# Du cours aux exercices (Savoir-faire à vérifier)

**Chapitre III — Structures algébriques**

Les principaux acquis à vérifier sont :

**Généralités sur les structures.**

✓ 1. Montrer qu'un ensemble est un groupe, est un anneau. ☐

✓ 2. Montrer qu'une application est un morphisme. ☐

✓ 3. Déterminer des automorphismes de corps en dimension finie. (📄) ☐

★ 4. Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter la donnée d'un isomorphisme. ☐

☢ 5. Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat. (📄) ☐

**Étude spécifique des groupes.**

✓ 1. Déterminer l'ordre d'un élément dans un groupe fini explicite. (📄) ☐

✓ 2. Décomposer une permutation en cycles à supports disjoints. ☐

✓ 3. Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. (📄) ☐

★ 4. Utiliser le théorème de Lagrange pour l'étude de sous-groupes et parties génératrices. (📄) ☐

★ 5. Utiliser la structure des groupes cycliques. ☐

★ 6. Déterminer les morphismes d'un groupe dans un autre. ☐

☢ 7. Penser au principe de conjugaison, en particulier dans $S_n$, pour simplifier une étude. ☐

☢ 8. Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc. (📄) ☐

L'icône « (📄) » signifie que les documents *Méthodes* donnent des compléments sur ces savoir-faire.
L'indication « **(G/H)** », dans le corrigé d'un savoir-faire, indique des approfondissements sur la structure d'ensemble quotient, hors programme mais susceptibles d'intéresser le féru d'algèbre.

**Généralités sur les structures**

✓ Montrer qu'un ensemble est un groupe, un anneau, un corps.

**Exemples.**

1. Soit $\mathbb{H}_8 = \{\mathrm{I}_2, -\mathrm{I}_2, I, -I, J, -J, K, -K\}$, avec : $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Montrer que $\mathbb{H}_8$ est un groupe pour le produit matriciel.
2. On pose : $j = e^{\frac{2i\pi}{3}}$. Soient $r : z \mapsto jz$ et $s : z \mapsto \bar{z}$. Montrer que $\mathrm{D}_3 = \left\{r^k \circ s^\ell \mid (k,\ell) \in \mathbb{Z}^2\right\}$ est un groupe pour $\circ$ (c'est le groupe diédral d'ordre 3, ou d'ordre 6 selon les auteurs).
3. Soient $r : z \mapsto iz$ et $s : z \mapsto \bar{z}$. Montrer que $\mathrm{D}_4 = \left\{r^k \circ s^\ell \mid (k,\ell) \in \mathbb{Z}^2\right\}$ est un groupe pour $\circ$ (c'est le groupe diédral d'ordre 4, ou d'ordre 8 selon les auteurs).
4. Soient $f, g : A \to B$ deux morphismes d'anneaux. Montrer que : $\{x \in A \mid f(x) = g(x)\}$ est un anneau.
5. Soit $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid (a,b) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\}),\ p \not| b\right\}$. Montrer que $\mathbb{Z}_{(p)}$ est un anneau. Est-ce un corps ?
6. Soit $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$. Montrer que c'est un corps.
7. Soit $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right] = \left\{P\left(e^{\frac{2i\pi}{n}}\right) \mid P \in \mathbb{Q}[X]\right\}$. Montrer que c'est un corps.
8. Soit $\mathbb{Q}[\pi] = \{P(\pi) \mid P \in \mathbb{Q}[X]\}$. Montrer que c'est un anneau, mais que ce n'est pas un corps.

✓ Montrer qu'une application est un morphisme.

**Exemples.**

1. Soient $G$ un groupe et $g \in G$. Montrer que $h \mapsto ghg^{-1}$ est un automorphisme du groupe $G$.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que l'application $f : \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n^2\mathbb{Z})^\times$ définie par $(\bar{m}, \bar{r}) \mapsto (1+n)^m r^n \bmod n^2$ est correctement définie et est un morphisme de groupes.

✓ Déterminer des automorphismes de corps en dimension finie.

**Exemples.** Soit $K$ un corps.

1. Soit $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$. Déterminer les automorphismes de $\mathbb{Q}[j]$.
2. Soit $K\left(X + \frac{1}{X}\right) = \left\{R\left(X + \frac{1}{X}\right) \mid R \in \mathbb{R}(X)\right\}$. Déterminer les automorphismes de corps de $K(X)$ dont la restriction à $K\left(X + \frac{1}{X}\right)$ est l'identité.

★ Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter un isomorphisme.

**Exemples.** Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de multiplication découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Soit T le sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ constitué des matrices triangulaires supérieures n'ayant que des 1 sur la diagonale. On reprend les définitions de $\mathrm{D}_3$ et $\mathrm{D}_4$ données plus haut.

1. Déterminer si les groupes suivants sont isomorphes :

| | | | | | |
|---|---|---|---|---|---|
| (a) | $\mathbb{R}^*$ et $\{-1,1\} \times \mathbb{R}_+^*$ | (b) | $\mathbb{C}^*$ et $\mathbb{R}_+^* \times \mathbb{U}$ | (c) | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$ |
| (d) | $(\mathbb{Z}/2\mathbb{Z})^3$ et $\mathbb{H}_8$ | (e) | $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{H}_8$ | (f) | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ |
| (g) | $\mathrm{D}_4$ et $\mathbb{H}_8$ | (h) | T et $\mathbb{H}_8$ | (i) | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{H}_8$ |
| (j) | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $S_3$ | (k) | $\mathrm{D}_3$ et $S_3$ | (l) | $\{\sigma \in S_n \mid \sigma(n) = n\}$ et $S_{n-1}$ |

2. Déterminer si $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$ et $\mathbb{Q}[i] = \{a + bi \mid (a,b) \in \mathbb{Q}^2\}$ sont des anneaux isomorphes.

3. Soient $A$ un cors, $B$ un anneau, et $f : A \to B$ un morphisme d'anneaux. On suppose que $f$ est un isomorphisme. Montrer que $B$ est un corps.
4. Soit $k \in \mathbb{N} \setminus \{0,1,2,3\}$. On admet que $\left((\mathbb{Z}/2^k\mathbb{Z})^\times, \times\right)$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}, +\right)$. Donner le nombre de solutions à l'équation : $x^4 \equiv 1 \bmod 2^k$, d'inconnue $x \in \mathbb{Z}$.
5. On admet le résultat difficile suivant : soit $G$ un groupe commutatif fini. Il existe une unique suite d'entiers naturels $d_1, \dots, d_r$ tels que $d_1 | d_2 | \cdots | d_r$, et tels que $G$ soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$. Déduire de ce résultat que pour tout groupe commutatif $G$ fini, si l'on note $d$ le plus grand ordre d'un élément de $G$, alors : $\forall g \in G,\ g^d = 1_G$.

☢ Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat.

**Exemples.**

1. Compter le nombre d'entiers au cube modulo 73. On admet que 73 est un nombre premier. *Vous aurez besoin d'un résultat hors programme.*
2. Démontrer que si $n$ est un entier naturel premier avec 10, il existe un nombre de la forme $11\cdots1$ (constitué uniquement du chiffre 1) qui soit un multiple de $n$.
3. Soit $p \in \mathbb{N}$ un entier qui n'est pas le cube d'un entier naturel. Montrer que $\sqrt{2}$ ne peut pas être obtenu comme une combinaison linéaire de puissances de $\sqrt[3]{p}$.

## Étude spécifique des groupes

✓ Déterminer l'ordre d'un élément dans un groupe fini explicite.

**Exemples.**

1. Donner l'ordre de tous les éléments de $((\mathbb{Z}/15\mathbb{Z})^\times, \cdot)$ (on admet que ce groupe est de cardinal 8 et qu'il contient les classes des éléments premiers avec 15).
2. Donner l'ordre de $\sigma = (6\ 2)(3\ 5\ 4)(1\ 10\ 8\ 9\ 7)$ dans $S_{10}$.
3. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que $1+n$ est d'ordre $n$ dans $((\mathbb{Z}/n^2\mathbb{Z})^\times, \cdot)$.

✓ Décomposer une permutation en cycles à supports disjoints.

**Exemples.**

1. Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 1 & 7 & 4 & 3 & 6 & 9 & 5 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 6 & 4 & 7 & 8 & 5 & 9 & 3 \end{pmatrix}$ en cycles à supports disjoints, et donner leurs signatures.
2. Soit $\sigma = (1\ 2\ 3\ 4\ 5\ 6) \in S_6$. Décomposer en cycles à supports disjoints $\sigma^k$ pour tout $k \in [\![2,5]\!]$.

✓ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances.

**Exemples.**

1. Calculer $13^{100000}$ modulo 101. On admet que 101 est un nombre premier.
2. Calculer $2^{5^{4^3}}$ modulo 105.

★ Utiliser le théorème de Lagrange pour l'étude de sous-groupes et de parties génératrices.

**Exemple.** Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de multiplication découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Décrire tous les sous-groupes de $\mathbb{H}_8$ et donner le cardinal minimal d'une partie génératrice.

★ Utiliser la structure des groupes cycliques.

**Exemples.**

1. Soit $q$ un entier naturel impair. Déterminer l'ordre de $\overline{2q-1}$ et $\overline{2q+1}$ dans $((\mathbb{Z}/4q\mathbb{Z})^\times, \cdot)$, puis déterminer si c'est un groupe cyclique ou non.
2. On admet que $((\mathbb{Z}/101\mathbb{Z})^\times, \cdot)$ est cyclique et de cardinal 100. Donner le nombre de solutions de l'équation : $\bar{x}^{50} = \bar{1}$, puis de : $\bar{x}^{12} = \bar{1}$ et enfin de : $\bar{x}^7 = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/101\mathbb{Z}$.

★ Déterminer les morphismes d'un groupe dans un autre.

**Exemples.** Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de Cayley découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{C}^*$.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{R}^*$.
3. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$ et de $\mathbb{U}_n$ dans $\mathbb{U}_{n^2}$.
4. Déterminer les morphismes de groupes de $\mathbb{H}_8$ dans $\mathbb{C}^*$.
5. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{H}_8$ et de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$.

☢ Penser au principe de conjugaison, en particulier dans $S_n$, pour simplifier une étude.

**Exemples.**

1. On pose : $V_4 = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \mathrm{Id}\}$. On admet que $V_4$ est un sous-groupe de $S_4$ (vous pouvez le vérifier si vous le souhaitez). Montrer que $V_4$ est commutatif.
2. Déterminer l'ensemble des matrices inversibles d'ordre 2 qui commutent avec toute matrice inversible. *On pourra s'intéresser au conjugué d'une matrice de symétrie.*

☢ Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc.

**Exemples.**

1. Soient $n \in \mathbb{N} \setminus \{0\}$ et $k \in [\![1, n]\!]$, et soit $I(k, n)$ l'ensemble des applications injectives de $[\![1, k]\!]$ dans $[\![1, n]\!]$. Définir un morphisme convenable $\sigma \mapsto \varphi_\sigma$, défini de $S_n$ dans $S_{I(k,n)}$, tel que l'étude d'une orbite $\{\varphi_\sigma(\iota) \mid \sigma \in S_n\}$ avec $\iota \in I(k, n)$ bien choisi, permette de redémontrer l'égalité bien connue :
$$\mathrm{card}(I(k, n)) = A_n^k = \frac{n!}{(n-k)!}.$$
2. On munit $\mathbb{C}$ de sa structure de $\mathbb{R}$-espace vectoriel. Soient $\mathrm{Is}(\mathbb{C}) = \{f \in \mathrm{GL}(\mathbb{C}) \mid \forall z \in \mathbb{C},\ |f(z)| = |z|\}$, et : $\mathrm{D}_n = \{f \in \mathrm{Is}(\mathbb{C}) \mid f(\mathbb{U}_n) \subseteq \mathbb{U}_n\}$. On vérifierait aisément que $\mathrm{D}_n$ est un sous-groupe de $\mathrm{GL}(\mathbb{C})$. Soient $r : z \mapsto e^{\frac{2i\pi}{n}} z \in \mathrm{D}_n$ et $s : z \mapsto \bar{z} \in \mathrm{D}_n$. Expliciter $\{f(1) \mid f \in \langle r \rangle\}$ et $\{f \in \mathrm{D}_n \mid f(1) = 1\}$. En déduire que $\mathrm{D}_n$ est engendré par $r$ et $s$.

**Généralités sur les structures**

✓ Montrer qu'un ensemble est un groupe, un anneau, un corps. □

**Réponse.**

1. On montre que $\mathbb{H}_8$ est un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \times)$. L'inclusion est claire (on a $I \cdot (-I) = \mathrm{I}_2$ et de même avec $J$ et $K$, ce qui prouve l'inversibilité de toutes les matrices en présence), la stabilité par produit vient des identités suivantes, qui procèdent d'un calcul matriciel sans mystère :

$$(\pm I)^2 = (\pm J)^2 = (\pm K)^2 = -\mathrm{I}_2, \quad IJ = K,\ JK = I,\ KI = J, \quad JI = -K,\ KJ = -I,\ IK = -J.$$

On obtient les autres produits *via* une multiplication par $-\mathrm{I}_2$. La stabilité par inversion découle des premières identités ci-dessus, qui impliquent : $I^{-1} = -I \in \mathbb{H}_8$, etc. Ainsi $\mathbb{H}_8$ est un sous-ensemble non vide de $\mathrm{GL}_2(\mathbb{C})$, stable par produit et inverse, donc c'est un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \times)$.

2. Montrons que c'est un sous-groupe de $\mathrm{GL}(\mathbb{C})$. Les applications $r$ et $s$ sont $\mathbb{R}$-linéaires, et bijectives car elles admettent respectivement pour bijections réciproques $z \mapsto j^{-1}z$ et $s$, donc $r^k \circ s^\ell \in \mathrm{GL}(\mathbb{C})$ pour tout $(k, \ell) \in \mathbb{Z}^2$. Ainsi $\mathrm{D}_3$ est bien un sous-ensemble de $\mathrm{GL}(\mathbb{C})$.
Montrons la stabilité par produit. Soit $(k, k', \ell, \ell') \in \mathbb{Z}^4$. On a :

$$\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right) = r^k \circ s^\ell \circ r^{k'} \circ s^{\ell'}.$$

Le problème est ce $s^\ell$ qui n'est « pas à la bonne place ». Néanmoins, si $\ell = 0$, on obtient $r^{k+k'} \circ s^{\ell'} \in \mathrm{D}_3$. Supposons à présent $\ell \neq 0$. Comme $s^2 = \mathrm{Id}$, il suffit en vérité de considérer $\ell = 1$. On remarque alors que l'on a pour tout $z \in \mathbb{C}$ : $s \circ r^{k'}(z) = s\left(j^{k'}z\right) = \bar{j}^{k'}\bar{z} = j^{-k'}\bar{z} = r^{-k'} \circ s(z)$, donc : $s \circ r^{k'} = r^{-k'} \circ s$ (formule très commode pour inverser l'ordre dans le produit, bien que ce ne soit pas commutatif : on la retrouve dans $S_3$), puis :

$$\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right) = r^k \circ r^{-k'} \circ s^{1+\ell'} = r^{k-k'} \circ s^{\ell+\ell'} \in \mathrm{D}_3,$$

d'où la stabilité par produit. Pour la stabilité par inverse, on écrit : $(r^k \circ s^\ell)^{-1} = s^{-\ell}r^{-k}$, et le même raisonnement que ci-dessus permet d'en déduire que si $\ell = 1$ alors : $\left(r^k \circ s\right)^{-1} = r^k \circ s \in \mathrm{D}_3$, le cas $\ell = 0$ étant trivial.
Ainsi $\mathrm{D}_3$ est un sous-ensemble de $\mathrm{GL}(\mathbb{C})$ non vide, stable par produit et inverse, donc c'est un sous-groupe de $(\mathrm{GL}(\mathbb{C}), \circ)$.
**Remarque.** On peut démontrer que $\mathrm{D}_3$ est l'ensemble des isométries du plan complexe qui laissent stable le triangle dont les sommets ont pour affixes 1, $j$ et $j^2$ (c'est même parfois la définition de $\mathrm{D}_3$).
**Remarque.** Pour la stabilité par inverse, il y a une autre façon de procéder, une fois qu'on a classifié les isométries du plan complexe. Les éléments de $\mathrm{D}_3$ sont en effet des isométries (c'est clairement le cas pour $r$ et $s$, et la stabilité par produit et inverse de $\mathrm{O}(\mathbb{C})$ donne le résultat pour $r^k \circ s^\ell$). Il suffit alors de remarquer que si $\ell$ est impair, alors $r^k \circ s^\ell$ est de déterminant $-1$ car $s$ l'est (et $r$ est de déterminant 1), donc c'est une isométrie indirecte du plan : c'est une symétrie. On en déduit : $(r^k \circ s^\ell)^{-1} = r^k \circ s^\ell \in \mathrm{D}_3$.

3. Ce sont exactement les mêmes calculs que ci-dessus.

4. Soit $C = \{x \in A \mid f(x) = g(x)\}$. Montrons que $C$ est un sous-anneau de $B$. Il est contenu dans $B$ car $f$ et $g$ sont à valeurs dans $B$, et non vide car $f(0_A) = g(0_A) = 0_B$, donc $0_A \in C$. Montrons qu'il est stable par somme et inversion pour $+$, le cas du produit étant en tout point analogue. Soit $(a_1, a_2) \in C^2$. On a : $f(a_1) = g(a_1)$, et : $f(a_2) = g(a_2)$, donc :

$$f(a_1 - a_2) = f(a_1) - f(a_2) = g(a_1) - g(a_2) = g(a_1 - a_2),$$

donc : $a_1 - a_2 \in C$, ce qui démontre la stabilité par somme.
Ainsi $C$ est un sous-anneau de $B$, ce qui démontre le résultat voulu.

5. Montrons que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Il est clairement inclus dans cet anneau, et non vide parce que $0 = \frac{0}{1} \in \mathbb{Z}_{(p)}$. Il est stable par somme et inverse pour $+$, car pour tous $(a,b) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ et $(a',b') \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ tels que $p$ ne divise pas $b$ et $b'$, on a :
$$\frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'},$$
et $p$ ne divise pas $bb'$ (sinon, par le lemme d'Euclide, il diviserait $b$ ou $b'$). Donc : $\frac{a}{b} - \frac{a'}{b'} \in \mathbb{Z}_{(p)}$. Raisonnement analogue pour la stabilité par produit, donc $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.
Il n'est pas un corps, puisque $p \in \mathbb{Z}_{(p)}$ et $\frac{1}{p} \notin \mathbb{Z}_{(p)}$. En effet, si $\frac{1}{p}$ s'écrit : $\frac{1}{p} = \frac{a}{b}$, avec $a$ et $b$ entiers tels que $p$ ne divise pas $b$, alors on a : $b = pa$, et donc $p$ divise $b$ : c'est contraire à l'hypothèse sur $b$.

6. Montrons que $\mathbb{Q}[j]$ est un sous-corps de $\mathbb{C}$. Il est clairement inclus dans $\mathbb{C}$, non vide et stable par somme. Montrons la stabilité par produit. Soit $(a,b,c,d) \in \mathbb{Q}^4$. Comme $j^2 = -1 - j$, on a :
$$(a+bj)(c+dj) = ac + (ad+bc)j + bdj^2 = ac - bd + (ad + bc - bd)j \in \mathbb{Q}[j],$$
et il reste à montrer que tout élément non nul est inversible. Soit $(a,b) \in \mathbb{Q}^2$ tel que : $a + bj \neq 0$. Pour construire son inverse, il est raisonnable de penser que son inverse dans $\mathbb{C}$ est aussi son inverse dans $\mathbb{Q}[j]$. On va mettre $\frac{1}{a+bj}$ sous forme algébrique pour vérifier qu'il est bien dans $\mathbb{Q}[j]$. C'est l'idée de ce qui suit. On a : $(a+bj)(a+b\bar{j}) = |a+bj|^2 \in \mathbb{Q}^*$, donc :
$$\frac{a+b\bar{j}}{|a+bj|^2} \cdot (a+bj) = (a+bj) \cdot \frac{a+b\bar{j}}{|a+bj|^2} = 1,$$
et on a : $\frac{a+b\bar{j}}{|a+bj|^2} = \frac{a}{|a+bj|^2} + \frac{b}{|a+bj|^2}(-1-j) \in \mathbb{Q}[j]$ (on a en effet : $\bar{j} = -1 - j$ d'après les relations coefficients-racines avec le polynôme $X^2 + X + 1$). Donc $a + bj$ est inversible dans $\mathbb{Q}[j]$, ce qu'il fallait démontrer.
On a montré que $\mathbb{Q}[j]$ est un sous-corps de $\mathbb{C}$.

7. L'ensemble $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est un sous-anneau de $\mathbb{C}$, puisque c'est l'image de l'anneau $\mathbb{Q}[X]$ par le morphisme d'évaluation $P \mapsto P\left(e^{\frac{2i\pi}{n}}\right)$ (qui est un morphisme d'anneaux de $\mathbb{Q}[X]$ dans $\mathbb{C}$). Montrons que c'est un corps. Nous proposons deux arguments différents.
*Premier argument.* Soit $z \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ un élément non nul. Alors l'application $x \mapsto xz$ est un endomorphisme du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ (parce qu'il est stable par produit), injectif parce que $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est intègre en tant que sous-anneau de $\mathbb{C}$ qui l'est. Or $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est de dimension finie. En effet, en effectuant la division euclidienne d'un polynôme $\mathbb{Q}[X]$ par $X^n - 1$, on peut montrer que pour tout $P \in \mathbb{Q}[X]$, il existe $R \in \mathbb{Q}_{n-1}[X]$ tel que : $P\left(e^{\frac{2i\pi}{n}}\right) = R\left(e^{\frac{2i\pi}{n}}\right)$. Cela implique concrètement que $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ admet pour partie génératrice *finie* la famille $\left(e^{\frac{2i\pi k}{n}}\right)_{0 \leqslant k \leqslant n-1}$, donc c'est un $\mathbb{Q}$-espace vectoriel de dimension finie.
Un endomorphisme injectif d'un espace vectoriel de dimension finie est aussi surjectif, donc $1 \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ admet un antécédent par $x \mapsto xz$ : il existe $x \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ tel que : $xz = 1$, ce qui démontre l'inversibilité de $z$. Ceci vaut pour tout $z \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ non nul, donc $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est un corps.
*Deuxième argument (nécessite le polynôme minimal, chapitre IV).* Comme $e^{\frac{2i\pi}{n}}$ est annulé par $X^n - 1 \in \mathbb{Q}[X]$, il admet un polynôme minimal sur $\mathbb{Q}$ qu'on note $\Phi_n$. Soit $z = P\left(e^{\frac{2i\pi}{n}}\right) \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ non nul. Comme $P\left(e^{\frac{2i\pi}{n}}\right) \neq 0$, le polynôme $\Phi_n$ ne divise pas $P$, et donc ils sont premiers entre eux (en effet, un diviseur unitaire commun à $\Phi_n$ et $P$ est en particulier un diviseur de $\Phi_n$, donc est égal à 1 ou $\Phi_n$ ; le second cas est exclu puisque le cas échéant, $\Phi_n$ diviserait $P$). Par le théorème de Bezout, il existe $(U,V) \in \mathbb{Q}[X]^2$ tel que : $UP + V\Phi_n = 1$. En évaluant cette égalité en $e^{\frac{2i\pi}{n}}$, on obtient : $U\left(e^{\frac{2i\pi}{n}}\right) P\left(e^{\frac{2i\pi}{n}}\right) = 1$ (en effet $\Phi_n\left(e^{\frac{2i\pi}{n}}\right) = 0$ par définition d'un polynôme minimal, qui est aussi annulateur). Donc : $U\left(e^{\frac{2i\pi}{n}}\right) z = zU\left(e^{\frac{2i\pi}{n}}\right) = 1$, avec $U\left(e^{\frac{2i\pi}{n}}\right) \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$, ce qui prouve que $z$ est inversible dans $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ : c'est ce qu'on voulait démontrer.

**Remarque.** Ces deux arguments se généralisent à tout anneau de la forme $\mathbb{Q}[z]$ avec $z$ annulé par un polynôme non nul à coefficients rationnels.

8. La démonstration que c'est un sous-anneau de $\mathbb{C}$ est la même que pour $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ traité ci-dessus. Justifions que ce n'est pas un corps. Si tel était le cas, on aurait $\frac{1}{\pi} \in \mathbb{Q}[\pi]$, donc il existerait $P \in \mathbb{Q}[X]$ tel que : $\frac{1}{\pi} = P(\pi)$, avec $P$ non nul sinon cette égalité impliquerait $\frac{1}{\pi} = 0$. Le polynôme non nul $XP-1$ admettrait donc $\pi$ comme racine, ce qui est impossible puisque $\pi$ n'est annulé par aucun polynôme à coefficients rationnels : il est transcendant (théorème de Lindemann). Par l'absurde, on a montré : $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$, donc $\pi$ n'est pas inversible dans $\mathbb{Q}[\pi]$. Ce n'est pas un corps.

✓ Montrer qu'une application est un morphisme. □

**Réponse.**

1. Notons $f_g$ l'application de l'énoncé. Elle est bien à valeurs dans $G$ car $G$ est stable par produit. Pour tout $(h_1, h_2) \in G^2$, on a :

$$f_g(h_1)f_g(h_2) = gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1} = f_g(h_1h_2),$$

donc $f_g$ est un morphisme de groupes de $G$ dans $G$. C'est un automorphisme, puisqu'un calcul direct montre que $f_{g^{-1}}$ est son application réciproque. Nous ne le détaillons que pour la composition dans un sens, l'autre étant analogue (inverser les rôles de $g$ et $g^{-1}$) :

$$\forall h \in G, \quad f_g \circ f_{g^{-1}}(h) = f_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h.$$

Donc $f_g$ est un morphisme bijectif de $G$ dans $G$ : c'est un automorphisme de $G$.

**Remarque.** Les automorphismes de cette forme sont appelés les *automorphismes intérieurs*.

2. Tout d'abord, $(1+n)^n \equiv 1 \bmod n^2$ (utiliser la formule du binôme de Newton), donc d'une part $1+n \in (\mathbb{Z}/n^2\mathbb{Z})^\times$ (son inverse étant $(1+n)^{n-1}$), et d'autre part l'application de $\mathbb{Z}$ dans $(\mathbb{Z}/n^2\mathbb{Z})^\times$, définie par $m \mapsto (1+n)^m \bmod n^2$, induit un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $(\mathbb{Z}/n^2\mathbb{Z})^\times$ défini par $\bar{m} \mapsto (1+n)^m \bmod n^2$ (théorème de factorisation des morphismes). Ensuite, pour que $f : (\bar{m}, \bar{r}) \mapsto (1+n)^m r^n \bmod n^2$ soit correctement définie, encore faut-il que le résultat ne dépende pas du choix du représentant dans la classe de $r$. Considérons donc $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ et $(r_1, r_2) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^2$ tel que : $\overline{r_1} = \overline{r_2}$. Montrons : $r_1^n \equiv r_2^n \bmod n^2$. Comme : $\overline{r_1} = \overline{r_2}$, il existe $k \in \mathbb{Z}$ tel que : $r_1 = r_2 + kn$. Alors : $r_1^n = (r_2+kn)^n = \sum_{i=0}^{n} \binom{n}{i} r_2^{n-i}(kn)^i \equiv r_2^n + \binom{n}{1} r_2^{n-1}(kn) \equiv r_2^n + r_2^{n-1}kn^2 \equiv r_2^n \bmod n^2$. Ainsi $r^n \bmod n^2$ ne dépend pas du choix du représentant de $\bar{r} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et cela suffit à démontrer que $f$ est bien définie. Montrons à présent que c'est un morphisme de groupes. Attention à ne pas s'emmêler les pinceaux : la loi de $\mathbb{Z}/n\mathbb{Z}$ est $+$ et celle de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\times$. On doit donc démontrer :

$$\forall ((\overline{m_1}, \overline{r_1}), (\overline{m_2}, \overline{r_2})) \in \left(\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times\right)^2, \quad f(\overline{m_1} + \overline{m_2}, \overline{r_1} \times \overline{r_2}) = f(\overline{m_1}, \overline{r_1}) \times f(\overline{m_2}, \overline{r_2}).$$

Soit $((\overline{m_1}, \overline{r_1}), (\overline{m_2}, \overline{r_2})) \in (\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times)^2$. On a :

$$f(\overline{m_1}, \overline{r_1}) \times f(\overline{m_2}, \overline{r_2}) \equiv (1+n)^{m_1} r_1^n \times (1+n)^{m_2} r_2^n = (1+n)^{m_1+m_2}(r_1r_2)^n = f(\overline{m_1} + \overline{m_2}, \overline{r_1} \times \overline{r_2}),$$

ce qui prouve que $f$ est un morphisme.

✓ Déterminer des automorphismes de corps en dimension finie. □

**Réponse.**

1. Soit $f$ un automorphisme de corps de $\mathbb{Q}[j]$. Pour tout $(a, b) \in \mathbb{Q}^2$, on a : $f(a+bj) = f(a) + f(b)f(j)$. Or, partant de $f(1) = 1$, il est classique de démontrer que $f(x) = x$ pour tout $x \in \mathbb{Q}$ (en le montrant d'abord pour $x \in \mathbb{N}$ par récurrence grâce à l'identité $f(n \cdot 1) = nf(1)$, puis pour $x \in \mathbb{Z}$ grâce à l'identité $f(x) = -f(-x)$, pour $x = \frac{p}{q} \in \mathbb{Q}$ grâce à l'identité $f(p) = qf\left(\frac{p}{q}\right)$ ; je préfère néanmoins le démontrer

en montrant que $\{x \in \mathbb{Q}[j] \mid f(x) = x\}$ est un corps et qu'il doit donc contenir le sous-corps premier de $\mathbb{Q}[j]$, qui est $\mathbb{Q}$). Donc : $\forall (a,b) \in \mathbb{Q}^2$, $f(a+bj) = a + bf(j)$. Il reste à déterminer $f(j)$.
Or : $j^2 + j + 1 = 0$. En prenant l'image par $f$ dans cette égalité, et en utilisant le fait que ce soit un morphisme de corps, on a : $f(j)^2 + f(j) + 1 = 0$, donc $f(j)$ est racine de $X^2 + X + 1$. On en déduit que $f(j) = j$ ou $f(j) = j^2$, ce qu'on résume en disant qu'il existe $k \in \{1,2\}$ tel que : $f(j) = j^k$. Par conséquent, si $f$ est un automorphisme de corps, alors : $\forall (a,b) \in \mathbb{Q}^2$, $f(a+bj) = a + bj^k$ (par ailleurs $j^2$ est bien dans $\mathbb{Q}[j]$, puisque : $j^2 = -1 - j$).
Réciproquement, pour tout $j \in \{1,2\}$, montrons que l'application définie par $a + bj \mapsto a + bj^k$ (elle est correctement définie car tout élément de $\mathbb{Q}[j]$ s'écrit sous la forme $a + bj$ de manière unique) est un automorphisme de corps. Le cas $k = 1$ est évident puisqu'on reconnaît là l'application identité. Supposons donc $k = 2$. Soit $(a,b,c,d) \in \mathbb{Q}^4$. On a $f(1) = 1$, et :

$$\begin{aligned} f(a+bj)f(c+dj) = (a+bj^2)(c+dj^2) &= ac + (ad+bc)j^2 + bdj^4 \\ &= ac + (ad+bc)j^2 + bdj \\ &= ac + (ad+bc)(-1-j) + bdj, \\ &= ac - ad - bc + (bd - ad - bc)j, \end{aligned}$$

tandis que :

$$\begin{aligned} f((a+bj)(c+dj)) = f\left(ac + (ad+bc)j + bdj^2\right) &= f\left(ac - bd + (ad+bc-bd)j\right) \\ &= ac - bd + (ad+bc-bd)j^2 \\ &= ac - bd + (ad+bc-bd)(-1-j) \\ &= ac - bd - ad - bc + bd - (ad+bc-bd)j \\ &= ac - ad - bc + (bd - ad - bc)j \\ &= f((a+bj)(c+dj)), \end{aligned}$$

donc $f$ est bien un morphisme de corps. Il est injectif comme tout morphisme de corps, et surjectif parce que 1 et $j$ sont dans son image : on a $1 = f(1)$ et $j = -j^2 - 1 = f(-j-1)$. Comme 1 et $j$ engendrent $\mathbb{Q}[j]$, par $\mathbb{Q}$-linéarité $f$ est surjectif. On a donc démontré que c'est un morphisme de corps de $\mathbb{Q}[j]$ dans lui-même et bijectif : c'est donc un automorphisme de corps.
**Conclusion.** Les automorphismes de $\mathbb{Q}[j]$ sont exactement les applications de la forme $a+bj \mapsto a+bj^k$ avec $k \in \{1,2\}$. Il y en a donc deux.
**Remarque.** Le caractère bijectif peut aussi se démontrer en notant que $f$ est un endomorphisme du $\mathbb{Q}$-espaces vectoriel $\mathbb{Q}[j]$, qui est injectif comme tout morphisme de corps ; comme $\mathbb{Q}[j]$ est de dimension finie (égale à 2) sur $\mathbb{Q}$, on en déduit que $f$ est bijectif.
**Remarque.** La vérification que $f$ est un morphisme est beaucoup, beaucoup moins calculatoire si l'on remarque que l'on a : $\mathbb{Q}[j] = \{P(j) \mid P \in \mathbb{Q}[X]\}$ (il suffit alors d'écrire : $f(P_1(j))f(P_2(j)) = P_1(j^k)P_2(j^k) = (P_1P_2)(j^k) = f(P_1P_2(j))$ pour avoir le résultat ! c'est tout !). En revanche, dans ce cas-là il faut vérifier que la définition de $f$ ne dépend pas de l'écriture d'un élément $z \in \mathbb{Q}[j]$ sous la forme $z = P(j)$ avec $P \in \mathbb{Q}[X]$ : si $P_1$ et $P_2$ vérifient : $z = P_1(j) = P_2(j)$, il faut vérifier que $f(P_1(j)) = f(P_2(j))$. Cette vérification nécessite la notion de polynôme minimal de $j$ sur $\mathbb{Q}$ (qui vaut $X^2 + X + 1$) pour être efficace : on dit que si $P_1(j) = P_2(j)$, alors $P_1 - P_2$ annule $j$ et est donc divisible par le polynôme minimal de $j$ sur $\mathbb{Q}$, qui vaut $X^2 + X + 1$. Il existe donc $Q \in \mathbb{Q}[X]$ tel que : $P_1 = P_2 + (X^2 + X + 1)Q$, et en évaluant cette égalité en $j^k$ (qui est racine de $X^2 + X + 1$ pour $k \in \{1,2\}$) on a : $P_1(j^k) = P_2(j^k)$, ce qu'il fallait démontrer.
L'avantage, aussi, de procéder comme décrit dans cette remarque, est que cela permet de traiter simultanément $k = 1$ et $k = 2$.

2. Soit $f$ un automorphisme de corps de $K(X)$ qui fixe $K\left(X + \frac{1}{X}\right)$. Déterminons $f$, en commençant par déterminer $f(X)$. Comme souvent, on cherche une relation vérifiée par $X$ sur $K\left(X + \frac{1}{X}\right)$ afin d'en déduire une relation vérifiée par $f(X)$. Or on a :

$$X^2 - X\left(X + \frac{1}{X}\right) + 1 = 0$$

(je me suis inspiré des relations coefficients-racines pour trouver cette expression : j'ai fabriqué un polynôme à *coefficients* dans $K\left(X+\frac{1}{X}\right)$ dont les racines sont $X$ et $\frac{1}{X}$), et comme $f$ est un morphisme de corps qui fixe $K\left(X+\frac{1}{X}\right)$ on en déduit : $f(X)^2 - f(X)\left(X+\frac{1}{X}\right)+1=0$, ce qui équivaut à : $(f(X)-X)\left(f(X)-\frac{1}{X}\right)=0$ (car $X$ et $\frac{1}{X}$ sont racines du polynôme $Y^2-\left(X+\frac{1}{X}\right)Y+1 \in K\left(X+\frac{1}{X}\right)[Y]$). Comme $K(X)$ est intègre, on en déduit : $f(X)=X$, ou : $f(X)=\frac{1}{X}$. On étend alors $f$ à tout élément de $K(X)$ par somme et produit. On en déduit que si $f$ est un automorphisme de $K(X)$ qui fixe $K\left(X+\frac{1}{X}\right)$, alors il est de la forme :

$$R \mapsto R(X), \quad \text{ou :} \quad R \mapsto R\left(\frac{1}{X}\right).$$

Réciproquement, il est facile de démontrer que ces deux applications sont des automorphismes de $K(X)$ fixant $K\left(X+\frac{1}{X}\right)$.

★ Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter un isomorphisme. □

**Réponse.**

1. (a) Intuitivement, $\mathbb{R}^*$ et $\{-1,1\}\times\mathbb{R}_+^*$ sont isomorphes puisque tout réel non nul est caractérisé par la donnée de son signe (qu'on représente par 1 ou $-1$) et de sa valeur absolue. Ceci conduit à considérer l'application $x \mapsto \left(\frac{x}{|x|},|x|\right)$, qui est un morphisme par multiplicativité de la valeur absolue et bijective puisqu'elle admet pour réciproque $(\varepsilon,r)\mapsto \varepsilon r$. La réponse est donc **positive**.
   (b) Intuitivement, $\mathbb{C}^*$ et $\mathbb{R}_+^*\times\mathbb{U}$ sont isomorphes puisque tout complexe non nul est caractérisé par la donnée de son module (qui est dans $\mathbb{R}_+^*$) et de son argument (ou, cela revient au même, un élément de $\mathbb{U}$, qui apparaît en facteur du module dans la forme exponentielle). Ceci conduit à considérer l'application $z\mapsto\left(|z|,\frac{z}{|z|}\right)$, qui est un morphisme par multiplicativité du module et bijective puisqu'elle admet pour réciproque $(r,\omega)\mapsto r\omega$. La réponse est donc **positive**.
   (c) Tous les éléments sont d'ordre 1 ou 2 dans $(\mathbb{Z}/2\mathbb{Z})^3$, tandis que $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ admet un élément d'ordre 4 (en l'occurrence : (0 mod 2,1 mod 4), comme on le vérifie facilement). Donc les groupes ne sont pas isomorphes : la réponse est **négative**.
   (d) Le premier groupe est commutatif et pas le second (on a $ij=k$ et $ji=-k\neq k$) : la réponse est **négative**.
   (e) Même argument : la réponse est **négative**.
   (f) Il s'avère que ces deux groupes sont isomorphes. Le plus rapide, pour le démontrer, est d'utiliser convenablement le théorème chinois (chapitre IV). Le groupe $\mathbb{Z}/6\mathbb{Z}$ est en effet isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, et il n'est pas difficile de se convaincre que cela implique un isomorphisme entre $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Encore par le théorème chinois, ce dernier groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. La réponse est donc **positive**.

   **Remarque.** Un isomorphisme explicite est donné par $(a \bmod 4, b \bmod 6) \mapsto (b \bmod 2, 4b-3a \bmod 12)$. On le trouve en explicitant l'isomorphisme réciproque de $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.
   (g) Le groupe $D_4$ admet deux éléments d'ordre 4, à savoir $r$ et $r^3=r^{-1}$ (on vérifiera que $r^k s$ est toujours d'ordre 2), tandis que $\mathbb{H}_8$ en admet beaucoup plus : $\pm i$, $\pm j$, $\pm k$. Les groupes ne sont donc pas isomorphes. La réponse est **négative**.
   (h) Soit $M=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\in T$. On a : $M^2=\begin{pmatrix}1&0&ac\\0&1&0\\0&0&1\end{pmatrix}$ (on a $2\cdot a=2\cdot b=2\cdot c=0$ vu qu'on raisonne dans $\mathbb{Z}/2\mathbb{Z}$). On en déduit que $M$ est d'ordre divisant 2 si et seulement si : $ac=0$, sans condition sur $b\in\mathbb{Z}/2\mathbb{Z}$. Cela fournit six éléments d'ordre divisant 2, or $\mathbb{H}_8$ n'en a que deux, à savoir 1 et $-1$. Ils ne sont donc pas isomorphes et la réponse est **négative**.

   **Remarque.** En fait, $D_4$ et T sont isomorphes, et comme nous avons démontré que $D_4$ n'est pas isomorphe à $\mathbb{H}_8$, il en est de même de T. Pour comprendre en quoi $D_4$ et T sont isomorphes, il

faut comprendre à quoi correspondent la rotation $r$ et la symétrie $s$ dans T : un élément d'ordre 4 est $R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ par exemple, tandis qu'un élément d'ordre 2 (qui n'est pas dans le groupe engendré par $R$) est $S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On vérifie alors que l'application $f : \mathrm{D}_4 \to \mathrm{T}$ définie par $r^k s^\ell \mapsto R^k S^\ell$ est bien définie, est un morphisme (cela ne va pas de soi du tout, et il faudra sans doute démontrer : $SRS = R^{-1}$), et est injectif : comme les deux groupes ont même cardinal, cela suffit à démontrer qu'ils sont isomorphes.

(i) Le premier groupe est commutatif et pas le second : la réponse est **négative**.

(j) Le premier groupe est commutatif et pas le second (on a $(1\ 2)(1\ 2\ 3) = (2\ 3)$ et $(1\ 2\ 3)(1\ 2) = (1\ 3) \neq (2\ 3)$) : la réponse est **négative**.

(k) Puisque $\mathrm{D}_3$ est engendré par $r : z \mapsto jz$ et $s : z \mapsto \bar{z}$ qui, géométriquement, permutent les trois sommets du triangle régulier dont les sommets sont d'affixes 1, $j$ et $j^2 = \bar{j}$, il ressemble de près au groupe $S_3$ qui consiste en la permutation de trois éléments (où $r$ serait un 3-cycle et $s$ une transposition). Montrons qu'ils sont isomorphes, en considérant l'application $f : \mathrm{D}_3 \to S_3$ qui envoie $r^k \circ s^\ell$ sur $(1\ 2\ 3)^k(2\ 3)^\ell$ pour tout $(k, \ell) \in \mathbb{Z}^2$ (en vérité, prendre $k \in \{0,1,2\}$ et $\ell \in \{0,1\}$ suffirait). Vérifions que c'est bien un morphisme. Soit $(k, \ell, k', \ell') \in \mathbb{Z}^4$. Comparons $f\left(r^k \circ s^\ell\right) \circ f\left(r^{k'} \circ s^{\ell'}\right)$ et $f\left(\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$. Si $\ell = 0$, alors on a directement :

$$f\left(r^k\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) = (1\ 2\ 3)^k \circ (1\ 2\ 3)^{k'}(1\ 2)^{\ell'} = (1\ 2\ 3)^{k+k'}(1\ 2)^{\ell'} = f\left(r^{k+k'} \circ s^{\ell'}\right) = f\left(r^k \circ r^{k'} \circ s^{\ell'}\right),$$

et si $\ell = 1$ nous allons utiliser le principe de conjugaison pour mettre cette composition sous la bonne forme (comme $s^2 = \mathrm{Id}$, prendre $\ell \in \{0,1\}$ suffit). On a :

$$\begin{aligned} f\left(r^k \circ s\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) &= (1\ 2\ 3)^k(1\ 2) \circ (1\ 2\ 3)^{k'}(1\ 2)^{\ell'} \\ &= (1\ 2\ 3)^k(1\ 2)(1\ 2\ 3)^{k'}(1\ 2)(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^k(2\ 1\ 3)^{k'}(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^k(1\ 2\ 3)^{-k'}(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^{k-k'}(1\ 2)^{\ell'+\ell}. \end{aligned}$$

Pour calculer $f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$, simplifions d'abord la composition $\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)$. Là encore, nous allons utiliser le principe de conjugaison (qui est un principe général et ne vaut pas que dans $S_n$, même si c'est là qu'on l'a illustré majoritairement). Pour tout $z \in \mathbb{C}$, on a :

$$s \circ r^{k'}(z) = s\left(j^{k'} z\right) = \bar{j}^{k'} \bar{z} = j^{-k'} \bar{z} = r^{-k'} \circ s(z),$$

donc :

$$f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right) = f\left(r^k \circ r^{-k'} \circ s^{1+\ell'}\right) = f\left(r^{k-k'} \circ s^{\ell+\ell'}\right) = (1\ 2\ 3)^{k-k'}(1\ 2)^{\ell'+\ell}.$$

On a donc bien : $f\left(r^k \circ s\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) = f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$, ce qui prouve que $f$ est un morphisme. Comme $\mathrm{D}_3$ et $S_3$ sont tous les deux de cardinal 6 (pour $\mathrm{D}_3$ on ne l'a pas démontré, mais sa description explicite, ainsi que les relations $r^3 = \mathrm{Id}$ et $s^2 = \mathrm{Id}$, permettent de s'en assurer rapidement), il suffit de montrer qu'il est injectif pour avoir le résultat. Soit $(k, \ell) \in \mathbb{Z}^2$ tel que : $f(r^k \circ s^\ell) = \mathrm{Id}$. Cela signifie : $(1\ 2\ 3)^k(1\ 2)^\ell = \mathrm{Id}$, donc : $(1\ 2\ 3)^k = (1\ 2)^\ell$. L'unicité de la décomposition en cycles à supports disjoints ne permet cette égalité que si chaque membre de l'égalité vaut Id, ce qui correspond à $k \equiv 0 \bmod 3$ et $\ell \equiv 0 \bmod 2$. Pour de telles conditions sur $k$ et $\ell$, on a aussi : $s^\ell = \mathrm{Id}$, et : $\forall z \in \mathbb{C}$, $r^k(z) = j^k z = z$, donc : $r^k = \mathrm{Id}$. Donc : $r^k \circ s^\ell = \mathrm{Id}$. Notre calcul montre donc que : $\ker(f) = \{\mathrm{Id}\}$, et $f$ est alors un morphisme injectif entre deux groupes de même cardinal : c'est un isomorphisme.

La réponse est donc **positive**.

**Remarque.** On a démontré en passant cette formule très commode qui permet d'inverser l'ordre dans le produit : $(1\ 2)(1\ 2\ 3)^{k'} = (1\ 2\ 3)^{-k'}(1\ 2)$. Formule analogue avec $r$ et $s$.

(l) Intuitivement, une permutation de $S_{n-1}$ et une permutation de $S_n$ fixant $n$ est la même chose. Les deux groupes devraient être isomorphes. On le démontre très simplement grâce à l'isomorphisme $\sigma \mapsto \sigma_{|[\![1,n-1]\!]}$, qui est correctement défini et va de $\{\sigma \in S_n \mid \sigma(n) = n\}$ dans $S_{n-1}$.

2. Intuitivement, deux anneaux isomorphes devraient avoir autant de solutions à toute équation polynomiale (en première approximation c'est un peu faux, sauf si les équations polynomiales sont à coefficients entiers voire rationnels, grâce au fait qu'un morphisme vérifie $f(1) = 1$). Mais le second a une solution de $X^2 + 1$ mais pas le premier : cela mène à la conjecture qu'ils ne sont pas isomorphes. Démontrons-le : supposons l'existence d'un isomorphisme d'anneaux $f : \mathbb{Q}[i] \to \mathbb{Q}[j]$. On a : $(f(i))^2 + 1 = f(i^2) + f(1) = f(i^2 + 1) = f(0) = 0$, donc $f(i) \in \mathbb{Q}[j]$ est racine de $X^2 + 1$. On a donc : $f(i) = \pm i$, or $i$ et $-i$ n'appartiennent pas à $\mathbb{Q}[j]$. En effet, si $i \in \mathbb{Q}[j]$, alors il existe $(a, b) \in \mathbb{Q}^2$ tel que : $i = a + bj$, et en utilisant les parties imaginaires : $1 = b\frac{\sqrt{3}}{2}$, puis : $b = \frac{2}{\sqrt{3}} = \frac{2}{3}\sqrt{3} \notin \mathbb{Q}$ : absurde.
On en déduit que $\mathbb{Q}[i]$ et $\mathbb{Q}[j]$ **ne** sont **pas** isomorphes.

3. Soit $a \in B \setminus \{0_B\}$ : montrons qu'il existe $b \in B$ tel que $ab = 1_B$. Nous allons « transporter » $a$ dans $A$ grâce à l'isomorphisme, pour y trouver un inverse : comme $f^{-1}(a) \in A$ et $f^{-1}(a) \neq 0_A$ (dans le cas contraire, on aurait : $a = f\left(f^{-1}(a)\right) = f\left(0_A\right) = 0_B$, ce qui est faux), et comme $A$ est un corps, il existe un élément $y \in A$ tel que : $f^{-1}(a)y = 1_A$. En prenant l'image par $f$, qui est un morphisme, on obtient : $af(y) = f(1_A) = 1_B$. Ainsi $f(y)$ est l'inverse de $a$, et tout élément non nul de $B$ est inversible.
On montrerait de même que $ab = ba$ pour tout $(a, b) \in A^2$ en utilisant le fait que $f(a)f(b) = f(b)f(a)$, donc $A$ est un anneau commutatif dont tout élément non nul est inversible : c'est un corps.

4. On remarque qu'une solution $\bar{x}$ est inversible modulo $2^k$, d'inverse $\bar{x}^3$. C'est pourquoi nous allons nous contenter de raisonner dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$.
Soit $\varphi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ un isomorphisme de groupes, qui existe par hypothèse de l'énoncé. Soit $\bar{x} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. Posons : $(a \bmod 2, b \bmod 2^{k-2}) = \varphi(\bar{x})$. Alors : $x^4 \equiv 1 \bmod 2^k \iff 4\varphi(\bar{x}) = \varphi(\bar{1}) \iff (4a \bmod 2, 4b \bmod 2^{k-2}) = (0 \bmod 2, 0 \bmod 2^{k-2})$. La condition $4a \equiv 0 \bmod 2$ est toujours vérifiée, car 4 est pair. Donc : $x^4 \equiv 1 \bmod 2^k \iff 4b \equiv 0 \bmod 2^{k-2} \iff \exists \ell \in \mathbb{Z}$, $4b = 2^{k-2}\ell \iff \exists \ell \in \mathbb{Z}$, $b = 2^{k-4}\ell$. Modulo $2^{k-2}$, cela fait 4 valeurs de $b$ possibles : 0, $2^{k-4}$, $2^{k-3}$, $3 \cdot 2^{k-4}$. Donc : $x^4 \bmod 1 \bmod 2^k \iff \varphi(\bar{x}) \in \mathbb{Z}/2\mathbb{Z} \times \left\{\ell 2^{k-4} \mid \ell \in [\![0,3]\!]\right\} \iff \bar{x} \in \varphi^{-1}\left(\mathbb{Z}/2\mathbb{Z} \times \left\{\ell 2^{k-4} \mid \ell \in [\![0,3]\!]\right\}\right)$. Comme $\varphi^{-1}$ est bijective, ce dernier ensemble a huit éléments : on en déduit que l'équation : $x^4 \equiv 1 \bmod 2^k$ admet huit solutions $\bar{x}$ dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$.

5. Puisque tout groupe commutatif fini est isomorphe à un groupe de la forme $G' = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, où $d_1|d_2|\cdots|d_r$, et qu'un isomorphisme conserve les ordres, il suffit de démontrer le résultat voulu pour un groupe de cette forme (attention, désormais la loi est notée additivement dans $G'$ : il faut donc que démontrer $dx = 0$ pour tout $x \in G'$).
Soit $d$ l'ordre maximal d'un élément de $G'$ : montrons d'abord que $d = d_r$. Si $(x_1, \ldots, x_r) \in G'$, alors : $\forall i \in [\![1, r]\!]$, $d_i x_i = 0$, et donc, comme $d_i$ divise $d_r$ pour tout $i \in [\![1, r]\!]$, on en déduit : $\forall i \in [\![1, r]\!]$, $d_r x_i = 0$, ce qui signifie que $d_r(x_1, \ldots, x_r) = (0, \ldots, 0)$. Par conséquent l'ordre de $(x_1, \ldots, x_r)$ divise $d_r$ : ceci montre que l'ordre de tout élément de $G'$ est inférieur ou égal à $d_r$, donc $d$ également, puisqu'il est supposé être le plus grand : on a $d \leqslant d_r$.
Mais il existe un élément qui est exactement d'ordre $d_r$ : en effet, $\forall k \in [\![1, d_r - 1]\!]$, $k(0, \ldots, 0, 1) = (0, \ldots, 0, k) \neq (0, \ldots, 0)$, et : $d_r(0, \ldots, 0, 1) = (0, \ldots, 0)$. Ainsi $d_r$ est le plus petit entier naturel non nul à annuler $(0, \ldots, 0, 1)$, donc c'est l'ordre de $(0, \ldots, 0, 1)$. Puisqu'il existe un élément d'ordre $d_r$, et que $d$ est supposément le plus grand, on a $d_r \leqslant d$.
Ayant démontré que $d \leqslant d_r$ et $d_r \leqslant d$, on a en vérité $d = d_r$. Il est alors clair, d'après le premier paragraphe, que $d(x_1, \ldots, x_r) = (0, \ldots, 0)$ pour tout $(x_1, \ldots, x_r) \in G'$, d'où le résultat.

☢ Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat. □

**Réponse.**

1. On nous demande de dénombrer : $\{\bar{y} \in \mathbb{Z}/73\mathbb{Z} \mid \exists \bar{x} \in \mathbb{Z}/73\mathbb{Z},\ \bar{y} = \bar{x}^3\}$. C'est presque l'image du morphisme $\bar{x} \mapsto \bar{x}^3$ de $(\mathbb{Z}/73\mathbb{Z})^\times$ dans lui-même (il faut simplement enlever $\bar{0}$ qui est trivialement un cube). On peut dénombrer son image grâce au théorème d'isomorphisme, qui implique l'égalité entre

cardinaux : $\text{card}((\mathbb{Z}/73\mathbb{Z})^\times) = \text{card}(\ker(f))\text{card}(\text{im}(f))$. Or, comme souvent, déterminer un noyau est plus facile que déterminer une image. Ici : $\ker(f) = \{\bar{x} \in (\mathbb{Z}/73\mathbb{Z})^\times \mid \bar{x}^3 = \bar{1}\}$ peut difficilement se trouver par une résolution explicite. Il est plus avisé de remarquer que $\ker(f)$ est l'ensemble des éléments de $(\mathbb{Z}/73\mathbb{Z})^\times$ dont l'ordre divise 3 ; or 73 est premier, donc $(\mathbb{Z}/73\mathbb{Z})^\times$ est cyclique (résultat hors programme à savoir redémontrer), donc la structure des sous-groupes des groupes cycliques implique qu'il y a exactement 3 éléments d'ordre divisant 3. On en déduit : $\text{card}(\ker(f)) = 3$, puis : $\text{card}(\text{im}(f)) = \frac{\text{card}((\mathbb{Z}/73\mathbb{Z})^\times)}{3} = \frac{72}{3} = 24$. En conclusion :

$$\text{card}\left(\{\bar{y} \in \mathbb{Z}/73\mathbb{Z} \mid \exists \bar{x} \in \mathbb{Z}/73\mathbb{Z},\ \bar{y} = \bar{x}^3\}\right) = \text{card}\left(\text{im}(f) \cup \{\bar{0}\}\right) = 25.$$

2. On demande de montrer qu'il existe $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sum_{i=0}^{k-1} 10^i \equiv 0 \bmod n$. Si l'on note $\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ l'application $\bar{x} \mapsto \overline{10x} + \bar{1}$, il est équivalent d'écrire qu'on veut l'existence de $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sigma^k(\bar{0}) = \bar{0}$. Or $\sigma$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$ (en effet, puisque 10 est premier avec $n$, il est inversible modulo $n$, et la bijection réciproque de $\sigma$ est alors $\bar{y} \mapsto \overline{10}^{-1}(\bar{y} - \bar{1})$), donc par le théorème de Lagrange il existe $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sigma^k = \text{Id}$ : il suffit de prendre $k = \text{card}(S_n) = n!$, même si l'on pourrait prendre largement plus petit. Pour ce choix de $k$, on a alors : $\sigma^k(\bar{0}) = \text{Id}(\bar{0}) = \bar{0}$, d'où le résultat : $n$ divise $\sum_{i=0}^{k-1} 10^i = 11\cdots1$.

3. Cela revient à montrer que l'inclusion : $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{p}]$, est fausse, où $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\right\}$, et : $\mathbb{Q}[\sqrt[3]{p}] = \left\{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid (a,b,c) \in \mathbb{Q}^3\right\}$. L'élève en exercice vérifiera que ce sont des corps, et qu'ils sont munis naturellement d'une structure de $\mathbb{Q}$-espace vectoriel, et on a facilement :

$$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2, \quad \dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{p}]) = 3.$$

Si l'inclusion $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{p}]$ était vraie, alors $\mathbb{Q}[\sqrt[3]{p}]$ serait également muni d'une structure de $\mathbb{Q}[\sqrt{2}]$-espace vectoriel, où la multiplication externe serait définie par le produit dans $\mathbb{Q}[\sqrt[3]{p}]$. Alors, en notant $(\vec{e}_1, \ldots, \vec{e}_n)$ une $\mathbb{Q}[\sqrt{2}]$-base de $\mathbb{Q}[\sqrt[3]{p}]$, on vérifie que $(\vec{e}_1, \ldots, \vec{e}_n) \cup \left(\sqrt{2}\vec{e}_1, \ldots, \sqrt{2}\vec{e}_n\right)$ serait une $\mathbb{Q}$-base de $\mathbb{Q}[\sqrt[3]{p}]$ (vérification à faire ! ce n'est pas trivial). On aurait donc : $3 = \dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{p}]) = 2n$, ce qui est impossible puisque 2 ne divise pas 3. Par l'absurde, on a donc : $\mathbb{Q}[\sqrt{2}] \not\subseteq \mathbb{Q}[\sqrt[3]{p}]$, et donc $\sqrt{2} \notin \mathbb{Q}[\sqrt[3]{p}]$ (en effet, la stabilité par produit et somme d'un corps impliquerait l'inclusion qu'on vient de contredire), ce qui démontre le résultat voulu.

## Étude spécifique des groupes

✓ Déterminer l'ordre d'un élément dans un groupe fini explicite. □

**Réponse.**

1. Explicitons le groupe $(\mathbb{Z}/15\mathbb{Z})^\times$. On a : $(\mathbb{Z}/15\mathbb{Z})^\times = \{\pm1, \pm2, \pm4, \pm7\}$.
Tout d'abord, 1 est bien sûr d'ordre 1 et $-1$ d'ordre 2. On a : $2^4 = 16 \equiv 1 \bmod 15$, donc 2 est d'ordre divisant 4, mais n'est pas d'ordre 1 ou 2 puisque : $2^2 = 4 \not\equiv 1 \bmod 5$. Donc 2 est d'ordre 4 et il en est de même de $-2$ comme on le vérifie aisément. Comme $4 = 2^2$, on en déduit aisément que 4 est d'ordre 2 (ce qu'un calcul direct montrerait), ainsi que $-4$. Il reste 7 et $-7$. Pour ces éléments, utilisons le théorème de Lagrange : comme $(\mathbb{Z}/15\mathbb{Z})^\times$ est de cardinal 8, l'ordre de 7 divise 8, et est donc égal à 1, 2, 4 ou 8. Or : $7^2 = 49 \equiv 4 \not\equiv 1 \bmod 15$, donc 7 n'est pas d'ordre 1 ou 2. Enfin : $7^4 \equiv 4^2 \equiv 1 \bmod 15$, donc 4 est la plus petite puissance à convenir et 7 est d'ordre 4. De même pour $-7$.
En conclusion, voici les différents ordres :

| élément | 1 | $-1$ | 2 | $-2$ | 4 | $-4$ | 7 | $-7$ |
|---|---|---|---|---|---|---|---|---|
| ordre | 1 | 2 | 4 | 4 | 2 | 2 | 4 | 4 |

On note que $(\mathbb{Z}/15\mathbb{Z})^\times$ n'est pas cyclique (aucun élément d'ordre 8, ou autre argument : il y a trois éléments d'ordre 2, à savoir 4, $-4$ et $-1$, alors qu'un groupe cyclique admet $\varphi(2) = 1$ éléments d'ordre 2, lorsque 2 divise son cardinal).

2. Comme $(6\ 2)^2 = \mathrm{Id}$, $(3\ 5\ 4)^3 = \mathrm{Id}$, et : $(1\ 10\ 8\ 9\ 7)^5 = \mathrm{Id}$, le fait que ces trois cycles commutent implique : $\sigma^{2\cdot3\cdot5} = \left((6\ 2)^2\right)^{3\cdot5}\left((3\ 5\ 4)^3\right)^{2\cdot5}\left((1\ 10\ 8\ 9\ 7)^5\right)^{2\cdot3} = \mathrm{Id}$. Donc l'ordre de $\sigma$ divise $2\cdot3\cdot5$ : il appartient donc à {1,2,3,5,6,10,15,30}. Mais $\sigma^k \neq \mathrm{Id}$ pour tout $k$ dans cet ensemble, excepté 30. Donc $\sigma$ est d'ordre 30.
3. Pour tout $k \in \mathbb{N}$, on a : $(1+n)^k = \sum_{j=0}^{k} \binom{k}{j} n^j \equiv 1 + kn \bmod n^2$. On en déduit que $(1+n)^k \equiv 1 \bmod n^2$ si et seulement si $kn \equiv 0 \bmod n^2$, si et seulement si $n$ divise $k$. Donc $n$ est le plus petit entier naturel au sens de la relation de divisibilité tel que $(1+n)^k \equiv 1 \bmod n^2$ : on en déduit que $1+n$ est d'ordre $n$ dans $\left((\mathbb{Z}/n^2\mathbb{Z})^\times, \cdot\right)$.

✓ Décomposer une permutation en cycles à supports disjoints. ☐

**Réponse.**

1. On a : $\sigma = (1\ 8\ 9\ 5\ 4\ 7\ 6\ 3)$, et : $\tau = (1\ 2)(3\ 6\ 8\ 9)(5\ 7)$. On en déduit : $\varepsilon(\sigma) = (-1)^7 = -1$, et : $\varepsilon(\tau) = (-1)\cdot(-1)^3\cdot(-1) = -1$.
2. On trouve, en utilisant le fait que $\sigma^6 = \mathrm{Id}$ pour les dernières puissances :

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

Peut-on trouver un lien entre le nombre de cycles, leur longueur, et l'exposant ?

✓ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. ☐

**Réponse.**

1. Par le petit théorème de Fermat, on a : $13^{100} \equiv 1 \bmod 101$. Donc, en élevant cette égalité à la puissance 1000, on a : $13^{10^5} \equiv 1^{10^3} \equiv 1 \bmod 101$.
2. La réponse anticipe légèrement sur le chapitre IV. Tout d'abord, 2 est premier avec $105 = 3\times5\times7$, donc il appartient à $(\mathbb{Z}/105\mathbb{Z})^\times$. De plus : $\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2\cdot4\cdot6 = 48$, donc par le théorème d'Euler : $2^{48} \equiv 1 \bmod 105$. Pour simplifier $2^{5^{4^3}}$, nous allons exprimer $5^{4^3}$ à l'aide d'un multiple de 48 (pour exploiter le fait que $2^{48} \equiv 1 \bmod 105$) et du reste dans la division euclidienne de $5^{4^3}$ par 48 (pour se ramener à un exposant aussi petit que possible), ce qui revient à calculer $5^{4^3}$ modulo 48. Or 5 est premier avec $48 = 2^4\times3$, donc il appartient à $(\mathbb{Z}/48\mathbb{Z})^\times$. De plus : $\varphi(48) = 8\cdot2 = 16$, donc par le théorème d'Euler : $5^{16} \equiv 1 \bmod 48$. En élevant cette égalité à la puissance 4, on en déduit : $5^{4^3} \equiv 1 \bmod 48$. Il existe donc $k \in \mathbb{Z}$ tel que : $5^{4^3} = 48k + 1$. Donc : $2^{5^{4^3}} = \left(2^{48}\right)^k \cdot 2 \equiv 2 \bmod 105$, d'où le résultat.

★ Utiliser le théorème de Lagrange pour l'étude de sous-groupes et de parties génératrices. ☐

**Réponse.** On montre aisément que 1 est d'ordre 1, $-1$ d'ordre 2, et $\pm i$, $\pm j$, $\pm k$ d'ordre 4 (et il n'y a pas d'autre élément). Cela fournit déjà les sous-groupes :

$$\{1\}, \quad \langle -1\rangle = \{-1,1\}, \quad \langle \pm i\rangle = \{i,-1,-i,1\}, \quad \langle \pm j\rangle = \{j,-1,-j,1\}, \quad \langle \pm k\rangle = \{k,-1,-k,1\}.$$

Montrons qu'il n'y a pas d'autre sous-groupe strict : soit $G$ un sous-groupe de $\mathbb{H}_8$. Par le théorème de Lagrange, son cardinal divise 8, donc il est égal à 1, 2, 4 ou 8. Les cas 1 et 8 sont triviaux (on a $G = \{1\}$ ou $G = \mathbb{H}_8$). S'il est de cardinal 2, alors il contient un élément non trivial qui doit être d'ordre 2, et c'est donc $-1$. On en déduit : $-1 \in G$, puis : $\langle -1\rangle \subseteq G$. En comparant les cardinaux : $G = \langle -1\rangle$.

Si $G$ est de cardinal 4, alors ses éléments sont d'ordre 1 ou 2 ou 4. Mais ils ne peuvent pas tous être d'ordre 1 ou 2 (vu qu'il n'y a que 1 et $-1$ à avoir ces ordres : c'est insuffisant), donc il doit contenir un élément d'ordre 4, disons $i$ par exemple. On a alors : $\langle i\rangle \subseteq G$, puis en comparant les cardinaux : $G = \langle i\rangle$. De même si $G$ contient $j$ ou $k$ plutôt que $i$.

On a traité toutes les possibilités de cardinaux, donc la liste des sous-groupes est complète.

On en déduit aussi que $\{i,j\}$ est une partie génératrice de $\mathbb{H}_8$. En effet, $\langle i,j\rangle$ contient au moins 5 éléments (parmi ceux de $\langle i\rangle$ et $\langle j\rangle$, à savoir : $i$, 1, $-1$, $-i$, $j$), et comme son cardinal divise 8 on a : $\langle i,j\rangle = \mathbb{H}_8$. On ne peut pas trouver de partie génératrice à un seul élément d'après la description ci-dessus, donc $\{i,j\}$ est une partie génératrice de cardinal minimal.

**Remarque.** Le groupe $\mathbb{H}_8$ n'est pas cyclique bien que tous ses sous-groupes stricts le soient.

★ Utiliser la structure des groupes cycliques. □

**Réponse.**

1. On a : $(\overline{2q-1})^2 = \overline{4q\cdot q} - \overline{4q} + \bar{1} = \bar{1}$, donc $\overline{2q-1}$ est d'ordre divisant 2. Voyons si l'ordre peut être égal à 1 : c'est le cas si et seulement si $\overline{2q-1} = \bar{1}$, si et seulement si : $2q \equiv 2 \bmod 4q$, si et seulement si : $q \equiv 1 \bmod 2q$. Cela ne peut arriver que si $q = 1$. Si $q = 1$ alors $\overline{2q-1}$ est d'ordre 1, et sinon il est d'ordre 2.

   Un calcul analogue montre que $\overline{2q+1}$ est toujours d'ordre 2 (y compris si $q = 1$). Voyons comment en déduire si $(\mathbb{Z}/4q\mathbb{Z})^\times$ est cyclique ou non : si $q = 1$ c'est le cas parce que $(\mathbb{Z}/4\mathbb{Z})^\times = \{-1,1\}$ est engendré par $-1$, et si $q > 1$ alors il n'est pas cyclique. En effet, s'il était cyclique, alors il admettrait un unique sous-groupe de cardinal 2 ; or $\langle 2q-1\rangle \neq \langle 2q+1\rangle$ (car $\overline{2q-1} \neq \overline{2q+1}$ pour $q \geqslant 1$), donc cela fournit deux sous-groupes de $(\mathbb{Z}/4q\mathbb{Z})^\times$ de cardinal 2. Par l'absurde, $(\mathbb{Z}/4q\mathbb{Z})^\times$ n'est pas cyclique. (Autre argument : il devrait y avoir $\varphi(2) = 1$ élément d'ordre 2, et là nous en avons fourni deux.)

   En conclusion, $(\mathbb{Z}/4q\mathbb{Z})^\times$ est cyclique si et seulement si : $q = 1$.

2. On nous demande respectivement le nombre d'éléments de $(\mathbb{Z}/101\mathbb{Z})^\times$ d'ordre divisant 50, d'ordre divisant 12 et d'ordre divisant 7 (notons bien qu'une solution de ces équations doit être inversible modulo 101). Pour le dernier cas, l'affaire est vite entendue : comme l'ordre d'un élément de $(\mathbb{Z}/101\mathbb{Z})^\times$ doit diviser le cardinal du groupe, à savoir 100, et qu'on ne peut diviser 7 et 100 qu'à condition de diviser pgcd(7,100) = 1, l'unique élément d'ordre divisant 7 est $\bar{x} = \bar{1}$. Ainsi l'équation $\bar{x}^7 = \bar{1}$ admet une unique solution dans $\mathbb{Z}/101\mathbb{Z}$.

   Passons aux éléments d'ordre divisant 50 : d'après la propriété du cours sur les sous-groupes d'un groupe cyclique, ces éléments sont exactement les éléments de l'unique sous-groupe de cardinal 50 de $(\mathbb{Z}/101\mathbb{Z})^\times$.

   Autre point de vue, si l'on n'utilise pas ce résultat de cours (hors programme) : si $\varphi : ((\mathbb{Z}/101\mathbb{Z})^\times, \cdot) \to (\mathbb{Z}/100\mathbb{Z}, +)$ est un isomorphisme (qui existe puisque $(\mathbb{Z}/101\mathbb{Z})^\times$ est cyclique de cardinal 100), alors : $\bar{x}^{50} = \bar{1} \iff 50\varphi(\bar{x}) = \varphi(\bar{1}) = \tilde{0}$ (attention, ce $\tilde{0}$ représente 0 modulo 100), si et seulement si 100 divise $50\varphi(\bar{x})$, si et seulement si 2 divise $\varphi(\bar{x})$ (ou, plus rigoureusement, un représentant dans $\mathbb{Z}$ de $\varphi(\bar{x})$, mais je les confonds abusivement pour alléger les notations), si et seulement si : $\varphi(\bar{x}) \in \left\{\tilde{2}\tilde{k} \mid \tilde{k} \in \mathbb{Z}/100\mathbb{Z}\right\} = \langle\tilde{2}\rangle$. Or $\langle\tilde{2}\rangle$ admet $\frac{100}{2} = 50$ éléments (soit en invoquant le cours sur la forme des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, soit par une description explicite), donc $\varphi(\bar{x})$ peut prendre 50 valeurs différents. En prenant l'image par $\varphi^{-1}$, cela fournit 50 valeurs possibles pour les solutions $\bar{x} \in (\mathbb{Z}/101\mathbb{Z})^\times$ de $\bar{x}^{50} = \bar{1}$.

   Autre résolution avec un point de vue polynomial : comme 101 est un nombre premier, d'après le théorème de Fermat on a : $\forall \bar{x} \in \mathbb{Z}/101\mathbb{Z} \setminus \{\bar{0}\}$, $\bar{x}^{100} = \bar{1}$, donc $X^{100} - \bar{1}$ admet 100 racines dans $\mathbb{Z}/101\mathbb{Z}$, et comme $\mathbb{Z}/101\mathbb{Z}$ est un corps il ne peut en admettre plus : ainsi $X^{100} - \bar{1}$ est scindé et à racines simples sur $\mathbb{Z}/101\mathbb{Z}$. Or : $X^{100} - \bar{1} = (X^{50} - \bar{1})(X^{50} + \bar{1})$, donc l'unicité de la décomposition en facteurs irréductibles implique que $X^{50} - \bar{1}$ est scindé à racines simples aussi, et admet exactement 50 racines. Il existe donc exactement 50 solutions de : $\bar{x}^{50} = \bar{1}$.

   Passons aux éléments d'ordre 12. Comme 12 ne divise pas 100, ce qu'on a fait ci-dessus pour 50 ne s'adapte pas directement. Néanmoins on se ramène à un diviseur de 100 en remarquant que si $\bar{x} \in (\mathbb{Z}/101\mathbb{Z})^\times$, alors : $\bar{x}^{12} = \bar{1} \iff \bar{x}^4 = \bar{1}$. Il y a plusieurs façons d'y parvenir, la plus directe étant : si $\bar{x}^{12} = \bar{1}$, alors l'ordre de $x$ divise 12. Mais l'ordre de $x$ divise aussi le cardinal de $(\mathbb{Z}/101\mathbb{Z})^\times$, à savoir 100, donc il divise pgcd(12,100) = 4 (comment calculer ce pgcd, d'ailleurs ?). Donc : $\bar{x}^4 = \bar{1}$, la réciproque étant facile (élever au cube). Une autre démonstration de cette équivalence passe par une relation de Bezout : il existe $(u,v) \in \mathbb{Z}^2$ tel que : $4 = 12u + 100v$, et donc : $\bar{x}^4 = \left(\bar{x}^{12}\right)^u \left(\bar{x}^{100}\right)^v = \bar{1}$. Comme 4 divise 100, il est facile de vérifier que le raisonnement effectué pour 50 ci-dessus se transpose sans difficulté à 12, et on trouve $\frac{100}{4} = 25$ solutions de l'équation $\bar{x}^{12} = \bar{1}$.

**Conclusion.** Les équations $\bar{x}^{50} = \bar{1}$, $\bar{x}^{12} = \bar{1}$ et $\bar{x}^{7} = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/101\mathbb{Z}$, ont respectivement 50, 4 et 1 solutions.

★ Déterminer les morphismes d'un groupe dans un autre. □

**Réponse.**

1. Soit $f : \mathbb{U}_n \to \mathbb{C}^*$ un morphisme de groupes. Pour déterminer $f$, il suffit de déterminer $f\left(e^{\frac{2i\pi}{n}}\right)$, puisque $e^{\frac{2i\pi}{n}}$ engendre $\mathbb{U}_n$. Or $e^{\frac{2i\pi}{n}}$ est d'ordre $n$, donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre divisant $n$ dans $\mathbb{C}^*$. Autrement dit : c'est une racine $n^{\text{e}}$ de l'unité. Considérons donc $k \in \mathbb{Z}$ tel que : $f\left(e^{\frac{2i\pi}{n}}\right) = e^{\frac{2i\pi k}{n}}$. Les morphismes $f$ et $g_k : \omega \mapsto \omega^k$ (c'est facile de vérifier que c'en est effectivement un) coïncident sur $e^{\frac{2i\pi}{n}}$ qui engendre $\mathbb{U}_n$, donc : $f = g_k$.
   **Conclusion.** Les morphismes de $\mathbb{U}_n$ dans $\mathbb{C}^*$ sont exactement les applications de la forme $g_k : \omega \mapsto \omega^k$ avec $k \in \mathbb{Z}$ (on peut même prendre $k \in [\![0, n-1]\!]$). On pourrait démontrer que l'application $\bar{k} \mapsto g_k$ est correctement définie et est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^*), \times)$ (on a un isomorphisme analogue en remplaçant $\mathbb{Z}/n\mathbb{Z}$ par n'importe quel groupe commutatif fini, mais la démonstration est subtile).
2. Soit $f : \mathbb{U}_n \to \mathbb{R}^*$ un morphisme de groupes. Pour déterminer $f$, il suffit de déterminer $f\left(e^{\frac{2i\pi}{n}}\right)$, puisque $e^{\frac{2i\pi}{n}}$ engendre $\mathbb{U}_n$. Or $e^{\frac{2i\pi}{n}}$ est d'ordre $n$, donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre divisant $n$ dans $\mathbb{R}^*$ ; mais les seuls éléments d'ordre fini dans $\mathbb{R}^*$ sont 1 (qui est d'ordre 1) et $-1$ (qui est d'ordre 2), donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre 1 ou 2 en plus de diviser $n$. On en déduit que si $n$ est impair, alors $f\left(e^{\frac{2i\pi}{n}}\right)$ ne peut être d'ordre 2 (sinon 2 diviserait $n$), et donc : $f\left(e^{\frac{2i\pi}{n}}\right) = 1$. Puisque $f$ et $z \mapsto 1$ sont deux morphismes qui coïncident en $e^{\frac{2i\pi}{n}}$, qui engendre $\mathbb{U}_n$, on obtient : $f = 1$.
   Si $n$ est pair, en revanche, il est possible que $f\left(e^{\frac{2i\pi}{n}}\right)$ soit d'ordre 2, et plus précisément que l'on ait : $f\left(e^{\frac{2i\pi}{n}}\right) = -1$. On obtient alors, par propriété de morphisme : $\forall k \in \mathbb{Z}$, $f\left(e^{\frac{2i\pi k}{n}}\right) = (-1)^k$. Réciproquement, cela définit bien un morphisme de $\mathbb{U}_n$ dans $\mathbb{R}^*$.
   **Conclusion.** Si $n$ est impair, alors le seul morphisme de $\mathbb{U}_n$ dans $\mathbb{R}^*$ est trivial. Si $n$ est pair, il y en a deux : le morphisme trivial, et le morphisme défini par $e^{\frac{2i\pi k}{n}} \mapsto (-1)^k$.
3. En raisonnant comme ci-dessus, on montre que si $f : \mathbb{U}_{n^2} \to \mathbb{U}_n$ est un morphisme de groupes, alors il existe $k \in \mathbb{Z}$ tel que : $f\left(e^{\frac{2i\pi}{n^2}}\right) = e^{\frac{2i\pi k}{n}} = \left(e^{\frac{2i\pi}{n^2}}\right)^{nk}$, donc $f$ et l'application $g_k : \omega \mapsto \omega^{nk}$ (dont on vérifie que c'est bien un morphisme de groupes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$) coïncident sur le générateur $e^{\frac{2i\pi}{n}}$ et on en déduit : $f = g_k$.
   **Conclusion.** Les morphismes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$ sont exactement ceux de la forme $g_k : \omega \mapsto \omega^{nk}$ avec $k \in \mathbb{Z}$. On pourrait même restreindre $k$ à $[\![0, n-1]\!]$.
   **Remarque.** Le noyau de $g_k$ est $\mathbb{U}_{nk} \cap \mathbb{U}_{n^2} = \mathbb{U}_{nd}$ avec $d = \mathrm{pgcd}(k, n)$, et son image est $\mathbb{U}_{\frac{n}{d}}$. Exercice. En raisonnant semblablement pour les morphismes de $\mathbb{U}_n$ dans $\mathbb{U}_{n^2}$, on trouve que ces morphismes sont exactement ceux de la forme $h_k : \omega \mapsto \omega^k$ avec $k \in \mathbb{Z}$, qu'on peut restreindre à $k \in [\![0, n-1]\!]$.
4. On va d'une part exploiter les ordres des éléments de $\mathbb{H}_8$, et d'autre part que $\mathbb{H}_8$ n'est pas commutatif alors que $\mathbb{C}^*$ l'est. Soit $f : \mathbb{H}_8 \to \mathbb{C}^*$ un morphisme de groupes. On a : $f(ij) = f(i)f(j) = f(j)f(i) = f(ji)$, car $f(i)$ et $f(j)$ sont dans $\mathbb{C}^*$ et commutent donc. On en déduit : $f(ij(ji)^{-1}) = f(ij)f(ji)^{-1} = 1$. Or : $ij(ji)^{-1} = k \cdot (-k)^{-1} = k^2 = -1$ (pour l'égalité $ji = -k$ : multiplier à gauche l'égalité $jk = i$ par $j$), donc : $f(-1) = 1$. Cela implique alors : $f(i) = f(-i)$, $f(j) = f(-j)$ et $f(k) = f(-k)$. Comme $f(1) = 1$ et $f(-1) = 1$ sont connus, on voit qu'il suffit de déterminer $f(i)$, $f(j)$ et $f(k)$ pour expliciter entièrement $f$. Mieux : comme $ij = k$, on a $f(i)f(j) = f(k)$, donc il suffit d'expliciter $f(i)$ et $f(j)$. On a : $f(i)^2 = f(i^2) = f(-1) = 1$, donc : $f(i) \in \mathbb{U}_2 = \{-1,1\}$, et il existe $\varepsilon_1 \in \{-1,1\}$ tel que : $f(i) = \varepsilon_1$. Par le même argument, il existe $\varepsilon_2 \in \{-1,1\}$ tel que : $f(j) = \varepsilon_2$. Ainsi, si $f$ est un morphisme de $\mathbb{H}_8$ dans $\mathbb{C}^*$, il est défini par : $f(\pm 1) = 1$, $f(\pm i) = \varepsilon_1$, $f(\pm j) = \varepsilon_2$, et : $f(\pm k) = f(\pm i)f(\pm j) = \varepsilon_2\varepsilon_2$, avec $(\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2$. Réciproquement, on vérifie que toute application ainsi définie est bien un morphisme.

**Conclusion.** Il y a quatre morphismes de $\mathbb{H}_8$ dans $\mathbb{C}^*$. On pourrait démontrer que l'application $(\varepsilon_1, \varepsilon_2) \mapsto f_{\varepsilon_1,\varepsilon_2}$ (où $f_{\varepsilon_1,\varepsilon_2}$ est ce que l'on a défini plus haut en fonction de $\varepsilon_1$ et $\varepsilon_2$) est un isomorphisme entre $(\{-1,1\}^2, \times)$ et $(\mathrm{Hom}(\mathbb{H}_8, \mathbb{C}^*), \times)$.

**Remarque.** Pour abréger la rédaction, on peut remarquer qu'une partie génératrice de $\mathbb{H}_8$ est $\{-1, i, j\}$ par exemple.

**Remarque (G/H).** Plus généralement, si $f : G \to A$ est un morphisme à valeurs dans un groupe $A$ commutatif, on a toujours $f(ghg^{-1}h^{-1}) = 1_A$, et donc $ghg^{-1}h^{-1} \in \ker(f)$. Par conséquent, si l'on note $D(G)$ le sous-groupe engendré par les éléments de la forme $ghg^{-1}h^{-1}$ (c'est le *sous-groupe dérivé* de $G$), alors $f$ induit un morphisme de $G/D(G)$ dans $A$ par le théorème de factorisation des morphismes. Il peut être plus facile à expliciter parce que $G/D(G)$ est toujours commutatif (exercice), et plus petit que $G$. Par exemple, dans le cadre de cet exercice, on a implicitement démontré que $D(\mathbb{H}_8) = \{-1,1\}$, et comme $\mathbb{H}_8/\{-1,1\} = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (pourquoi ?), déterminer les morphismes $f : \mathbb{H}_8 \to \mathbb{C}^*$ se ramène à déterminer les morphismes $(\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{C}^*$. Les morphismes d'un tel groupe commutatif dans $\mathbb{C}^*$ s'obtiennent toujours assez facilement, en envoyant les générateurs « naturels » du groupe de départ sur n'importe quelles racines de l'unité dans $\mathbb{C}^*$ compatibles avec leurs ordres.

5. En imitant le raisonnement de la question précédente, on trouve qu'un morphisme $f : \mathbb{H}_8 \to \mathbb{Z}/n\mathbb{Z}$ vérifie : $f(-1) = \bar{0}$, puis qu'il suffit de déterminer $f(i)$ et $f(j)$ pour caractériser $f$. Or : $2 \cdot f(i) = f(i^2) = f(-1) = \bar{0}$, donc $f(i)$ est d'ordre divisant 2 dans $(\mathbb{Z}/n\mathbb{Z}, +)$. De même pour $f(j)$. On doit faire une distinction de cas pour poursuivre.

   Si $n$ est impair, alors 2 ne divise pas le cardinal de $\mathbb{Z}/n\mathbb{Z}$ et donc, par la contraposée du théorème de Lagrange, $f(i)$ ne peut pas être d'ordre 2. Le seul élément d'ordre 1 dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est $\bar{0}$, donc : $f(i) = f(j) = \bar{0}$, et par suite $f$ est identiquement nulle.

   Si $n$ est pair, alors 2 divise $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}/n\mathbb{Z}$ est cyclique et on sait qu'il admet exactement un élément d'ordre 2 (à savoir $\overline{\frac{n}{2}}$). Comme $f(i)$ est d'ordre divisant 2, on a $f(i) = \bar{0}$ ou $f(i) = \overline{\frac{n}{2}}$, ce qu'on résume en disant qu'il existe $\varepsilon_1 \in \{\bar{0}, \bar{1}\}$ tel que : $f(i) = \overline{\varepsilon_1 \frac{n}{2}}$. De même, il existe $\varepsilon_2 \in \{\bar{0}, \bar{1}\}$ tel que : $f(j) = \overline{\varepsilon_2 \frac{n}{2}}$. Ainsi, si $f$ est un morphisme de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$, avec $n$ pair, il est défini par : $f(\pm 1) = \bar{0}$, $f(\pm i) = \overline{\varepsilon_1 \frac{n}{2}}$, $f(\pm j) = \overline{\varepsilon_2 \frac{n}{2}}$, et : $f(\pm k) = f(\pm i) + f(\pm j) = \overline{(\varepsilon_1 + \varepsilon_2)\frac{n}{2}}$, avec $(\varepsilon_1, \varepsilon_2) \in \{\bar{0}, \bar{1}\}^2$. Réciproquement, on vérifie que toute application ainsi définie est bien un morphisme.

   **Conclusion.** Si $n$ est impair, alors le seul morphisme de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$ est le morphisme trivial. Si $n$ est pair, alors il y a quatre morphismes de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$.

☢ Penser au principe de conjugaison, en particulier dans $S_n$, pour simplifier une étude. □

**Réponse.**

1. On doit montrer que pour toutes doubles-transpositions $\sigma$ et $\tau$ de $S_4$, on a : $\tau\sigma = \sigma\tau$, ce qui équivaut à : $\tau\sigma\tau^{-1} = \sigma$. Or, par le principe de conjugaison, si $\sigma = (a\ b)(c\ d)$ alors : $\tau\sigma\tau^{-1} = (\tau(a)\ \tau(b))(\tau(c)\ \tau(d))$. C'est égal à $\sigma$ si et seulement si, par unicité de la décomposition en cycles à supports disjoints, on a une des deux conditions suivantes :
   — on a $\{\tau(a), \tau(b)\} = \{a, b\}$ et $\{\tau(c), \tau(d)\} = \{c, d\}$ ;
   — on a $\{\tau(a), \tau(b)\} = \{c, d\}$ et $\{\tau(c), \tau(d)\} = \{a, b\}$.

   On remarque que toutes les doubles-transpositions de $S_4$ (et l'identité) vérifient l'une ou l'autre condition : en effet, si une double-transposition $\tau$ ne vérifie pas l'une de ces deux conditions, on doit avoir par exemple $\{\tau(a), \tau(b)\} = \{a, c\}$ (quitte à inverser les rôles de $a$ et $b$, ou de $c$ et $d$, on peut nécessairement se ramener à ce cas), et dans ce cas $\tau(a) = c$ car une double-transposition de $S_4$ ne peut pas avoir de point fixe, et $\tau(b) = a$. Mais on doit aussi avoir : $\tau(c) = \tau^2(a) = a$ (en effet $\tau^2 = \mathrm{Id}$ car les transpositions sont d'ordre 2), donc $\tau(b) = \tau(c)$ : cela contredit l'injectivité de $\tau$.

   En résumé : toute double-transposition $\tau$ vérifie les conditions ci-dessus, donc $\tau\sigma\tau^{-1} = \tau$ est toujours vrai, et donc $\tau\sigma = \sigma\tau$ aussi. Ceci vaut pour tout $(\sigma, \tau) \in (V_4)^2$, donc c'est un groupe commutatif.

   **Remarque.** Un groupe dont tous les éléments sont d'ordre 1 ou 2 est toujours commutatif. C'est un exercice de travaux dirigés.

2. Soit $M$ une matrice inversible d'ordre 2 telle que : $\forall A \in \mathrm{GL}_2(K)$, $AM = MA$. On a en particulier : $\forall A \in \mathrm{GL}_2(K)$, $A = MAM^{-1}$. Or, si $D$ est une droite quelconque de $K^2$, et si $A$ est la matrice de la symétrie

par rapport à $D$ et parallèlement à n'importe quel supplémentaire de $D$, alors on vérifie aisément que $MAM^{-1}$ est toujours une matrice de symétrie (car $(MAM^{-1})^2 = MA^2M^{-1} = M\mathrm{I}_2M^{-1} = \mathrm{I}_2$), par rapport à $M(D)$ (peu importe parallèlement à quoi : nous ne nous en servirons pas) puisque : $\forall X \in \mathrm{M}_{2,1}(K)$, $MAM^{-1}X = X \iff A(M^{-1}X) = M^{-1}X \iff M^{-1}X \in D \iff X \in M(D)$. L'égalité $A = MAM^{-1}$ implique donc que $A$ serait une symétrie à la fois par rapport à $D$ et $M(D)$, donc : $M(D) = D$.

Ceci vaut pour toute droite $D$ de $K^2$, et c'est un résultat classique que cela implique : $\exists \lambda \in K^*$, $M = \lambda \mathrm{I}_2$. Pour le démontrer dans ce cas particulier : si $(\vec{e}_1, \vec{e}_2)$ est la base canonique de $K^2$, prendre successivement $D = K\vec{e}_1$, $D = K\vec{e}_2$ et $D = K(\vec{e}_1 + \vec{e}_2)$, et traduire l'égalité $M(D) = D$, implique l'existence de $\alpha$, $\beta$ et $\lambda$ dans $K$ tels que : $M\vec{e}_1 = \alpha\vec{e}_1$, $M\vec{e}_2 = \beta\vec{e}_2$, $M(\vec{e}_1 + \vec{e}_2) = \lambda(\vec{e}_1 + \vec{e}_2)$. On a donc : $\lambda(\vec{e}_1 + \vec{e}_2) = M(\vec{e}_1 + \vec{e}_2) = M\vec{e}_1 + M\vec{e}_2 = \alpha\vec{e}_1 + \beta\vec{e}_2$. Par indépendance linéaire de $\vec{e}_1$ et $\vec{e}_2$, cela implique : $\alpha = \beta = \lambda$. Donc : $M\vec{e}_1 = \lambda\vec{e}_1$, et : $M\vec{e}_2 = \lambda\vec{e}_2$. On en déduit : $M = \lambda \mathrm{I}_2$.

Réciproquement, toute matrice de cette forme commute avec les matrices de $\mathrm{GL}_2(K)$.

☢ Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc. □

**Réponse.**

1. On fait agir $S_n$ sur $I(k,n)$ *via* le morphisme de $S_n$ dans $S_{I(k,n)}$ défini par :

$$\sigma \mapsto (\varphi_\sigma : \iota \mapsto \sigma \circ \iota)\,.$$

La composée d'une injection et d'une bijection est une injection, donc $\varphi_\sigma$ est effectivement à valeurs dans $I(k,n)$ pour tout $\sigma \in S_n$. Soit $\iota_0 : [\![1,k]\!] \to [\![1,n]\!]$ l'injection naturelle définie par $x \mapsto x$. On va étudier, comme souvent pour une action :

$$\mathcal{O} = \{\varphi_\sigma(\iota_0) \mid \sigma \in S_n\}\,, \quad \text{et :} \quad S_{\iota_0} = \{\sigma \in S_n \mid \varphi_\sigma(\iota_0) = \iota_0\}\,.$$

Nous allons montrer qu'en composant $\iota_0$ par toutes les permutations de $S_n$, on obtient toutes les injections de $[\![1,k]\!]$ dans $[\![1,n]\!]$. Soit $\iota : [\![1,k]\!] \to [\![1,n]\!]$ ; montrons l'existence de $\sigma \in S_n$ telle que $\iota = \sigma \circ \iota_0 = \varphi_\sigma(\iota_0)$. Pour cela, on note que si $\sigma$ existe, alors $\sigma^{-1} \circ \iota = \iota_0$. Puisque $\iota_0$ est « presque » l'identité, $\sigma^{-1}$ est « presque » l'application réciproque de $\iota$ ; une telle chose n'existe pas, puisque $\iota$ n'est pas bijective, mais néanmoins $\iota$ induit une bijection sur son image et nous allons y utiliser son application réciproque pour construire $\sigma$.

En effet, $\iota : [\![1,k]\!] \to [\![1,n]\!]$ induit une bijection de $[\![1,k]\!]$ dans $\iota([\![1,k]\!])$ ; notons $j : \iota([\![1,k]\!]) \to [\![1,k]\!]$ son application réciproque, qu'on complète arbitrairement en une application bijective $\tilde{j} : [\![1,n]\!] \to [\![1,n]\!]$ (par exemple en envoyant le plus petit élément de $[\![1,n]\!] \setminus \iota([\![1,k]\!])$ sur le plus petit élément de $[\![1,n]\!] \setminus [\![1,k]\!]$, puis de même avec le deuxième plus petit élément, etc. Ce procédé donne nécessairement une application injective de $[\![1,n]\!]$ dans lui-même, donc une bijection). En sa qualité d'application réciproque, on a :

$$\forall m \in [\![1,k]\!],\ \tilde{j} \circ \iota(m) = j \circ \iota(m) = m = \iota_0(m),$$

donc : $\tilde{j} \circ \iota = \iota_0$ ; il suffit alors de poser $\sigma = \tilde{j}^{-1}$ pour avoir : $\iota = \varphi_\sigma(\iota_0)$. On a montré :

$$\mathcal{O} = \{\varphi_\sigma(\iota_0) \mid \sigma \in S_n\} = I(k,n).$$

Passons au second ensemble : $S_{\iota_0} = \{\sigma \in S_n \mid \varphi_\sigma(\iota_0) = \iota_0\} = \{\sigma \in S_n \mid \forall m \in [\![1,k]\!],\ \sigma(m) = m\}$. On se convainc aisément que cet ensemble est un groupe isomorphe à $S_{[\![k+1,n]\!]}$, *via* l'application $\sigma \mapsto \sigma_{|[\![k+1,n]\!]}$. En particulier : $\mathrm{card}\,(S_{\iota_0}) = (n-k)!$.

On peut conclure en répondant à la question posée. Le cardinal cherché est : $\mathrm{card}(I(k,n)) = \mathrm{card}\,(\mathcal{O})$. On déduit de cette description une application naturelle surjective :

$$\left\{ \begin{array}{ccc} S_n & \to & I(k,n) = \mathcal{O} \\ \sigma & \mapsto & \varphi_\sigma(\iota_0) \end{array} \right.$$

et nous allons calculer le nombre d'antécédents de chaque élément de $I(k,n)$. Soit $\iota \in I(k,n)$, dont on note $\sigma$ un antécédent. Alors :

$$\forall \sigma' \in S_n, \quad \varphi_{\sigma'}(\iota_0) = \varphi_\sigma(\iota_0) \iff \sigma' \circ \iota_0 = \sigma \circ \iota_0 \iff \sigma^{-1} \circ \sigma' \circ \iota_0 = \iota_0 \iff \sigma^{-1} \circ \sigma' \in S_{\iota_0} \iff \sigma' \in \sigma S_{\iota_0}.$$

Autrement dit : l'ensemble des antécédents de $\iota$ est $\sigma S_{\iota_0}$, et il y en a donc $\mathrm{card}(S_{\iota_0})$. Cela vaut pour tout $\iota$. Donc, par le principe des bergers :

$$\mathrm{card}(S_n) = \mathrm{card}(S_{\iota_0})\mathrm{card}(I(k,n)),$$

et donc :

$$\mathrm{card}(I(k,n)) = \frac{\mathrm{card}(S_n)}{\mathrm{card}(S_{\iota_0})} = \frac{n!}{(n-k)!},$$

d'où le résultat.

2. On a : $\mathcal{O} = \{f(1) \mid f \in \langle r\rangle\} = \left\{r^k(1) \mid k \in \mathbb{Z}\right\} = \left\{e^{\frac{2i\pi k}{n}} \mid k \in \mathbb{Z}\right\} = \mathbb{U}_n$. Déterminons à présent : $S = \{f \in \mathrm{D}_n \mid f(1) = 1\}$. Si l'on interprète géométriquement $S$ : il s'agit des transformations permutant les sommets d'un polygone régulier à $n$ côtés (traduction de la condition $f(\mathbb{U}_n) \subseteq \mathbb{U}_n$) sans déplacer le sommet d'affixe 1 (traduction de l'égalité $f(1) = 1$). Il semble que seules l'identité et la réflexion par rapport à l'axe des abscisses conviennent. Montrons-le. Soit $f \in S$. Pour déterminer une application $\mathbb{R}$-linéaire, il suffit de l'expliciter sur une $\mathbb{R}$-base, disons la base $(1, i)$ de $\mathbb{C}$. On a $f(1) = 1$ par définition de $S$, et comme $f \in \mathrm{Is}(\mathbb{C})$ on a : $|f(i)| = |i| = 1$, donc il existe $\theta \in \mathbb{R}$ tel que : $f(i) = e^{i\theta}$. Au vu de notre conjecture formulée ci-dessus, on aimerait montrer : $f(i) = \pm i$, c'est-à-dire : $\theta \equiv \frac{\pi}{2} \bmod \pi$. Or on a d'une part : $|f(i) + f(1)|^2 = |f(i+1)|^2 = |i+1|^2 = 2$, et d'autre part : $|f(i) + f(1)|^2 = \left|e^{i\theta} + 1\right|^2 = 2^2\left(\cos\left(\frac{\theta}{2}\right)\right)^2$, donc : $\left(\cos\left(\frac{\theta}{2}\right)\right)^2 = \frac{1}{2}$, puis : $\frac{\theta}{2} \equiv \frac{\pi}{4} \bmod \frac{\pi}{2}$ (je formule de manière succincte le fait que les quatre angles à convenir modulo $2\pi$ soient $\frac{\pi}{4}$, $\frac{3\pi}{4}$, et leurs opposés). On en déduit : $\theta \equiv \frac{\pi}{2} \bmod \pi$, ce que je voulais démontrer. Donc : $f(i) = i$, ou : $f(i) = -i$. Dans le premier cas, $f$ coïncide avec l'endomorphisme $\mathrm{Id}_{\mathbb{C}}$ sur la $\mathbb{R}$-base $(1, i)$, donc : $f = \mathrm{Id}_{\mathbb{C}}$. Dans le second cas, $f$ coïncide avec l'endomorphisme $s : z \mapsto \bar{z}$, donc : $f = s$. Réciproquement, on vérifie aisément que ces deux endomorphismes sont dans $S$, donc : $S = \{\mathrm{Id}_{\mathbb{C}}, s\} = \langle s\rangle$.

On nous demande d'en déduire que $\mathrm{D}_n$ est engendré par $r$ et $s$. Soit $f \in \mathrm{D}_n$. Comme $1 \in \mathbb{U}_n$, on a par définition de $\mathrm{D}_n$ l'appartenance suivante : $f(1) \in \mathbb{U}_n$. Or : $\mathbb{U}_n = \mathcal{O}$, donc il existe $k \in \mathbb{Z}$ tel que : $f(1) = r^k(1)$. Ainsi : $r^{-k} \circ f(1) = 1$, donc : $r^{-k} \circ f \in S = \langle s\rangle$, donc il existe $\ell \in \mathbb{Z}$ tel que : $r^{-k} \circ f = s^\ell$. On conclut : $f = r^k \circ s^\ell \in \langle r, s\rangle$, donc : $\mathrm{D}_n \subseteq \langle r, s\rangle$. L'inclusion réciproque est immédiate car $r$ et $s$ sont dans $\mathrm{D}_n$, donc : $\mathrm{D}_n = \langle r, s\rangle$. Ce qu'il fallait démontrer.

**Remarque.** L'idée de calculer $|f(i) + f(1)|^2$ sera plus naturelle lorsqu'on définira les isométries au chapitre XII, et qu'on montrera notamment qu'une application $\mathbb{R}$-linéaire qui conserve les longueurs doit aussi conserver les angles droits (c'est ce que je fais implicitement pour montrer que, ayant : $1 \perp i$, on doit avoir : $1 = f(1) \perp f(i)$, et donc $f(i) = \pm i$). On le démontrera en passant par une identité de polarisation : c'est implicitement ce que je fais ici, puisque $(z_1, z_2) \mapsto \mathrm{Re}(\overline{z_1}z_2) = \frac{1}{2}\left(|z_1 + z_2|^2 - |z_1|^2 - |z_2|^2\right)$ est l'écriture intrinsèque du produit scalaire usuel du plan complexe.