10 Groupes

I. Groupes

Groupes et sous-groupes

Définition 19 *(Groupe)*

Ensemble G muni d'une loi de composition interne $*$:
- → (associative) $a*(b*c)=(a*b)*c$,
- → (élément neutre) $\exists e\in G$, $\forall g\in G$, $g*e=e*g=g$,
- → (symétrique) $\forall g\in G$, $\exists g'\in G$ tel que $g*g'=g'*g=e$ (g' noté g^{-1})

On a
- → G est commutatif (ou abélien) lorsque $g*g'=g'*g$ pour tout $g,g'\in G$.
- → G est fini lorsqu'il a un nombre fini d'éléments. On appelle alors *ordre* de G son nombre d'éléments.

Définition 20 *(Sous-groupes)*

$H\subset G$ est un sous-groupe de G lorsque H est non vide, que la loi est stable dans H et que $(H,*)$ a une structure de groupe. En pratique :
- → H est non vide
- → pour tout $g,h\in H$, $g*h\in H$ et $g^{-1}\in H$ (ou simplement $g*h^{-1}\in H$).

L'essentiel - Groupes et sous-groupes

- → calculs : unicité de l'élément neutre, de l'inverse
- → si $a\in G$, l'application « de translation à gauche » $g\mapsto a*g$ (ou « à droite » $g\mapsto g*a$) est une bijection de G sur G (lorsque g décrit G entièrement, les éléments $a*g$ redécrivent - d'une autre manière - tous les éléments de G (une et une seule fois).
- → Opérations sur les groupes/sous-groupes (et construction) : structure de groupe sur un produit fini de groupes, intersection de sous-groupes de G, sous-groupe engendré par une partie de G.
- → G est un sous-groupe de $(\mathbb{Z},+)$ si et seulement si il existe $n\in\mathbb{Z}$ tel que $G=n\mathbb{Z}$.

Morphismes de groupes

L'essentiel - Morphismes

- → définition d'une morphisme entre les groupes $(G,*)$ et $(G',*')$, isomorphismes, automorphismes.
- → propriétés : $f(e_G)=e_{G'}$ et $f(g^{-1})=(f(g))^{-1}$.
- → **image et noyau** de $f:G\to G'$ un morphisme de groupes. $\operatorname{Im} f$ et $\ker f$ sont des sous-groupes respectivement de G' et G. Plus généralement l'image directe d'un sous-groupe de G est un sous-groupe de G' et l'image réciproque d'un sous-groupe de G' est un sous-groupe de G.

II. Groupes monogènes, cycliques

L'essentiel - Groupes monogènes

Soit $(G,*)$ un groupe.
- → On définit $H=<x>=\{x^k, k\in\mathbb{Z}\}$. L'application $k\in\mathbb{Z}\mapsto x^k$ est soit injective, soit de noyau $n\mathbb{Z}$ où $n\in\mathbb{N}^*$. Il y a alors un isomorphisme entre H et $\mathbb{Z}/n\mathbb{Z}$ (si H cyclique d'ordre n) ou $\mathbb{Z}$. On appelle *ordre* de x l'ordre du sous-groupe $<x>$ s'il est fini.
- → Si x est d'ordre d, alors $<x>=\left\{1,x,x^2,\dots,x^{d-1}\right\}$.
- → si x est d'ordre d, alors on a $x^n=e$ si et seulement si $d|n$.
- → théorème de Lagrange : si G est un groupe fini
  - l'ordre d'un sous-groupe divise l'ordre du groupe (hors prog),
  - l'ordre d'un élément divise l'ordre du groupe.

III. EXERCICES

Exercice 1

Montrer qu'un isomorphisme de groupes conserve l'ordre des éléments.

Exercice 2

Les groupes $(\mathbb{Z}/8\mathbb{Z},+)$ et $(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}/4\mathbb{Z},+)$ sont-ils isomorphes ?

Exercice 3

Pour $\theta\in\mathbb{R}$, on note $A(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$ et $B(\theta)=\begin{pmatrix}\mathrm{ch}\,\theta & \mathrm{sh}\,\theta\\ \mathrm{sh}\,\theta & \mathrm{ch}\,\theta\end{pmatrix}$. On définit $G=\{A(\theta),\theta\in\mathbb{R}\}$ et $H=\{B(\theta),\theta\in\mathbb{R}\}$.

1. Vérifier que G et H sont deux sous-groupes de $GL_2(\mathbb{R})$.
2. Résoudre l'équation $X^2=I_2$ dans G et H. Les deux sous-groupes sont-ils isomorphes ?

Exercice 4

Soit G un groupe abélien d'ordre n, et k un entier naturel non nul premier avec n. Montrer que l'application $f:x\mapsto x^k$ est un automorphisme de G, et expliciter sa réciproque.

Exercice 5

Soit G un groupe commutatif, x et y deux éléments de G d'ordre respectif p et q avec $p\wedge q=1$. Déterminer l'ordre de xy.

Exercice 6 ☆

Soient G un groupe abélien, x et y deux éléments de G d'ordres respectifs p et q. Démontrer qu'il existe un élément de G d'ordre $\mathrm{PPCM}(p,q)$.

Exercice 7

Soit G un groupe cyclique. Montrer que tout sous-groupe de G est cyclique.

Exercice 8

Soit G un groupe possédant un nombre fini de sous-groupes. Démontrer que G est fini.

Exercice 9

Soient G et H des groupes finis.

1. Soit f un morphisme de G dans H. Montrer que la relation $x\mathcal{R}y$ lorsque $f(x)=f(y)$ définit une relation d'équivalence sur G. Combien y-a-t-il de classes d'équivalences ? On pourra utiliser l'application suivante, après avoir justifié qu'elle existe :
$$\tilde{f}:\bar{x}\in G/\mathcal{R}\mapsto f(x)\in \mathrm{Im}\, f.$$
2. En déduire $|G|=|\mathrm{Im}\, f|.|\ker f|$.
3. Soit f un morphisme de groupes de G dans lui-même. Montrer que $\ker f=\ker f^2\Leftrightarrow \mathrm{Im}\, f=\mathrm{Im}\, f^2$.

Exercice 10

Soit $G=\{x+\sqrt{2}y, x\in\mathbb{N}^*, y\in\mathbb{Z} \text{ et } x^2-2y^2=1\}$.

1. Vérifier que $G\subset\mathbb{R}_+^*$.
2. Montrer que G est un sous-groupe de $(\mathbb{R}_+^*,\times)$. Quel est le symétrique de $x+y\sqrt{2}$?
3. Soit $x+y\sqrt{2}\in G$ avec $y\in\mathbb{N}^*$. Vérifier que $x-y\sqrt{2}\in]0,1[$.
4. Montrer qu'il existe un plus petit élément g_0 dans $G\cap]1,+\infty[$ et le déterminer.
5. Montrer que $G=\{g_0^n, n\in\mathbb{Z}\}$. Qu'a-t-on prouvé ?

Exercice 11 ☆

Soit G un groupe fini tel que, pour tout $g \in G, g^2 = e$ (ou e est l'élément neutre de G). On suppose que $G \neq \{e\}$.

1. Montrer que G est commutatif.
2. Soit $a \neq e$ dans G. Montrer que $\{e, a\}$ est un sous-groupe de G. En déduire que G est d'ordre pair.
3. Soit H un sous-groupe strict de G et $a \notin H$. Montrer que $H \cup aH$ est un sous-groupe de G d'ordre $2\operatorname{card} H$.
4. Prouver que $\operatorname{card} G$ est une puissance de 2.
5. Soit G un groupe d'ordre $2p$ avec p premier. Montrer qu'il existe un élément d'ordre p.

Exercice 12 ***(Mines MP 2013)***

Soit $(G, \cdot)$ un groupe de neutre noté e. Soient H et K deux sous-groupes de G. On note $HK = \{hk, h \in H, k \in K\}$.

1. Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$.
2. On définit $f : (h, k) \in H \times K \mapsto hk \in HK$. Donner une condition nécessaire et suffisante pour que f soit un morphisme de groupes. Dans ce cas, montrer que f est injective si et seulement si $H \cap K = \{e\}$.

Exercice 13

Soit G un groupe cyclique engendré par a, de cardinal n.

1. Montrer que tout sous-groupe de G est cyclique, de cardinal divisant n.
2. Soit d un diviseur de n. Montrer que G possède un unique sous-groupe de cardinal d.
3. Démontrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d. En déduire $n = \sum_{d|n} \varphi(d)$.

Exercice 14 ☆

Soit p un nombre premier. On pose $G_p = \{z \in \mathbb{C} \mid \exists k \in \mathbb{N}, z^{p^k} = 1\}$.

1. Montrer que G_p est un sous-groupe multiplicatif de $\mathbb{C}^*$.
2. Montrer que les sous-groupes propres de G_p sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion.
3. Montrer que G_p n'est pas engendré par un nombre fini d'éléments.

EXERCICES EN VRAC

Exercice 15 ***(Mines MP 2019)***

Soit $n \in \mathbb{N}^*$. Déterminer les morphismes de $(\mathscr{S}_n, \circ)$ dans $\left(\mathbb{C}^*, \times\right)$.

Exercice 16 ***(Centrale MP 2021)***

Soit G un groupe. On note $\widehat{G}$ l'ensemble des morphismes de groupes de G dans $\left(\mathbb{C}^*, \times\right)$.

1. Rappeler les définitions d'un groupe et d'un morphisme de groupes. Montrer que $\widehat{G}$ est une groupe.
2. Déterminer $\widehat{G}$ dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$.

Exercice 17 ***(ENS MP 2022)***

Si G est un groupe, on note $\operatorname{sub}(G)$ l'ensemble des sous-groupes de G. Soit G, H deux groupes finis de cardinaux premiers entre eux.
Montrer que $|\operatorname{sub}(G \times H)| = |\operatorname{sub}(G)| \times |\operatorname{sub}(H)|$.