

Groupes

Corrigé de l'exercice 1 : Une loi de groupe sur $\mathbb{R}$ privé de -1

1. En développant, $(1+x)(1+y) - 1 = 1 + x + y + xy - 1 = x + y + xy = x * y$.
Soient maintenant $x, y \in G$. Alors $1+x \neq 0$ et $1+y \neq 0$, donc $(1+x)(1+y) \neq 0$. Par conséquent, $x * y \neq -1$. **La loi $*$ est bien une loi de composition interne sur G .**
2. L'application φ est à valeurs dans $\mathbb{R}^*$, car $1+x \neq 0$ pour $x \in G$. De plus, l'application $u \rightarrow u - 1$, de $\mathbb{R}^*$ dans G , est sa réciproque. Enfin, d'après la question 1, $\varphi(x * y) = 1 + x * y = (1+x)(1+y) = \varphi(x)\varphi(y)$. **Ainsi φ est une bijection qui transforme $*$ en produit.**
3. On transporte la structure de $(\mathbb{R}^*, \times)$. D'abord, pour $x, y, z \in G$, on a $\varphi((x * y) * z) = \varphi(x)\varphi(y)\varphi(z) = \varphi(x * (y * z))$, et φ est injective : la loi est associative. De même, $\varphi(x * y) = \varphi(y * x)$, donc elle est commutative. Ensuite, $\varphi(0) = 1$, d'où $x * 0 = \varphi^{-1}(\varphi(x) \times 1) = x$: 0 est neutre. Enfin, le symétrique de x est $\varphi^{-1}(1/(1+x)) = \frac{1}{1+x} - 1$. **$(G, *)$ est un groupe abélien de neutre 0, et le symétrique de x est $-\frac{x}{1+x}$.** On vérifie : $x * \left(-\frac{x}{1+x}\right) = (1+x) \cdot \frac{1}{1+x} - 1 = 0$.
4. Par récurrence, $\varphi(x^{*n}) = \varphi(x)^n = (1+x)^n$. Donc $x^{*n} = (1+x)^n - 1$. Ensuite, $x * x * x = 7$ équivaut à $(1+x)^3 - 1 = 7$, soit $(1+x)^3 = 8$. La fonction cube étant bijective sur $\mathbb{R}$, cela donne $1+x = 2$. **L'unique solution est $x = 1$.** Vérification : $1 * 1 = 3$, puis $3 * 1 = 3 + 1 + 3 = 7$.

Point de méthode : dès qu'une loi s'écrit $\varphi^{-1}(\varphi(x)\varphi(y))$, transportez la structure de groupe par la bijection φ au lieu de vérifier l'associativité à la main.

Corrigé de l'exercice 2 : Structures de groupe ou non

1. Dans $(\mathbb{N}, +)$, le neutre est 0 , mais $1 + n \geq 1$ pour tout $n \in \mathbb{N}$: 1 n'a pas de symétrique. $(\mathbb{N}, +)$ **n'est pas un groupe**. En revanche, $2\mathbb{Z}$ contient 0 , et $2a - 2b = 2(a - b) \in 2\mathbb{Z}$. C'est donc un sous-groupe de $(\mathbb{Z}, +)$. $(2\mathbb{Z}, +)$ **est un groupe**.
2. Dans $(\mathbb{Z}, \times)$, le neutre est 1 . Or $2u = 1$ n'a pas de solution entière. $(\mathbb{Z}, \times)$ **n'est pas un groupe**. Ensuite, $\{-1, 1\}$ est stable par produit, contient 1 , et chaque élément est son propre inverse. $(\{-1, 1\}, \times)$ **est un groupe**, sous-groupe de $\mathbb{R}^*$.
3. Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2} \times \bar{3} = \bar{6} = \bar{0}$. Le produit de deux éléments de $\mathbb{Z}/6\mathbb{Z} \setminus \{\bar{0}\}$ peut donc en sortir : **ce n'est pas un groupe**, la loi n'est même pas interne. En revanche, 7 est premier. D'une part, si $7 \mid ab$, alors $7 \mid a$ ou $7 \mid b$ (lemme d'Euclide) : la loi est interne. D'autre part, tout $\bar{k} \neq \bar{0}$ est inversible par Bézout. $(\mathbb{Z}/7\mathbb{Z} \setminus \{\bar{0}\}, \times)$ **est un groupe abélien d'ordre 6**.
4. Le neutre de $(\mathcal{M}_2(\mathbb{R}), \times)$ est I_2 . Or la matrice nulle vérifie $0 \times B = 0 \neq I_2$ pour tout B . **Ce n'est pas un groupe**.
5. La loi $-$ n'est pas associative : $(0 - 0) - 1 = 0 - 1 = -1$, tandis que $0 - (0 - 1) = 0 - (-1) = 1$. $(\mathbb{R}, -)$ **n'est pas un groupe**. Remarquons aussi qu'il n'y a pas de neutre : $x - 0 = x$, mais $0 - x = -x$.

Corrigé de l'exercice 3 : Reconnaître des sous-groupes

1. On a $1 \in \mathbb{U}$. De plus, si $|z| = |w| = 1$, alors $|zw^{-1}| = |z|/|w| = 1$. $\mathbb{U}$ **est un sous-groupe de $\mathbb{C}^*$** .
2. On a $1 \in \mathbb{Q}_+^*$, et le quotient de deux rationnels strictement positifs l'est aussi. $\mathbb{Q}_+^*$ **est un sous-groupe de $\mathbb{Q}^*$** .
3. Le neutre 0 est pair, donc $0 \notin 2\mathbb{Z} + 1$. **Ce n'est pas un sous-groupe**. D'ailleurs, $1 + 1 = 2$ n'est pas impair.
4. D'abord, $I_2 \in H$. Ensuite, le produit de deux éléments de H vaut

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix},$$

avec $aa'dd' \neq 0$. Enfin, l'inverse vaut

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & -b/(ad) \\ 0 & 1/d \end{pmatrix},$$

qui est encore dans H . H est un sous-groupe de $GL_2(\mathbb{R})$.

- On a $SL_2(\mathbb{R}) = \ker(\det)$, où $\det: GL_2(\mathbb{R}) \rightarrow \mathbb{R}^*$ est un morphisme. **C'est donc un sous-groupe**, comme tout noyau.
- On a $2 \in H$, mais $2^{-1} = \frac{1}{2} \notin H$. H n'est pas un sous-groupe de $\mathbb{R}^*$.

Corrigé de l'exercice 4 : Sous-groupes de $\mathbb{Z}$ et sous-groupe engendré

- On a $0 = a \times 0 \in a\mathbb{Z}$. De plus, $ak - al = a(k - l) \in a\mathbb{Z}$. $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
- L'ensemble $6\mathbb{Z} + 15\mathbb{Z}$ contient 0 , et la différence de $6u + 15v$ et $6u' + 15v'$ vaut $6(u - u') + 15(v - v')$. C'est donc un sous-groupe, égal à $d\mathbb{Z}$ avec d son plus petit élément strictement positif. Or $3 = 15 - 2 \times 6$ lui appartient, donc $d \mid 3$. De plus, tous ses éléments sont multiples de 3, donc 1 n'en fait pas partie. **Ainsi** $d = 3$: $\langle 6, 15 \rangle = 3\mathbb{Z}$.
- Un entier est dans $6\mathbb{Z} \cap 15\mathbb{Z}$ s'il est multiple de 6 et de 15, donc de 2, 3 et 5. Ces trois nombres sont premiers entre eux deux à deux, donc il est multiple de 30. Réciproquement, 30 est multiple de 6 et de 15. **Donc** $6\mathbb{Z} \cap 15\mathbb{Z} = 30\mathbb{Z}$, et $m = 30 = \text{ppcm}(6, 15)$.
- On a 4 et 6 dans la réunion, mais $6 - 4 = 2$ n'est multiple ni de 4, ni de 6. $4\mathbb{Z} \cup 6\mathbb{Z}$ n'est pas un sous-groupe.
- Comme à la question 2, $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, non nul car il contient a et b . D'après le théorème de classification, il s'écrit $d\mathbb{Z}$ avec $d \geq 1$. D'une part, $a = a \times 1 + b \times 0 \in d\mathbb{Z}$ et de même $b \in d\mathbb{Z}$: d divise a et b . D'autre part,

$d \in a\mathbb{Z} + b\mathbb{Z}$ s'écrit $d = au + bv$. Par conséquent, tout diviseur commun de a et b divise d . **L'entier d est donc le plus grand diviseur commun positif :**
 $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$.

Corrigé de l'exercice 5 : Ordre des éléments de $\mathbb{Z}/12\mathbb{Z}$ et des racines de l'unité

1. On applique la formule du cours : l'ordre de $\bar{k}$ dans $\mathbb{Z}/12\mathbb{Z}$ vaut $12/\text{pgcd}(12, k)$. Ainsi, $\bar{8}$ est d'ordre $12/4 = 3$, $\bar{9}$ d'ordre $12/3 = 4$, et $\bar{5}$ d'ordre $12/1 = 12$. Vérifions pour $\bar{9}$: ses multiples successifs sont $\bar{9}, \bar{6}, \bar{3}, \bar{0}$. **Les ordres sont 3, 4 et 12.**
2. L'élément $\bar{k}$, avec $0 \leq k \leq 11$, est d'ordre 12 si et seulement si $\text{pgcd}(k, 12) = 1$. Il est d'ordre 6 si et seulement si $\text{pgcd}(k, 12) = 2$. **Les éléments d'ordre 12 sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}$; ceux d'ordre 6 sont $\bar{2}$ et $\bar{10}$.**
3. Soit $z = e^{2i\pi p/q}$ avec $\text{pgcd}(p, q) = 1$. Alors $z^m = 1 \Leftrightarrow q \mid pm \Leftrightarrow q \mid m$, par le lemme de Gauss. Donc z est d'ordre q . Ensuite, $\omega = e^{2i\pi \cdot 5/12}$ avec $\text{pgcd}(5, 12) = 1$, et $\zeta = e^{2i\pi \cdot 3/8}$ avec $\text{pgcd}(3, 8) = 1$. **Donc ω est d'ordre 12 et ζ d'ordre 8.**
4. On a $|1 + i| = \sqrt{2}$, donc $|(1 + i)^n| = 2^{n/2} > 1$ pour tout $n \geq 1$. Ainsi $(1 + i)^n \neq 1$. **L'élément $1 + i$ est d'ordre infini.**

Corrigé de l'exercice 6 : Noyau et image de morphismes usuels

1. On a $|zw| = |z||w|$, donc f est un morphisme. Son noyau est $\{z : |z| = 1\} = \mathbb{U}$. De plus, tout réel $r > 0$ vérifie $f(r) = r$. **Ainsi $\ker f = \mathbb{U}$ et $\text{Im } f = \mathbb{R}_+^*$: f est surjective, non injective.**
2. On a $(xy)^2 = x^2 y^2$, donc g est un morphisme. Ensuite, $x^2 = 1 \Leftrightarrow x = \pm 1$. Enfin, un réel y est un carré non nul si et seulement si $y > 0$, avec $y = (\sqrt{y})^2$. **Ainsi $\ker g = \{-1, 1\}$ et $\text{Im } g = \mathbb{R}_+^*$: g n'est ni injective, ni surjective.**

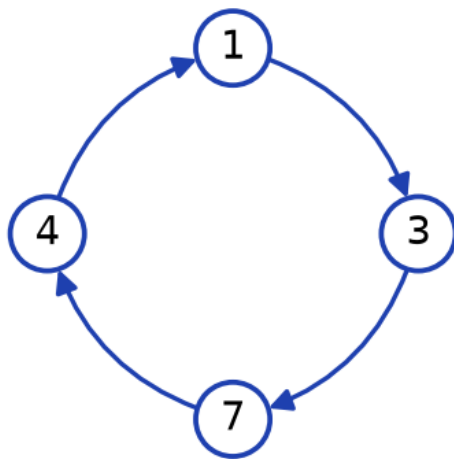
3. La formule $\det(AB) = \det A \det B$ montre que $\det$ est un morphisme. Son noyau est $\text{SL}_n(\mathbb{R})$. Pour $t \in \mathbb{R}^*$, la matrice diagonale $\text{diag}(t, 1, \dots, 1)$ est inversible de déterminant t . **Donc** $\ker(\det) = \text{SL}_n(\mathbb{R})$ **et** $\text{Im}(\det) = \mathbb{R}^*$: **le déterminant est surjectif, et non injectif dès que $n \geq 2$** . Par exemple, $\text{diag}(2, 1/2)$ est dans le noyau. Pour $n = 1$, en revanche, $\det$ est l'identité de $\mathbb{R}^*$.
4. Si $\bar{k} = \bar{l}$, alors $6 \mid k - l$, donc $6 \mid 2k - 2l$ et $\overline{2k} = \overline{2l}$: h est bien définie. Ensuite, $h(\bar{k} + \bar{l}) = \overline{2k + 2l} = h(\bar{k}) + h(\bar{l})$. Le noyau est formé des $\bar{k}$ avec $6 \mid 2k$, c'est-à-dire $3 \mid k$. L'image est $\{\overline{0}, \overline{3}\}$. **Ainsi** $\ker h = \{\overline{0}, \overline{3}\}$ **et** $\text{Im } h = \{\overline{0}, \overline{3}\}$: h **n'est ni injective, ni surjective**. On remarque que $2 \times 3 = 6$.

Point de méthode : sur un ensemble quotient comme $\mathbb{Z}/n\mathbb{Z}$, vérifiez toujours qu'une formule ne dépend pas du représentant choisi avant de parler de morphisme.

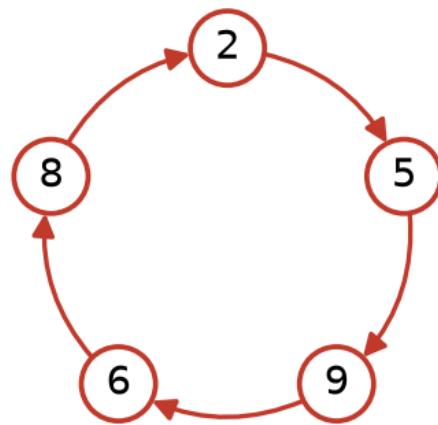
Corrigé de l'exercice 7 : Décomposition d'une permutation en cycles

1. On suit les flèches à partir de 1 : $1 \rightarrow 3 \rightarrow 7 \rightarrow 4 \rightarrow 1$. Ensuite, le plus petit élément restant est 2 : $2 \rightarrow 5 \rightarrow 9 \rightarrow 6 \rightarrow 8 \rightarrow 2$. Tous les entiers de 1 à 9 sont atteints. **Donc**
- $$\sigma = \begin{pmatrix} 1 & 3 & 7 & 4 \\ 3 & 7 & 4 & 1 \\ 2 & 5 & 9 & 6 & 8 \end{pmatrix}$$
- . La figure ci-dessous montre ces deux orbites.

ordre de σ : $\text{ppcm}(4, 5) = 20$



$c_1 = (1\ 3\ 7\ 4)$: ordre 4



$c_2 = (2\ 5\ 9\ 6\ 8)$: ordre 5

2. Les deux cycles sont disjoints, de longueurs 4 et 5. L'ordre vaut donc $\text{ppcm}(4, 5) = 20$. De plus, un k -cycle a pour signature $(-1)^{k-1}$. **L'ordre de σ est 20 et**
 $\varepsilon(\sigma) = (-1)^3 (-1)^4 = -1$.

3. L'inverse d'un cycle s'obtient en le parcourant à l'envers. Comme les deux cycles commutent,

$$\sigma^{-1} = (1, 4, 7, 3)(2, 8, 6, 9, 5) .$$

$\sigma^{-1} = c_1^{-1} c_2^{-1}$. **Donc**

4. On a $2026 = 20 \times 101 + 6$, donc $\sigma^{2026} = \sigma^6$. Ensuite, les cycles commutent :

$$\sigma^6 = c_1^6 c_2^6 . \text{ Or } c_1^4 = \text{Id} \text{ et } c_2^5 = \text{Id} , \text{ d'où } c_1^6 = c_1^2 \text{ et } c_2^6 = c_2 . \text{ Enfin, } c_1^2$$

$\sigma^{2026} = (1, 7)(3, 4)(2, 5, 9, 6, 8)$
 envoie $1 \rightarrow 7$, $7 \rightarrow 1$, $3 \rightarrow 4$ et $4 \rightarrow 3$. **Ainsi**

5. On utilise $(a_1, a_2, \dots, a_k) = (a_1, a_2, \dots, a_{k-1}, a_k)$. **Donc** $\sigma = (1, 3)(3, 7)(7, 4)(2, 5)(5, 9)(9, 6)(6, 8)$. On retrouve la signature : sept transpositions
- donnent $(-1)^7 = -1$.

Corrigé de l'exercice 8 : Ordres de matrices et produit d'éléments d'ordre fini

1. Le calcul donne

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A^3 = A^2 A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2.$$

Par conséquent, $A^6 = (-I_2)^2 = I_2$, et l'ordre de A divise 6. Or $A \neq I_2$, $A^2 \neq I_2$ et $A^3 \neq I_2$. **La matrice A est d'ordre 6.**

2. On calcule $B^2 = -I_2$, donc $B^4 = I_2$, tandis que $B \neq I_2$ et $B^2 \neq I_2$. **B est d'ordre 4.** Ensuite,

$$C^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad C^3 = C^2 C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Comme $C \neq I_2$, l'ordre divise 3 et vaut 3. **C est d'ordre 3.**

3. On obtient $BC = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par récurrence, $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$, donc $(BC)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2$ pour $n \geq 1$. **BC est d'ordre infini.** Ainsi, dans un groupe non abélien, le produit de deux éléments d'ordre fini peut être d'ordre infini.

4. Comme G est abélien, $(ab)^k = a^k b^k$ pour tout k . D'abord, $(ab)^{mn} = (a^m)^n (b^n)^m = e$. Ensuite, supposons $(ab)^k = e$. Alors $a^k = b^{-k}$ appartient à $\langle a \rangle \cap \langle b \rangle$. Ce sous-groupe a un ordre qui divise m et n par Lagrange, donc il

vaut 1. Ainsi $a^k = e$ et $b^k = e$, d'où $m \mid k$ et $n \mid k$. Comme m et n sont premiers entre eux, $mn \mid k$. **L'élément ab est d'ordre mn .**

Corrigé de l'exercice 9 : Morphismes de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/18\mathbb{Z}$

- Pour $k \geq 0$, on a $\bar{k} = \bar{1} + \dots + \bar{1}$ (k termes). Comme f est un morphisme, $f(\bar{k}) = ka$. Tout élément de $\mathbb{Z}/12\mathbb{Z}$ a un représentant $k \in \left\{ \begin{smallmatrix} 0, \\ \text{fs}4\dots, 11 \end{smallmatrix} \right\}$, donc f est entièrement déterminé par a . Enfin, $12a = f(\bar{12}) = f(\bar{0}) = \bar{0}$. **Donc $f(\bar{k}) = ka$ et $12a = \bar{0}$.**
- Si $\bar{k} = \bar{l}$ dans $\mathbb{Z}/12\mathbb{Z}$, alors $k - l = 12q$, et $ka - la = q(12a) = \bar{0}$. La formule ne dépend donc pas du représentant. De plus, $(k + l)a = ka + la$. **L'application $\bar{k} \rightarrow ka$ est un morphisme.**
- Écrivons $a = \bar{\alpha}$ avec $0 \leq \alpha \leq 17$. La condition $12a = \bar{0}$ s'écrit $18 \mid 12\alpha$, soit $3 \mid 2\alpha$, soit $3 \mid \alpha$ par le lemme de Gauss. **Les morphismes sont les $f_\alpha : \bar{k} \rightarrow \alpha \bar{k}$ avec $\alpha \in \{0, 3, 6, 9, 12, 15\}$: il y en a 6.** On remarque que $6 = \text{pgcd}(12, 18)$.
- Pour $a = \bar{3}$, on a $f(\bar{k}) = \bar{3k}$. Ensuite, $18 \mid 3k \Leftrightarrow 6 \mid k$. Dans $\mathbb{Z}/12\mathbb{Z}$, cela donne deux classes. De plus, l'image est formée des multiples de $\bar{3}$ dans $\mathbb{Z}/18\mathbb{Z}$. **Donc $\ker f = \{\bar{0}, \bar{6}\}$ et $\text{Im } f = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\}$.** On vérifie que $2 \times 6 = 12$.
- Un morphisme injectif aurait une image à 12 éléments. Cette image serait un sous-groupe de $\mathbb{Z}/18\mathbb{Z}$, donc son ordre diviserait 18 par Lagrange. Or 12 ne divise pas 18. **Il n'existe aucun morphisme injectif de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/18\mathbb{Z}$.**

Corrigé de l'exercice 10 : Centre et automorphismes intérieurs

- D'abord, $e \in Z(G)$. Soient ensuite $a, b \in Z(G)$ et $x \in G$. De $bx = xb$, on tire $xb^{-1} = b^{-1}x$ en multipliant par b^{-1} à gauche et à droite. Donc $ab^{-1}x = axb^{-1} = xab^{-1}$. **Ainsi $Z(G)$ est un sous-groupe de G .**

2. On a $\varphi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$. De plus,
 $\varphi_{g^{-1}}(\varphi_g(x)) = g^{-1}gxg^{-1}g = x$, et de même dans l'autre ordre. **Donc φ_g est un automorphisme de G , de réciproque $\varphi_{g^{-1}}$.**

3. Pour $g, h, x \in G$, $\varphi_{gh}(x) = ghxh^{-1}g^{-1} = \varphi_g(\varphi_h(x))$. Donc
 $\Phi(gh) = \Phi(g) \circ \Phi(h)$. Ensuite, $\varphi_g = \text{Id}$ signifie $gxg^{-1} = x$ pour tout x , soit
 $gx = xg$. **Φ est un morphisme de noyau $Z(G)$.**

4. On calcule, en appliquant d'abord le facteur de droite :

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

Donc $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ ne sont pas dans le centre. De même, $\begin{pmatrix} 2 \\ 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 3 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, donc

$\begin{pmatrix} 2 \\ 3 \end{pmatrix} \notin Z(S_3)$. Ensuite, $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, donc $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \notin Z(S_3)$. Enfin, $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ est l'inverse de

$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$; comme $Z(S_3)$ est un sous-groupe, il n'y est pas non plus. **Donc $Z(S_3) = \{\text{Id}\}$, et**

Φ est injectif : S_3 est isomorphe au sous-groupe $\Phi(S_3)$ de $\text{Aut}(S_3)$.

Corrigé de l'exercice 11 : Groupes d'exposant 2

1. L'hypothèse $x^2 = e$ signifie $x^{-1} = x$ pour tout x . Donc, pour $x, y \in G$,
 $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. **Le groupe G est abélien.**

2. Une double transposition $(a\ b)(c\ d)$, à supports disjoints, a pour carré $(a\ b)^2(c\ d)^2 = \text{Id}$. Calculons ensuite les

produits, en appliquant d'abord le facteur de droite :

$$\begin{aligned} & (1\ 2)(3\ 4) \cdot (1\ 3)(2\ 4) = (1\ 4)(2\ 3), \\ & (1\ 3)(2\ 4) \cdot (1\ 2)(3\ 4) = (1\ 4)(2\ 3). \end{aligned}$$

De même, $(1\ 2)(3\ 4) \cdot (1\ 4)(2\ 3) = (1\ 3)(2\ 4)$ et $(1\ 4)(2\ 3) \cdot (1\ 2)(3\ 4) = (1\ 3)(2\ 4)$. Ainsi, le produit de deux éléments distincts non triviaux est le troisième. Par conséquent, V contient Id , est stable par produit et par inverse. **V est un**

sous-groupe de S_4 d'ordre 4 dont tous les éléments vérifient $x^2 = \text{Id}$.

3. Soit $x \neq e$ dans G . Alors $x^2 = e$, donc x est d'ordre 2. Par le théorème de Lagrange, l'ordre de x divise $|G|$. **Donc $|G|$ est pair.**
4. Le groupe $(\mathbb{Z}, +)$ est abélien, mais $1 + 1 = 2 \neq 0$. **Un groupe abélien n'est pas forcément d'exposant 2.**

Corrigé de l'exercice 12 : Élément d'ordre 2 dans un groupe d'ordre pair

1. Si $x \in A$, alors $x^{-1} \neq x = (x^{-1})^{-1}$, donc $x^{-1} \in A$. Ainsi, $x \rightarrow x^{-1}$ est une involution de A sans point fixe. Elle regroupe les éléments de A en paires disjointes $\{x, x^{-1}\}$. **Donc $|A|$ est pair.**
2. Le complémentaire $G \setminus A$ est l'ensemble des x tels que $x^2 = e$. Il contient e et les éléments d'ordre 2. Son cardinal $|G| - |A|$ est pair, comme différence de deux nombres pairs. Par conséquent, le nombre d'éléments d'ordre 2 vaut $|G| - |A| - 1$, qui est impair. **G possède un nombre impair, donc non nul, d'éléments d'ordre 2.**
3. Par Lagrange, l'ordre de tout élément divise $|G|$. Or 2 ne divise pas un nombre impair. **Un groupe d'ordre impair n'a aucun élément d'ordre 2.**
4. Dans S_3 , les éléments d'ordre 2 sont les trois transpositions. Dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{k}$ est d'ordre 2 si et seulement si $8/\text{pgcd}(8, k) = 2$, soit $k = 4$. **On trouve 3 et 1 éléments d'ordre 2 : ce sont bien des nombres impairs.**

Corrigé de l'exercice 13 : Classes à gauche et à droite dans S_3

1. L'ensemble H contient Id , et $\begin{pmatrix} 1 & \\ & 2 \end{pmatrix}^2 = \text{Id}$: il est stable par produit et par inverse. Ensuite,

$(1, 2, 3)^2 = (1, 3, 2)$ et $(1, 2, 3)^3 = \text{Id}$. Donc $H = \langle (1, 2, 3) \rangle$ et $K = \langle (1, 2) \rangle$. H et K sont des sous-groupes de S_3 , d'ordres 2 et 3.

2. Une classe à gauche s'écrit $\sigma H = \{ \sigma, \sigma(1, 2) \}$. On calcule $(1, 2)(1, 2, 3) = (1, 3, 2)$ et $(1, 2)(1, 3, 2) = (1, 2, 3)$. Pour les

classes à droite $H\sigma = \{ \sigma, (1, 2)\sigma \}$, on calcule $(1, 2)(1, 2, 3) = (1, 3, 2)$ et $(1, 2)(1, 3, 2) = (1, 2, 3)$. On obtient :

$[?][?] \text{ gauche : } H,$
 $\{ (1, 2, 3), (1, 3, 2) \},$
 $\{ (1, 2, 3), (1, 3, 2) \};$

$[?][?] \text{ droite : } H,$
 $\{ (1, 2, 3), (1, 3, 2) \},$
 $\{ (1, 2, 3), (1, 3, 2) \}.$

Les partitions diffèrent : par exemple $(1, 3)H \neq H(1, 3)$. La figure ci-dessous compare les deux partitions.

classes à gauche σH	classes à droite $H\sigma$
id (1 2)	id (1 2)
(1 3) (1 2 3)	(1 3) (1 3 2)
(2 3) (1 3 2)	(2 3) (1 2 3)

3. Les classes à gauche modulo K forment une partition en parts de 3 éléments. L'une est K , l'autre est donc le complémentaire $\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}$. Le même argument vaut à droite. **Modulo K ,**

les classes à gauche et à droite coïncident : K et l'ensemble des transpositions.

4. On a $|H| = 2$, qui divise 6, avec 3 classes : $6 = 2 \times 3$. De même, $|K| = 3$, avec 2 classes : $6 = 3 \times 2$. **Le théorème de Lagrange est vérifié dans les deux cas.**

Point de méthode : un sous-groupe d'indice 2 a toujours les mêmes classes à gauche et à droite, car l'unique classe différente de H est son complémentaire.

Corrigé de l'exercice 14 : Lagrange et calculs modulaires

1. L'ensemble des inversibles d'un anneau contient $\bar{1}$, est stable par produit, car $(xy)^{-1} = y^{-1}x^{-1}$, et par inverse. C'est donc un groupe. D'après le cours, $\bar{k}$ est inversible si et seulement si $\text{pgcd}(k, n) = 1$. Il y a donc $\varphi(n)$ inversibles. Par le corollaire de Lagrange, $\bar{a}^{\varphi(n)} = \bar{1}$. Si $\text{pgcd}(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.
2. On a $7^2 = 49 = 3 \times 15 + 4$, donc $\bar{7}^2 = \bar{4}$, puis $\bar{7}^4 = \bar{16} = \bar{1}$. L'ordre divise 4 et n'est ni 1 ni 2 : il vaut 4. De plus, $\varphi(15) = \varphi(3)\varphi(5) = 8$, et 4 divise 8. Enfin, $100 = 4 \times 25$.
Donc $7^{100} \equiv 1 \pmod{15}$.
3. Les puissances de 2 modulo 13 sont $2, 4, 8, 16 \equiv 3$, puis $2^6 = 64 \equiv 12 \equiv -1$. Donc $2^{12} \equiv 1$. L'ordre divise 12 ; or $2^1, 2^2, 2^3, 2^4, 2^6$ ne valent pas 1. L'ordre de $\bar{2}$ est donc 12. Ensuite, $1000 = 12 \times 83 + 4$, d'où $2^{1000} \equiv 2^4 \equiv 3$. **Le reste de 2^{1000} modulo 13 est 3.**
4. L'ordre d'un sous-groupe divise p , donc vaut 1 ou p . **Les seuls sous-groupes sont $\{e\}$ et G .**

Corrigé de l'exercice 15 : Conjugaison et produit de cycles

1. Comparons les deux permutations en tout point y . Si $y = \tau(a_i)$ avec $i < k$, alors $\tau \circ \tau^{-1}(y) = \tau(\tau^{-1}(y)) = \tau(a_i)$. De même, $\tau \circ \tau^{-1}(\tau(a_k)) = \tau(a_1)$. Enfin, si y n'est aucun des $\tau(a_i)$, alors $\tau^{-1}(y)$ n'est aucun des a_i et il est fixé par τ . Donc $\tau \circ \tau^{-1} = (\tau(a_1) \dots \tau(a_k))$.
 $\tau \circ \tau^{-1}(y) = y$. **Ainsi** $\tau \circ \tau^{-1} = (\tau(a_1) \dots \tau(a_k))$.
2. On applique d'abord τ , puis τ^{-1} : $1 \rightarrow 1 \rightarrow 2$, $2 \rightarrow 3 \rightarrow 1$, $3 \rightarrow 4 \rightarrow 4$ et $4 \rightarrow 2 \rightarrow 3$. **Donc** $\tau \circ \tau^{-1} = (1 \ 2 \ 3 \ 4)$. Remarquons que la signature est cohérente : $(+1)(+1) = (-1)(-1)$.

3. D'après la question 1, $\begin{pmatrix} \rho(1) \\ \rho(3) \end{pmatrix} \rho^{-1} = \begin{pmatrix} \rho(1) \\ \rho(3) \end{pmatrix}$. **Donc** $\begin{pmatrix} \rho(1) \\ \rho(3) \end{pmatrix} \rho^{-1} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$.

4. Soient $\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ et $\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$ deux cycles. Les ensembles $\{a_i\}$ et $\{b_i\}$ ont k éléments, donc leurs complémentaires ont $n - k$ éléments. On définit τ par $\tau(a_i) = b_i$, puis on la complète par une bijection quelconque entre les complémentaires. D'après la question 1, $\begin{pmatrix} \tau(a_1) \\ \vdots \\ \tau(a_k) \end{pmatrix} \tau^{-1} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$:

les deux cycles sont conjugués.

Corrigé de l'exercice 16 : Ordres des éléments de S_5 et S_6

1. Un k -uplet $(a_1, \dots, a_k)$ d'éléments distincts se choisit de $n(n-1) \dots (n-k+1) = \frac{n!}{(n-k)!}$ façons. Or chaque k -cycle est décrit par exactement k tels uplets, obtenus par permutation

circulaire : $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_2 \\ \vdots \\ a_k \\ a_1 \end{pmatrix}$. **Il y a donc $\frac{n!}{k(n-k)!}$ cycles de longueur k .**

2. L'ordre d'une permutation est le ppcm des longueurs de ses cycles. Pour S_5 , les longueurs possibles (en omettant les points fixes) sont : 5 ; 4 ; 3, 2 ; 3 ; 2, 2 ; 2 ; aucune. Les ordres correspondants sont 5, 4, 6, 3, 2, 2, 1. Pour S_6 , les types autres que l'identité sont 6 ; 5 ; 4, 2 ; 4 ; 3, 3 ; 3, 2 ; 3 ; 2, 2, 2 ; 2, 2 ; 2, d'ordres 6, 5, 4, 4, 3, 6, 3, 2, 2, 2. **Dans les deux cas, l'ensemble des ordres est $\{1, 2, 3, 4, 5, 6\}$.**

3. Dans S_5 , un élément d'ordre 6 est forcément le produit d'un 3-cycle et d'une transposition disjointe. On choisit le 3-cycle de $\frac{5!}{3 \times 2!} = 20$ façons. Ensuite, la transposition est imposée : elle échange les deux éléments restants. **S_5 contient 20 éléments d'ordre 6.**

4. Un sous-groupe cyclique d'ordre 10 serait engendré par un élément d'ordre 10. Or, d'après la question 2, aucun élément de S_5 n'est d'ordre 10. **S_5 n'a pas de sous-groupe cyclique d'ordre 10.**

Corrigé de l'exercice 17 : Le groupe des isométries du carré

1. Une isométrie g de D_4 est linéaire, donc elle conserve la distance à O . Or les sommets sont exactement les points du carré à distance $\sqrt{2}$ de O . Donc g permute les sommets, et $\Phi(g) \in \mathcal{S}_4$ est bien défini. Ensuite, le sommet image de i par gh est l'image par g de l'image par h : $\Phi(gh) = \Phi(g)\Phi(h)$. Enfin, si $\Phi(g) = \text{Id}$, alors g fixe les vecteurs $(1, 1)$ et $(-1, 1)$, qui forment une base de $\mathbb{R}^2$. Comme g est linéaire, $g = \text{Id}$. **Φ est un morphisme injectif.**
2. La rotation r s'écrit $(x, y) \rightarrow (-y, x)$: elle envoie $(1, 1)$ sur $(-1, 1)$, c'est-à-dire 1 sur 2, puis 2 sur 3, 3 sur 4 et 4 sur 1. Pour les symétries, $s_1 : (x, y) \rightarrow (y, x)$, $s_2 : (x, y) \rightarrow (-y, -x)$, $s_3 : (x, y) \rightarrow (-x, y)$ et $s_4 : (x, y) \rightarrow (x, -y)$. On obtient :

$$\begin{aligned} \Phi(r) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \Phi(r^2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \\ \Phi(r^3) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \\ \Phi(s_1) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\ \Phi(s_2) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\ \Phi(s_3) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \\ \Phi(s_4) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}. \end{aligned}$$

Avec $\Phi(\text{Id}) = \text{Id}$, ce sont les huit permutations cherchées.

- calcul : $(\begin{smallmatrix} 1 \\ 2 \\ 3 \\ 4 \end{smallmatrix}) = (\begin{smallmatrix} 1 \\ 2 \end{smallmatrix})(\begin{smallmatrix} 3 \\ 4 \end{smallmatrix})$. Comme $rs_1 \neq s_1 r$, le groupe D_4 n'est pas abélien.

- Ainsi $\overline{17} \times \overline{-7} = 1$. **L'inverse de $\overline{17}$ dans $\mathbb{Z}/60\mathbb{Z}$ est $\overline{53}$.** Vérification :
 $17 \times 53 = 901 = 15 \times 60 + 1$.

5. Soit $a \neq 0$ et $m_a: x \rightarrow ax$. Si $ax = ay$, alors $a(x - y) = 0$, donc $x = y$ par intégrité : m_a est injective. Comme A est fini, m_a est aussi surjective. Il existe donc x avec $ax = 1$. **Tout élément non nul est inversible : A est un corps.**

Corrigé de l'exercice 19 : Idéaux de $\mathbb{Z}$ et de $\mathbb{R}[X]$

- D'après l'exercice 4, $12\mathbb{Z} + 18\mathbb{Z} = \text{pgcd}(12, 18)\mathbb{Z}$ et $12\mathbb{Z} \cap 18\mathbb{Z} = \text{ppcm}(12, 18)\mathbb{Z}$.
On obtient $6\mathbb{Z}$ et $36\mathbb{Z}$. Ce sont des sous-groupes de $\mathbb{Z}$, et $k \times nm = n(km)$: ils absorbent la multiplication. Ce sont donc des idéaux.
- L'évaluation $\text{ev}_1: P \rightarrow P(1)$ est un morphisme d'anneaux : $(P + Q)(1) = P(1) + Q(1)$, $(PQ)(1) = P(1)Q(1)$ et le polynôme constant 1 vaut 1 en 1. Donc $I = \ker \text{ev}_1$ est un idéal. Ensuite, $(X - 1)\mathbb{R}[X] \subset I$ clairement. Inversement, si $P(1) = 0$, la division euclidienne donne $P = (X - 1)Q + c$, avec c constant. En évaluant en 1, on trouve $c = 0$. **Donc $I = (X - 1)\mathbb{R}[X]$.**
- On a $J = \ker \text{ev}_1 \cap \ker \text{ev}_2$, intersection de deux idéaux : c'est un idéal. Si $P \in J$, alors $P = (X - 1)Q$ par la question 2. Puis $0 = P(2) = Q(2)$, donc $Q = (X - 2)R$. La réciproque est immédiate. **Ainsi $J = (X - 1)(X - 2)\mathbb{R}[X]$.**
- Soit I un idéal de K non réduit à $\{0\}$, et $x \in I$ non nul. Alors x est inversible, donc $1 = x^{-1}x \in I$. Par conséquent, $a = a \times 1 \in I$ pour tout $a \in K$. **Les seuls idéaux de K sont $\{0\}$ et K .**
- On a $1 \in \mathbb{Z}$, mais $\frac{1}{2} \times 1 = \frac{1}{2} \notin \mathbb{Z}$. **$\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$, mais pas un idéal.**
C'est cohérent avec la question 4.

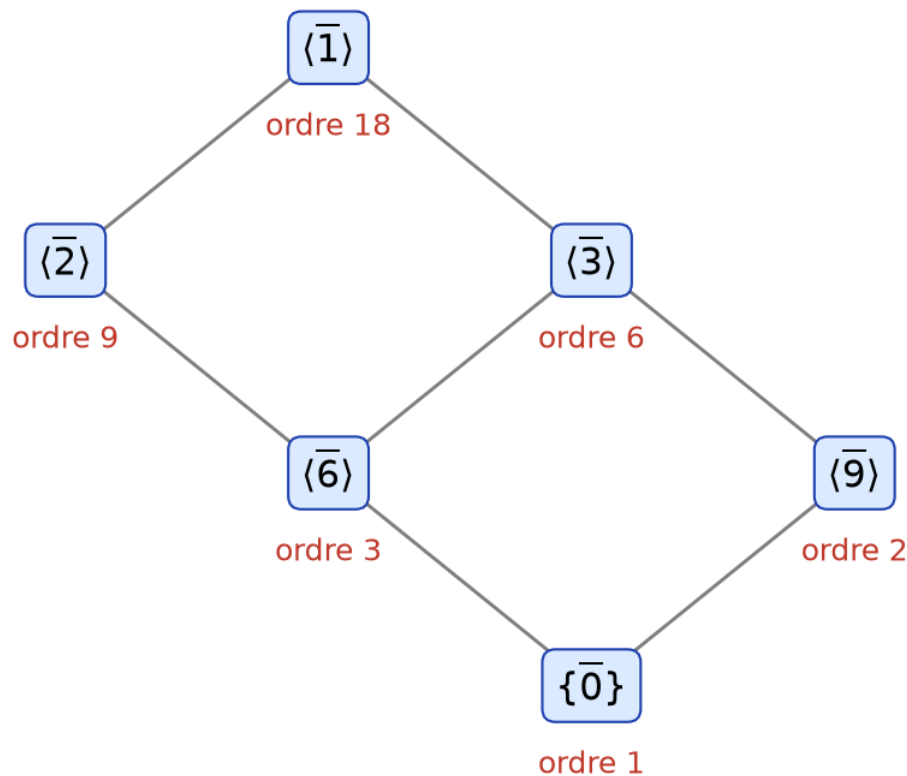
Corrigé de l'exercice 20 : Sous-groupes d'un groupe cyclique

- L'application $\psi: \mathbb{Z} \rightarrow G$, $k \rightarrow a^k$, est un morphisme surjectif. L'ensemble $L = \{k: a^k \in H\} = \psi^{-1}(H)$ est donc un sous-groupe de $\mathbb{Z}$. Il s'écrit $m\mathbb{Z}$, avec

$m \geq 1$ car $n \in L$. Ensuite, tout $h \in H$ s'écrit a^k avec $k \in L$, donc $k = mj$ et $h = (a^m)^j$. Ainsi $H = \langle a^m \rangle$ est cyclique.

2. D'abord, $a^{n/d}$ est d'ordre $\frac{n}{\text{pgcd}(n, n/d)} = \frac{n}{n/d} = d$. Donc $\langle a^{n/d} \rangle$ est d'ordre d . Soit maintenant H un sous-groupe d'ordre d , et $x = a^k \in H$. Par Lagrange, $x^d = e$, donc $n \mid kd$, puis $\frac{n}{d} \mid k$. Par conséquent, $x \in \langle a^{n/d} \rangle$. On a donc $H \subset \langle a^{n/d} \rangle$, et les deux ont d éléments. $\langle a^{n/d} \rangle$ est l'unique sous-groupe d'ordre d .

3. Les diviseurs de 18 sont 1, 2, 3, 6, 9 et 18. Le sous-groupe d'ordre d est engendré par $\overline{18/d}$. Ensuite, le sous-groupe d'ordre d est inclus dans celui d'ordre d' si et seulement si $d \mid d'$. En effet, la condition est nécessaire par Lagrange ; elle est suffisante car $\overline{18/d}$ est alors un multiple de $\overline{18/d'}$. Les sous-groupes sont $\{\bar{0}\}$, $\langle \bar{9} \rangle$ (ordre 2), $\langle \bar{6} \rangle$ (ordre 3), $\langle \bar{3} \rangle$ (ordre 6), $\langle \bar{2} \rangle$ (ordre 9) et $\mathbb{Z}/18\mathbb{Z}$. La figure ci-dessous résume les inclusions.



4. Chaque $x \in G$ engendre $\langle x \rangle$, dont l'ordre d divise n . C'est l'unique sous-groupe H_d d'ordre d , et x en est un générateur. Ainsi, G est la réunion disjointe, pour $d \mid n$, des ensembles de générateurs de H_d . Or H_d est cyclique d'ordre d , isomorphe à $\mathbb{Z}/d\mathbb{Z}$, donc il a $\varphi(d)$ générateurs. Par conséquent, $\sum_{d \mid n} \varphi(d) = n$. Pour $n = 18$:
 $1 + 1 + 2 + 2 + 6 + 6 = 18$.

Corrigé de l'exercice 21 : Générateurs du groupe symétrique

1. On applique les facteurs de droite à gauche. D'abord, $i \rightarrow 1 \rightarrow j \rightarrow j$. Ensuite,

$j \rightarrow j \rightarrow 1 \rightarrow i$. De plus, $1 \rightarrow i \rightarrow i \rightarrow 1$, et les autres points sont fixes. Donc $(1, i)(1, j)(1, i) = (i, j)$.

. Or toute permutation est un produit de transpositions, et chaque transposition est de la forme $(1, k)$.

ou s'écrit avec elles. **Les transpositions $(1, k)$ engendrent S_n .**

2. Posons $\tau = (k, k+1)$, qui vérifie $\tau^{-1} = \tau$. D'après la formule de conjugaison, $(\tau(k)) = (1, k+1)$, car $\tau(1) = 1$ pour $k \geq 2$. Par récurrence sur k , toutes les $(1, k)$ sont dans $\langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.

Par la question 1, les transpositions $(k, k+1)$ engendrent S_n .

3. Par la formule de conjugaison, $(c^k t c^{-k}) = (c^k(1), c^k(2)) = (k+1, k+2)$ pour $0 \leq k \leq n-2$. **Donc**

$c^k t c^{-k} = (k+1, k+2)$. Ainsi, $\langle t, c \rangle$ contient toutes les transpositions $(k, k+1)$. **Par la question 2, $S_n = \langle t, c \rangle$.**

4. Les deux transpositions fixent 4. Or l'ensemble $F = \{\sigma \in S_4 : \sigma(4) = 4\}$ est un

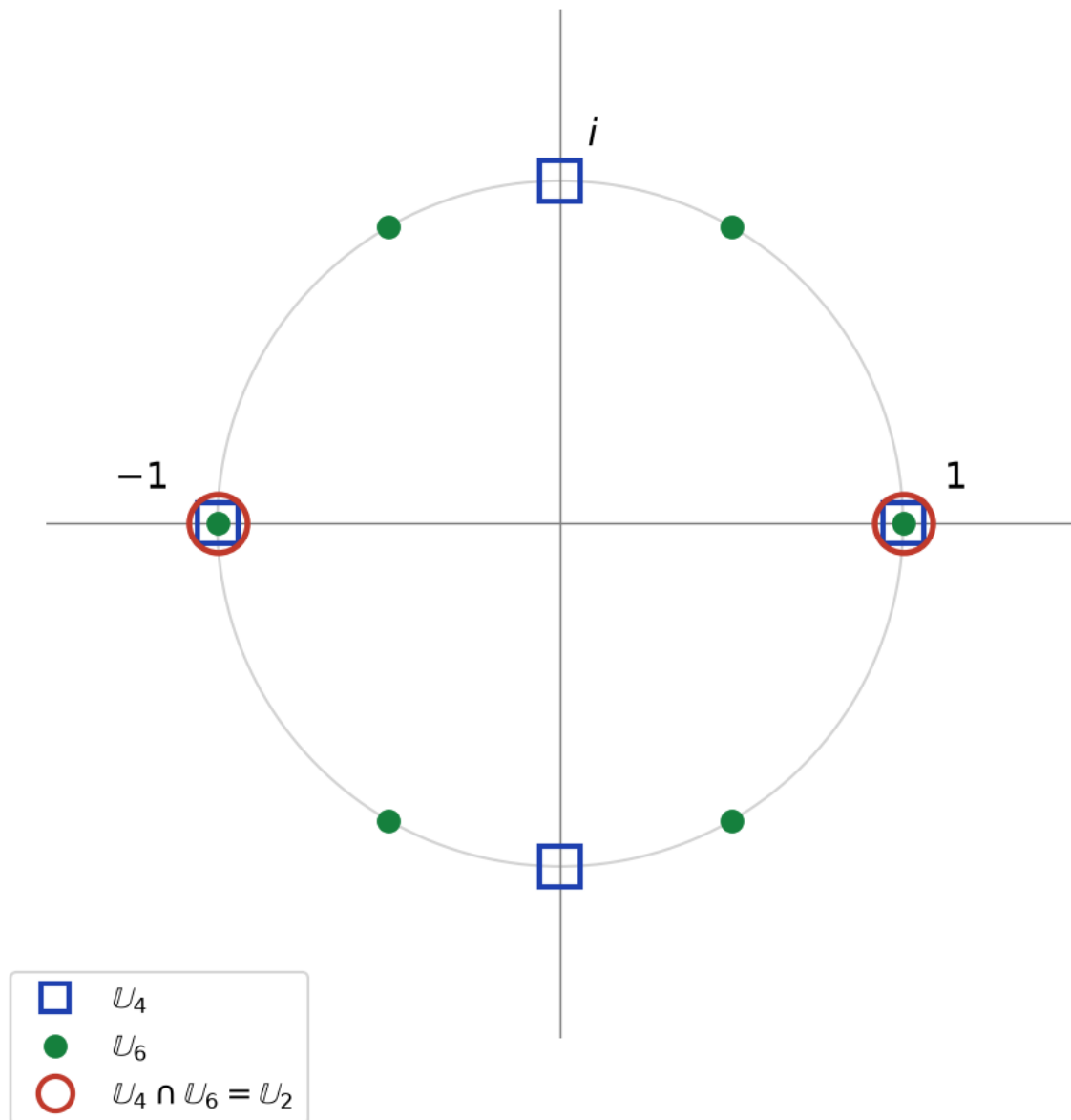
sous-groupe. Donc $\langle (1, 2), (1, 3) \rangle$. De plus, $(2, 3) \in F$ par la question 1. Le sous-groupe engendré contient donc les trois transpositions de F , $(1, 2), (1, 3), (2, 3)$.

engendré contient donc les trois transpositions de $\{1, 2, 3\}$, qui engendrent les permutations de

$\{1, 2, 3\}$. Elles n'engendrent pas S_4 , mais le sous-groupe F , d'ordre 6, isomorphe à S_3 .

Corrigé de l'exercice 22 : Sous-groupes finis de $\mathbb{C}^*$

- On a $1 \in \mathbb{U}_n$, et si $z^n = w^n = 1$, alors $(zw^{-1})^n = 1$. Donc $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$. De plus, $\mathbb{U}_n = \{\omega^k : 0 \leq k \leq n-1\}$ avec $\omega = e^{2i\pi/n}$, qui est d'ordre n .
 $\mathbb{U}_n = \langle \omega \rangle$ **est cyclique d'ordre n .**
- Par le corollaire de Lagrange, tout $z \in G$ vérifie $z^n = 1$, donc $G \subset \mathbb{U}_n$. Les deux ensembles ont n éléments. **Donc $G = \mathbb{U}_n$, et tout sous-groupe fini de $\mathbb{C}^*$ est cyclique.**
- Si $z \in \mathbb{U}_m \cap \mathbb{U}_n$, son ordre divise m et n , donc d : ainsi $z^d = 1$. Réciproquement, si $z^d = 1$, alors $z^m = (z^d)^{m/d} = 1$ et de même $z^n = 1$. **Donc $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_d$.**
 Pour $m = 4$ et $n = 6$, on a $d = 2$. Comme le montre la figure, les carrés de $\mathbb{U}_4$ et les points de $\mathbb{U}_6$ ne se rencontrent qu'en 1 et -1 .



4. Si $z \in U_m$ et $w \in U_n$, alors $(zw)^{mn} = (z^m)^n (w^n)^m = 1$, donc $zw \in U_{mn}$.
 Ensuite, si $zw = z'w'$, alors $z z'^{-1} = w' w^{-1} \in U_m \cap U_n = U_1 = \{1\}$. Donc $z = z'$ et $w = w'$: l'application est injective. Enfin, les deux ensembles ont mn éléments. **L'application $(z, w) \rightarrow zw$ est une bijection de $U_m \times U_n$ sur U_{mn} .**
5. D'abord, $1 \in U_\infty$. Ensuite, si $z \in U_m$ et $w \in U_n$, alors $zw^{-1} \in U_{mn}$. C'est donc un sous-groupe. Il est infini, car les $e^{2i\pi/n}$, $n \geq 1$, sont deux à deux distincts. Par définition, chacun de ses éléments est d'ordre fini. Supposons enfin $U_\infty = \langle z \rangle$. Alors $z \in U_n$ pour un certain n , et $\langle z \rangle \subset U_n$ serait fini. **U_∞ est un sous-groupe infini, non monogène, dont tous les éléments sont d'ordre fini.**

Corrigé de l'exercice 23 : Problème, sous-groupes additifs de $\mathbb{R}$

1. Soit $h \in H$ non nul. Si $h > 0$, il est dans $H \cap \mathbb{R}_+^*$. Sinon, $-h \in H$ et $-h > 0$. Cet ensemble est donc non vide et minoré par 0. **Sa borne inférieure a existe, et $a \geq 0$.**
2. Supposons $a > 0$ et $a \notin H$. Comme $2a > a$, la caractérisation de la borne inférieure fournit $x \in H$ avec $a \leq x < 2a$. Comme $a \notin H$, on a même $a < x$. De nouveau, il existe $y \in H$ avec $a \leq y < x$, et donc $a < y < x$. Alors $x - y \in H$ et

$$0 < x - y < x - a < 2a - a = a.$$

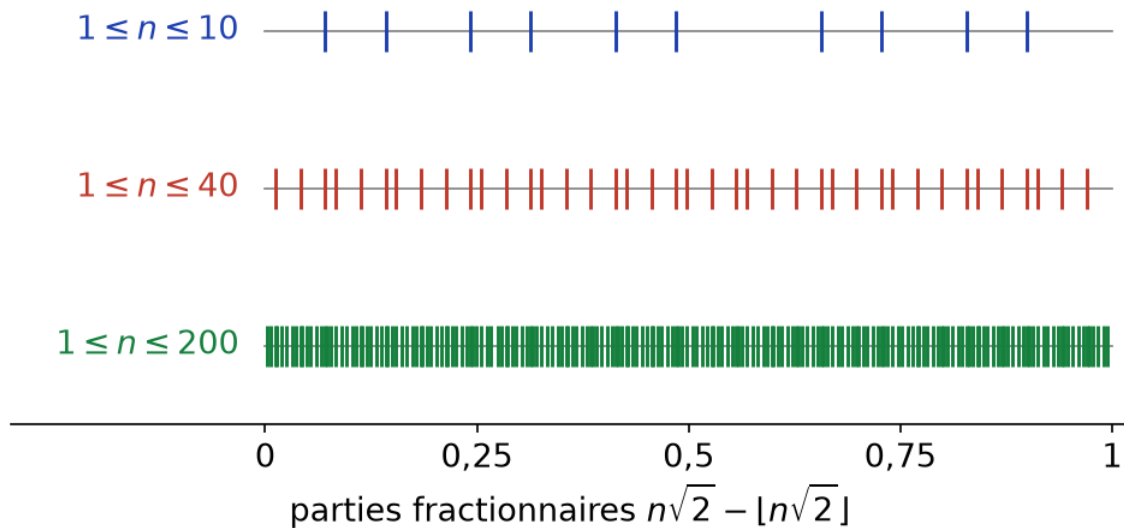
Cela contredit la définition de a . **Donc $a \in H$.**

3. Comme $a \in H$, on a $a\mathbb{Z} \subset H$. Soit $x \in H$ et $n = \lfloor x/a \rfloor$. Alors $r = x - na$ est dans H et $0 \leq r < a$. Si $r > 0$, on contredit la minimalité de a . Donc $r = 0$ et $x = na$. **Ainsi $H = a\mathbb{Z}$.**

4. Soient $x < y$. Comme $a = 0$, il existe $h \in H$ avec $0 < h < y - x$. Posons $k = \lfloor x/h \rfloor + 1$. D'une part, $k > x/h$, donc $kh > x$. D'autre part, $k \leq x/h + 1$, donc $kh \leq x + h < y$. Or $kh \in H$. **Tout intervalle $]x, y[$ contient un élément de H : H est dense dans $\mathbb{R}$.**

5. L'ensemble $H = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ contient 0 et $(m + n\sqrt{2}) - (m' + n'\sqrt{2}) = (m - m') + (n - n')\sqrt{2}$. C'est donc un sous-groupe, non nul. Supposons $a > 0$. Alors $H = a\mathbb{Z}$, donc $1 = pa$ et $\sqrt{2} = qa$ avec p, q entiers et $p \neq 0$. On en déduit $\sqrt{2} = q/p \in \mathbb{Q}$, ce qui est faux. Donc $a = 0$. **Par la question 4, $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans $\mathbb{R}$.**

6. Soient $0 \leq x < y \leq 1$. Par la question 5, il existe m, n entiers avec $t = m + n\sqrt{2} \in]x, y[\subset]0, 1[$. Alors $n\sqrt{2} = -m + t$, avec $-m$ entier et $0 < t < 1$. Donc $\lfloor n\sqrt{2} \rfloor = -m$, et la partie fractionnaire de $n\sqrt{2}$ vaut t . **Les parties fractionnaires des $n\sqrt{2}$ sont denses dans $[0, 1]$.** La figure ci-dessous le suggère : pour n de 1 à 200, les points remplissent déjà tout le segment.



Point de méthode : pour un sous-groupe de $\mathbb{R}$, tout se joue sur $\alpha = \inf(H \cap \mathbb{R}_+^*)$: soit H est discret de la forme $\alpha\mathbb{Z}$, soit il est dense.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en L2

- Le cours : [groupes, cours de maths en L2](#)
- Les énoncés : [exercices de maths en L2 sur groupes](#)
- À maîtriser avant : [Arithmétique et anneau \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre précédent : [Arithmétique et anneau \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre suivant : [Normes et topologie de \$\mathbb{R}^n\$](#)
- Le même thème en maths spé : [groupes, exercices de maths spé](#)

- Tester vos connaissances : [QCM de maths en L2 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L2](#) et la [licence de maths de L1 à L3](#)