal{A}$ est un

sev de $\mathcal{M}_3(\mathbb{R})$.

- Si $M = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in \mathcal{A}$ et $M' = \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \in \mathcal{A}$, alors $MM' = \begin{pmatrix} aa' + bc' + cb' & ab' + a'b + cc' & ac' + a'c + bb' \\ ac' + a'c + bb' & aa' + bc' + cb' & ab' + a'b + cc' \\ ab' + a'b + cc' & ac' + a'c + bb' & aa' + bc' + cb' \end{pmatrix}$
donc $MM' \in \mathcal{A}$.

D'où $\mathcal{A}$ est une algèbre. De plus, la famille (I_3, M, N) est libre, donc $\dim \mathcal{A} = 3$.

Corrigé de l'exercice 29. • Soit Σ_0 le système $\begin{cases} x \equiv 1[6] \\ x \equiv 2[7] \end{cases}$.

Les entiers 6 et 7 sont premiers entre eux et l'on peut écrire $7 \times 1 + 6 \times (-1) = 1$. L'entier

$$x = 1 \times 7 \times 1 + 2 \times 6 \times (-1) = -5$$

est alors solution du système Σ_0 et donc $\Sigma_0 \iff \begin{cases} x \equiv -5[6] \\ x \equiv -5[7] \end{cases}$.

Par le théorème des restes chinois $\begin{cases} x \equiv -5[6] \\ x \equiv -5[7] \end{cases} \iff x \equiv -5[42]$.

Finalement, les solutions du système sont donc les $-5 + 42k$ avec $k \in \mathbb{Z}$.

- Soit Σ_1 le système $\begin{cases} 3x \equiv 2[5] \\ 5x \equiv 1[6] \end{cases}$.

Les entiers 3 et 5 sont premiers entre eux donc $\bar{3}$ est inversible dans l'anneau $\mathbb{Z}/5\mathbb{Z}$ et l'on peut écrire $5 \times 2 + 3 \times (-3) = 1$ donc l'inverse de $\bar{3}$ dans l'anneau $\mathbb{Z}/5\mathbb{Z}$ est $\bar{-3}$.

De même, l'inverse de $\bar{5}$ dans l'anneau $\mathbb{Z}/6\mathbb{Z}$ est $\bar{-1}$. Ainsi, $\Sigma_1 \iff \begin{cases} x \equiv -6[5] \\ x \equiv -1[6] \end{cases}$.

Par la même démarche que précédemment, les solutions du système sont donc les $-1 + 30k$ avec $k \in \mathbb{Z}$.

- On utilise deux fois le théorème chinois :
$$\begin{cases} x \equiv 3[4] \\ x \equiv 4[5] \\ x \equiv 1[3] \end{cases} \iff \begin{cases} x \equiv 3[4] \\ x \equiv -11[15] \end{cases} \iff x \equiv 19[60].$$

Ainsi, les solutions du système sont donc les $19 + 60k$ avec $k \in \mathbb{Z}$.

Corrigé de l'exercice 30. Résolution de l'équation $x^2 - 4x + 3 = \bar{0}$ dans $\mathbb{Z}/11\mathbb{Z}$. On écrit :

$$x^2 - 4x + 3 = \bar{0} \iff (x - \bar{2})^2 - \bar{1} = \bar{0} \iff (x - \bar{3})(x - \bar{1}) = \bar{0}.$$

L'anneau $\mathbb{Z}/11\mathbb{Z}$ étant intègre (car 11 est premier) donc $x = \bar{3}$ ou $\bar{1}$. L'ensemble des solutions est donc $\{\bar{1}, \bar{3}\}$.

Résolution de l'équation $x^2 - 4x + 3 = \bar{0}$ dans $\mathbb{Z}/8\mathbb{Z}$. On a

$$x^2 - 4x + 3 = \bar{0} \iff (x - \bar{2})^2 = \bar{1}.$$

Il suffit alors de déterminer les éléments $\mathbb{Z}/8\mathbb{Z}$ dont le carré vaut $\bar{1}$.

k	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
k^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$

Donc, l'ensemble des solutions de l'équation $k^2 = \bar{1}$ dans $\mathbb{Z}/8\mathbb{Z}$ est $\{-\bar{7}, -\bar{5}, -\bar{3}, -\bar{1}, \bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Ainsi, l'équation est équivalente $x - \bar{2} \in \{-\bar{7}, -\bar{5}, -\bar{3}, -\bar{1}, \bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. L'ensemble des solutions est donc $\{-\bar{5}, -\bar{3}, -\bar{1}, \bar{1}, \bar{3}, \bar{5}\}$.

Corrigé de l'exercice 31. 1. On a $x^2 = \bar{1} \iff (x - \bar{1})(x + \bar{1}) = 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $x = -\bar{1}$ ou $x = \bar{1}$.

Dans le corps $\mathbb{Z}/p\mathbb{Z}$, tout élément de $\{\bar{1}, \dots, \overline{p-1}\}$ est inversible et son inverse est différent de lui-même, sauf pour $\bar{1}$ et $-\bar{1}$ d'après ci-dessus. Dans le produit $\bar{2} \times \dots \times \overline{p-2}$, on regroupe chaque terme avec son inverse et par suite, on a $\bar{1} \times \dots \times \overline{p-1} = \bar{1} \times \overline{p-1} = -\bar{1}$. D'où $(p-1)! \equiv -1 [p]$.

2. Puisque $k \in \{1, \dots, n-1\}$, alors k est un facteur de $(n-1)!$ et il existe $\ell \in \mathbb{N}$ tel que $(n-1)! = k\ell$ donc $k \times (-\ell) \equiv 1 [n]$ et k est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Comme k est inversible dans $\mathbb{Z}/n\mathbb{Z}$, alors k est premier avec n et ceci est vrai pour tout $k \in \{1, \dots, n-1\}$ et par suite, n est premier. (sinon k divise n donc $k \wedge n \neq 1$)!

Corrigé de l'exercice 32. L'algorithme d'Euclide (divisions euclidiennes successives) donne :

$$\begin{aligned} X^4 - 4X^3 + 2X^2 + X + 6 &= (X^4 - 3X^3 + 2X^2 + X + 5) \times 1 + (-X^3 + 1) \\ X^4 - 3X^3 + 2X^2 + X + 5 &= (-X^3 + 1)(-X + 3) + \underbrace{(2X^2 + 2X + 2)}_{\text{dernier reste non nul}} \\ -X^3 + 1 &= (2X^2 + 2X + 2) \left(-\frac{1}{2}X + \frac{1}{2} \right) + 0 \end{aligned}$$

donc $D = A \wedge B = X^2 + X + 1$ (D est unitaire). Trouvons les coefficients de Bézout U et V tels que $AU + BV = D$. En remontant l'algorithme précédent, on a successivement :

$$\begin{aligned} 2X^2 + 2X + 2 &= (-X^3 + 1)(X - 3) + B \\ 2X^2 + 2X + 2 &= (A - B)(X - 3) + B = A.(X - 3) + (-X + 4).B \end{aligned}$$

On peut donc choisir $U = \frac{1}{2}X - \frac{3}{2}$ et $V = -\frac{1}{2}X + 2$.

Corrigé de l'exercice 33. P est à racines simples si, et seulement si, P et P' n'ont aucune racine complexes en commun si, et seulement si, $P \wedge P' = 1$.

Corrigé de l'exercice 34. 1. Si $\alpha \in \mathbb{K}$ est une racine de P , alors le polynôme $X - \alpha$ divise P et par suite, P n'est pas irréductible sur $\mathbb{K}$.

2. Soit $P \in \mathbb{K}[X]$ tel que $\deg P = 2$ ou 3. Supposons P n'est pas irréductible sur $\mathbb{K}$. On peut écrire P sous la forme $P = AB$ avec $\deg A \geq 1$, $\deg B \geq 1$. Comme $\deg P = 2$ ou 3, nécessairement $\deg A = 1$ ou $\deg B = 1$ et dans les deux cas, P admet une racine dans $\mathbb{K}$.

3. La réciproque n'est pas vraie si $\deg P \geq 4$. En effet : le polynôme $X^4 + 1$ n'a pas de racines dans $\mathbb{R}$ pourtant P n'est pas irréductible sur $\mathbb{R}$ puisque $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ et les deux trinômes obtenus sont à discriminant strictement négatif.

4. Soit $\alpha \in \mathbb{Z}$ une racine de $X^2 - X - 1$. On a $\alpha^2 = \alpha + 1$ donc α divise $\alpha + 1$ ce qui est absurde donc, le polynôme $X^2 - X - 1$ n'a pas de racines dans $\mathbb{Z}$ et par suite, $X^2 - X - 1$ est irréductible sur $\mathbb{Z}$.

De même, le polynôme $X^3 - X - 1$ est irréductible sur $\mathbb{Z}$.

5. Soit $\alpha = \frac{p}{q} \in \mathbb{Q}$ avec $p \wedge q = 1$ une racine de $8X^3 - 6X - 1$. On a

$$8\alpha^3 - 6\alpha - 1 = 0 \iff 8p^3 - 6pq^2 = q^3 \iff 8p^3 = q^2(q + 6p) \implies p \mid q^2(q + 6p) \xrightarrow{\text{Gauss}} p \mid q + 6p \implies p \mid q$$

et ceci est absurde car $p \wedge q = 1$. On en déduit que $8X^3 - 6X - 1$ est irréductible sur $\mathbb{Q}$.

Par linéarisation, on a

$$\cos^3\left(\frac{\pi}{9}\right) = \frac{1}{4} \cos\left(\frac{3\pi}{9}\right) + \frac{3}{4} \cos\left(\frac{\pi}{9}\right) = \frac{1}{8} + \frac{3}{4} \cos\left(\frac{\pi}{9}\right)$$

donc $\cos\left(\frac{\pi}{9}\right)$ est racine de $8X^3 - 6X - 1$ et, par suite, $\cos\left(\frac{\pi}{9}\right)$ est irrationnel.

Corrigé de l'exercice 35. Soit $q \in \llbracket 1, n \rrbracket$ et $\omega_q = e^{2i\pi/q}$. On a

$$\omega_q \text{ est racine de } X^k - 1 \iff \omega_q^k = 1 \iff e^{2ik\pi/q} = 1 \iff \frac{k}{q} \in \mathbb{Z} \iff q \text{ divise } k.$$

Donc le facteur $(X - \omega_q)$ apparaît α_k fois pour chaque $k \in \llbracket 1, n \rrbracket$ tel que q divise k . Ainsi, La multiplicité de ω_q en tant que racine de P vaut $\sum_{\substack{k=1 \\ q \mid k}}^n \alpha_k$.

Corrigé de l'exercice 36. Soit $P \in \mathbb{C}[X]$, $\deg P = n$ tel que P' divise P . Notons $z_1, \dots, z_k$ les racines de P' de multiplicité $\alpha_1, \dots, \alpha_k$.

On a $\sum_{i=1}^k \alpha_i = n - 1$. Comme P' divise P , toute racine de P' est racine de P : $P(z_i) = P'(z_i) = 0$, $1 \leq i \leq k$. Donc

z_i est racine de P de multiplicité $\alpha_i + 1$ et on a, $n \geq \sum_{i=1}^k \alpha_i + 1 = n - 1 + k$ et par suite, $k \leq 1$ c'est-à-dire P' admet une seule racine. On en déduit que $P' = c(X - \alpha)^{n-1}$ avec $c, \alpha \in \mathbb{C}$. Finalement, $P = \lambda(X - \alpha)^n$ avec $\lambda, \alpha \in \mathbb{C}$.

Réciproquement, les polynômes de la forme ci-dessus est solution.

Corrigé de l'exercice 37. On commence par chercher les racines de P . On a :

$$\begin{aligned} P(x) = 0 &\iff \left(\frac{1+x}{1-x}\right)^m = e^{2i\pi\alpha} \text{ avec } \theta_k = \frac{\pi\alpha + k\pi}{m} \\ &\iff \frac{1+x}{1-x} = e^{2i\theta_k} \text{ avec } 1 \leq k \leq m-1 \\ &\iff x = \frac{e^{2i\theta_k} - 1}{e^{2i\theta_k} + 1} \\ &\iff x = \frac{e^{i\theta_k} e^{i\theta_k} - e^{-i\theta_k}}{e^{i\theta_k} e^{i\theta_k} + e^{-i\theta_k}} \text{ règle de l'arc moitié} \\ &\iff x = \frac{2i \sin(\theta_k)}{2 \cos(\theta_k)} \\ &\iff x = i \tan \theta_k \text{ qui est bien défini puisque } \frac{\alpha}{\pi} \text{ n'est pas rationnel.} \end{aligned}$$

On trouve m racines distinctes pour P polynôme de degré m donc $P = \lambda \prod_{k=0}^{m-1} (X - i \tan \theta_k)$ avec λ est le coefficient dominant de P . Or $\lambda = 1 + (-1)^{m+1} e^{2i\pi\alpha}$. Finalement :

$$P = \left(1 + (-1)^{m+1} e^{2i\pi\alpha}\right) \prod_{k=0}^{m-1} (X - i \tan \theta_k).$$

Corrigé de l'exercice 38. Les racines de $X^n - 1$ sont les $e^{2ik\pi/n}$ avec $1 \leq k \leq n-1$ donc $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n})$ (*).

On écrit $\sin\left(x + \frac{k\pi}{n}\right) = \frac{e^{i(x+k\pi/n)} - e^{-i(x+k\pi/n)}}{2i} = \frac{e^{2ik\pi/n} - e^{-2ix}}{2i e^{-ix} e^{ik\pi/n}}$ d'où, en utilisant les relations

- $\prod_{k=0}^{n-1} (e^{-2ix} - e^{2ik\pi/n}) = e^{-2inx} - 1$ obtenue en remplaçant X par e^{-2ix} dans (*) et
- $\prod_{k=0}^{n-1} e^{ik\pi/n} = \exp\left(\frac{i\pi}{n} \frac{n(n-1)}{2}\right) = i^{n-1}$ car $\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}$,

on obtient :

$$\begin{aligned} \Pi_s &= \frac{1}{(2i)^n e^{-inx}} \prod_{k=0}^{n-1} \left(\frac{e^{2ik\pi/n} - e^{-2ix}}{e^{ik\pi/n}} \right) \\ &= \frac{(-1)^n}{(2i)^n e^{-inx}} \frac{\prod_{k=0}^{n-1} (e^{-2ix} - e^{2ik\pi/n})}{\prod_{k=0}^{n-1} e^{ik\pi/n}} \\ &= \frac{(-1)^n}{(2i)^n e^{-inx}} \frac{e^{-2inx} - 1}{i^{n-1}} \\ &= \frac{(-1)^n (-2i \sin nx)}{2^n i^{2n-1}} = \frac{\sin nx}{2^{n-1}}. \end{aligned}$$

De même, $\Pi_c = \frac{\sin(nx + \pi/2)}{2^{n-1}}$ car $\cos x = \sin(x + \pi/2)$.

Corrigé de l'exercice 39. Si $\frac{p}{q}$ est une racine de (*), alors

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \dots + a_1 p q^{n-1} + a_0 q^n = 0 \quad (1).$$

- D'après (1), on a : $a_n p^n = -q(a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q + \dots + a_1 p q^{n-2} + a_0 q^{n-1})$. On en déduit que q divise $a_n p^n$. Comme p et q sont premiers entre eux, par le lemme de Gauss, q divise a_n .
- D'après (1), on a : $-p(a_n p^{n-1} + a_{n-1} p^{n-2} q + a_{n-2} p^{n-3} q^2 + \dots + a_1 q^{n-1}) = a_0 q^n$. On en déduit que p divise $a_0 q^n$. Comme p et q sont premiers entre eux, par le lemme de Gauss, p divise a_0 .