Plaquette 1 – Groupes, sous-groupes, morphismes, anneaux et corps

Structures algébriques — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Groupes.

— $(G, *)$ est un **groupe** si $*$ est associative, possède un **neutre** e, et si tout élément admet un **inverse**. Le groupe est **abélien** si $*$ est commutative.

— **Caractérisation des sous-groupes** : $H \subset G$ est un sous-groupe si et seulement si

$$H \neq \emptyset \quad \text{et} \quad \forall x, y \in H,\ x * y^{-1} \in H$$

— **Morphisme de groupes** : $f(x * y) = f(x) \star f(y)$. Alors $f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$.

— **Noyau et image** : $\ker f = \{x \in G \mid f(x) = e_H\}$ est un sous-groupe de G ; $\mathrm{Im} f$ est un sous-groupe de H.

$$f \text{ injectif} \Leftrightarrow \ker f = \{e_G\}$$

— **Ordre d'un élément** : le plus petit $n \geq 1$ tel que $x^n = e$ (s'il existe). Dans un groupe fini, l'ordre d'un élément **divise** l'ordre du groupe (Lagrange).

— **Sous-groupes de** $(\mathbb{Z}, +)$: exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

Anneaux et corps.

— $(A, +, \times)$ est un **anneau** si $(A, +)$ est un groupe abélien, $\times$ est associative avec un neutre 1_A, et distributive sur $+$.

— **Anneau intègre** : anneau commutatif non nul sans **diviseur de zéro** ($xy = 0 \Rightarrow x = 0$ ou $y = 0$).

— **Corps** : anneau commutatif dans lequel **tout élément non nul est inversible**.

— **Éléments inversibles** : $\mathbb{Z}^\times = \{-1, 1\}$; $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \mid \mathrm{pgcd}(k, n) = 1\}$.

— $\mathbb{Z}/n\mathbb{Z}$ est un **corps** si et seulement si n est **premier**.

— **Formule du binôme** dans un anneau **commutatif** : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Correction de l'exercice 1 – Vérifier une structure de groupe

— **Stabilité** : pour $x, y \in]-1\,;1[$, on a $1 + xy > 0$ et

$$1 - x * y = \frac{1 + xy - x - y}{1 + xy} = \frac{(1-x)(1-y)}{1+xy} > 0$$

De même $1 + x * y = \dfrac{(1+x)(1+y)}{1+xy} > 0$. Donc $x * y \in]-1\,;1[$.

— **Commutativité** : l'expression est symétrique en x et y.

— **Neutre** : $x * 0 = \dfrac{x}{1} = x$, donc $e = 0$.

— **Inverse** : $x * (-x) = \dfrac{0}{1 - x^2} = 0$, donc l'inverse de x est $-x$ (qui est bien dans G).

— **Associativité** : le calcul donne, dans les deux sens,

$$(x * y) * z = \frac{x + y + z + xyz}{1 + xy + yz + zx}$$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— **Conclusion** : $(G, *)$ est un groupe abélien.
— **Remarque physique** : c'est la loi de **composition des vitesses** en relativité restreinte, avec $c = 1$ — d'où l'impossibilité de dépasser 1.

Réponse. Groupe abélien, de neutre 0, l'inverse de x étant $-x$.

Correction de l'exercice 2 – Sous-groupe

On applique la **caractérisation**.

— **Non vide** : $2^0 = 1 \in H$.
— **Stabilité par** xy^{-1} : soient $x = 2^n$ et $y = 2^m$ avec $n, m \in \mathbb{Z}$. Alors

$$xy^{-1} = 2^n \times 2^{-m} = 2^{n-m}$$

— Comme $n - m \in \mathbb{Z}$, on a bien $xy^{-1} \in H$.
— **Conclusion** : H est un sous-groupe de $\left(\mathbb{R}_+^*, \times\right)$.
— **Structure** : $n \mapsto 2^n$ est un **isomorphisme** de $(\mathbb{Z}, +)$ sur $(H, \times)$ — H est donc un groupe monogène infini, isomorphe à $\mathbb{Z}$.

Réponse. Non vide et $2^n(2^m)^{-1} = 2^{n-m} \in H$.

Correction de l'exercice 3 – Morphisme et noyau

a) Pour tous réels x, y : $f(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y = f(x) \times f(y)$.

— La loi de départ $(+)$ est envoyée sur la loi d'arrivée $(\times)$: f est un **morphisme**.
— Contrôle : $f(0) = 1$, qui est bien le neutre multiplicatif.

b) - **Noyau** : $f(x) = 1 \Leftrightarrow \mathrm{e}^x = 1 \Leftrightarrow x = 0$, donc $\ker f = \{0\}$: f est **injective**.

— **Image** : exp atteint tout réel strictement positif, donc $\mathrm{Im} f = \mathbb{R}_+^*$: f est **surjective**.
— **Conclusion** : f est un **isomorphisme** de $(\mathbb{R}, +)$ sur $\left(\mathbb{R}_+^*, \times\right)$, d'isomorphisme réciproque ln.
— **Portée** : c'est pour cela que « additionner les exposants » et « multiplier les nombres » sont deux lectures du même calcul (principe de la règle à calcul et des échelles logarithmiques).

Réponse. b) $\ker f = \{0\}$, $\mathrm{Im} f = \mathbb{R}_+^*$: isomorphisme.

Correction de l'exercice 4 – Ordre d'un élément

L'ordre de $\overline{a}$ est le plus petit $n \geq 1$ tel que $na \equiv 0 \pmod{12}$.

— **Pour** $\overline{3}$: $3, 6, 9, 12 \equiv 0$. L'ordre est 4.
— **Pour** $\overline{5}$: $5, 10, 15 \equiv 3, 20 \equiv 8, 25 \equiv 1, \ldots$; il faut $12 \mid 5n$, et comme $\mathrm{pgcd}(5, 12) = 1$, cela impose $12 \mid n$. L'ordre est 12.
— **Formule générale** : l'ordre de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$ vaut $\dfrac{n}{\mathrm{pgcd}(a, n)}$.
— **Contrôle** : $\dfrac{12}{\mathrm{pgcd}(3, 12)} = \dfrac{12}{3} = 4$ et $\dfrac{12}{\mathrm{pgcd}(5, 12)} = 12$. Cohérent.
— **Lagrange** : 4 et 12 divisent bien 12, l'ordre du groupe. $\overline{5}$ est un **générateur** de $\mathbb{Z}/12\mathbb{Z}$.

Réponse. $\overline{3}$ est d'ordre 4, $\overline{5}$ d'ordre 12.

Correction de l'exercice 5 – Groupe symétrique

a) - σ envoie $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. Donc σ^2 envoie $1 \mapsto 3$, $3 \mapsto 2$, $2 \mapsto 1$: $\sigma^2 = (1\ 3\ 2)$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $\sigma^3 = \mathrm{id}$: σ est d'**ordre 3**.
— $\tau^2 = \mathrm{id}$: toute transposition est d'**ordre 2**.

b) On compare $\sigma\tau$ et $\tau\sigma$ (composition, τ appliquée en premier pour $\sigma\tau$).

— $\sigma\tau$: $1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3$, donc $1 \mapsto 3$.
— $\tau\sigma$: $1 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 1$, donc $1 \mapsto 1$.
— Les deux permutations diffèrent : S_3 n'est **pas abélien**.
— **Remarque** : $|S_3| = 3! = 6$, et c'est le plus petit groupe non abélien. Les ordres des éléments (1, 2, 3) divisent bien 6.

Réponse. a) $\sigma^2 = (1\ 3\ 2)$, $\sigma^3 = \tau^2 = \mathrm{id}$ · b) non abélien.

Correction de l'exercice 6 – Anneau et diviseurs de zéro

a) $2 \times 3 = 6 \equiv 0 \pmod 6$, donc $\overline{2} \times \overline{3} = \overline{0}$.

b) - Ni $\overline{2}$ ni $\overline{3}$ n'est nul, et leur produit l'est : ce sont des **diviseurs de zéro**. L'anneau n'est donc **pas intègre**.

— Ce n'est **pas un corps** non plus : $\overline{2}$ n'est pas inversible (un inverse donnerait $\overline{3} = \overline{2}^{-1}\overline{2}\overline{3} = \overline{0}$, faux).
— **Inversibles de** $\mathbb{Z}/6\mathbb{Z}$: $\overline{1}$ et $\overline{5}$, les classes des entiers premiers avec 6.
— **Critère général** : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier. Ici $6 = 2 \times 3$ est composé.
— **À comparer** : $\mathbb{Z}/5\mathbb{Z}$ est un corps, où tout élément non nul a un inverse ($\overline{2}^{-1} = \overline{3}$ car $6 \equiv 1$).

Réponse. a) $\overline{0}$ · b) non intègre, donc pas un corps.

Correction de l'exercice 7 – Sous-groupes de Z

— **Intersection** : un entier est dans les deux si et seulement s'il est multiple de 2 **et** de 3, donc multiple de $\mathrm{ppcm}(2, 3) = 6$:

$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$$

— **Sous-groupe engendré par la réunion** : il contient 2 et 3, donc $3 - 2 = 1$, donc $\mathbb{Z}$ tout entier :

$$\langle 2\mathbb{Z} \cup 3\mathbb{Z} \rangle = \mathbb{Z} = \mathrm{pgcd}(2, 3)\mathbb{Z}$$

— **Remarque importante** : la **réunion** $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est **pas** un sous-groupe ($2 + 3 = 5$ n'y est pas). Une réunion de sous-groupes n'en est un que si l'un contient l'autre.
— **Règle générale** : $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{ppcm}(a, b)\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = \mathrm{pgcd}(a, b)\mathbb{Z}$ — c'est une reformulation de Bézout.

Réponse. $6\mathbb{Z}$ et $\mathbb{Z}$.

Correction de l'exercice 8 – Morphisme d'anneaux

— **Compatibilité avec l'addition** : $\overline{k + l} = \overline{k} + \overline{l}$ par définition des classes.
— **Compatibilité avec la multiplication** : $\overline{kl} = \overline{k} \times \overline{l}$, propriété qui repose sur la compatibilité des congruences avec le produit.
— **Unité** : $f(1) = \overline{1}$, neutre de $\mathbb{Z}/n\mathbb{Z}$.
— f est donc un **morphisme d'anneaux surjectif** (la projection canonique).
— **Noyau** : $f(k) = \overline{0} \Leftrightarrow n \mid k$, donc $\ker f = n\mathbb{Z}$.
— **Lecture** : $\mathbb{Z}/n\mathbb{Z}$ s'obtient en « écrasant » $n\mathbb{Z}$ sur 0 — c'est le prototype du **quotient** par un idéal.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Réponse. Oui, morphisme surjectif de noyau $n\mathbb{Z}$.

Correction de l'exercice 9 – Groupe des inversibles

$\overline{k}$ est inversible si et seulement si $\text{pgcd}(k, 10) = 1$.

— Les entiers de $\{0, \ldots, 9\}$ premiers avec 10 sont 1, 3, 7, 9.
— Donc $(\mathbb{Z}/10\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$, groupe multiplicatif d'**ordre 4**.
— **Inverse de** $\overline{7}$: on cherche x tel que $7x \equiv 1 \pmod{10}$. On teste : $7 \times 3 = 21 \equiv 1$. Donc $\overline{7}^{-1} = \overline{3}$.
— **Vérification par Bézout** : $7 \times 3 - 10 \times 2 = 21 - 20 = 1$. Cohérent.
— **Indicatrice d'Euler** : $\varphi(10) = \varphi(2)\varphi(5) = 1 \times 4 = 4$, ce qui confirme le cardinal trouvé.

Réponse. $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ et $\overline{7}^{-1} = \overline{3}$.

Correction de l'exercice 10 – Corps

— **Sous-anneau de** $\mathbb{R}$: la somme est évidente, et pour le produit

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

reste de la même forme. Il contient $1 = 1 + 0\sqrt{2}$.
— **Inverses** : soit $z = a + b\sqrt{2} \neq 0$. On multiplie par le « conjugué » $a - b\sqrt{2}$:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

— Le dénominateur $a^2 - 2b^2$ est **non nul** : sinon $\left(\frac{a}{b}\right)^2 = 2$ ferait de $\sqrt{2}$ un rationnel (avec $b \neq 0$), ce qui est faux ; et si $b = 0$ alors $a \neq 0$.
— L'inverse est donc de la forme $a' + b'\sqrt{2}$ avec $a', b' \in \mathbb{Q}$.
— **Conclusion** : $\mathbb{Q}\left(\sqrt{2}\right)$ est un **corps**, le plus petit contenant $\mathbb{Q}$ et $\sqrt{2}$.
— **Exemple** : $\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{1-2} = \sqrt{2} - 1$. Contrôle : $(1 + \sqrt{2})(\sqrt{2} - 1) = 2 - 1 = 1$. Cohérent.

Réponse. Oui : $\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$, le dénominateur étant non nul.

Correction de l'exercice 11 – Centre d'un groupe

— **Non vide** : le neutre e commute avec tout élément, donc $e \in Z(G)$.
— **Stabilité par** ab^{-1} : soient $a, b \in Z(G)$ et $x \in G$.
— D'abord, b commute avec x, donc $bx = xb$; en multipliant à gauche et à droite par b^{-1} : $xb^{-1} = b^{-1}x$. Donc $b^{-1} \in Z(G)$.
— Ensuite $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$.
— Donc $ab^{-1} \in Z(G)$: $Z(G)$ est un **sous-groupe**.
— **Cas particuliers** : $Z(G) = G$ si et seulement si G est abélien ; $Z(S_3) = \{\text{id}\}$.
— **Remarque** : $Z(G)$ est même un sous-groupe **normal**, ce qui en fait un outil central de la théorie des groupes.

Réponse. $e \in Z(G)$ et $a, b \in Z(G) \Rightarrow ab^{-1} \in Z(G)$.

Correction de l'exercice 12 – Table de Cayley et groupe de Klein

a) On calcule les produits modulo 8 (par exemple $3 \times 5 = 15 \equiv 7$, $5 \times 7 = 35 \equiv 3$) :

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

$\times$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

— La table ne sort pas de V : la loi est **interne**. L'associativité et la commutativité sont héritées de la multiplication de $\mathbb{Z}/8\mathbb{Z}$. Le neutre est $\overline{1}$, et chaque ligne contient $\overline{1}$ sur la diagonale : **chaque élément est son propre inverse**.

b) $\overline{1}$ est d'ordre 1 ; $\overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$: les trois autres sont d'ordre 2. Aucun élément n'est d'ordre $4 = \mathrm{card} V$: V n'est **pas cyclique**.

c) Un isomorphisme conserve l'ordre des éléments, puisque

$$f(x)^k = f(x^k) \quad \text{et} \quad f \text{ injectif}$$

— $\mathbb{Z}/4\mathbb{Z}$ a un élément d'ordre 4 ($\overline{1}$), V n'en a pas : ils ne sont pas isomorphes.

— $(\mathbb{Z}/2\mathbb{Z})^2 = \{(0,0),(1,0),(0,1),(1,1)\}$ a aussi trois éléments d'ordre 2 ; l'application $\overline{1} \mapsto (0,0)$, $\overline{3} \mapsto (1,0)$, $\overline{5} \mapsto (0,1)$, $\overline{7} \mapsto (1,1)$ transforme la table de V en celle de l'addition (par exemple $\overline{3} \times \overline{5} = \overline{7}$ et $(1,0)+(0,1)=(1,1)$) : c'est un isomorphisme. C'est le **groupe de Klein**.

Réponse. Groupe abélien, chaque élément est son propre inverse ; non cyclique ; $V \simeq (\mathbb{Z}/2\mathbb{Z})^2 \not\simeq \mathbb{Z}/4\mathbb{Z}$.

Correction de l'exercice 13 – Exponentielle imaginaire et cercle unité

a) Pour $s, t \in \mathbb{R}$, la propriété fondamentale de l'exponentielle donne

$$\varphi(s+t) = \mathrm{e}^{\mathrm{i}(s+t)} = \mathrm{e}^{\mathrm{i}s}\mathrm{e}^{\mathrm{i}t} = \varphi(s)\varphi(t)$$

— U contient 1, et pour $z, w \in \mathrm{U}$: $|zw^{-1}| = \dfrac{|z|}{|w|} = 1$. C'est un sous-groupe de $\mathbb{C}^*$.

b) $|\mathrm{e}^{\mathrm{i}t}| = 1$, donc $\mathrm{Im}\varphi \subset \mathrm{U}$; réciproquement tout $z \in \mathrm{U}$ s'écrit $\mathrm{e}^{\mathrm{i}\theta}$ (un argument de z). Donc $\mathrm{Im}\varphi = \mathrm{U}$.

— $\ker\varphi = \{t,\ \mathrm{e}^{\mathrm{i}t} = 1\} = 2\pi\mathbb{Z}$, qui n'est pas réduit à $\{0\}$: φ **n'est pas injectif**.

c) $\varphi(t) \in U_n \Leftrightarrow \mathrm{e}^{\mathrm{i}nt} = 1 \Leftrightarrow nt \in 2\pi\mathbb{Z} \Leftrightarrow t \in \dfrac{2\pi}{n}\mathbb{Z}$. Donc $\varphi^{-1}(U_n) = \dfrac{2\pi}{n}\mathbb{Z}$, un sous-groupe de $\mathbb{R}$ contenant le noyau ✓.

Interprétation : « l'angle t n'est défini qu'à 2π près » est exactement l'énoncé $\ker\varphi = 2\pi\mathbb{Z}$.

Réponse. Morphisme surjectif sur U, de noyau $2\pi\mathbb{Z}$; $\varphi^{-1}(U_n) = \dfrac{2\pi}{n}\mathbb{Z}$.

Correction de l'exercice 14 – Réunion de deux sous-groupes

a) $e \in H \cap K$. Pour $x, y \in H \cap K$, xy^{-1} est dans H (sous-groupe) et dans K : on applique la caractérisation

$$H \cap K \neq \varnothing \quad \text{et} \quad \forall x, y \in H \cap K,\ xy^{-1} \in H \cap K$$

b) Si $H \subset K$, alors $H \cup K = K$ est un sous-groupe ; de même si $K \subset H$.

— Réciproquement, supposons $H \cup K$ sous-groupe, et par l'absurde $H \not\subset K$ et $K \not\subset H$: il existe $h \in H \setminus K$ et $k \in K \setminus H$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $hk \in H \cup K$. Si $hk \in H$, alors $k = h^{-1}(hk) \in H$: exclu. Si $hk \in K$, alors $h = (hk)k^{-1} \in K$: exclu. Contradiction.

c) $2 \in 2\mathbb{Z}$ et $3 \in 3\mathbb{Z}$, mais $2 + 3 = 5$ n'est multiple ni de 2 ni de 3 : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est **pas** un sous-groupe (conforme à b), aucun des deux ne contenant l'autre).

— Le plus petit sous-groupe le contenant est $2\mathbb{Z} + 3\mathbb{Z} = (2 \wedge 3)\mathbb{Z} = \mathbb{Z}$: il contient $3 - 2 = 1$.

Piège : une réunion de sous-groupes n'est presque jamais un sous-groupe ; c'est l'intersection qui se comporte bien.

Réponse. $H \cap K$ sous-groupe ; $H \cup K$ sous-groupe $\Leftrightarrow H \subset K$ ou $K \subset H$; $2\mathbb{Z} \cup 3\mathbb{Z}$ n'en est pas un, il engendre $\mathbb{Z}$.

Correction de l'exercice 15 – Synthèse : groupe des racines de l'unité

a) - **Non vide** : $1^n = 1$, donc $1 \in U_n$.

— **Stabilité** : si $z^n = 1$ et $w^n = 1$, alors $\left(zw^{-1}\right)^n = z^n (w^n)^{-1} = 1$.

— Donc U_n est un sous-groupe de $\left(\mathbb{C}^*, \times\right)$, de cardinal n (les $\mathrm{e}^{2\mathrm{i}k\pi/n}$, $0 \leq k \leq n-1$).

b) On pose $\varphi : \mathbb{Z} \to U_n$, $k \mapsto \mathrm{e}^{2\mathrm{i}k\pi/n}$.

— **Morphisme** : $\varphi(k + l) = \mathrm{e}^{2\mathrm{i}(k+l)\pi/n} = \varphi(k)\varphi(l)$.

— **Surjectif** : tout élément de U_n s'écrit sous cette forme.

— **Noyau** : $\varphi(k) = 1 \Leftrightarrow \frac{2k\pi}{n} \equiv 0 \pmod{2\pi} \Leftrightarrow n \mid k$, donc $\ker \varphi = n\mathbb{Z}$.

— Le morphisme induit donc un **isomorphisme** $\mathbb{Z}/n\mathbb{Z} \simeq U_n$.

— **Conséquence** : tout groupe **cyclique** d'ordre n est isomorphe à U_n — ce groupe est le modèle géométrique du polygone régulier à n sommets muni de ses rotations.

Réponse. a) sous-groupe de cardinal n · b) $U_n \simeq \mathbb{Z}/n\mathbb{Z}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).