

Groupes

Corrigé de l'exercice 1 : Sous-groupes engendrés dans $\mathbb{Z}$

1. Tout élément $12u + 18v$ est multiple de 6, donc $\langle 12, 18 \rangle \subset 6\mathbb{Z}$. Inversement, $6 = 18 - 12$ appartient à $\langle 12, 18 \rangle$. Par conséquent, tous les multiples de 6 y sont aussi. **On obtient** $\langle 12, 18 \rangle = 6\mathbb{Z}$.
2. De même, tout élément $-8u + 20v$ est multiple de 4. De plus, $4 = 20 + 2 \times (-8)$. **Ainsi**, $\langle -8, 20 \rangle = 4\mathbb{Z}$.
3. Le sous-groupe cherché est $d\mathbb{Z}$ avec $d = 15 \wedge 21 \wedge 35$. Or $15 \wedge 21 = 3$ et $3 \wedge 35 = 1$, donc $d = 1$. Pour la relation, on part de $3 = 3 \times 15 - 2 \times 21 = 45 - 42$. Ensuite, $1 = 12 \times 3 - 35 = 36 - 35$. En remplaçant,
$$1 = 12(3 \times 15 - 2 \times 21) - 35 = 36 \times 15 - 24 \times 21 - 35.$$
On vérifie : $540 - 504 - 35 = 1$. **Donc** $\langle 15, 21, 35 \rangle = \mathbb{Z}$, avec $(a, b, c) = (36, -24, -1)$.

Question 4

4. On a $6 \wedge 10 = 2$, $6 \wedge 15 = 3$ et $10 \wedge 15 = 5$. Ainsi, les parties à deux éléments engendrent $2\mathbb{Z}$, $3\mathbb{Z}$ et $5\mathbb{Z}$, qui sont distincts de $\mathbb{Z}$. En revanche, $6 \wedge 10 \wedge 15 = 1$. Explicitement, $1 = 6 + 10 - 15$. **Donc** $\{6, 10, 15\}$ engendre $\mathbb{Z}$, sans qu'aucune paire n'y suffise.

Point de méthode : dans $\mathbb{Z}$, le sous-groupe engendré par des entiers est toujours $d\mathbb{Z}$, où d est leur pgcd ; une relation de Bézout fournit l'inclusion difficile.

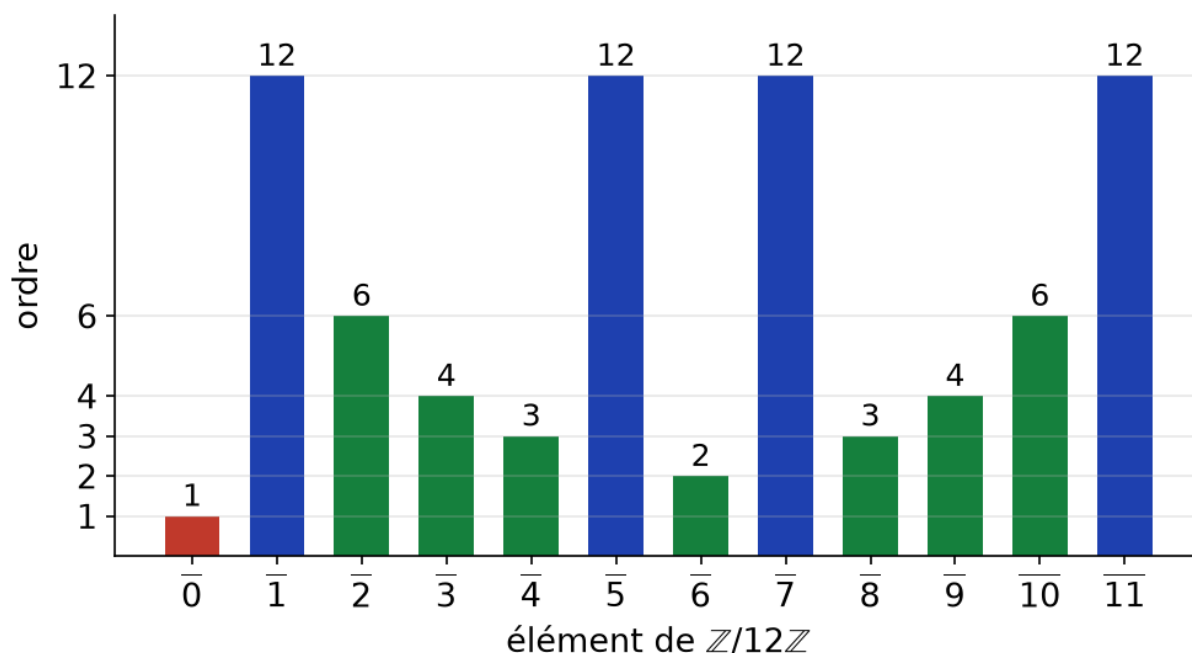
Corrigé de l'exercice 2 : Somme et intersection de sous-groupes de $\mathbb{Z}$

1. L'ensemble $S = a\mathbb{Z} + b\mathbb{Z}$ contient $0 = a \cdot 0 + b \cdot 0$. De plus, $(au + bv) - (au' + bv') = a(u - u') + b(v - v')$ appartient à S . C'est donc un sous-groupe de $\mathbb{Z}$. D'après le théorème de structure, $S = \delta\mathbb{Z}$ avec $\delta \geq 1$ car $a \in S$. D'une part, a et b sont dans S , donc δ divise a et b , puis δ divise d . D'autre part, d divise tout $au + bv$, en particulier δ . **Ainsi $\delta = d$ et $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.**
2. L'intersection $I = a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe, donc $I = \mu\mathbb{Z}$. Elle contient $ab \neq 0$, donc $\mu \geq 1$. Les éléments de I sont les multiples communs de a et b . Or μ est le plus petit d'entre eux qui soit strictement positif. **Par définition du ppcm, $\mu = m$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.**
3. On a $12 \wedge 18 = 6$ et $12 \vee 18 = 36$. **Donc $12\mathbb{Z} + 18\mathbb{Z} = 6\mathbb{Z}$ et $12\mathbb{Z} \cap 18\mathbb{Z} = 36\mathbb{Z}$.**
4. Les entiers 2 et 3 appartiennent à $2\mathbb{Z} \cup 3\mathbb{Z}$. Cependant, leur somme 5 n'est ni paire ni multiple de 3. La réunion n'est donc pas stable par addition. Le sous-groupe engendré contient $3 - 2 = 1$. **Par conséquent, $\langle 2\mathbb{Z} \cup 3\mathbb{Z} \rangle = \mathbb{Z}$.**

Corrigé de l'exercice 3 : Ordres des éléments de $\mathbb{Z}/12\mathbb{Z}$

1. D'après le cours, $\overline{k}$ est d'ordre $\frac{12}{12 \wedge k}$. On obtient ainsi :
 - $\overline{0}$ est d'ordre 1 ;
 - $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ sont d'ordre 12, car premiers avec 12 ;
 - $\overline{2}$ et $\overline{10}$ sont d'ordre 6, car $12 \wedge 2 = 12 \wedge 10 = 2$;
 - $\overline{3}$ et $\overline{9}$ sont d'ordre 4 ;
 - $\overline{4}$ et $\overline{8}$ sont d'ordre 3 ;
 - $\overline{6}$ est d'ordre 2.

Par exemple, $3\bar{4} = \bar{12} = \bar{0}$ alors que $\bar{4} \neq \bar{0}$ et $2 \cdot \bar{4} = \bar{8} \neq \bar{0}$. **Le diagramme ci-dessous résume ces douze ordres.**



- On compte 1 élément d'ordre 1, 1 d'ordre 2, 2 d'ordre 3, 2 d'ordre 4, 2 d'ordre 6 et 4 d'ordre 12. Aucun élément n'a un autre ordre. **Le total vaut** $1 + 1 + 2 + 2 + 2 + 4 = 12$.
- Les ordres obtenus sont 1, 2, 3, 4, 6 et 12, qui sont tous des diviseurs de 12, conformément au théorème de Lagrange. Enfin, un générateur est un élément d'ordre 12. **Les générateurs sont** $\bar{1}, \bar{5}, \bar{7}$ et $\bar{11}$.

Corrigé de l'exercice 4 : Générateurs de $\mathbb{Z}/n\mathbb{Z}$

- La classe $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.** C'est une conséquence du théorème de Bézout.
- On a $15 = 3 \times 5$. On garde donc les entiers de 1 à 14 divisibles ni par 3 ni par 5. **Les générateurs de $\mathbb{Z}/15\mathbb{Z}$ sont $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}$, soit 8 classes.** De même,

$18 = 2 \times 3^2$. On écarte les entiers pairs et les multiples de 3. **Les générateurs de $\mathbb{Z}/18\mathbb{Z}$ sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}$, soit 6 classes.**

3. On cherche u tel que $7u \equiv 1 \pmod{15}$. L'algorithme d'Euclide donne $15 = 2 \times 7 + 1$, donc $1 = 15 - 2 \times 7$. Ainsi, $u = -2$ convient, soit $u = 13$ dans $\llbracket 0, 14 \rrbracket$. Vérification : $13 \times 7 = 91 = 6 \times 15 + 1$. **On a donc $13 \cdot \bar{7} = \bar{1}$.**
4. Soit $n \geq 3$ et E l'ensemble des $k \in \llbracket 1, n-1 \rrbracket$ premiers avec n . L'application $s: k \rightarrow n - k$ envoie E dans E . En effet, un diviseur commun à $n - k$ et n divise aussi k . De plus, $s \circ s = \text{id}$. Supposons que $s(k) = k$. Alors $n = 2k$, et $k \wedge n = k$. Comme $k \wedge n = 1$, on aurait $k = 1$, puis $n = 2$, ce qui est exclu. Ainsi, s regroupe les éléments de E par paires $\{k, n - k\}$ disjointes. **Le nombre de générateurs est donc pair.**

Corrigé de l'exercice 5 : Ordre d'une matrice et d'une permutation

1. Un calcul direct donne

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

Or $A \neq I_2$ et $A^2 \neq I_2$. **Donc A est d'ordre 3.**

2. On sait que $R_\theta^k = R_{k\theta}$. Ainsi, $R_\theta^k = I_2$ si et seulement si $k\theta \in 2\pi\mathbb{Z}$. Avec $\theta = \frac{5\pi}{6}$, cela s'écrit $\frac{5k}{12} \in \mathbb{Z}$, c'est-à-dire $12 \mid 5k$. Comme $5 \wedge 12 = 1$, le lemme de Gauss donne $12 \mid k$. **La rotation $R_{5\pi/6}$ est donc d'ordre 12.**

3. Les cycles $c = (1, 2, 3)$ et $t = (4, 5)$ sont à supports disjoints, donc ils commutent. Ainsi,

$$\sigma^2 = c^2 = (1, 3, 2) \quad \text{et} \quad \sigma^3 = c^3 t^3 = t = (4, 5).$$

$\sigma^k = c^k t^k$. On obtient $\sigma^3 = c^3 t^3 = t$ car $t^2 = \text{id}$. Ensuite,

Enfin, $\sigma^k = \text{id}$ exige $c^k = \text{id}$ et $t^k = \text{id}$, car les supports sont disjoints. Cela équivaut à $3 \mid k$ et $2 \mid k$, soit $6 \mid k$. **L'ordre de σ est 6.**

4. Par récurrence, $B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ pour tout $k \in \mathbb{N}$. En effet, $B^{k+1} = B^k B$ a pour coefficient en haut à droite $k + 1$. Ainsi, $B^k \neq I_2$ pour $k \geq 1$. **La matrice B est**

d'ordre infini.

Corrigé de l'exercice 6 : Racines dixièmes de l'unité

1. L'élément ω est d'ordre 10, donc ω^k est d'ordre $\frac{10}{10 \wedge k}$. **On trouve : ω^0 d'ordre 1 ; $\omega^5 = -1$ d'ordre 2 ; $\omega^2, \omega^4, \omega^6, \omega^8$ d'ordre 5 ; $\omega, \omega^3, \omega^7, \omega^9$ d'ordre 10.**
2. Les racines primitives sont $\omega, \omega^3, \omega^7, \omega^9$. Posons $\zeta = \omega^2$, d'ordre 5. On remarque que $-\zeta^k = \omega^5 \omega^{2k} = \omega^{2k+5}$. Pour $k = 1, 2, 3, 4$, les exposants $2k+5$ valent 7, 9, 11, 13, soit 7, 9, 1, 3 modulo 10. Ainsi, les racines primitives dixièmes sont les opposées des racines primitives cinquièmes $\zeta, \zeta^2, \zeta^3, \zeta^4$. Or $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$, car $\zeta \neq 1$ et $\zeta^5 = 1$. Par conséquent,
- $$\omega + \omega^3 + \omega^7 + \omega^9 = -(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = -(-1) = 1.$$

La somme des racines primitives dixièmes vaut 1.

3. Supposons $n \mid m$, avec $m = nq$. Si $z^n = 1$, alors $z^m = (z^n)^q = 1$. Donc $\mathbb{U}_n \subset \mathbb{U}_m$. Réciproquement, supposons $\mathbb{U}_n \subset \mathbb{U}_m$. L'élément $e^{2i\pi/n}$ est d'ordre n et vérifie $z^m = 1$. D'après la caractérisation de l'ordre, n divise m . **Ainsi,**
- $$\mathbb{U}_n \subset \mathbb{U}_m \Leftrightarrow n \mid m.$$
4. Posons $\delta = m \wedge n$. D'abord, δ divise m et n , donc $\mathbb{U}_\delta \subset \mathbb{U}_m \cap \mathbb{U}_n$ par la question 3. Inversement, soit z dans l'intersection, d'ordre r . Comme $z^m = z^n = 1$, l'entier r divise m et n , donc δ . Ainsi, $z^\delta = 1$. **On conclut $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m \wedge n}$, et $\mathbb{U}_{10} \cap \mathbb{U}_4 = \mathbb{U}_2 = \{1, -1\}$.**

Corrigé de l'exercice 7 : Ordre d'une puissance

1. Posons $\delta = n \wedge k$, puis $n = \delta n'$ et $k = \delta k'$ avec $n' \wedge k' = 1$. Pour $m \in \mathbb{Z}$, on a $(x^k)^m = x^{km}$. Donc $(x^k)^m = e$ si et seulement si $n \mid km$, c'est-à-dire $\delta n' \mid \delta k' m$, soit $n' \mid k' m$. Comme $n' \wedge k' = 1$, le lemme de Gauss donne l'équivalence avec $n' \mid m$. Ainsi, les entiers m tels que $(x^k)^m = e$ sont les multiples de n' . **L'ordre de x^k est $n' = \frac{n}{n \wedge k}$.**

- On a $\langle x^k \rangle \subset \langle x \rangle$, et le second a n éléments. Ainsi, x^k engendre $\langle x \rangle$ si et seulement si $\langle x^k \rangle$ a n éléments. Cela signifie que x^k est d'ordre n , soit $n \wedge k = 1$. **Donc x^k engendre $\langle x \rangle$ si et seulement si $k \wedge n = 1$.**
- Avec $n = 20$, on a $20 \wedge 6 = 2$, $20 \wedge 15 = 5$ et $20 \wedge 8 = 4$. **Les ordres sont donc 10 pour x^6 , 4 pour x^{15} et 5 pour x^{-8} .**
- D'après la question 1 avec $k = -1$, l'élément x^{-1} est d'ordre $n / (n \wedge 1) = n$. Soit maintenant $f: G \rightarrow G'$ un isomorphisme et $x \in G$. Pour tout k , on a $f(x)^k = f(x^k)$. Par injectivité, $f(x^k) = e'$ équivaut à $x^k = e$. Les ensembles d'entiers qui annulent x et $f(x)$ sont donc égaux. **Par conséquent, x et $f(x)$ ont le même ordre, fini ou infini.**

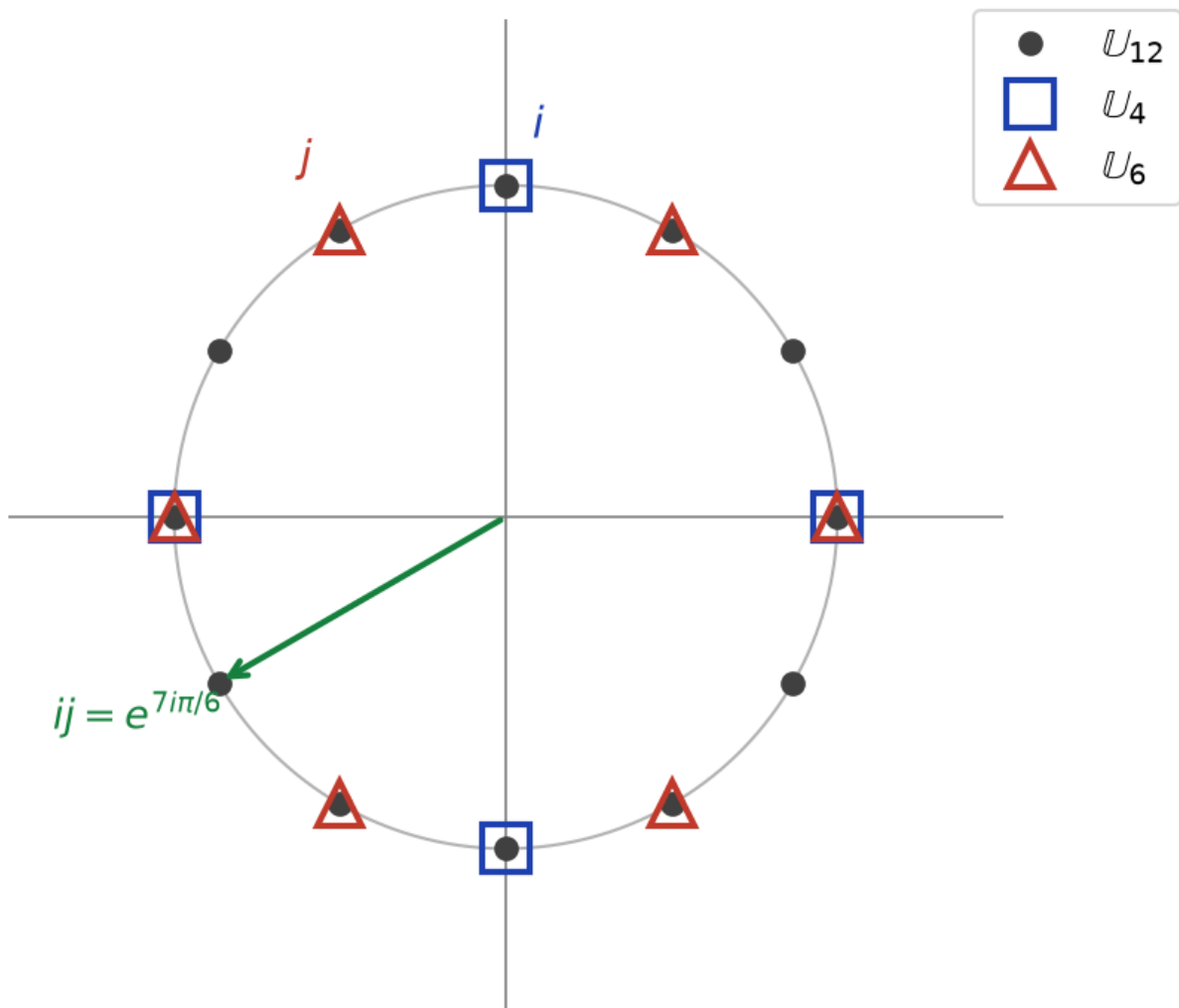
Corrigé de l'exercice 8 : Un isomorphisme explicite entre $\mathbb{Z}/n\mathbb{Z}$ et les racines de l'unité

- Pour $k, l \in \mathbb{Z}$, on a $f(k+l) = \omega^{k+l} = \omega^k \omega^l = f(k) f(l)$. C'est donc un morphisme. De plus, $(\omega^k)^n = (\omega^n)^k = 1$, donc f est à valeurs dans $\mathbb{U}_n$. Il est surjectif car $\mathbb{U}_n = \{\omega^k, 0 \leq k \leq n-1\}$. Enfin, ω est d'ordre n , donc $\omega^k = 1 \Leftrightarrow n \mid k$. **Le noyau de f est $n\mathbb{Z}$.**
- Si $\bar{k} = \bar{l}$, alors $k-l \in n\mathbb{Z}$, donc $\omega^{k-l} = 1$ et $\omega^k = \omega^l$. Ainsi, g est bien définie. Ensuite, $g(\bar{k} + \bar{l}) = g(\overline{k+l}) = \omega^{k+l} = g(\bar{k}) g(\bar{l})$. Elle est surjective comme f . Pour l'injectivité, $g(\bar{k}) = 1$ implique $k \in n\mathbb{Z}$, soit $\bar{k} = \bar{0}$. **Donc g est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur $(\mathbb{U}_n, \times)$.**
- Pour $n = 6$, on a $\omega^3 = e^{i\pi} = -1$. Donc l'antécédent de -1 est $\bar{3}$. Par ailleurs, un isomorphisme conserve l'ordre, donc il envoie les générateurs sur les générateurs. Ceux de $\mathbb{Z}/6\mathbb{Z}$ sont $\bar{1}$ et $\bar{5}$. **Les générateurs de $\mathbb{U}_6$ sont $\omega = e^{i\pi/3}$ et $\omega^5 = e^{-i\pi/3}$.**

Point de méthode : sur un quotient comme $\mathbb{Z}/n\mathbb{Z}$, on vérifie toujours d'abord que l'image ne dépend pas du représentant choisi.

Corrigé de l'exercice 9 : Sous-groupe engendré par i et j

1. On a $i^4 = 1$ et $4 \mid 12$, donc $i^{12} = 1$. De même, $j^3 = 1$ et $3 \mid 12$, donc $j^{12} = 1$.
Ainsi, i et j appartiennent à $\mathbb{U}_{12}$.
2. On écrit $i = e^{i\pi/2} = e^{2i\pi \cdot 3/12}$ et $j = e^{2i\pi \cdot 4/12}$. Alors
 $ij = e^{2i\pi \cdot 7/12} = e^{7i\pi/6}$. C'est ω^7 avec $\omega = e^{2i\pi/12}$ d'ordre 12. Comme
 $7 \wedge 12 = 1$, l'élément $ij = e^{7i\pi/6}$ **est d'ordre 12.**
3. Notons $H = \langle i, j \rangle$. D'une part, $\mathbb{U}_{12}$ est un sous-groupe contenant i et j , donc
 $H \subset \mathbb{U}_{12}$. D'autre part, $ij \in H$, donc $\langle ij \rangle \subset H$. Or $\langle ij \rangle$ a 12 éléments, comme
 $\mathbb{U}_{12}$. Ainsi, $\langle ij \rangle = \mathbb{U}_{12} \subset H$. **On conclut $\langle i, j \rangle = \mathbb{U}_{12}$.** La figure ci-dessous montre
les deux sous-groupes de départ et le générateur ij obtenu.



4. Comme $m \mid l$ et $n \mid l$, l'exercice 6 donne $\mathbb{U}_m \cup \mathbb{U}_n \subset \mathbb{U}_l$. Par conséquent, le sous-groupe K engendré par cette réunion est inclus dans $\mathbb{U}_l$. Inversement, posons $d = m \wedge n$, de sorte que $l = mn/d$. Le théorème de Bézout fournit u, v tels que $um + vn = d$. En divisant par mn , on obtient

$$\frac{1}{l} = \frac{d}{mn} = \frac{u}{n} + \frac{v}{m}.$$

Donc $e^{2i\pi/l} = (e^{2i\pi/n})^u (e^{2i\pi/m})^v$ appartient à K . Or $e^{2i\pi/l}$ engendre $\mathbb{U}_l$. **Ainsi,** $\langle \mathbb{U}_m \cup \mathbb{U}_n \rangle = \mathbb{U}_{m \vee n}$. Pour $m = 4$ et $n = 6$, on retrouve $\mathbb{U}_{12}$.

Corrigé de l'exercice 10 : Le groupe $(\mathbb{Q}, +)$ n'est pas monogène

- Notons $H = \langle \frac{1}{2}, \frac{1}{3} \rangle = \left\{ \frac{u}{2} + \frac{v}{3}, (u, v) \in \mathbb{Z}^2 \right\}$. Tout élément s'écrit $\frac{3u+2v}{6}$, donc $H \subset \frac{1}{6}\mathbb{Z}$. Inversement, $\frac{1}{6} = \frac{1}{2} - \frac{1}{3}$ appartient à H . **Par conséquent,** $H = \frac{1}{6}\mathbb{Z}$.
- Pour chaque j , on a $r_j = \frac{p_j(q/q_j)}{q}$, où q/q_j est un entier. Ainsi, chaque r_j appartient au sous-groupe $\frac{1}{q}\mathbb{Z}$. Donc $\langle r_1, \dots, r_s \rangle \subset \frac{1}{q}\mathbb{Z}$. Ensuite, l'application $x \rightarrow qx$ est un isomorphisme de $\frac{1}{q}\mathbb{Z}$ sur $\mathbb{Z}$. Elle envoie notre sous-groupe sur un sous-groupe de $\mathbb{Z}$, c'est-à-dire sur un $c\mathbb{Z}$. **Le sous-groupe $\langle r_1, \dots, r_s \rangle$ vaut donc $\frac{c}{q}\mathbb{Z}$: il est monogène.**
- Supposons que $\mathbb{Q} = \langle a \rangle = a\mathbb{Z}$ pour un rationnel a . Comme $\mathbb{Q} \neq \{0\}$, on a $a \neq 0$. Or $\frac{a}{2} \in \mathbb{Q}$, donc il existe $k \in \mathbb{Z}$ tel que $\frac{a}{2} = ka$. En simplifiant par a , on obtient $k = \frac{1}{2}$, ce qui est absurde. **Donc $(\mathbb{Q}, +)$ n'est pas monogène.**
- Si $\mathbb{Q}$ admettait une partie génératrice finie $\{r_1, \dots, r_s\}$, il serait monogène d'après la question 2. Cela contredit la question 3. **Ainsi, $(\mathbb{Q}, +)$ n'admet aucune partie génératrice finie.**

Corrigé de l'exercice 11 : Sous-groupes d'un groupe cyclique

- L'ensemble K contient 0. De plus, si $k, l \in K$, alors $g^{k-l} = g^k(g^l)^{-1} \in H$. C'est donc

un sous-groupe de $\mathbb{Z}$, de la forme $a\mathbb{Z}$. Comme $g^n = e \in H$, on a $n \in K$, donc $a \neq 0$ et $a \mid n$. Enfin, tout élément de H est de la forme g^k avec $k \in K = a\mathbb{Z}$. **Donc**
 $H = \left\{ g^{aq}, q \in \mathbb{Z} \right\} = \langle g^a \rangle$, avec $a \mid n$.

2. D'après l'exercice 7, g^a est d'ordre $n / (n \wedge a) = n/a$ lorsque $a \mid n$. Ainsi, $\langle g^a \rangle$ est d'ordre d si et seulement si $a = n/d$. L'existence est donc assurée par $\langle g^{n/d} \rangle$. Pour l'unicité, un sous-groupe d'ordre d est un $\langle g^a \rangle$ avec $a \mid n$, et nécessairement $a = n/d$. **Il existe un unique sous-groupe d'ordre d , à savoir $\langle g^{n/d} \rangle$.**

3. Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. On obtient donc six sous-groupes :

- $\{\bar{0}\}$, d'ordre 1 ;
- $\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$, d'ordre 2 ;
- $\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$, d'ordre 3 ;
- $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, d'ordre 4 ;
- $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$, d'ordre 6 ;
- $\mathbb{Z}/12\mathbb{Z}$, d'ordre 12.

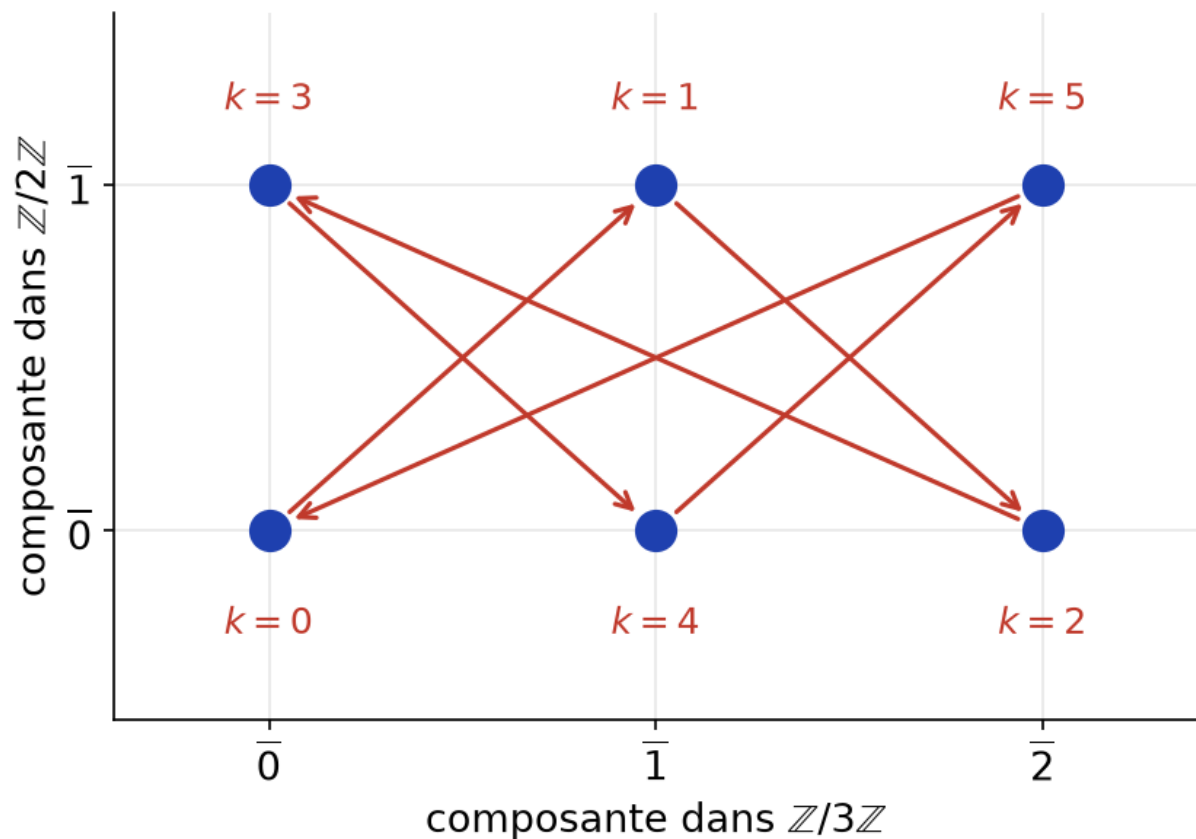
Ce sont les six sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.

4. On a $100 = 2^2 \times 5^2$, qui possède $3 \times 3 = 9$ diviseurs : 1, 2, 4, 5, 10, 20, 25, 50, 100. Le sous-groupe d'ordre 20 est engendré par $\overline{100/20} = \bar{5}$. **Il y a 9 sous-groupes, et celui d'ordre 20 est $\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}, \bar{30}, \bar{35}, \bar{40}\}$.**

Corrigé de l'exercice 12 : Produits de petits groupes cycliques

1. On a $(x, y)^k = (x^k, y^k)$. Ainsi, $(x, y)^k$ est le neutre si et seulement si $x^k = e$ et $y^k = e$. Cela équivaut à $a \mid k$ et $b \mid k$, c'est-à-dire à $a \vee b \mid k$. **Donc (x, y) est d'ordre $a \vee b$.**
2. L'élément $(\bar{1}, \bar{1})$ est d'ordre $2 \vee 3 = 6$, égal au cardinal du groupe. Il engendre donc

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. D'après la classification, l'application $\bar{k} \rightarrow k \cdot (\bar{1}, \bar{1})$ est un isomorphisme depuis $\mathbb{Z}/6\mathbb{Z}$. Autrement dit, la classe de k modulo 6 est envoyée sur le couple (classe de k modulo 2, classe de k modulo 3). **Le groupe est cyclique et isomorphe à $\mathbb{Z}/6\mathbb{Z}$** . La figure ci-dessous montre le parcours des multiples $k \cdot (\bar{1}, \bar{1})$: il visite les six éléments.



3. Tout élément (a, b) de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ vérifie $2 \cdot (a, b) = (\bar{0}, \bar{0})$. Aucun élément n'est donc d'ordre 4. Le groupe n'est pas cyclique. En revanche, $\mathbb{U}_4$ contient i , d'ordre 4. Or un isomorphisme conserve l'ordre (exercice 7). **Ainsi, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique et n'est pas isomorphe à $\mathbb{U}_4$.**
4. Dans $\mathbb{Z}/4\mathbb{Z}$, les ordres divisent 4 ; dans $\mathbb{Z}/6\mathbb{Z}$, ils divisent 6. D'après la question 1, l'ordre d'un couple divise donc $4 \vee 6 = 12$. De plus, $(\bar{1}, \bar{1})$ est d'ordre 12. Comme 12 est strictement inférieur au cardinal 24, aucun élément n'engendre le groupe. **Le plus grand ordre vaut 12, et le groupe n'est pas cyclique.**

Corrigé de l'exercice 13 : Quand le produit de deux groupes cycliques est-il cyclique ?

1. L'élément $\bar{1}$ est d'ordre m et $\bar{1}$ d'ordre n . D'après l'exercice 12, $(\bar{1}, \bar{1})$ est d'ordre $m \vee n$. Or $m \vee n = mn$ lorsque $m \wedge n = 1$. Ainsi, $\langle (\bar{1}, \bar{1}) \rangle$ a mn éléments, autant que G . **Donc G est cyclique, engendré par $(\bar{1}, \bar{1})$.**
2. Soit $(\bar{a}, \bar{b}) \in G$ et $l = m \vee n$. On a $l \cdot (\bar{a}, \bar{b}) = (l\bar{a}, l\bar{b})$. Or $m \mid l$, donc $m \mid l\bar{a}$ et $l\bar{a} = \bar{0}$. De même, $l\bar{b} = \bar{0}$. Par conséquent, l'ordre de tout élément divise l , donc est au plus l . Or $l = mn/d \leq mn/2 < mn$. **Aucun élément n'est d'ordre mn , donc G n'est pas cyclique.**
3. En réunissant les deux questions précédentes, **$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $m \wedge n = 1$.**

Questions 4 à 5

4. D'abord, ψ est bien définie. En effet, si $k \equiv k'$ modulo 12, alors $k \equiv k'$ modulo 4 et modulo 3, car 4 et 3 divisent 12. Ensuite, ψ est un morphisme, car on additionne composante par composante. Son noyau est formé des classes des k multiples de 4 et de 3. Comme $4 \wedge 3 = 1$, ce sont les multiples de 12. Le noyau est donc trivial et ψ est injective. Enfin, les deux groupes ont 12 éléments, donc ψ est bijective. Cherchons ensuite k tel que $k \equiv 1 \pmod{4}$ et $k \equiv 2 \pmod{3}$. Parmi 1, 5, 9, seul 5 vérifie $5 \equiv 2 \pmod{3}$. **Ainsi, ψ est un isomorphisme, et l'antécédent de $(\bar{1}, \bar{2})$ est la classe de 5 modulo 12.**
5. On a $2 \wedge 6 = 2 \neq 1$. D'après la question 3, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ n'est pas cyclique. Or $\mathbb{Z}/12\mathbb{Z}$ l'est, et un isomorphisme transporte un générateur en un générateur. **Les deux groupes ne sont donc pas isomorphes, bien qu'ils aient tous deux 12 éléments.**

Corrigé de l'exercice 14 : Ordre d'un produit dans un groupe commutatif

1. Soit $z \in \langle x \rangle \cap \langle y \rangle$, d'ordre r . Le groupe $\langle x \rangle$ est commutatif de cardinal m , donc $r \mid m$ par le théorème de Lagrange. De même, $r \mid n$. Ainsi, r divise $m \wedge n = 1$, donc $r = 1$. **On obtient** $\langle x \rangle \cap \langle y \rangle = \{e\}$.
2. Comme G est commutatif, $(xy)^{mn} = (x^m)^n (y^n)^m = e$. Inversement, soit k tel que $(xy)^k = e$. Alors $x^k = y^{-k}$. Cet élément appartient à $\langle x \rangle \cap \langle y \rangle$, donc il vaut e . Ainsi, $x^k = e$ et $y^k = e$, d'où $m \mid k$ et $n \mid k$. Comme $m \wedge n = 1$, on en déduit $mn \mid k$. **L'ordre de xy est donc mn .**
3. Dans $\mathbb{Z}/4\mathbb{Z}$, prenons $x = \bar{1}$ et $y = \bar{3}$, tous deux d'ordre 4. Leur somme vaut $\bar{4} = \bar{0}$, d'ordre 1. **Ainsi, l'ordre du produit n'est pas 4×4 quand les ordres ne sont pas premiers entre eux.**

Question 4

4. La transposition τ est d'ordre 2 et le cycle c est d'ordre 3. En composant de droite à gauche, $\tau c(1) = \tau(2) = 1$, $\tau c(2) = \tau(3) = 3$ et $\tau c(3) = \tau(1) = 2$. Donc $\tau c = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, d'ordre 2 et non 6. Il n'y a pas de contradiction : on calcule de même $c\tau = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$, donc $\tau c \neq c\tau$. **L'hypothèse de commutativité est indispensable.**

Point de méthode : pour obtenir un élément d'ordre mn , on multiplie deux éléments d'ordres m et n premiers entre eux, à condition qu'ils commutent.

Corrigé de l'exercice 15 : Groupes commutatifs d'ordre premier

1. Soit $x \neq e$. D'après le théorème de Lagrange, son ordre divise p . Il vaut donc 1 ou p . Or l'ordre 1 correspond à $x = e$. **Donc x est d'ordre p .**
2. Comme $p \geq 2$, il existe $x \neq e$. Le sous-groupe $\langle x \rangle$ a p éléments, donc il est égal à G . Ainsi, G est cyclique. D'après la classification, $\bar{k} \rightarrow x^k$ est un isomorphisme. **On conclut que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.**

3. D'après la question 1, tous les éléments distincts de e sont générateurs. De plus, un sous-groupe H de G est soit $\{e\}$, soit contient un $x \neq e$. Dans le second cas, $H \supset \langle x \rangle = G$. **Il y a $p-1$ générateurs, et les seuls sous-groupes sont $\{e\}$ et G .**
4. Soit a d'ordre 2 et b d'ordre 3 dans G' . Ces éléments commutent et $2 \wedge 3 = 1$. D'après l'exercice 14, ab est d'ordre 6, égal au cardinal de G' . **Donc $G' = \langle ab \rangle$ est cyclique, isomorphe à $\mathbb{Z}/6\mathbb{Z}$.**

Corrigé de l'exercice 16 : Théorème de Lagrange dans le cas commutatif

1. Notons $\tau(y) = xy$ et $\tau'(y) = x^{-1}y$. Alors $\tau'(\tau(y)) = x^{-1}xy = y$, et de même $\tau(\tau'(y)) = y$. **Donc τ est une bijection de G sur G , de réciproque τ' .**
2. Posons $P = \prod_{y \in G} y$. Ce produit a un sens sans préciser d'ordre, car G est commutatif. Comme τ est une bijection, les éléments xy , pour y parcourant G , sont les éléments de G dans un autre ordre. Donc $\prod_{y \in G} (xy) = P$. Par commutativité, ce produit vaut aussi $x^n P$. Ainsi, $x^n P = P$, et en multipliant par P^{-1} , $x^n = e$. **D'après la caractérisation de l'ordre, l'ordre de x divise n .**
3. Les ordres possibles sont les diviseurs de $35 = 5 \times 7$, soit 1, 5, 7 et 35. Soit x tel que $x^5 \neq e$ et $x^7 \neq e$. Son ordre ne divise ni 5 ni 7, donc il n'est ni 1, ni 5, ni 7. Il vaut donc 35. **Par conséquent, $\langle x \rangle = G$ et G est cyclique.**
4. Posons $\rho(x) = x^k$. Par commutativité, $\rho(xy) = x^k y^k = \rho(x)\rho(y)$: c'est un endomorphisme. Si $\rho(x) = e$, l'ordre de x divise k et n , donc $k \wedge n = 1$, et $x = e$. Ainsi, ρ est injectif. Comme G est fini, ρ est bijectif. Pour la réciproque, écrivons $uk + vn = 1$. Alors, pour tout x , $x = x^{uk+vn} = (x^k)^u (x^n)^v = (x^k)^u$. **Donc ρ est un automorphisme, de réciproque $y \rightarrow y^u$.**

Corrigé de l'exercice 17 : Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$

- Supposons qu'un tel morphisme f existe. Alors $na = nf(\bar{1}) = f(n\bar{1}) = f(\bar{0}) = 0$. De plus, $f(\bar{k}) = f(k\bar{1}) = ka$, ce qui prouve l'unicité. Réciproquement, supposons $na = 0$ et posons $f(\bar{k}) = ka$. Si $\bar{k} = \bar{l}$, on écrit $k - l = qn$, et $ka - la = q(na) = 0$. Ainsi, f est bien définie. C'est clairement un morphisme. **Il existe donc un morphisme envoyant $\bar{1}$ sur a si et seulement si $na = 0$, et il est unique.**
- Écrivons $m = dm'$ et $n = dn'$, avec $m' \wedge n' = 1$. La condition $nu = \bar{0}$ signifie $m \mid nu$, soit $m' \mid n'u$. Par le lemme de Gauss, cela équivaut à $m' \mid u$. Dans $\llbracket 0, m-1 \rrbracket$, les multiples de m' sont $0, m', \dots, (d-1)m'$. Il y en a d . D'après la question 1, chaque tel u donne exactement un morphisme. **Il existe donc exactement $d = m \wedge n$ morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.**

Questions 3 à 4

- Pour $n = 4$ et $m = 6$, on a $d = 2$ et $m' = 3$. Les valeurs possibles de $f(\bar{1})$ sont $\bar{0}$ et $\bar{3}$. **Les morphismes sont l'application nulle et $\bar{k} \rightarrow \bar{3}k$.** On vérifie que $4 \cdot \bar{3} = \bar{12} = \bar{0}$. Pour $n = 5$ et $m = 7$, on a $d = 1$. **Seul le morphisme nul existe.**
- Avec $m = n$, les endomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les $f_u : \bar{k} \rightarrow \overline{uk}$, pour $u \in \llbracket 0, n-1 \rrbracket$. L'image de f_u est $\langle \bar{u} \rangle$. Comme le groupe est fini, f_u est bijectif si et seulement s'il est surjectif. Cela signifie que $\bar{u}$ engendre $\mathbb{Z}/n\mathbb{Z}$, soit $u \wedge n = 1$. Pour $n = 12$, on garde $u \in \{1, 5, 7, 11\}$. **Il y a 4 automorphismes de $\mathbb{Z}/12\mathbb{Z}$.**

Corrigé de l'exercice 18 : Éléments d'ordre fini du cercle unité

- Si z est d'ordre fini n , alors $z^n = 1$, donc $z \in \mathbb{U}_n$. Inversement, un élément de $\mathbb{U}_n$ vérifie $z^n = 1$ et est d'ordre fini. Ainsi, $T = \bigcup_{n \geq 1} \mathbb{U}_n$. Ensuite, $1 \in T$. Soient $z \in \mathbb{U}_a$ et $w \in \mathbb{U}_b$. Alors $(zw^{-1})^{ab} = (z^a)^b (w^b)^{-a} = 1$, par commutativité de $\mathbb{C}^*$. **Donc T est un sous-groupe de $\mathbb{U}$.**
- Si $z \in \mathbb{U}_n$, alors $z = e^{2ik\pi/n}$ pour un entier k , donc $z = e^{2i\pi r}$ avec $r = k/n \in \mathbb{Q}$. Inversement, si $r = p/q$ avec $q \geq 1$, alors $(e^{2i\pi p/q})^q = e^{2i\pi p} = 1$. **Ainsi, $T = \left\{ e^{2i\pi r}, r \in \mathbb{Q} \right\}$.**

3. Supposons que $(e^i)^k = e^{ik} = 1$ pour un entier $k \geq 1$. Alors $k \in 2\pi\mathbb{Z}$: il existe $l \in \mathbb{Z}$ tel que $k = 2\pi l$, avec $l \neq 0$. On en déduit $\pi = \frac{k}{2l} \in \mathbb{Q}$, ce qui contredit l'irrationalité de π . Donc e^i est d'ordre infini. **D'après la classification, $\langle e^i \rangle$ est monogène infini, donc isomorphe à $(\mathbb{Z}, +)$.**
4. Supposons $T = \langle z \rangle$. Comme $z \in T$, il est d'ordre fini n . Alors $T = \langle z \rangle$ a exactement n éléments. Or T contient $\cup_{n+1}$, qui en a $n+1$. C'est absurde. **Le groupe T n'est donc pas monogène.**

Corrigé de l'exercice 19 : Exposant d'un groupe commutatif fini

1. Décomposons $a = \prod_p p^{\alpha_p}$ et $b = \prod_p p^{\beta_p}$ en facteurs premiers. Posons

$$a' = \prod_{\alpha_p \geq \beta_p} p^{\alpha_p}, \quad b' = \prod_{\alpha_p < \beta_p} p^{\beta_p}.$$

Alors $a' \mid a$ et $b' \mid b$. Ces entiers n'ont aucun facteur premier commun. De plus,

$a' b' = \prod_p p^{\max(\alpha_p, \beta_p)} = a \vee b$. Pour $a = 12 = 2^2 \times 3$ et $b = 18 = 2 \times 3^2$, on trouve $a' = 4$ et $b' = 9$. **On a bien $4 \wedge 9 = 1$ et $4 \times 9 = 36 = 12 \vee 18$.**

2. D'après l'exercice 7, l'élément $x^{a/a'}$ est d'ordre $\frac{a}{a \wedge (a/a')} = \frac{a}{a'} = a'$. De même, $y^{b/b'}$ est d'ordre b' . Ces deux éléments commutent et leurs ordres sont premiers entre eux. Par l'exercice 14, leur produit est d'ordre $a' b'$. **Ainsi, $x^{a/a'} y^{b/b'}$ est d'ordre $a \vee b$.**

3. Les ordres sont bornés par le cardinal de G , donc un ordre maximal M existe. Soit y d'ordre b . Par la question 2, il existe un élément d'ordre $M \vee b$. Or $M \vee b \geq M$, donc par maximalité $M \vee b = M$. **Par conséquent, b divise M .**

Questions 4 à 5

4. Dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, l'ordre d'un couple divise $4 \vee 6 = 12$ (exercice 12). De plus, $(\bar{1}, \bar{1})$ est d'ordre 12. **L'exposant vaut 12, atteint par $(\bar{1}, \bar{1})$.**

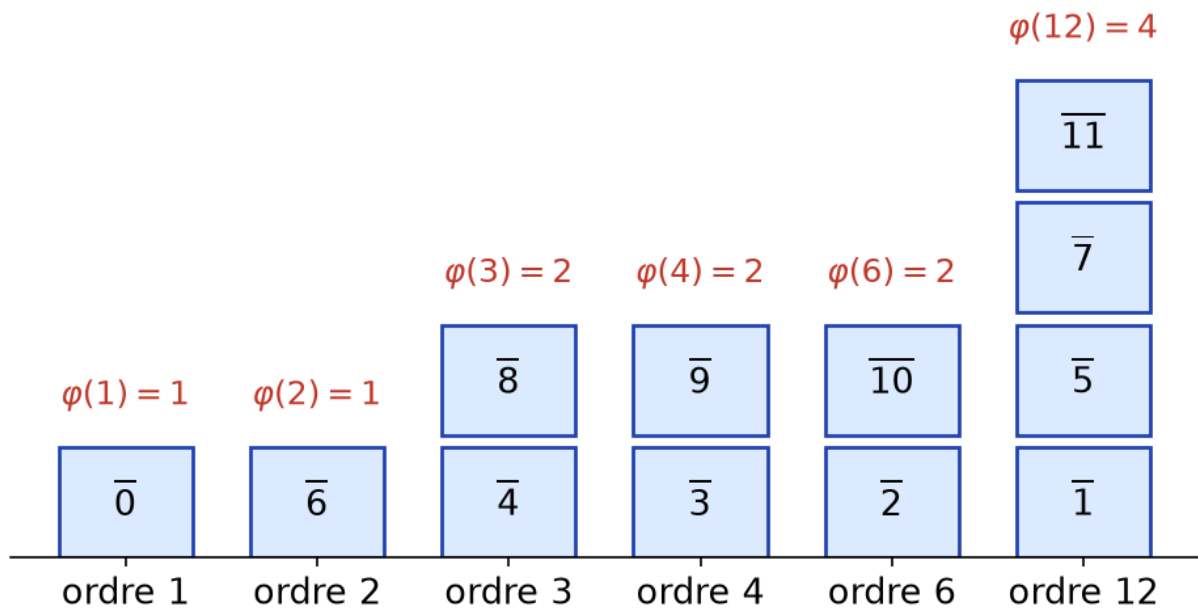
5. Notons n le cardinal de G . Si G est cyclique, un générateur est d'ordre n . Tout ordre divisant n , l'exposant vaut n . Réciproquement, si l'exposant vaut n , il existe un élément z d'ordre n , et $\langle z \rangle = G$. **Donc G est cyclique si et seulement si son exposant égale son cardinal.**

Corrigé de l'exercice 20 : Problème : caractérisation des groupes cycliques

Partie A

- Si p est premier, tous les entiers de 1 à $p-1$ sont premiers avec p , et p ne l'est pas. Donc $\varphi(p) = p-1$. Ensuite, un entier est premier avec p^α si et seulement s'il n'est pas multiple de p . Or $[1, p^\alpha]$ contient $p^\alpha - 1$ multiples de p . **Ainsi, $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.**
- Un élément d'ordre d engendre un sous-groupe d'ordre d . D'après l'exercice 11, ce sous-groupe est l'unique sous-groupe H_d d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Ainsi, les éléments d'ordre d sont exactement les générateurs de H_d . Or H_d est cyclique d'ordre d , donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Un isomorphisme conservant les générateurs, $\mathbb{Z}/n\mathbb{Z}$ **contient exactement $\varphi(d)$ éléments d'ordre d .**
- Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ a un ordre qui divise n , par le théorème de Lagrange. En regroupant les n éléments selon leur ordre, on obtient une partition. **Par la question 2, on en déduit $\sum_{d|n} \varphi(d) = n$.** Pour $n = 12$, on a $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$. La figure ci-dessous montre cette partition de $\mathbb{Z}/12\mathbb{Z}$ selon l'ordre.

$$1 + 1 + 2 + 2 + 2 + 4 = 12$$



Partie B

- Le sous-groupe $\langle x \rangle = \{e, x, \dots, x^{d-1}\}$ compte d éléments. Chacun vérifie $(x^k)^d = (x^d)^k = e$. On dispose donc de d solutions de $y^d = e$. Comme il y en a au plus d , ce sont toutes les solutions. Ensuite, un élément d'ordre d vérifie $y^d = e$, donc il appartient à $\langle x \rangle$. Or $\langle x \rangle$ est cyclique d'ordre d : ses éléments d'ordre d sont ses générateurs, au nombre de $\varphi(d)$. **Ainsi, $N(d) \geq 1$ entraîne $N(d) = \varphi(d)$.**

- Le groupe G est commutatif de cardinal n . Par le théorème de Lagrange, chaque ordre divise n . En classant les éléments selon leur ordre, on obtient $\sum_{d|n} N(d) = n$. D'après la question précédente, $N(d) \leq \varphi(d)$ pour tout d , que $N(d)$ soit nul ou non. Par la partie A,

$$\sum_{d|n} (\varphi(d) - N(d)) = n - n = 0.$$

C'est une somme de termes positifs ou nuls. **Chacun est donc nul : $N(d) = \varphi(d)$ pour tout diviseur d de n .**

- En particulier, $N(n) = \varphi(n) \geq 1$, car 1 est premier avec n . Il existe donc un élément d'ordre n , qui engendre G . **Le groupe G est cyclique.**

Partie C

1. Le groupe G est commutatif, comme sous-groupe de $\mathbb{C}^*$. Pour tout $d \mid n$, les solutions de $z^d = 1$ sont des racines du polynôme $X^d - 1$, de degré d . Il y en a donc au plus d . La partie B s'applique : G est cyclique. Par ailleurs, le théorème de Lagrange donne $z^n = 1$ pour tout $z \in G$, soit $G \subset \mathbb{U}_n$. Les deux ensembles ont n éléments. **Donc $G = \mathbb{U}_n$, qui est bien cyclique.**
2. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de cardinal 4, et $2 \mid 4$. Or ses quatre éléments vérifient $2 \cdot (a, b) = (\bar{0}, \bar{0})$. L'équation associée à $d = 2$ a donc 4 solutions, soit plus que 2. **L'hypothèse de la partie B n'est pas satisfaite, ce qui est cohérent avec le fait que ce groupe n'est pas cyclique.**

Point de méthode : le critère de la partie B est l'outil standard pour montrer qu'un sous-groupe fini d'un groupe multiplicatif d'un corps commutatif est cyclique.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en maths spé

- Le cours : [groupes, cours de maths spé](#)
- Les énoncés : [exercices de maths spé sur groupes](#)
- Chapitre suivant : [Anneaux, idéaux, \$\mathbb{Z}/n\mathbb{Z}\$ et algèbres](#)
- Le même thème en L2 : [groupes, exercices de maths en L2](#)
- Tester vos connaissances : [QCM de maths spé par chapitre](#)
- Le sommaire : [tous les chapitres de maths spé](#) et les [chapitres de maths sup](#)