

Corrigé du contrôle de maths spé : groupes monogènes, ordre d'un élément et $\mathbb{Z}/n\mathbb{Z}$

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours	5 points
Exercice 2 : Générateurs de $\mathbb{Z}/12\mathbb{Z}$ et racines de l'unité	4 points
Exercice 3 : Ordre d'un produit	4 points
Exercice 4 : Sous-groupes de $(\mathbb{Z}, +)$	3 points
Exercice 5 : Groupes commutatifs finis et ordre premier	4 points
Total	20 points

Exercice 1 : Question de cours (5 points)

- a. Soit $\varphi: \mathbb{Z} \rightarrow G$, $k \rightarrow a^k$. Pour tous entiers k et l , on a $a^{k+l} = a^k a^l$, donc φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans G . Son image est $\{a^k: k \in \mathbb{Z}\} = \langle a \rangle = G$, donc φ est surjectif.

Le noyau $\ker \varphi$ est un sous-groupe de $(\mathbb{Z}, +)$, donc il existe $n \in \mathbb{N}$ tel que $\ker \varphi = n\mathbb{Z}$.

Cas $n = 0$. Le noyau est réduit à $\{0\}$, donc φ est injectif. C'est alors un isomorphisme de $\mathbb{Z}$ sur G , et G est infini.

Cas $n \geq 1$. Pour $k \in \mathbb{Z}$, la division euclidienne donne $k = qn + r$ avec $0 \leq r \leq n-1$. Comme $a^n = e$, on obtient $a^k = (a^n)^q a^r = a^r$. Ainsi $G = \{e, a, a^2, \dots, a^{n-1}\}$ est fini.

Par contraposée, si G est infini, on est dans le premier cas : G est isomorphe à $(\mathbb{Z}, +)$.

Si G est fini, φ ne peut pas être injectif ($\mathbb{Z}$ est infini), donc $n \geq 1$. Définissons $\psi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ par $\psi(\bar{k}) = a^k$. Elle est bien définie : si $\bar{k} = \bar{l}$, alors $k - l \in n\mathbb{Z} = \ker \varphi$, donc $a^k = a^l$. C'est un morphisme, car $\psi(\bar{k} + \bar{l}) = a^{k+l} = \psi(\bar{k})\psi(\bar{l})$. Elle est surjective, comme φ . Enfin, $\psi(\bar{k}) = e$ signifie $k \in n\mathbb{Z}$, soit $\bar{k} = \bar{0}$: ψ est injective. Par conséquent ψ est un isomorphisme, et G a n éléments. **Un groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.**

- b. L'application $\varphi_x: k \rightarrow x^k$ est un morphisme de $(\mathbb{Z}, +)$ dans G . Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$.

Par définition, d est le plus petit entier $k \geq 1$ tel que $x^k = e$; il existe, donc le noyau n'est pas réduit à $\{0\}$ et $m \geq 1$. Or le plus petit élément strictement positif de $m\mathbb{Z}$ est m . Ainsi $m = d$, et $\ker \varphi_x = d\mathbb{Z}$.

En conclusion, $x^n = e \Leftrightarrow n \in \ker \varphi_x = d\mathbb{Z} \Leftrightarrow d$ divise n .

Barème : a) 3 points : 0,5 pour le morphisme surjectif, 0,5 pour la forme du noyau, 0,5 pour le cas infini, 0,5 pour la finitude quand $n \geq 1$, 1 pour l'isomorphisme ψ bien défini, injectif et surjectif ; b) 2 points : 1 pour le noyau $m\mathbb{Z}$, 1 pour l'identification $m = d$.

Exercice 2 : Générateurs de $\mathbb{Z}/12\mathbb{Z}$ et racines de l'unité (4 points)

- a. Le sous-groupe engendré par $\bar{k}$ est $\{u\bar{k} : u \in \mathbb{Z}\}$. Comme $\bar{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$, on a : $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\bar{1} \in \langle \bar{k} \rangle$.

Cela équivaut à l'existence de $u \in \mathbb{Z}$ tel que $uk \equiv 1 \pmod{n}$, donc à l'existence d'entiers u et v tels que $uk + vn = 1$. D'après le théorème de Bézout, $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

- b. Les entiers de $\{0, \dots, 11\}$ premiers avec 12 sont 1, 5, 7 et 11. **Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{1}$, $\bar{5}$, $\bar{7}$ et $\bar{11}$.**

L'ordre de $\bar{8}$ est le plus petit $m \geq 1$ tel que 12 divise $8m$, soit 3 divise $2m$, c'est-à-dire 3 divise m : **$\bar{8}$ est d'ordre 3** ($3 \times 8 = 24$). De même, 12 divise $9m$ équivaut à 4 divise $3m$, soit 4 divise m : **$\bar{9}$ est d'ordre 4** ($4 \times 9 = 36$). On retrouve la formule $\frac{12}{k \wedge 12}$.

- c. Posons $\omega = e^{2i\pi/n}$. On sait que $\mathbb{U}_n = \{\omega^k : 0 \leq k \leq n-1\}$, donc $\mathbb{U}_n = \langle \omega \rangle$ est monogène, fini de cardinal n : il est cyclique. D'après l'exercice 1, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, par l'isomorphisme $\psi : \bar{k} \rightarrow \omega^k$.

Un isomorphisme envoie les générateurs sur les générateurs. Ainsi les générateurs de $\mathbb{U}_n$ sont les $e^{2ik\pi/n}$ avec $k \wedge n = 1$. Pour $n = 12$, on prend $k \in \{1, 5, 7, 11\}$: **les générateurs de $\mathbb{U}_{12}$ sont $e^{i\pi/6}$, $e^{5i\pi/6}$, $e^{7i\pi/6}$ et $e^{11i\pi/6}$.**

Barème : a) 1,5 point : 0,5 pour la traduction $\bar{1} \in \langle \bar{k} \rangle$, 1 pour l'équivalence avec Bézout ; b) 1 point : 0,5 pour les générateurs, 0,5 pour les deux ordres ; c) 1,5 point : 0,5 pour le caractère cyclique, 0,5 pour l'isomorphisme, 0,5 pour la liste.

Exercice 3 : Ordre d'un produit (4 points)

- a. Comme x et y commutent, $(xy)^{ab} = x^ab y^ab = (x^a)^b (y^b)^a = e$. **Donc $(xy)^{ab} = e$.**
- b. Soit $z \in \langle x \rangle \cap \langle y \rangle$. Il existe k tel que $z = x^k$, donc $z^a = (x^a)^k = e$. De même, $z^b = e$. D'après l'exercice 1 b), l'ordre δ de z divise a et b . Il divise donc $a \wedge b = 1$, d'où $\delta = 1$ et $z = e$. **Ainsi $\langle x \rangle \cap \langle y \rangle = \{e\}$.**
- c. Notons m l'ordre de xy , fini d'après a). Comme x et y commutent, $(xy)^m = e$ s'écrit $x^m = y^{-m}$. Cet élément appartient à $\langle x \rangle \cap \langle y \rangle$, donc il vaut e d'après b).

Ainsi $x^m = e$ et $y^m = e$, donc a divise m et b divise m . Comme $a \wedge b = 1$, le produit ab divise m . Par ailleurs m divise ab d'après a) et l'exercice 1 b). **L'ordre de xy est donc ab .**

- d. Dans $\mathbb{C}^*$, commutatif, i est d'ordre 4 et $e^{2i\pi/3}$ est d'ordre 3. Comme $4 \wedge 3 = 1$, $i e^{2i\pi/3}$ est d'ordre 12. En effet, $i e^{2i\pi/3} = e^{7i\pi/6} = e^{2i\pi \times 7/12}$, avec $7 \wedge 12 = 1$.

Barème : a) 0,5 point ; b) 1,5 point : 0,5 pour $z^a = z^b = e$, 1 pour la conclusion par le PGCD ; c) 1,5 point : 0,5 pour $x^m = y^{-m}$, 0,5 pour ab divise m , 0,5 pour la conclusion ; d) 0,5 point.

Erreur fréquente : sans l'hypothèse $a \wedge b = 1$, le résultat est faux : x et x^{-1} ont le même ordre, mais leur produit vaut e .

Exercice 4 : Sous-groupes de $(\mathbb{Z}, +)$ (3 points)

- a. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un entier non nul h , ainsi que son opposé : $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément n .

Comme H est un sous-groupe contenant n , il contient $n\mathbb{Z}$. Réciproquement, soit $h \in H$; écrivons $h = qn + r$ avec $0 \leq r < n$. Alors $r = h - qn \in H$. Par minimalité de n , on a $r = 0$, donc $h \in n\mathbb{Z}$. Ainsi $H = n\mathbb{Z}$.

- b. L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ contient 0 ; il est stable par somme et par passage à l'opposé, car $(au + bv) - (au' + bv') = a(u - u') + b(v - v')$. C'est donc un sous-groupe de $\mathbb{Z}$, égal à $d\mathbb{Z}$ avec $d \in \mathbb{N}$, et $d \neq 0$ car a ou b est non nul.

D'abord, a et b sont dans $d\mathbb{Z}$, donc d est un diviseur commun de a et b . Ensuite, d s'écrit $au + bv$: tout diviseur commun de a et b divise donc d . Ainsi $d = a \wedge b$. Comme $12 \wedge 18 = 6$, $12\mathbb{Z} + 18\mathbb{Z} = 6\mathbb{Z}$.

- c. Un entier appartient à $12\mathbb{Z} \cap 18\mathbb{Z}$ si et seulement si c'est un multiple commun de 12 et 18, donc un multiple de leur PPCM, qui vaut $\frac{12 \times 18}{6} = 36$. Donc $m = 36$.

Barème : a) 1,5 point : 0,5 pour l'existence du minimum, 1 pour la division euclidienne ; b) 1 point : 0,5 pour la structure de sous-groupe, 0,5 pour $d = a \wedge b$ et l'application ; c) 0,5 point.

Exercice 5 : Groupes commutatifs finis et ordre premier (4 points)

- a. L'application $g \rightarrow x^{-1}g$ vérifie $x^{-1}(xg) = g$ et $x(x^{-1}g) = g$. C'est donc une réciproque de τ_x . **Ainsi τ_x est une bijection de G sur G .**
- b. Comme τ_x est une bijection de G et que G est commutatif, le produit des xg est le produit de tous les éléments de G dans un autre ordre :

$$\prod_{g \in G} (xg) = \prod_{h \in G} h = P.$$

D'autre part, la commutativité permet de regrouper les n facteurs x :

$$\prod_{g \in G} (xg) = x^n \prod_{g \in G} g = x^n P.$$

Donc $x^n P = P$. En multipliant par P^{-1} , on obtient $x^n = e$.

- c. Soit $x \in G$, d'ordre d . D'après b), $x^n = e$, donc, par l'exercice 1 b), d **divise** $n = \text{card } G$.
- d. Soit $x \neq e$ dans G . Son ordre d divise p et $d \neq 1$, donc $d = p$. Alors $\langle x \rangle$ contient les p éléments distincts $e, x, \dots, x^{p-1}$: c'est G tout entier. Ainsi G est monogène fini. **G est cyclique, engendré par tout $x \neq e$, et isomorphe à $\mathbb{Z}/p\mathbb{Z}$** d'après l'exercice 1 a).
- e. Soit x d'ordre 2 et y d'ordre 3. Ils commutent et $2 \wedge 3 = 1$, donc xy est d'ordre 6 d'après l'exercice 3. Alors $\langle xy \rangle$ a 6 éléments : c'est G . **Le groupe est cyclique, isomorphe à $\mathbb{Z}/6\mathbb{Z}$.**

Barème : a) 0,5 point ; b) 1,5 point : 0,5 pour le changement d'indice par la bijection, 0,5 pour le regroupement des x , 0,5 pour la simplification par P ; c) 0,5 point ; d) 1 point : 0,5 pour l'ordre p , 0,5 pour la conclusion ; e) 0,5 point.

Erreur fréquente : citer le théorème de Lagrange général pour la question c) alors que l'énoncé demande de le déduire de b). Il faut utiliser le résultat démontré.

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : groupes monogènes, ordre d'un élément et $\mathbb{Z}/n\mathbb{Z}$

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Groupes](#) » en maths spé puis entraînez-vous avec les **exercices corrigés groupes**.

Retrouvez tous les [contrôles de maths spé classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).