Groupes | 1

Compétences

On cherchera dans ce chapitre à :

- ▷ Savoir utiliser et mettre en œuvre les notions générales de groupe, sous-groupe, etc.

  Exercices 1 à 18.
- ▷ Savoir travailler avec des morphismes de groupes.

  Exercices 5 à 10.
- ▷ Savoir reconnaître et décrire les sous-groupe engendré par un élément, identifier les groupes monogènes, en particulier les groupes cycliques.

  Exercices 15 à 18.
- ▷ Savoir calculer ou exploiter l'ordre d'un élément donné d'un groupe.

  Exercices 3, 4, 11 à 14.

Coup d'œil sur le chapitre

Il faut lire attentivement les énoncés. Un groupe « général » n'est, en effet, ni commutatif, ni fini.

Pour un groupe, le fait d'être fini (cas des exercices 11 à 14) est une propriété importante. Elle entraîne en particulier que tout élément a un ordre fini, qui divise le cardinal du groupe.

Un mot sur la propriété de commutativité, qui concerne les notations : l'emploi de la notation additive est réservé aux groupes commutatifs. L'usage de la notation additive est tout à fait minoritaire dans le présent chapitre.

Certains groupes commutatifs le sont car ils sont engendrés par un élément : on dit alors qu'ils sont *monogènes*. Notons que dans ce cas il n'y a pas, en général, unicité d'un tel élément générateur du groupe. Il faut aussi observer que la réciproque est fausse : il existe des groupes commutatifs non monogènes (penser, par exemple, au groupe additif d'un espace vectoriel réel de dimension 2).

Un groupe à la fois monogène et fini est dit *cyclique*. Un groupe de cardinal n est cyclique si, et seulement si, il est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$: c'est un résultat important, qui sert souvent, parce que $\mathbb{Z}/n\mathbb{Z}$ est un objet bien connu, ne serait-ce que parce qu'il appartient, aussi, à l'arithmétique.

Le saviez-vous ?

Plusieurs branches des mathématiques font appel à la notion de groupe. Au début du XIX^e siècle, Galois l'utilise pour établir la non résolubilité de certaines équations algébriques ; en 1872, Klein lance un programme visant à classifier les géométries grâce aux groupes. Le concept général de groupe abstrait finit par émerger à la fin du XIX^e siècle.

En 1963, Feit et Thompson publient la démonstration de leur célèbre théorème qui dit que tout groupe fini de cardinal impair est résoluble. Celle-ci occupe plus de 250 pages dans le *Pacific Journal of Mathematics*...

Énoncés des exercices

Sauf mention expresse du contraire, un groupe G est noté multiplicativement et son neutre est noté e.

Généralités

Exercice 1.

Montrer que pour tout groupe G,

$$\forall n \in \mathbb{N}^*,\ \forall (x_1, ..., x_n) \in G^n,\ (x_1 ... x_n)^{-1} = x_n^{-1} \dots x_1^{-1}.$$

Exercice 2.

Soit G un groupe multiplicatif et H une partie finie de G non vide, stable par multiplication. Montrer que H est un sous-groupe de G.

Exercice 3.

Soit G un groupe. Soit $(a, b) \in G^2$. Montrer que si a, b et ab sont d'ordre 2, alors $ab = ba$.

Exercice 4.

Soit G un groupe multiplicatif. Soit $g \in G$ un élément d'ordre pq avec $p \wedge q = 1$. Montrer qu'il existe un unique couple (x, y) d'éléments de G tel que : x est d'ordre p, y est d'ordre q et $g = xy = yx$.

Morphismes de groupes

Exercice 5.

Soit G un groupe additif et $f : G \to G'$ un morphisme de groupes.

1. Montrer que, pour tout sous-groupe H de G, on a : $f^{-1}(f(H)) = H + \operatorname{Ker} f$.
2. Montrer que pour tout sous-groupe H' de G' on a : $f(f^{-1}(H')) = H' \cap \operatorname{Im} f$.

Exercice 6. $(\star)$

Soit G un groupe. On note $Z(G) = \{a \in G \ / \ \forall b \in G,\ ab = ba\}$. On suppose que $x \longmapsto x^n$ est un automorphisme de G. Montrer que :

$$\text{pour tout } x \in G,\ x^{n-1} \in Z(G).$$

Exercice 7.

Montrer que tout homomorphisme de groupes de $(\mathbb{Q}, +)$ vers $(\mathbb{Z}, +)$ est identiquement nul.

Exercice 8. ($\star$)

Soit f un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$, c'est-à-dire une application de $\mathbb{R}$ dans $\mathbb{C}^*$ telle que :

$$\forall (x, y) \in \mathbb{R}^2,\ f(x + y) = f(x)f(y).$$

1. Si f est dérivable, montrer qu'il existe $\lambda \in \mathbb{C}$ tel que : $\forall x \in \mathbb{R},\ f(x) = e^{\lambda x}$.
2. Établir le même résultat si f est seulement supposée continue.

Exercice 9. ($\star$)

Soit G un groupe fini, G' un groupe, f un morphsime de G dans G'. Montrer que :

$$\operatorname{card}(\operatorname{Ker} f)\ \operatorname{card}(\operatorname{Im} f) = \operatorname{card}(G).$$

Exercice 10.

Soit G un groupe fini, H et K deux sous-groupes de G. On considère l'application :

$$\phi : H \times K \to G, (h, k) \mapsto hk.$$

1. Donner une condition nécessaire et suffisante portant sur H et K pour que ϕ soit un morphisme de groupes.
2. On note $HK = \phi(H \times K)$. Soit $g_0 \in HK$. Il existe $(h_0, k_0) \in H \times K$ tel que $g_0 = h_0 k_0$. Montrer que les antécédents de g_0 par ϕ sont les couples $(h_0 x, x^{-1} k_0)$, $x \in H \cap K$.
3. En déduire que : $\operatorname{card}(HK)\ \operatorname{card}(H \cap K) = \operatorname{card}(H)\ \operatorname{card}(K)$.
4. Montrer que les conditions suivantes sont équivalentes :
   a) HK est un sous-groupe de G ;
   b) $HK \subseteq KH$;
   c) $HK = KH$.

Groupes finis

Exercice 11.

Soit G un groupe fini. Montrer qu'il existe un entier N tel que $x^N = e$ pour tout x dans G.

Exercice 12.

1. Soit G un groupe fini de cardinal impair. Montrer que pour chaque $a \in G$, il existe un unique $b \in G$ tel que $b^2 = a$.
2. Soit G un groupe fini et m un entier premier avec $\operatorname{card}(G)$. Montrer que : $\forall x \in G,\ \exists!\ y \in G$ tq $x = y^m$.

Exercice 13.

1. Soit G un groupe fini de cardinal impair. Montrer que l'application $x \longmapsto x^2$ est bijective.
2. Soit G un groupe fini. On note A l'ensemble des éléments d'ordre impair de G. Montrer que l'application $x \longmapsto x^2$ est une permutation de A.

Exercice 14.

Soit G un groupe commutatif fini de cardinal $n = ab$ avec $a \wedge b = 1$.
On pose $A = \{x \in G \ / \ x^a = e\}$ et $B = \{x \in G \ / \ x^b = e\}$.

1. Montrer que A et B sont des sous-groupes de G.
2. Montrer que $A \cap B = \{e\}$ et $AB = G$.

Groupes cycliques

Exercice 15.

Un groupe G est *cyclique* lorsque G est fini et il existe un élément a de G tel que $\forall x \in G,\ \exists k \in \mathbb{N} \,/\, x = a^k$.
Montrer qu'un sous-groupe d'un groupe cyclique est lui-même cyclique.

Exercice 16.

Soit G un groupe non réduit à $\{e\}$ n'ayant pas de sous-groupe non trivial. Montrer que G est monogène, fini, et que $\mathrm{card}(G)$ est un nombre premier.

Exercice 17. ($\star\star$) *Groupes abéliens simples*

Soit $(G, +)$ un groupe abélien. On dit que G est *simple* lorsque G n'est pas réduit à $\{0\}$ et G ne possède aucun autre sous-groupe que $\{0\}$ et G.

1. Montrer que si p est premier, $(\mathbb{Z}/p\mathbb{Z}, +)$ est simple.
2. Montrer que les deux conditions suivantes sont équivalentes :
   a) G est abélien et simple ;
   b) G est cyclique de cardinal premier.

Exercice 18.

Soit $n \in \mathbb{N}^* \setminus \{1\}$. On considère le groupe $\mathbb{Z}/n\mathbb{Z}$ additif. Soit $k \in \mathbb{Z}$ et $d = k \wedge n$.

1. Déterminer l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
3. Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?

Un petit coup de pouce

Ex. 1. On pourra procéder par récurrence sur n.

Ex. 2. $\alpha_x : \mathbb{N}^* \to G, k \mapsto x^k$ n'est pas injective.

Ex. 3. Considérer $(ab)^{-1} = b^{-1}a^{-1}$.

Ex. 4. Utiliser le théorème de Bezout.

Ex. 5. On rappelle que, pour $Y \in \mathcal{P}(G')$, $f^{-1}(Y) = \{x \in G \ f(x) \in Y\}$.

Ex. 6. Observer que $(xy)^n$ est égal à $x(yx)^{n-1}y$.

Ex. 7. Observer que : $\forall q \in \mathbb{N}^*$, $\forall r \in \mathbb{Q}$, $f(qr) = qf(r)$.

Ex. 8. 2. Si f est seulement supposée continue, prendre une primitive, F, de f, et montrer que F est de classe $\mathcal{C}^1$.

Ex. 9. Pour chaque $y \in G'$, considérer $f^{-1}(y) = \{x \in G \ / \ f(x) = y\}$. Observer que $\left(f^{-1}(y)\right)_{y \in G'}$ est une partition de G, et que pour $y \in \operatorname{Im} f$, $f^{-1}(y)$ est en bijection avec $\operatorname{Ker} f$.

Ex. 10. 1. ϕ est un morphisme de groupes si, et seulement si, tout élément de H commute avec tout élément de K.

3. Observer que $\left(\phi^{-1}(g)\right)_{g \in G}$ est une partition de $H \times K$

4. On pourra établir : c) $\Rightarrow$ a), a) $\Rightarrow$ b), b) $\Rightarrow$ c).

Ex. 11. Montrer d'abord que pour chaque $g_i \in G$, il existe $k_i \in \mathbb{N}^*$ tel que $g_i^{k_i} = e$, en observant que l'application de $\mathbb{Z}$ dans G qui à k associe g_i^k n'est pas injective.

Ex. 12. Remarquer que seule la seconde question est à traiter. On pourra utiliser le théorème de Bezout.

Ex. 13. 1. Tout élément d'un groupe fini est d'ordre fini et son ordre divise le cardinal du groupe.

2. On pourra montrer que $x \mapsto x^2$ est une application de A dans A, et qu'elle est surjective.

Ex. 14. 2. On pourra utiliser le théorème de Bezout. Celui-ci montre qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $ua + vb = 1$.

Ex. 15. Notant $n = \operatorname{card}(G)$, on montrera d'abord que pour chaque $x \in G$, il existe un unique $k \in [\![1, n]\!]$ tel que $x = a^k$. Si H est un sous-groupe de G, on pourra considérer $\min\left(\{i \in [\![1, n]\!] \ / \ a^i \in H\}\right)$.

Ex. 16. Considérer le sous-groupe engendré par un élément différent du neutre.

Ex. 17. 2. Pour prouver a) $\Rightarrow$ b), on pourra utiliser la question précédente ; et pour montrer b) $\Rightarrow$ a), on pourra utiliser l'exercice précédent.

Ex. 18. 1. Considérer les quotients respectifs n' et k' de n et k par d. L'ordre cherché est n'.

2. On pourra procéder par double inclusion.

3. Ce sont les $\langle \overline{d} \rangle$, pour d diviseur de n.

Solutions

Exercice 1.

Soit $(a, b) \in G^2$.
Alors, par associativité,
$(b^{-1}a^{-1})(ab) = b^{-1}\big(a^{-1}a\big)b = b^{-1}eb = b^{-1}b = e$.
Donc : $(ab)^{-1} = b^{-1}a^{-1}$.
En utilisant cette propriété et l'associativité, on montre aisément par récurrence sur $n \in \mathbb{N}^*$ la propriété

$$I(n)=[\forall (x_1, ..., x_n) \in G^n,\ (x_1...x_n)^{-1} = x_n^{-1}...x_1^{-1}].$$

Exercice 2.

Soit $x \in H$.
Considérons l'application α_x de $\mathbb{N}^*$ dans G définie par :
$\forall k \in \mathbb{N}^*$, $\alpha_x(k) = x^k$.
Comme H est stable, une récurrence aisée prouve que :
pour tout $k \in \mathbb{N}^*$, $\alpha_x(k) \in H$.
Donc $\alpha_x(\mathbb{N}^*)$ est inclus dans H, donc, comme H est fini, l'application α_x n'est pas injective, et il existe deux entiers naturels non nuls p et q tels que :
$p < q$ et $\alpha_x(p) = \alpha_x(q)$ soit $x^p = x^q$.
Il vient : $e = x^q(x^p)^{-1} = x^{q-p}$, donc $x^{-1} = x^{q-p-1}$.
Si $q = p + 1$ alors $x = e$, donc $x^{-1} = e = x$.
Si $q > p + 1$, alors $q - p - 1 \in \mathbb{N}^*$, donc $x^{q-p-1} = \alpha_x(q - p - 1) \in H$.
Dans les deux cas, $x^{-1} \in H$.
Ainsi : pour tout $x \in H$, $x^{-1} \in H$.
Prenons un élément fixé h de H, alors $h^{-1} \in H$ vu ce qui précède, donc, comme H est stable, $e = hh^{-1} \in H$.
Récapitulons : H contient e, est stable et vérifie : pour tout $x \in H$, $x^{-1} \in H$.
Ainsi H est un sous-groupe de G.

Exercice 3.

Rappelons que si un élément x est d'ordre 2, alors il vérifie : $x^2 = e$, soit : $x = x^{-1}$.
Il vient : $ab = (ab)^{-1}$, $a = a^{-1}$ et $b = b^{-1}$.
Or : $(ab)^{-1} = b^{-1}a^{-1}$.
Donc : $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Exercice 4.

p et q sont premiers entre eux donc, d'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $pu + qv = 1$.

• *Unicité* : Supposons que $(x, y) \in G^2$ vérifie : x est d'ordre p, y est d'ordre q, et $g = xy = yx$.

Comme x et y commutent entre eux, on a : pour tout $k \in \mathbb{Z}$, $g^k = x^k y^k$.

Alors : $g^p = (xy)^p = x^p y^p = ey^p = y^p$.

Puis : $g^{pu} = (g^p)^u = (y^p)^u = y^{pu} = y^{1-qv}$.

Or $y^{1-qv} = y(y^q)^{-v} = ye^{-v} = y = y$.

Donc $y = g^{pu}$.

De même, échangeant les rôles de (x, p, u) et (y, q, v), on obtient : $x = g^{qv}$.

• *Existence* : Posons $x = g^{qv}$ et $y = g^{pu}$.

Alors $xy = yx = g^{pu+qv} = g^1 = g$, et :

pour tout $k \in \mathbb{Z}$, $x^k = (g^{qv})^k = g^{qvk}$,

donc, puisque g est d'ordre pq :

$x^k = e \Leftrightarrow g^{qvk} = e \Leftrightarrow pq | qvk \Leftrightarrow p | vk$.

Or, comme $pu + qv = 1$, p et v sont premiers entre eux, donc : p divise vk si, et seulement si, p divise k.

Ainsi : $x^k = e \Leftrightarrow p | k$. Donc x est d'ordre p.

De même, échangeant les rôles de (x, p, u) et (y, q, v), on voit que y est d'ordre q.

En conclusion, il existe un unique $(x, y) \in G^2$ tel que x est d'ordre p, y est d'ordre q, et $g = xy = yx$.

Exercice 5.

1. Soit H un sous-groupe de G. Alors, pour $x \in G$:

$$\begin{aligned} x \in f^{-1}(f(H)) &\Leftrightarrow f(x) \in H \Leftrightarrow (\exists h \in H \ / \ f(x) = f(h)) \\ &\Leftrightarrow (\exists h \in H \ / \ f(x - h) = e_{G'}) \Leftrightarrow (\exists h \in H \ / \ x - h \in \operatorname{Ker} f) \\ &\Leftrightarrow x \in H + \operatorname{Ker} f \ . \end{aligned}$$

2. Soit H' un sous-groupe de G'.

– Évidemment $f(f^{-1}(H'))$ est inclus dans $f(G) = \operatorname{Im} f$.

Par définition, $f^{-1}(H') = \{x \in G \ / \ f(x) \in H'\}$, donc $f(f^{-1}(H'))$ est inclus dans H'.

Ainsi $f(f^{-1}(H')) \subseteq H' \cap \operatorname{Im} f$.

– Réciproquement soit $y \in H' \cap \operatorname{Im} f$.

Alors comme $y \in \operatorname{Im} f$, il existe $x \in G$ tel que $y = f(x)$. Cet élément x vérifie $f(x) = y \in H'$, donc : $x \in f^{-1}(H')$. Donc $y \in f(f^{-1}(H'))$.

En conclusion : $f(f^{-1}(H')) = H' \cap \operatorname{Im} f$.

Exercice 6.

Soit $(x, y) \in G^2$.

Remarquons que $(xy)^n$ est égal à $x(yx)^{n-1}y$.

Or l'hypothèse faite entraîne : $x^n y^n = (xy)^n$.