

5

GROUPES, ANNEAUX

I. GROUPES

GROUPES ET SOUS-GROUPES

Définition 12 (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 13 (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 $f : G \rightarrow G'$ un morphisme de groupes. $\text{Im } f$ et $\text{ker } f$ 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 $H = \langle x \rangle = \{x^k, k \in \mathbb{Z}\}$. 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 $\langle x \rangle$ s'il est fini.
- Si x est d'ordre d , alors $\langle x \rangle = \{1, x, x^2, \dots, x^{d-1}\}$.
- 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. AUTRES STRUCTURES

ANNEAUX (2 LOIS)

Définition 14 (Anneau)

ensemble A muni de deux lois $+$ et \times tel que

1. $(A, +)$ groupe commutatif (élément neutre noté 0).
2. la loi (produit) \times est interne et associative.
3. le produit est distributif à droite et à gauche par rapport à l'addition.
4. il existe un élément neutre, noté 1_A (ou 1), pour la multiplication.

Définition 15 (Vocabulaire)

soit $(A, +, \times)$ un anneau

- A est *commutatif* si la loi \times est commutative.
- $a \in A$ est un *diviseur de 0* s'il est non nul et s'il existe $b \neq 0$ tel que $a \times b = 0$.
- A est *intègre* s'il n'a aucun diviseur de 0. Cela revient à dire que pour tout $a, b \in A$, $a \times b = 0$ si et seulement si $a = 0$ ou $b = 0$.

Définition 16 (Sous-anneau)

$B \subset A$ est un sous-anneau de A s'il contient 1 , est stable pour les deux lois et B muni des lois induites $(+, \times)$ possède une structure d'anneau. On montre que B est un sous-anneau de A en montrant :

- $B \subset A$ et $1_A \in B$,
- pour tout $a, b \in B$, $a - b$ et $a \times b \in B$.

EXEMPLE

- $(\mathbb{Z}, +, \times)$ et $(\mathbb{R}[X], +, \times)$ sont des anneaux commutatifs et intègres.
- $(\mathcal{C}^0(I, \mathbb{R}), +, \times)$ est un anneau commutatif mais il n'est pas intègre.
- Si E est un espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau non commutatif, non intègre.

Définition 17 (Morphisme d'anneaux)

Soit A et A' deux anneaux, $f: A \rightarrow A'$ est un morphisme d'anneaux si

- $f(1_A) = 1_{A'}$
- $\forall (a_1, a_2) \in A \times A, f(a_1 + a_2) = f(a_1) + f(a_2)$ et $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$

Propriété 33 (Règles de calcul)

si $a, b \in A$ commutent alors

- $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k},$
- $a^n - b^n = (a - b) \left(\sum_{k=0}^{n-1} a^k b^{n-1-k} \right).$

CORPS (2 LOIS)

Définition 18 (Corps)

On dit que $(K, +, \times)$ est un corps si

1. $(K, +, \times)$ est un anneau commutatif. On note 0 l'élément neutre pour $+$ (appelé élément nul) et 1 l'élément neutre pour \times
2. tout $x \in K$ non nul est inversible : il existe $y \in K$ tel que $x \times y = y \times x = 1$ (on note alors $y = x^{-1}$).

on définit comme précédemment les notions de sous-corps et de morphismes de corps.

EXEMPLE

- \mathbb{Q}, \mathbb{R} et \mathbb{C} sont des corps. Dans cet ordre, ils sont des sous-corps du corps suivant.
- Dans un corps, tous les éléments non nuls sont simplifiables, il n'y a donc pas de diviseur de zéro. Pour qu'un anneau ait une chance d'être un corps, il faut donc qu'il soit intègre (mais ce n'est pas suffisant).

ESPACES VECTORIELS (2 LOIS)

Définition 19 (Espace vectoriel)

Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif. On dit que $(E, +, \cdot)$ est un espace vectoriel sur \mathbb{K} si

1. la loi $+$ est une loi interne et $(E, +)$ est un groupe commutatif.

2. la loi \cdot est une loi externe : $\begin{cases} \mathbb{K} \times E & \rightarrow E \\ (\lambda, x) & \mapsto \lambda \cdot x \end{cases}$ qui vérifie

$$\rightarrow (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$$

$$\rightarrow \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$$

$$\rightarrow \lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$$

$$\rightarrow 1 \cdot x = x$$

Les éléments d'un espace vectoriel sont appelés les *vecteurs*, les éléments du corps de base \mathbb{K} sont appelés *scalaires*. Le vecteur $\lambda \cdot x$ est noté simplement λx .

Proposition 34 (Règles de calcul)

Soit E un \mathbb{K} -espace vectoriel, on a $(x, y \in E$ et $\lambda \in \mathbb{K})$

$$1. 0_{\mathbb{K}} \cdot x = 0_E.$$

$$2. \lambda \cdot 0_E = 0_E.$$

$$3. -(\lambda x) = (-\lambda)x = \lambda(-x)$$

$$4. \lambda(x - y) = \lambda x - \lambda y$$

ALGÈBRE (3 LOIS)

Définition 20 (Algèbre)

Soit \mathbb{K} un corps. On dit que $(A, +, \star, \cdot)$ est une \mathbb{K} -algèbre si

1. $(A, +, \cdot)$ est un \mathbb{K} -espace vectoriel.

2. $(A, +, \star)$ est un anneau.

3. $(\lambda \cdot x) \star y = x \star (\lambda \cdot y) = \lambda \cdot (x \star y)$ pour $\lambda \in \mathbb{K}$ et $x, y \in A$.

En pratique, il y a une loi interne « additive » et deux lois « multiplicatives », l'une correspond à la multiplication par les constantes, l'autre à une multiplication interne. On peut également voir une algèbre comme un espace vectoriel muni d'une multiplication interne (avec des propriétés entre les deux multiplications).

EXEMPLE

- $\mathcal{F}(A, \mathbb{K})$ (ensemble des applications d'un ensemble A dans $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}) est une algèbre.
- $\mathcal{C}^0(I, \mathbb{K}), \mathcal{C}^k(I, \mathbb{K})$ ou $\mathcal{C}^\infty(I, \mathbb{K})$ sont des algèbres.
- $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont des algèbres.
- $\mathbb{R}^{\mathbb{N}}$ ou $\mathbb{C}^{\mathbb{N}}$ les ensembles des suites à valeurs dans \mathbb{R} ou \mathbb{C} sont des algèbres.
- $(\mathcal{L}(E), +, \circ, \cdot)$ l'ensemble des endomorphismes d'un espace vectoriel E est une algèbre.
- $M_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n est une algèbre.

IV. ANNEAUX $\mathbb{Z}/n\mathbb{Z}$

L'ESSENTIEL - ANNEAU $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$,

- la relation de congruence modulo n est compatible avec l'addition et la multiplication. Cela permet de définir une structure d'anneau sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ avec $\overline{x+y} = \overline{x} + \overline{y}$ et $\overline{x \times y} = \overline{x} \times \overline{y}$.
- un élément $a = \overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $k \wedge n = 1$.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Proposition 35 (Théorème chinois)

L'application

$$\varphi: \begin{cases} \mathbb{Z}/(mn)\mathbb{Z} & \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \mapsto (\overline{x}, \overline{x}) \end{cases}$$

est un isomorphisme d'anneaux si et seulement si $m \wedge n = 1$ (les classes sont prises respectivement modulo mn, m et n).

Propriété 36 (Indicatrice d'Euler)

- on note $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. C'est aussi le nombre d'entier entre 1 et n qui sont premiers avec n .
- la fonction est multiplicative : si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$.
- Si p est premier alors $\varphi(p) = p - 1$ et $\varphi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$.
- Si $n = \prod_{i=1}^k p_i^{\alpha_i}$ alors $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$
- Si a est un élément inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $a^{\varphi(n)} = 1$. Notamment pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ non nul, avec p premier, on a $a^{p-1} = 1$ - ou pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

V. 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 (Petit théorème de Fermat)

Soit p un nombre premier.

1. Montrer que pour $k \in \llbracket 1; p-1 \rrbracket$, p divise $\binom{p}{k}$.
2. En déduire que, pour tout $(a, b) \in \mathbb{Z}^2$, $(a+b)^p \equiv a^p + b^p \pmod{p}$.
3. Montrer par récurrence que, pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$, et que si p ne divise pas a , alors $a^{p-1} \equiv 1 \pmod{p}$.

Exercice 4

Pour $\theta \in \mathbb{R}$, on note $A(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ et $B(\theta) = \begin{pmatrix} \operatorname{ch} \theta & \operatorname{sh} \theta \\ \operatorname{sh} \theta & \operatorname{ch} \theta \end{pmatrix}$. 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 5

Déterminer le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$. Ce groupe est-il cyclique ?

Exercice 6

On dit qu'un groupe abélien G est simple lorsque ses seuls sous-groupes sont G et $\{0_G\}$.

1. À quelle condition le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est-il simple?
2. Montrer qu'un groupe abélien fini est simple si et seulement si il est cyclique d'ordre premier.

Exercice 7

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 8

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 9

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 10

☆

1. 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 PPCM(p, q).
2. Soit G le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ où p est un nombre premier différent de 2. Montrer que G est cyclique (*Indication* : on pourra s'intéresser au polynôme $X^s - 1$ où s est le ppcm des ordres des éléments de G).

Exercice 11

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

Exercice 12

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

Exercice 13 (Mines MP/MPI)

On pose $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$. Montrer que $\mathbb{Z}[i]$ est un anneau intègre et déterminer ses inversibles.

Exercice 14

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 :

$$\tilde{f} : \bar{x} \in G/\mathcal{R} \mapsto f(x) \in \text{Im } f.$$

2. En déduire $|G| = |\text{Im } f| \cdot |\ker f|$.
3. Soit f un morphisme de groupes de G dans lui-même. Montrer que $\ker f = \ker f^2 \Leftrightarrow \text{Im } f = \text{Im } f^2$.

Exercice 15 (Centrale MP)

☆

Soit p premier impair.

1. Montrer que le nombre de carrés de $\mathbb{Z}/p\mathbb{Z}$ est $\frac{p+1}{2}$ (*indic* : considérer l'application $x \mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$).
2. Montrer que $x \in \mathbb{Z}/p\mathbb{Z}$ est un carré si, et seulement si, $x^{(p+1)/2} = x$ (*Indic* : on pourra s'intéresser au polynôme $X^{\frac{p+1}{2}} - X$).
3. Pour quels p la classe de -1 modulo p est-elle un carré de $\mathbb{Z}/p\mathbb{Z}$?
4. Déterminer le cardinal de l'ensemble $S = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2, x^2 + y^2 = 1\}$.

Exercice 16

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 17

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 $2\text{card } H$.
4. Prouver que $\text{card } G$ 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 18 (Mines MP)

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 19

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 20 (Mines MP)**

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

Exercice 21 (Mines MP/MPI)

Soient G un groupe et $k \in \mathbb{N}$. On suppose que : $\forall i \in \llbracket k; k+2 \rrbracket, \forall (a, b) \in G^2, (ab)^i = a^i b^i$. Montrer que G est abélien.

Exercice 22 (Mines MP)

Pour $n \in \mathbb{N}^*$, soit $\sigma(n)$ la somme des diviseurs de n dans \mathbb{N}^* . Donner un équivalent de $U_n = \sum_{k=1}^n \sigma(k)$.

Exercice 23 (ENS MP)

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