

Groupes

Exercice 1 : Sous-groupes engendrés dans $\mathbb{Z}$

On travaille dans le groupe $(\mathbb{Z}, +)$. Pour chaque partie, on demande un entier $n \geq 0$ tel que le sous-groupe engendré soit $n\mathbb{Z}$.

1. Déterminer $\langle 12, 18 \rangle$.
2. Déterminer $\langle -8, 20 \rangle$.
3. Déterminer $\langle 15, 21, 35 \rangle$, puis écrire 1 sous la forme $15a + 21b + 35c$ avec a, b, c entiers.
4. Montrer que $\{6, 10, 15\}$ est une partie génératrice de $\mathbb{Z}$, mais qu'aucune de ses parties à deux éléments ne l'est.

Exercice 2 : Somme et intersection de sous-groupes de $\mathbb{Z}$

Soient a et b deux entiers strictement positifs, $d = a \wedge b$ et $m = a \vee b$.

1. Montrer que $a\mathbb{Z} + b\mathbb{Z} = \{au + bv, (u, v) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{Z}$, puis que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
2. Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
3. Expliciter $12\mathbb{Z} + 18\mathbb{Z}$ et $12\mathbb{Z} \cap 18\mathbb{Z}$.

- Montrer que $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$, puis déterminer le sous-groupe qu'il engendre.

Exercice 3 : Ordres des éléments de $\mathbb{Z}/12\mathbb{Z}$

- Déterminer l'ordre de chacun des douze éléments de $\mathbb{Z}/12\mathbb{Z}$.
- Pour chaque entier d , compter les éléments d'ordre d . Vérifier que le total vaut 12.
- Vérifier que chaque ordre divise 12. Quels sont les générateurs de $\mathbb{Z}/12\mathbb{Z}$?

Exercice 4 : Générateurs de $\mathbb{Z}/n\mathbb{Z}$

- Rappeler une condition nécessaire et suffisante sur k pour que $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$.
- Lister les générateurs de $\mathbb{Z}/15\mathbb{Z}$, puis ceux de $\mathbb{Z}/18\mathbb{Z}$.
- Dans $\mathbb{Z}/15\mathbb{Z}$, trouver un entier $u \in \llbracket 0, 14 \rrbracket$ tel que $u \cdot \bar{7} = \bar{1}$.
- Montrer que pour $n \geq 3$, le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ est pair.

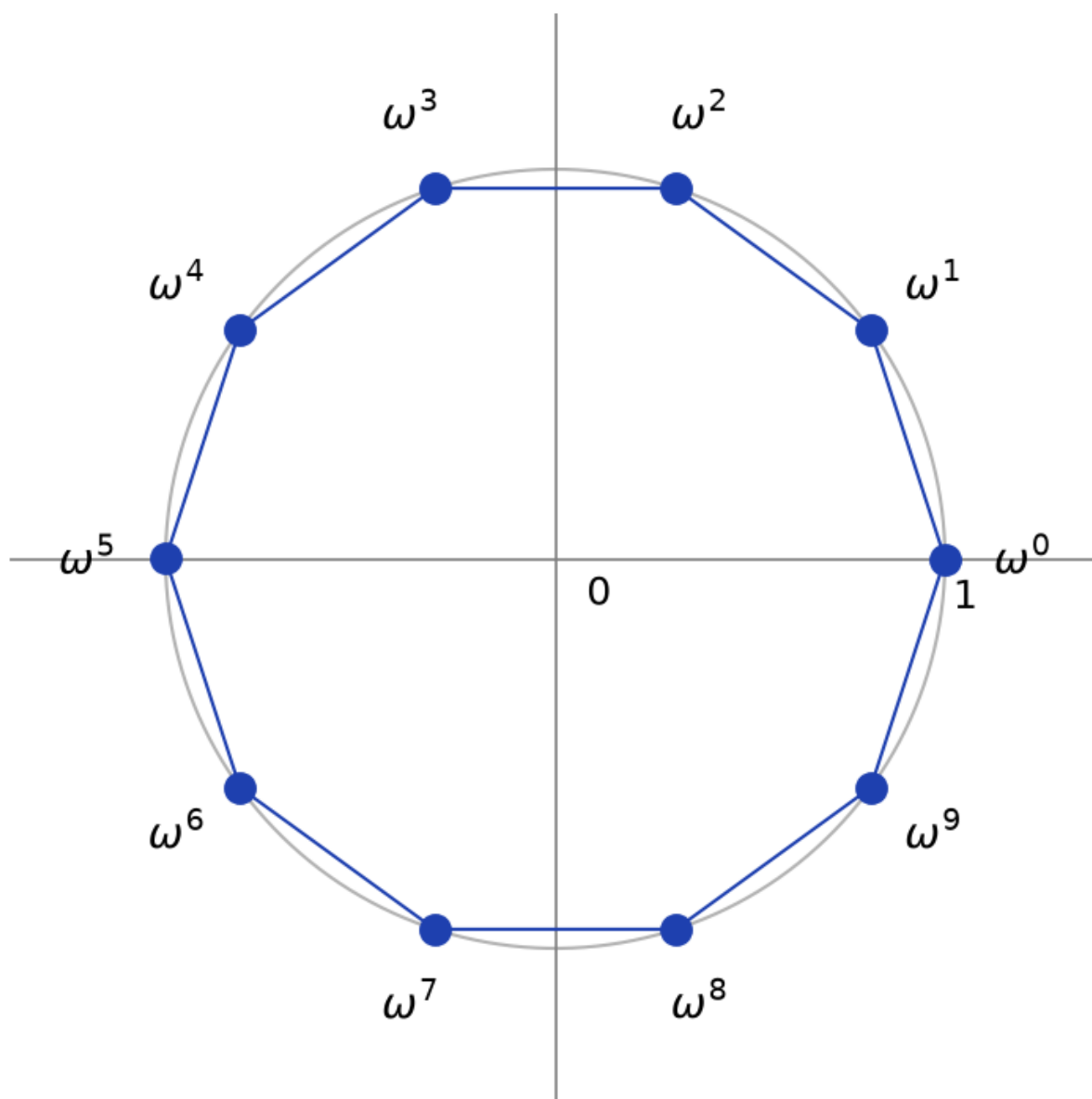
Exercice 5 : Ordre d'une matrice et d'une permutation

- Soit $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Calculer A^2 et A^3 . En déduire l'ordre de A dans $\text{GL}_2(\mathbb{R})$.
- Déterminer l'ordre de la matrice de rotation $R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ pour $\theta = \frac{5\pi}{6}$.

3. Dans le groupe symétrique S_5 , on considère $\sigma = (1, 2, 3)(4, 5)$. Calculer σ^2 et σ^3 , puis déterminer l'ordre de σ .
4. La matrice $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est-elle d'ordre fini ?

Exercice 6 : Racines dixièmes de l'unité

On pose $\omega = e^{2i\pi/10}$. La figure ci-dessous représente les dix éléments de $\mathbb{U}_{10}$.



1. Donner l'ordre de ω^k pour chaque $k \in \llbracket 0, 9 \rrbracket$.
2. Lister les racines primitives dixièmes de l'unité et calculer leur somme.
3. Soient $m, n \geq 1$. Montrer que $\mathbb{U}_n \subset \mathbb{U}_m$ si et seulement si n divise m .
4. Montrer que $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m \wedge n}$. Expliciter $\mathbb{U}_{10} \cap \mathbb{U}_4$.

Exercice 7 : Ordre d'une puissance

Soit G un groupe et $x \in G$ d'ordre fini n .

1. Soit $k \in \mathbb{Z}$. Montrer que x^k est d'ordre $\frac{n}{n \wedge k}$.
2. En déduire que x^k engendre $\langle x \rangle$ si et seulement si $k \wedge n = 1$.
3. On suppose $n = 20$. Déterminer les ordres de x^6 , x^{15} et x^{-8} .
4. Montrer que x et x^{-1} ont le même ordre. Plus généralement, montrer qu'un élément et son image par un isomorphisme de groupes ont le même ordre.

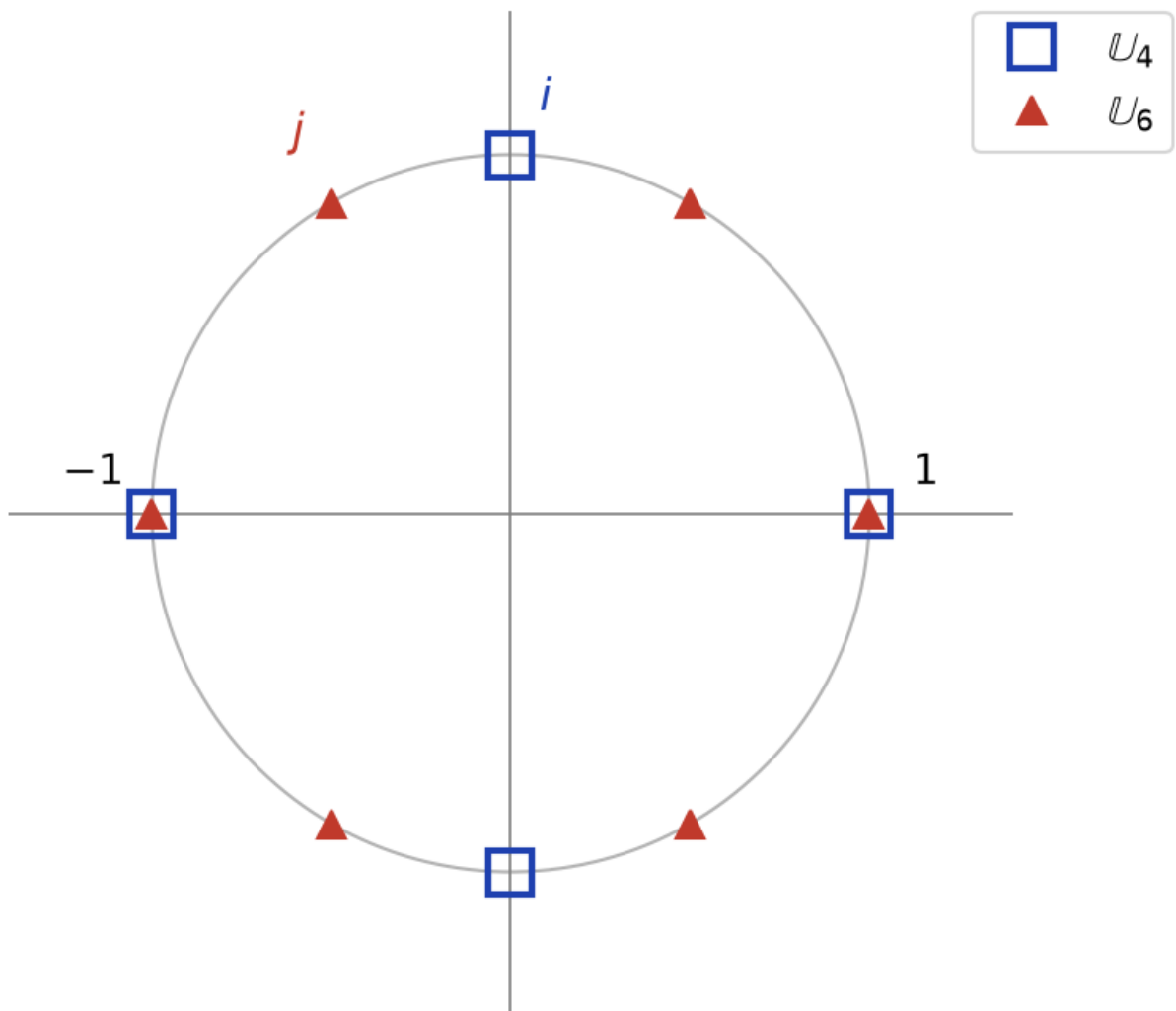
Exercice 8 : Un isomorphisme explicite entre $\mathbb{Z}/n\mathbb{Z}$ et les racines de l'unité

Soit $n \geq 1$ et $\omega = e^{2i\pi/n}$.

1. Montrer que $f : k \rightarrow \omega^k$ est un morphisme surjectif de $(\mathbb{Z}, +)$ sur $(\mathbb{U}_n, \times)$, et déterminer son noyau.
2. Montrer que $g : \bar{k} \rightarrow \omega^k$ est bien définie sur $\mathbb{Z}/n\mathbb{Z}$, et que c'est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur $(\mathbb{U}_n, \times)$.
3. On prend $n = 6$. Déterminer l'antécédent de -1 par g , puis les générateurs de $\mathbb{U}_6$.

Exercice 9 : Sous-groupe engendré par i et j

On note $j = e^{2i\pi/3}$. La figure montre les groupes $\mathbb{U}_4$ et $\mathbb{U}_6$ sur le cercle unité.



1. Vérifier que i et j appartiennent à $\mathbb{U}_{12}$.
2. Calculer ij sous forme exponentielle et déterminer son ordre.
3. En déduire que le sous-groupe de $(\mathbb{C}^*, \times)$ engendré par $\{i, j\}$ est $\mathbb{U}_{12}$.
4. Plus généralement, soient $m, n \geq 1$ et $l = m \vee n$. Montrer que le sous-groupe engendré par $\mathbb{U}_m \cup \mathbb{U}_n$ est $\mathbb{U}_l$.

Exercice 10 : Le groupe $(\mathbb{Q}, +)$ n'est pas monogène

1. Déterminer le sous-groupe de $(\mathbb{Q}, +)$ engendré par $\frac{1}{2}$ et $\frac{1}{3}$.

2. Soient $r_1 = \frac{p_1}{q_1}, \dots, r_s = \frac{p_s}{q_s}$ des rationnels, avec $q_j \geq 1$. On pose $q = q_1 \cdots q_s$.
Montrer que $\langle r_1, \dots, r_s \rangle \subset \frac{1}{q}\mathbb{Z}$, puis que ce sous-groupe est monogène.
3. Montrer par l'absurde que $(\mathbb{Q}, +)$ n'est pas monogène.
4. En déduire que $(\mathbb{Q}, +)$ n'admet aucune partie génératrice finie.

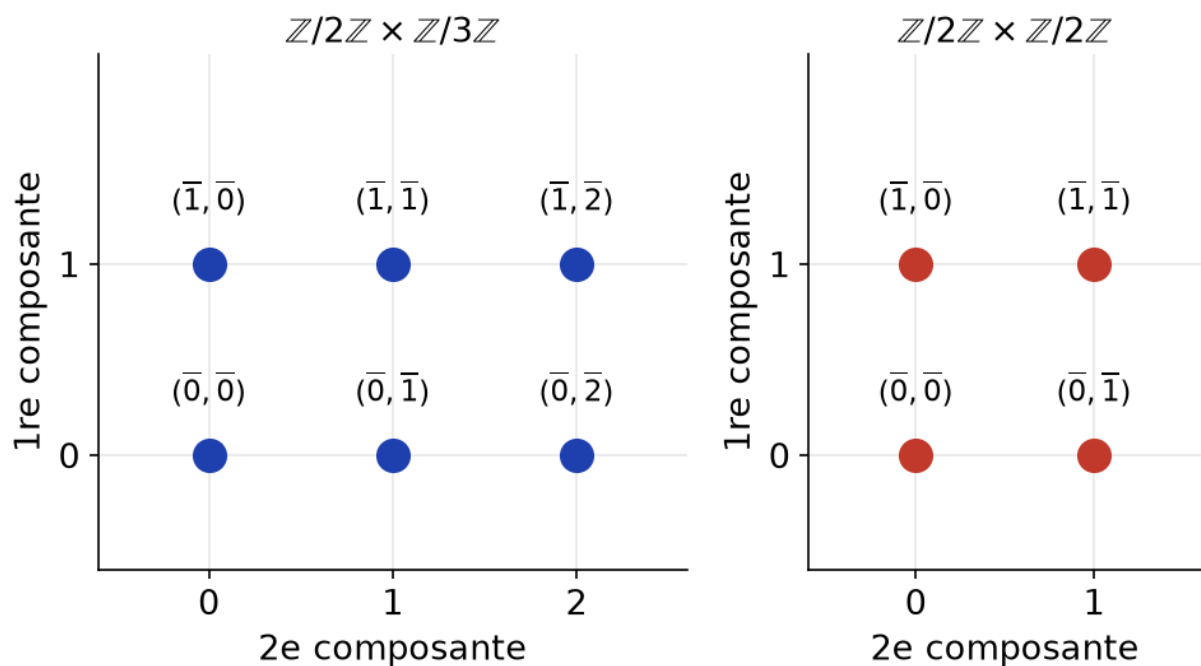
Exercice 11 : Sous-groupes d'un groupe cyclique

Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n .

1. Soit H un sous-groupe de G . En considérant $K = \left\{ \begin{matrix} k \\ \mathbb{Z} \\ g^k \end{matrix} \right\}$, montrer que
 $H = \langle g^a \rangle$ pour un diviseur a de n .
2. Montrer que pour tout diviseur d de n , G possède un unique sous-groupe d'ordre d .
3. Lister les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ avec leurs éléments.
4. Combien $\mathbb{Z}/100\mathbb{Z}$ possède-t-il de sous-groupes ? Donner celui d'ordre 20.

Exercice 12 : Produits de petits groupes cycliques

Si G et H sont deux groupes, $G \times H$ est muni de la loi produit composante par composante. La figure représente les éléments de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.



1. Soient $x \in G$ d'ordre a et $y \in H$ d'ordre b . Montrer que (x, y) est d'ordre $a \vee b$.
2. Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique, et donner un isomorphisme explicite avec $\mathbb{Z}/6\mathbb{Z}$.
3. Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique. Est-il isomorphe à $\mathbb{U}_4$?
4. Quel est le plus grand ordre d'un élément de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$? Ce groupe est-il cyclique ?

Exercice 13 : Quand le produit de deux groupes cycliques est-il cyclique ?

Soient $m, n \geq 1$ et $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Pour éviter les confusions, on note $\bar{k}$ la classe de k modulo m et $\bar{k}$ sa classe modulo n .

1. On suppose $m \wedge n = 1$. Montrer que $(\bar{1}, \bar{1})$ est d'ordre mn . En déduire que G est cyclique.
2. On suppose $d = m \wedge n \geq 2$. Montrer que tout élément de G vérifie $l \cdot (\bar{a}, \bar{b}) = (\bar{0}, \bar{0})$ avec $l = m \vee n$. En déduire que G n'est pas cyclique.
3. Conclure : G est cyclique si et seulement si $m \wedge n = 1$.

- On prend $m = 4$ et $n = 3$. Montrer que $\psi : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, qui envoie la classe de k modulo 12 sur $(\bar{k}, \bar{k})$, est un isomorphisme. Trouver l'antécédent de $(\bar{1}, \bar{2})$.
- Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ est-il isomorphe à $\mathbb{Z}/12\mathbb{Z}$?

Exercice 14 : Ordre d'un produit dans un groupe commutatif

Soit G un groupe commutatif, x d'ordre m et y d'ordre n , avec $m \wedge n = 1$.

- Montrer que $\langle x \rangle \cap \langle y \rangle = \{e\}$.
- Montrer que xy est d'ordre mn .
- Montrer par un exemple que la conclusion tombe si $m \wedge n \neq 1$.
- Dans S_3 , on pose $\tau = \begin{pmatrix} 1 & c \\ & 2 \end{pmatrix}$ et $c = \begin{pmatrix} 1 & 2 \\ & 3 \end{pmatrix}$. Donner leurs ordres et calculer τc . Pourquoi cela ne contredit-il pas la question 2 ?

Exercice 15 : Groupes commutatifs d'ordre premier

Soit p un nombre premier et G un groupe commutatif de cardinal p .

- Montrer que tout élément $x \neq e$ de G est d'ordre p .
- En déduire que G est cyclique et isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Combien G possède-t-il de générateurs ? Quels sont ses sous-groupes ?
- Soit G' un groupe commutatif de cardinal 6. Montrer que si G' contient un élément d'ordre 2 et un élément d'ordre 3, alors il est cyclique.

Exercice 16 : Théorème de Lagrange dans le cas commutatif

Soit G un groupe commutatif fini de cardinal n .

1. Soit $x \in G$. Montrer que $y \rightarrow xy$ est une bijection de G sur lui-même.
2. En comparant $\prod_{y \in G} (xy)$ et $\prod_{y \in G} y$, montrer que $x^n = e$. En déduire que l'ordre de x divise n .
3. On suppose $n = 35$. Quels sont les ordres possibles des éléments ? Montrer que G est cyclique dès qu'il contient un élément x tel que $x^5 \neq e$ et $x^7 \neq e$.
4. Soit k un entier premier avec n . Montrer que $x \rightarrow x^k$ est un automorphisme de G , et exprimer sa réciproque à l'aide d'une relation de Bézout.

Exercice 17 : Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$

Soient $m, n \geq 1$ et $d = m \wedge n$. On note $\bar{k}$ la classe de k modulo n et $\dot{k}$ sa classe modulo m .

1. Soit $(G, +)$ un groupe commutatif et $a \in G$. Montrer qu'il existe un morphisme $f: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ tel que $f(\bar{1}) = a$ si et seulement si $na = 0$. Montrer qu'il est alors unique.
2. Déterminer les $u \in \llbracket 0, m-1 \rrbracket$ tels que $n\dot{u} = \dot{0}$. En déduire qu'il existe exactement d morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.
3. Expliciter les morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$, puis ceux de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$.
4. Montrer que les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k} \rightarrow \overline{uk}$ avec $u \wedge n = 1$. Combien y en a-t-il pour $n = 12$?

Exercice 18 : Éléments d'ordre fini du cercle unité

On note $\mathbb{U}$ le groupe des complexes de module 1 et T l'ensemble de ses éléments d'ordre fini.

1. Montrer que $T = \bigcup_{n \geq 1} \mathbb{U}_n$ et que T est un sous-groupe de $\mathbb{U}$.
2. Montrer que $T = \left\{ e^{2\pi i r}, r \in \mathbb{Q} \right\}$.
3. Montrer que $e^{2\pi i}$ est d'ordre infini. Quel groupe classique reconnaît-on dans $\langle e^{2\pi i} \rangle$?
4. Montrer que T n'est pas monogène.

Exercice 19 : Exposant d'un groupe commutatif fini

Soit G un groupe commutatif fini. On pourra utiliser les résultats des exercices 7 et 14.

1. Soient $a, b \geq 1$. Montrer qu'il existe $a' \mid a$ et $b' \mid b$ premiers entre eux tels que $a'b' = a \vee b$. Illustrer avec $a = 12$ et $b = 18$.
2. Soient x d'ordre a et y d'ordre b dans G . Montrer que G contient un élément d'ordre $a \vee b$.
3. Soit z un élément d'ordre maximal M . Montrer que l'ordre de tout élément de G divise M . L'entier M s'appelle l'exposant de G .
4. Calculer l'exposant de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et en donner un élément d'ordre maximal.
5. Montrer que G est cyclique si et seulement si son exposant est égal à son cardinal.

Exercice 20 : Problème : caractérisation des groupes cycliques

Pour $d \geq 1$, on note $\varphi(d)$ le nombre d'entiers $k \in \llbracket 1, d \rrbracket$ premiers avec d . C'est aussi le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$.

Partie A : une formule de sommation.

1. Calculer $\varphi(p)$ pour p premier, puis $\varphi(p^\alpha)$ pour $\alpha \geq 1$.
2. Soit $n \geq 1$ et d un diviseur de n . Montrer que $\mathbb{Z}/n\mathbb{Z}$ contient exactement $\varphi(d)$ éléments d'ordre d .
3. En déduire que $\sum_{d|n} \varphi(d) = n$. Vérifier cette formule pour $n = 12$.

Partie B : un critère de cyclicité. Soit G un groupe commutatif de cardinal n . On suppose que, pour tout diviseur d de n , l'équation $x^d = e$ a au plus d solutions dans G . On note $N(d)$ le nombre d'éléments d'ordre d .

1. Soit $d|n$ tel que $N(d) \geq 1$, et x d'ordre d . Montrer que les solutions de $y^d = e$ sont exactement les éléments de $\langle x \rangle$. En déduire que $N(d) = \varphi(d)$.
2. Montrer que $\sum_{d|n} N(d) = n$, puis que $N(d) = \varphi(d)$ pour tout $d|n$.
3. Conclure que G est cyclique.

Partie C : applications.

1. Soit G un sous-groupe fini de $(\mathbb{C}^*, \times)$, de cardinal n . Montrer que G est cyclique, puis que $G = \mathbb{U}_n$.

2. Vérifier que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne satisfait pas l'hypothèse de la partie B.

Le corrigé des exercices

Chaque exercice est corrigé en détail, question par question, sur la page suivante.



Pour aller plus loin en maths spé

- Le cours : [groupes, cours de maths spé](#)
- 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](#)