

Fiche d'exercices n° 1 - Corrigés

Groupes et géométrie

Exercice 1.

Soit $\mathbb{Q}$ l'ensemble des nombres rationnels muni de la loi de composition interne notée $*$, définie par :

$$\begin{aligned} (\mathbb{Q} \times \mathbb{Q}) &\longrightarrow \mathbb{Q} \\ (a, b) &\longmapsto a * b = a + b + ab \end{aligned}$$

$(\mathbb{Q}, *)$ est-il un groupe ?

- Associativité : OK
On vérifie aisément que, pour tout $a, b, c \in \mathbb{Q}$, $(a * b) * c = a * (b * c)$.
- Existence d'un élément neutre : OK
On remarque que, pour tout $a \in \mathbb{Q}$, $a * 0 * 0 * a = a$.
- Existence d'un symétrique : $a * b = 0 \Leftrightarrow b = \frac{-a}{1+a}$
-1 ne possède donc pas de symétrique pour la loi $*$.

$(\mathbb{Q}; *)$ n'est donc pas un groupe, mais $(\mathbb{Q} \setminus \{1\}; *)$ en est un.

Exercice 2. (*Proposition 5, Chap. 1*).

Soient deux groupes G_1 et G_2 . Montrons que :

Un groupe G est isomorphe à $G_1 \times G_2$ si, et seulement s'il contient deux sous-groupes H_1 et H_2 tels que :

1. $H_i \simeq G_i$, pour $i = 1, 2$.
2. $\forall h_1 \in H_1, \forall h_2 \in H_2, h_1 h_2 = h_2 h_1$.
3. $G = H_1 H_2$.
4. $H_1 \cap H_2 = \{e\}$, où e est l'élément neutre de G

@ Supposons G isomorphe à $G_1 \times G_2$

On peut supposer que $G = G_1 \times G_2$ sans restreindre la généralité.

On a vu (remarque 6.b)) que $G_1 \times G_2$ possède au moins un sous-groupe isomorphe à G_1 et un sous-groupe isomorphe à G_2 (démontrez le!).

Posons $H_1 = \text{Im}(q_1)$ et $H_2 = \text{Im}(q_2)$ où les q_i sont les injections canoniques.

— On a $H_1 \simeq G_1$ et $H_2 \simeq G_2$

— D'autre part, si $h_1 \in H_1$ et $h_2 \in H_2$,

$\exists x_1 \in G_1$ et $x_2 \in G_2$ tel que $h_1 = (x_1; e_2)$ et $h_2 = (e_1; x_2)$

d'où $(x_1; x_2) = h_1 h_2 = h_2 h_1$.

(en fait, $H_1 H_2 = H_2 H_1 \Rightarrow$ ce produit est un sous-groupe de G)

— De plus, pour $x = (x_1; x_2) \in G_1 \times G_2$, on a

$$\begin{aligned}(x_1; x_2) &= (p_1(x); p_2(x)) \\ &= (p_1(x); e_2) \cdot (e_1; p_2(x)) \\ &= q_1(x_1) \cdot q_2(x_2) \\ &= q_2(x_2) \cdot q_1(x_1)\end{aligned}$$

donc $G = H_1 H_2$

— Enfin, soit $x = (x_1; x_2) \in H_1 \cap H_2$.

$$(x_1; x_2) \in H_1 \Rightarrow x_2 = e_2 \text{ et } (x_1; x_2) \in H_2 \Rightarrow x_1 = e_1$$

$$\text{Donc } H_1 \cap H_2 = \{(e_1; e_2)\}$$

@ Réciproquement, supposons que G contient deux sous-groupes vérifiant les 4 propriétés de la proposition.

Soient H_1 et H_2 deux sous-groupes de G comme attendus.

Soit $g \in G$, d'après les hypothèses 2 et 3, $\exists h_1 \in H_1$ et $h_2 \in H_2$ tel que $g = h_1 h_2 = h_2 h_1$.

— Montrons que l'écriture est unique.

$$\text{Soient } h'_1 \in H_1 \text{ et } h'_2 \in H_2 \text{ tel que } g = h'_1 h'_1 = h'_2 h'_1$$

$$\begin{aligned}h_1 h_2 = h'_1 h'_2 &\Rightarrow (h'_1)^{-1} h_1 = h_2 (h'_2)^{-1} \\ &\Rightarrow (h'_1)^{-1} h_1 = h_2 (h'_2)^{-1} = e(\text{hypothèse 4}) \\ &\Rightarrow h_1 = h'_1 \text{ et } h_2 = h'_2\end{aligned}$$

— D'après l'hypothèse 1, soit $\varphi_i : H_i \longrightarrow G_i$ des isomorphismes.

On considère alors :

$$\begin{aligned}(\varphi : \quad G &\longrightarrow G_1 \times G_2 \\ g = h_1 h_2 &\longmapsto (\varphi_1(h_1); \varphi_2(h_2))\end{aligned}$$

Pour $g = h_1 h_2$ et $g' = h'_1 h'_2$, on a $gg' = h_1 h_2 h'_1 h'_2 = h_1 h'_1 h_2 h'_2$ d'où :

$$\begin{aligned}\varphi(gg') &= (\varphi_1(h_1 h'_1); \varphi_2(h_2 h'_2)) \\ &= (\varphi_1(h_1) \varphi_1(h'_1); \varphi_2(h_2) \varphi_2(h'_2)) (\text{hypothèse 2}) \\ &= \varphi(g) \varphi(g')\end{aligned}$$

Donc φ est un morphisme de groupes.

—

$$\begin{aligned}\varphi(h_1 h_2) = (e_1; e_2) &\Rightarrow \varphi_1(h_1) = e_1 \text{ et } \varphi_2(h_2) = e_2 \\ &\Rightarrow h_1 = h_2 = e \text{ car } \varphi_i \text{ injective}\end{aligned}$$

Donc $\text{Ker } \varphi = \{e\}$ et φ injectif.

- Si $(x_1; x_2) \in G_1 \times G_2$, comme φ_i surjectif, $\exists(h_1; h_2) \in H_1 \times H_2$ tel que $x_1 = \varphi_1(h_1)$ et $x_2 = \varphi_2(h_2)$ c'est à dire $(x_1; x_2) = \varphi(h_1 h_2)$.
Donc φ est surjectif.

Exercice 3.

Soit G un groupe.

On considère l'application

$$\begin{array}{ccc} f & G & \longrightarrow G \\ & x & \longmapsto x^{-1} \end{array}$$

a. Montrons que f est une permutation de G

- f est bien définie car x^{-1} existe car G est un groupe.
- De plus, si $y \in G$, comme $f(y^{-1}) = (y^{-1})^{-1} = y$, c'est que y possède un antécédent, qui est unique (car G est un groupe).
- L'application f est donc bijective.

b. Montrons que f est un morphisme (et donc un automorphisme) si, et seulement si G est abélien.

Soient $x, y \in G$,

$$\begin{aligned} f(xy) &= f(x)f(y) \\ \Leftrightarrow (xy)^{-1} &= x^{-1}y^{-1} \\ \Leftrightarrow y^{-1}x^{-1} &= x^{-1}y^{-1} \\ \Leftrightarrow y^{-1}x^{-1}yx &= e \text{ on a multiplié, à droite, par } y \text{ puis par } x \\ \Leftrightarrow yx = xy &\text{ on a multiplié, à gauche, par } y \text{ puis par } x \end{aligned}$$

Donc, f automorphisme $\Leftrightarrow G$ abélien

Exercice 4.

Soit G un groupe dont tous les éléments (sauf le neutre) sont d'ordre 2.

En notation multiplicative, cela signifie que $\forall x \in G, x^2 = e$.

En notation additive, cela signifie que $\forall x \in G, 2x = e$.

a. $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; +)$ est un exemple de tel groupe, non réduit à l'élément neutre.

En effet :

$$\begin{aligned} (\bar{1}; \bar{0}) + (\bar{1}; \bar{0}) &= 2 \times (\bar{1}; \bar{0}) = (\bar{2}; \bar{0}) = (\bar{0}; \bar{0}) \\ 2 \times (\bar{0}; \bar{1}) &= (\bar{0}; \bar{2}) = (\bar{0}; \bar{0}) \\ 2 \times (\bar{1}; \bar{1}) &= (\bar{2}; \bar{2}) = (\bar{0}; \bar{0}) \end{aligned}$$

b. Montrons qu'un tel groupe G est abélien.

On rappelle que pour $x \in G, x^2 = e \Leftrightarrow x = x^{-1}$

Soit $x, y \in G$,

$$\begin{aligned} xy &= (xy)^{-1} \\ \Rightarrow xy &= y^{-1}x^{-1} \\ \Rightarrow xy &= yx \\ \Rightarrow G &\text{ abélien} \end{aligned}$$

c. Montrons que si G est fini, son cardinal est alors une puissance de 2.

Comme G abélien et que tous ses éléments sont d'ordre 2, G est muni d'une structure de $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel.

Si G est fini, G est de dimension finie n sur $\mathbb{Z}/2\mathbb{Z}$ et donc $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

Donc $\#G = 2^n$

Exercice 5.

Montrons qu'un groupe fini d'ordre pair possède au moins un élément d'ordre 2.

On écrit $G = \{e; x_1; \dots; x_n\}$ où n est pair.

On partitionne G ainsi : $G = \{x_1; x_1^{-1}\} \cup \dots \cup \{x_n; x_n^{-1}\}$.

Comme e est seul dans sa "classe", un autre x_i au moins est nécessairement aussi seul dans sa classe. Notons le x_i .

Ce x_i est tel que $x_i = x_i^{-1}$, c'est à dire $(x_i)^2 = e$.

Donc tout groupe fini d'ordre pair possède au moins un élément d'ordre 2.

Exercice 6.

Soit $(G, \times)$ un groupe fini d'ordre n , et soit m un entier premier avec l'ordre de G .

Montrons que, pour tout $a \in G$, l'équation $x^m = a$ possède une solution unique.

D'après le théorème de Bézout, on peut se donner deux entiers u et v tels que $mu + nv = 1$.

Soit $a \in G$,

$$\begin{aligned} x^m &= a \\ \Leftrightarrow (x^m)^u &= a^u \\ \Leftrightarrow x^{mu} &= a^u \\ \Leftrightarrow x^{mu+nv} &= a^u x^{nv} \\ \Leftrightarrow x &= a^u (x^n)^v \\ \Leftrightarrow x &= a^u \text{ car } \#G = n \end{aligned}$$

Donc, pour tout entier relatif m premier à $\#G$, et $a \in G$, l'équation

$x^m = a$ possède une unique solution.

Exercice 7.

Montrons que $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq S_3$.

Soit $\varphi \in \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

φ envoie l'élément neutre $(\bar{0}; \bar{0})$ sur lui même et permute les 3 éléments d'ordre 2.

Montrons que l'application :

$$\begin{aligned} \chi : \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) &\longrightarrow S_3 \\ \varphi &\longmapsto \varphi|_3 \text{ éléments d'ordre 2} \end{aligned}$$

est un automorphisme.

- χ est un morphisme par construction.
- Tout φ étant déterminé par sa restriction aux 3 éléments d'ordre 2 de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donc χ est injectif.
- Le nombre d'éléments de $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ correspond au nombre de bases de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ -espace vectoriel.
En effet, tout automorphisme linéaire pour le $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, est un automorphisme de groupe.
Or, pour construire une base, on a 3 choix pour le premier vecteur, deux choix pour le deuxième, et plus qu'un choix pour le troisième vecteur.
Donc $\#\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \#(\text{bases de } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = 3 \times 2 \times 1 = 6$.
Donc χ est surjectif.

CQFD.

Exercice 8.

- a.** Montrons que $\Gamma_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$
est un sous-groupe de $(GL_2(\mathbb{R}), \times)$.

En notant $\Gamma_1 = \{a, b, c, d\}$, muni de la multiplication des matrices, on vérifie que :

- a est le neutre et est son propre inverse
- b est d'ordre 4, $b^{-1} = d$ et $b^2 = c$
- c est d'ordre 2 et $c^{-1} = c$
- Γ_1 est commutatif

Γ_1 est donc bien un sous-groupe de $GL_2(\mathbb{R})$, un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$

L'isomorphisme s'exhibe aisément : a est envoyé sur $\bar{0}$, b sur $\bar{1}$, c sur $\bar{2}$ et d sur $\bar{3}$.

- b.** Montrons que $\Gamma_2 = \{1, i, -1, -i\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

— $i^2 = -1 \in \Gamma_2$ et $i^4 = 1 \in \Gamma_2 : i$ est d'ordre 4.

Γ_2 est cyclique donc commutatif.

— $-i$ est l'autre générateur de $\Gamma_2 \simeq \mathbb{Z}/4\mathbb{Z}$.

c. Montrons que $\Gamma_3 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ est un sous-groupe pour la multiplication, du corps $(\mathbb{Z}/5\mathbb{Z}, +, \times)$.

— $\bar{2}$ et $\bar{3}$ sont d'ordre 4 : $(\Gamma_3, \times)$ est cyclique donc commutatif.

Ce sont les deux générateurs de $(\Gamma_3, \times) \simeq (\mathbb{Z}/4\mathbb{Z}, +)$.

— $(\bar{4})^2 = \bar{16} = \bar{1}$ donc $\bar{4}$ est d'ordre 2

— $\bar{1}$ est le neutre.

En fait, $\Gamma_3 = (\mathbb{Z}/5\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z}, +)$ et on peut exhiber un isomorphisme :

$$\begin{array}{ccc} (\mathbb{Z}/5\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ \bar{1} & \longmapsto & \bar{0} \\ \bar{2} & \longmapsto & \bar{1} \text{ ou } \bar{3} \\ \bar{3} & \longmapsto & \bar{3} \text{ ou } \bar{1} \\ \bar{4} & \longmapsto & \bar{2} \end{array}$$

d. Montrons que $\Gamma_1, \Gamma_2, \Gamma_3$ sont trois groupes isomorphes.

Vu aux questions précédentes : $\Gamma_1 \simeq \Gamma_2 \simeq \Gamma_3 \simeq \mathbb{Z}/4\mathbb{Z}$.

Exercice 9.

Soit $f : G \longrightarrow H$ un morphisme de groupes finis, et soit G' un sous-groupe de G .

a. Montrons que l'ordre de $f(G')$ divise à la fois l'ordre de H et l'ordre de G' .

$f(G')$ est un sous-groupe de H , donc $o(f(G')) \mid o(H)$.

De plus, $G'/\text{Ker } f \simeq f(G')$ donc $o(f(G')) \mid o(G')$ ($f|_{G'}$ est un morphisme).

b. Déduisons en que si l'ordre de G' est premier à l'ordre de H , $G' \subset \text{Ker } f$.

$o(f(G'))$ divise $o(H)$ et $o(G')$ donc divise leur *pgcd*.

Donc si $o(H)$ et $o(G')$ sont premiers entre eux, $o(f(G'))=1$ ce qui veut dire que $f(G') = e$ et donc que $G' \subset \text{Ker } f$.

Exercice 10.

Montrons que dans un groupe d'ordre 35, il existe un élément d'ordre 5, et un élément d'ordre 7.

Soit G un groupe d'ordre 35.

Les éléments différents du neutre e sont d'ordre 5, 7 ou 35 (Théorème de Lagrange).

— Si G est cyclique, et g un générateur, on a $g^{35} = e$ et donc g^5 est d'ordre 7 et g^7 est d'ordre 5.

- Si G est non cyclique, et ne possède pas d'élément d'ordre 7, alors G est réunion de ses sous-groupes d'ordre 5.
Mais de tels sous-groupes sont soit égaux soit d'intersection égale à e (car 5 est premier).
D'où l'existence d'un entier n tel que $35 = 4n + 1$. Contradiction. (34 n'est pas divisible par 4) Le groupe G possède donc un élément d'ordre 7.
- Si G est non cyclique, et ne possède pas d'élément d'ordre 5, on applique le même raisonnement pour aboutir à une contradiction.

Exercice 11.

Soit G un groupe d'ordre $2p$ avec p un nombre premier.

Montrons qu'il existe un élément d'ordre 2, et un élément d'ordre p .

1. Si $p = 2$, $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ ou $G \simeq (\mathbb{Z}/4\mathbb{Z})$.
Dans le premier cas, $(1; 0)$ (par exemple) est d'ordre 2, et dans le second cas, $\bar{2}$ est d'ordre 2.
2. Supposons p impair. Les éléments différents du neutre dans G sont alors d'ordre 2 ou p .
 - Si G est cyclique avec g un générateur. On a $g^{2p} = e$, et donc g^2 est d'ordre p et g^p est d'ordre 2.
 - Si G est non cyclique et ne possède pas d'élément d'ordre 2, alors on a :
 $2p = (p - 1) \times k + 1$ et donc $2p - 1 = k(p - 1)$
Mais $2p - 1$ est impair, et $k(p - 1)$ est pair.
Il y a contradiction, et il existe donc un élément d'ordre 2.
 - Si G ne contient que des éléments d'ordre 2 (excepté e), on a alors, d'après l'exercice 4, $\#G = 2^n$.
D'où une contradiction car $\#G = 2p$ avec p impair.
Il existe donc un élément d'ordre p .