Arithmétique
FICHE II: Groupes quotients, groupes cycliques et théorème de Lagrange

---

Exercice 1. Dans les ensembles munis de lois suivants, déterminer si c'est un groupe, et si oui, préciser son élément neutre et s'il est commutatif.

(1) $\mathbb{N}$ muni de l'addition ;
(2) $\mathbb{Z}$ muni de l'addition ;
(3) $\mathbb{R}$ (ou $\mathbb{C}$) muni de l'addition ;
(4) $\mathbb{R}$ (ou $\mathbb{C}$) muni de la multiplication ;
(5) $\mathbb{R}^*$ (ou $\mathbb{C}^*$) muni de la multiplication ;
(6) L'ensemble des matrices carrées de taille n muni de l'addition ;
(7) L'ensemble des matrices carrées de taille n muni de la multiplication ;
(8) L'ensemble des matrices carrées inversibles de taille n muni de la multiplication.
(9) $\mathcal{S}_n$, les permutations de $\{1, 2, \dots, n\}$ muni de la composition.
(10) L'ensemble des applications linéaires $\mathbb{R}^2 \to \mathbb{R}^2$ qui envoient le carré de sommets $\{(\pm 1, \pm 1)\}$ bijectivement sur lui-même.

Exercice 2. Montrer que tout groupe de cardinal au plus 5 est abélien. Trouver tous ces groupes, à isomorphisme près. On pourra distinguer les cardinaux 1, 2, 3 et 5 du cardinal 4. Que se passe-t-il pour le cardinal 6 (quels groupes de cardinal 6 connaissez-vous) ?

Exercice 3. Dans le groupe symétrique $\mathcal{S}_3$, trouver le sous-groupe engendré par chacun des ensembles suivants :

— $\{(1, 2)\}$
— $\{(1, 2, 3)\}$
— $\{(1, 2), (2, 3)\}$
— $\{(1, 2), (1, 2, 3)\}$

Exercice 4. Trouver tous les sous-groupes normaux du groupe symétrique $\mathcal{S}_3$. En particulier, retenir un exemple de sous-groupe qui n'est pas normal.

Exercice 5. Trouver tous les sous-groupes additifs de $\mathbb{Z}/7\mathbb{Z}$. De même avec $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 6. Soient $m, n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $\mathrm{pgcd}(m, n) = 1$.

Exercice 7. On considère un nombre entier $n \geq 1$ et le groupe linéaire $\mathrm{GL}_n(\mathbb{R})$, c'est-à-die le groupe des matrices carrées inversibles de taille n, à coefficients dans $\mathbb{R}$, muni de la multiplication.

(1) Quel est l'élément neutre de ce groupe ?

(2) Ce groupe est-il commutatif ?

(3) Si $A \in \mathrm{GL}_n$, à quelle condition sur le polynôme minimal (ou caractéristique) de A le sous-groupe engendré par A est-il fini ?

Exercice 8. Montrer que si H est un sous-groupe de G et que G/H est de cardinal 2, alors H est normal.

Exercice 9. Soit $f : G \to H$ un morphisme de groupes finis, et soit G' un sous-groupe de G. Montrer que $\#f(G')$ divise $\#G'$ et $\#H$.

Exercice 10. Soient H et K deux sous-groupes d'un groupe G avec H normal, $\#H$ et $\#(G/H)$ premiers entre eux et $\#H = \#K$. Montrer que $H = K$.

Exercice 11. Soit G un groupe abélien fini, tout de même noté multiplicativement pour une fois.

(1) Soient $g \in G$ d'ordre m et $h \in G$ d'ordre n. Montrer que l'ordre de gh divise $\mathrm{ppcm}(m, n)$.

(2) Donner un exemple où il y a égalité, et un exemple où il n'y a pas égalité.

(3) Montrer que si $\mathrm{pgcd}(m, n) = 1$, alors l'ordre de gh est mn.

(4) Montrer que si G possède deux élément d'ordre m et n, il possède un élément d'ordre $\mathrm{ppcm}(m, n)$.

(5) Montrer qu'il existe $g \in G$ et $d \in \mathbb{N}^*$ tels que g soit d'ordre d et $h^d = 1$ pour tout $h \in G$.

Exercice 12. Soit p un nombre premier. On considère le corps $\mathbb{Z}/p\mathbb{Z}$, et son groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$.

(1) Quel est son cardinal ?

(2) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. On pourra pour cela trouver un g et un d comme dans le point (5) de l'exercice 11 et montrer que $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$, en s'appuyant sur le fait que le polynôme $X^{p-1} - 1$ a au plus $p - 1$ racines dans $\mathbb{Z}/p\mathbb{Z}$.

(En fait, ce raisonnement montre plus généralement que tout sous-groupe fini du groupe des éléments inversible d'un corps quelconque est cyclique.)

Exercice 13. Soit $n \in \mathbb{N}^*$. On note μ_n l'ensemble des racines n-ièmes de 1 dans $\mathbb{C}$.

(1) Montrer c'est un sous-groupe de $\mathbb{C}^\times$, et qu'il est cyclique.

Soit $\xi \in \mu_n$. On dit que ξ est une racine *primitive* de l'unité si $\langle \xi \rangle = \mu_n$. On note μ_n^{prim} l'ensemble des racines primitives n-ièmes de l'unité.

(2) Montrer que si ξ est primitive, alors $\zeta = \xi^m$ est également primitive si et seulement si $\mathrm{pgcd}(m, n) = 1$.

(3) Calculer $\#\mu_n^{\text{prim}}$ en utilisant la fonction indicatrice d'Euler ϕ.

(4) Montrer que si $\xi \in \mu_n$, alors il existe un unique d tel que $d|n$ et $\xi \in \mu_d$ est une racine primitive d-ième.

(5) En déduire que $\mu_n = \bigsqcup_{d|n} \mu_d^{\text{prim}}$ (union disjointe).

(6) En déduire une preuve de la formule $n = \sum_{d|n} \phi(d)$.