
MAT35B - L3A ALGÈBRE
Premier semestre — 2021-2022

Fiche 2: Groupes, sous-groupes et morphismes

1. Soit (G, \cdot) un groupe. Pour $a \in G$, on note τ_a, δ_a et γ_a les applications de G dans G définies par $\tau_a(x) = ax$, $\delta_a(x) = xa$ et $\gamma_a(x) = axa^{-1}$, pour tout $x \in G$. Elles sont appelées **translation à gauche**, **translation à droite** et **conjugaison** par a , respectivement.
 - (a) Ces applications sont-elles des permutations de G ? des automorphismes de groupe?
 - (b) En quoi la table d'un groupe fini ressemble-t-elle à une grille de sudoku? En déduire qu'il n'y a qu'un groupe d'ordre 2 et qu'un groupe d'ordre 3 à isomorphisme près.
 - (c) Les applications $\tau : a \mapsto \tau_a$, $\delta : a \mapsto \delta_a$ et $\gamma : a \mapsto \gamma_a$ sont-elles des morphismes de (G, \cdot) dans $(\text{Aut}_{\text{Ens}}(G), \circ)$? Si, oui quel est leur noyau?
2. Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$. L'objet de l'exercice est de montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les parties de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$.
 - (a) Montrer que si $a \in \mathbb{Z}$, alors $a\mathbb{Z}$ est un sous-groupe de \mathbb{Z} .
 - (b) Soit H un sous-groupe de \mathbb{Z} . Montrer que H est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$ et que cet entier a est uniquement déterminé. On distinguera deux cas, suivant que H est ou non réduit à $\{0\}$.
3. Soient G un groupe et $a \in G$. On note $f_a : \mathbb{Z} \rightarrow G$ l'application qui associe a^k à un entier k .
 - (a) Montrer que f_a est un morphisme de groupes.
 - (b) Montrer que l'image de f_a est $\langle a \rangle$, le sous-groupe engendré par a .
 - (c) Expliquer pourquoi le noyau de f_a est de la forme $d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$, uniquement déterminé.

Remarque : pour tout $n \in \mathbb{Z}$, on a $a^n = 1_G$ si et seulement si $d|n$. Cette équivalence est très utile dans les exercices sur l'ordre d'un élément.
 - (d) Si $d = 0$, à quel groupe est isomorphe le sous-groupe $\langle a \rangle$ engendré par a ? En déduire que a est d'ordre infini.
 - (e) Si $d \in \mathbb{N}^*$, montrer que le sous-groupe $\langle a \rangle$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et donner la liste de ses éléments. En déduire que a est d'ordre fini d , et que d divise $|G|$ si G est fini.
 - (f) Montrer que si a est d'ordre fini d , alors pour tout $\ell \in \mathbb{Z}$, l'ordre de a^ℓ est $d / \text{PGCD}(d, \ell)$. En déduire que a^{-1} a le même ordre que a .
 - (g) Montrer que si a est d'ordre fini d , tout conjugué de a (i.e., tout élément de la forme gag^{-1} avec $g \in G$) a le même ordre que a .
 - (h) Soit $\phi : G \rightarrow G'$ un morphisme de groupes. Si $a \in G$ est d'ordre fini d , que peut-on dire de l'ordre de $\phi(a)$ dans G' ?
4. Soit G un groupe de cardinal $n \in \mathbb{N}^*$ et g un élément de G tel que $G = \langle g \rangle$ (on dit dans ce cas que G est **cyclique**). Un élément a de G est appelé un **générateur** de G si l'on a aussi $G = \langle a \rangle$.

- (a) Montrer que G contient $\varphi(n)$ générateurs, qui sont exactement les éléments de la forme g^k avec k premier à n .
- (b) Soit $d \in \mathbb{N}^*$ un diviseur de n .
- (i) Montrer que l'ensemble $E_d = \{x \in G : x^d = 1_G\}$ est un sous-groupe cyclique de G de cardinal d , engendré par $g^{n/d}$.
- (ii) Soit H un sous-groupe de G de cardinal d . Montrer que $H = E_d$.
- (c) Dédire de la question précédente que tous les sous-groupes d'un groupe cyclique sont cycliques.
- (d) Montrer que si d est un diviseur de n , le groupe G contient exactement $\varphi(d)$ éléments d'ordre d .
- (e) Dédire des questions précédentes que la somme des $\varphi(d)$ vaut n pour tout d diviseur de n .

5. Soient p et q deux nombres premiers distincts.

- (a) Montrer que $a^{p-1} \equiv 1 \pmod{p}$ si a est un entier non multiple de p .
- (b) Montrer que $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{Z}$.
- (c) On fixe $e \in \mathbb{N}^*$ et $d \in \mathbb{N}^*$ tels que $de \equiv 1 \pmod{(p-1)(q-1)}$. Montrer que $M^{de} \equiv M \pmod{pq}$ pour tout $M \in \mathbb{Z}$.
- Indication** : montrer la congruence modulo p et modulo q . Ce résultat est à la base de l'algorithme RSA introduit par R. Rivest, A. Shamir et L. Adleman en 1977.
- (d) Soit $n \in \mathbb{N}^*$. Montrer que $a^{\varphi(n)} \equiv 1 \pmod{n}$ pour tout entier a premier avec n .

6. Soient G_1 et G_2 deux groupes.

- (a) Montrer que $G_1 \times G_2$ possède une structure naturelle de groupe.
- (b) Soient $a_1 \in G_1$ d'ordre fini d_1 et $a_2 \in G_2$ d'ordre fini d_2 . Quel est l'ordre de (a_1, a_2) dans le groupe $G_1 \times G_2$?
- (c) Montrer que $G_1 \times G_2$ est cyclique si et seulement si G_1 et G_2 sont cycliques et d'ordres premiers entre eux.

7. (a) Soit p un nombre premier. Montrer que tout groupe fini d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

- (b) Montrer que tout groupe fini d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $(\mathbb{Z}/2\mathbb{Z})^2$

8. Soit G un groupe abélien.

- (a) On suppose que tous les éléments de G sont d'ordre fini. Le groupe G est-il fini? Même question si les ordres sont bornés.
- (b) On utilisera désormais la notation additive. On suppose qu'il existe un entier premier p tel que tous les éléments non nuls de G soient d'ordre p . Montrer que le groupe G possède une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel. En déduire que si le groupe G est fini alors il existe un entier positif d tel que G soit isomorphe au groupe produit $(\mathbb{Z}/p\mathbb{Z})^d$.

9. Soit G un groupe dont tous les éléments sont d'ordre 1 ou 2. Montrer que G est abélien. Si de plus G est fini, pourquoi son ordre est-il une puissance de 2 ?

10. Soit G un groupe. Soient a et b deux éléments d'ordres finis dans G , tels que $ab = ba$. On note $\text{ord}(a) = m$ et $\text{ord}(b) = n$ les ordres, $d = \text{PGCD}(m, n)$, $m = dm'$, $n = dn'$.

- (a) Montrer ab est d'ordre fini divisant $\text{PPCM}(m, n)$.

- (b) Montrer que cette divisibilité peut être stricte.
- (c) Montrer que l'ordre de ab est multiple de $\text{PPCM}(m, n)/\text{PGCD}(m, n)$.
Indication : poser $r = \text{ord}(ab)$ et, en utilisant l'égalité $a = (ab)b^{-1}$, montrer que m divise rn .
- (d) En déduire que si $\text{PGCD}(m, n) = 1$, alors $\text{ord}(ab) = mn = \text{ord}(a)\text{ord}(b)$.
- (e) Montrer que ces conclusions peuvent être fausses sans l'hypothèse $ab = ba$.

11. Soit G un groupe abélien fini. On note m le PPCM des ordres des éléments de G . Cet entier s'appelle l'**exposant** de G .

- (a) Montrer que m divise l'ordre de G , et que cette divisibilité peut être stricte.
- (b) Montrer que G possède au moins un élément d'ordre m .
Indication : utiliser les résultats des exercices précédents et la décomposition de m en facteurs premiers.

12. On va montrer que $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{S}_3 = \text{Aut}_{\text{Ens}}(\{1, 2, 3\})$ sont les seuls groupes d'ordre 6 à isomorphisme près.

- (a) On note τ et γ les bijections de $\{1, 2, 3\}$ définies par $\tau(1) = 2, \tau(2) = 1, \tau(3) = 3$ et $\gamma(1) = 2, \gamma(2) = 3, \gamma(3) = 1$. Déterminer les images de 1, 2, 3 par $\tau^2 = \tau \circ \tau, \gamma^2, \gamma^3, \tau \circ \gamma$ et $\tau \circ \gamma^2, \gamma \circ \tau, \gamma^2 \circ \tau$. Mettre les résultats sous forme de tableau. En déduire que $\mathbb{S}_3 = \{\text{id}_{\{1,2,3\}}, \gamma, \gamma^2, \tau, \tau \circ \gamma, \tau \circ \gamma^2\}$ et donner la table du groupe (\mathbb{S}_3, \circ) .
- (b) Soit G un groupe d'ordre 6, non isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
 (i) Montrer que G possède nécessairement un élément d'ordre 3.
 (ii) Montrer que G possède nécessairement un élément d'ordre 2.
 (iii) Soient α un élément d'ordre 3 et β un élément d'ordre 2. Montrer que $G = \{1_G, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$.
 (iv) En remarquant que $\alpha\beta \neq \beta\alpha$ (pourquoi?), dresser la table de multiplication de G et en déduire que G est isomorphe à \mathbb{S}_3 .
- (c) Soit $A_1A_2A_3$ un triangle non-aplati de \mathbb{R}^2 d'isobarycentre $O = (0, 0)$. Soit T le sous-groupe de $\text{GL}(\mathbb{R}^2)$ formé des endomorphismes de \mathbb{R}^2 laissant l'ensemble $\{A_1, A_2, A_3\}$ globalement invariant. Exhiber un isomorphisme de \mathbb{S}_3 vers T .

13. Soient E un ensemble, G un groupe et $\phi : E \rightarrow G$ une bijection.

- (a) Montrer que l'on peut définir une loi de groupe sur E par

$$a * b = \phi^{-1}(\phi(a)\phi(b)),$$

pour tous $a, b \in E$. Que peut-on dire alors de l'application ϕ ?

- (b) On munit $\{0, 1\}$ de l'addition modulo 2, notée \oplus . On note encore \oplus l'addition sur $\{0, 1\}^E$ définie par $(f \oplus g)(x) = f(x) \oplus g(x)$, pour tous $f, g \in \{0, 1\}^E$ et $x \in \{0, 1\}$. On rappelle que, à toute partie A de E , on associe sa fonction indicatrice $\mathbf{1}_A : E \rightarrow \{0, 1\}$ définie par $\mathbf{1}_A(x) = 1$ si $x \in A$, et $\mathbf{1}_A(x) = 0$ si $x \in E \setminus A$. Montrer que l'application $\Phi : \mathcal{P}(E) \rightarrow \{0, 1\}^E$ donnée par $\Phi(A) = \mathbf{1}_A$ est une bijection, et que la loi de groupe induite sur $\mathcal{P}(E)$ par transport de structure est la différence symétrique.

14. On veut montrer que tout sous-groupe de \mathbb{R} est soit dense dans \mathbb{R} , soit de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}_{\geq 0}$. On prend donc G un sous-groupe de \mathbb{R} différent de $\{0\} = 0\mathbb{Z}$ et on pose $\alpha = \inf(G \cap \mathbb{R}_{>0})$.

- (a) Montrer que $\alpha \in \mathbb{R}_{\geq 0}$.
- (b) Montrer que si $\alpha = 0$, alors G est dense dans \mathbb{R} .
- (c) Montrer que si $\alpha > 0$, alors $G = \alpha\mathbb{Z}$.

15. Soit G un sous-groupe fini du groupe multiplicatif \mathbb{C}^\times . On considère le sous-groupe de \mathbb{C}^* donné par $U(1) = \{z \in \mathbb{C}^* : |z| = 1\}$ et l'application $f : \mathbb{R} \rightarrow U(1)$ donnée par $f(t) = e^{2i\pi t}$.

- (a) Montrer que G est un sous-groupe du groupe $U(1)$.
- (b) Montrer que $f^{-1}(G)$ est un sous-groupe de \mathbb{R} qui contient \mathbb{Z} .
- (c) Montrer que $f^{-1}(G)$ n'est pas dense dans \mathbb{R} .
- (d) En déduire que $f^{-1}(G)$ est de la forme $n^{-1}\mathbb{Z}$ avec $n \in \mathbb{N}^*$.
- (e) En déduire que G est un groupe cyclique d'ordre n .

16. Soient a et b dans \mathbb{N}^* .

- (a) Soit f l'application de \mathbb{Z} dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ définie par $f(k) = (k + a\mathbb{Z}, k + b\mathbb{Z})$. Montrer que f est un morphisme de groupes. Déterminer $\text{Ker}(f)$.
- (b) En déduire que si a et b sont premiers entre eux, le groupe $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Qu'en est-il dans le cas contraire ?
- (c) Lorsque a et b sont premiers entre eux, expliciter l'isomorphisme réciproque en utilisant une relation de Bézout. On pourra commencer par chercher les images réciproques de $(1 + a\mathbb{Z}, 0 + b\mathbb{Z})$ et de $(0 + a\mathbb{Z}, 1 + b\mathbb{Z})$.

17. Pour $1 \leq n \leq 17$, déterminer si le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique et donner une partie génératrice minimale.

18. Soient (G, \cdot) et (G', \cdot) deux groupes et A une partie génératrice de (G, \cdot) .

- (a) Montrer que si deux morphismes de groupes de (G, \cdot) dans (G', \cdot) coïncident sur A , ils sont égaux.
- (b) Montrer que si un élément $g \in G$ commute avec tous les éléments de A , alors il appartient au centre de G .

Indication : utiliser l'automorphisme intérieur associé à g .

19. Soit (G, \cdot) un groupe et $n \in \mathbb{N}^*$.

- (a) Quels sont les morphismes de groupes de $(\mathbb{Z}, +)$ dans (G, \cdot) ? Les endomorphismes de $(\mathbb{Z}, +)$? Les automorphismes de $(\mathbb{Z}, +)$?
- (b) Quels sont les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans (G, \cdot) ? Les endomorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$? Les automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$?
- (c) Quels sont les morphismes de groupes de $(\mathbb{Z}^2, +)$ dans (G, \cdot) ? Les endomorphismes de $(\mathbb{Z}^2, +)$? Les automorphismes de $(\mathbb{Z}^2, +)$?

20. Soient (G, \cdot) , (G', \cdot) deux groupes isomorphes et f un isomorphisme de (G, \cdot) dans (G', \cdot) . On note $\text{Aut}_{\text{Gr}}(G)$ le groupe des automorphismes de G . On considère l'application $\Phi : \text{Aut}_{\text{Gr}}(G) \rightarrow \text{Aut}_{\text{Gr}}(G')$ donnée par $\Phi(\varphi) = f \circ \varphi \circ f^{-1}$, pour tout $\varphi \in \text{Aut}_{\text{Gr}}(G)$. Montrer que Φ est un isomorphisme de groupes.

21. On considère le groupe additif $(\mathbb{Z}^2, +)$. Soient $u = (a, b) \in \mathbb{Z}^2$ et $v = (c, d) \in \mathbb{Z}^2$.

- (a) À quelle condition a-t-on $\mathbb{Z}^2 = \langle u, v \rangle$?
- (b) Soit $H = \{(x, y) \in \mathbb{Z}^2 : x + y \in 2\mathbb{Z}\}$.
 - (i) Montrer que H est un sous-groupe de \mathbb{Z}^2 .
 - (ii) Donner une partie génératrice de H à deux éléments.

(iii) Déterminer \mathbb{Z}^2/H .

(c) On suppose que $ad - bc \neq 0$ et on note $H = \langle u, v \rangle$.

(i) Soit $P = \{\alpha u + \beta v : 0 \leq \alpha < 1, 0 \leq \beta < 1\}$. Établir une bijection entre $P \cap \mathbb{Z}^2$ et \mathbb{Z}^2/H .

(ii) On prend $u = (1, 4)$ et $v = (2, 3)$. Déterminer l'ordre du groupe \mathbb{Z}^2/H .

22. Soit E un espace vectoriel euclidien de dimension $n \geq 3$. En utilisant le fait que les réflexions de E engendrent $O(E)$, montrer que les renversements de E engendrent $SO(E)$.

Indication : montrer que si u et v sont deux vecteurs unitaires orthogonaux, la composée des réflexions par rapport aux hyperplans $(\mathbb{R}u)^\perp$ et $(\mathbb{R}v)^\perp$ est un renversement. Puis montrer que pour deux vecteurs unitaires quelconques u_1 et u_2 , la composée des réflexions par rapport aux hyperplans $(\mathbb{R}u_1)^\perp$ et $(\mathbb{R}u_2)^\perp$ est une composée de deux renversements.

23. On se propose de classifier les isométries vectorielles de \mathbb{R}^3 . Soit f une isométrie de \mathbb{R}^3 . On sait que f s'écrit comme la composée de 0, 1, 2 ou 3 réflexions orthogonales.

(a) Quel est le déterminant de f dans chacun des cas ci-dessus ?

(b) Dans cette question, on suppose que $f = s_2 \circ s_1$, où s_1 et s_2 sont les réflexions orthogonales par rapport à des plans P_1 et P_2 avec $P_1 \neq P_2$. Ces deux plans se coupent selon une droite D .

(i) Vérifier que le plan orthogonal à D , noté D^\perp , est stable par f .

(ii) En déduire que l'endomorphisme induit par f sur ce plan est une rotation. On dit dans ce cas que f est une **rotation d'axe D** .

En déduire que toute isométrie directe de \mathbb{R}^3 est une rotation.

(c) Dans cette question, on suppose que $f = s_3 \circ s_2 \circ s_1$, où s_1 et s_2 et s_3 sont des réflexions orthogonales.

(i) Vérifier que $-f$ est une isométrie directe de \mathbb{R}^3 . Dans la suite, on suppose que $f \neq -\text{id}_{\mathbb{R}^3}$, donc $-f$ est une rotation autre que $\text{id}_{\mathbb{R}^3}$. On note D son axe.

(ii) Soient r le renversement d'axe D et s la réflexion par rapport au plan D^\perp . Que valent $s \circ r$ et $r \circ s$? En déduire que soit $f = s$, soit f est le produit commutatif d'une rotation non triviale d'axe D avec s .

On appelle **antirotation d'axe D** toute isométrie qui s'écrit comme le produit (commutatif) d'une rotation non triviale d'axe D et de la réflexion orthogonale par rapport au plan D^\perp . En déduire que toute isométrie indirecte de \mathbb{R}^3 est soit une réflexion orthogonale, soit une antirotation.

(d) Déduire des questions précédentes la classification des isométries vectorielles de \mathbb{R}^3 en fonction de leurs vecteurs fixes.