8

Structure de groupe

I Structure de groupe (MP2I)

Définition 1 : Groupe

On appelle **groupe** tout couple $(G, \star)$ où G est un ensemble tel que

(i) $\star$ est une loi de composition interne sur G

(ii) $\star$ est associative

(iii) G admet un élément neutre pour $\star$

(iv) Tout élément de G admet un symétrique dans G pour $\star$.

Si, de plus, $\star$ est commutative, on dit que $(G, \star)$ est un **groupe commutatif** ou **groupe abélien**.

II Puissances ou itérées d'un élément (MP2I)

Définition 2 : Itérées d'un élément

Soir E un ensemble muni d'une loi de composition interne $\star$ (notée multiplicativement) **associative** et possédant un élément neutre e.

Pour tout $x \in E$ et tout $n \in \mathbb{N}$, on définit récursivement

$$x^n = \begin{cases} e & \text{si } n = 0 \\ x^{n-1} \star x & \text{sinon.} \end{cases}$$

Propriété 1 : des exposants

Soient $x, y \in E$ et $n, m \in \mathbb{N}$.

(i) $x^{n+m} = x^n \star x^m = x^m \star x^n$

(ii) $(x^n)^m = x^{nm} = (x^m)^n$.

(iii) *Si* $x \star y = y \star x$, $(x \star y)^n = x^n \star y^n$.

(iv) *Si x est inversible, x^n est inversible et* $(x^n)^{-1} = \left(x^{-1}\right)^n$.

Notation 1 : Exposant négatif

Si $x \in E$ inversible et $n \in \mathbb{N}$, on note x^{-n} l'élément $\left(x^{-1}\right)^n = (x^n)^{-1}$.

III Régularité

Soit[1] E un ensemble muni d'une loi de composition interne associative $\star$ et possédant un élément neutre e.

Définition 3 : Régularité

Soit $x \in E$. On dit que x est **régulier** (ou **simplifiable**)

- **à gauche** lorsque

$$\forall\, a, b \in E,\quad x \star a = x \star b \Longrightarrow a = b$$

- **à droite** lorsque

$$\forall\, a, b \in E,\quad a \star x = b \star x \Longrightarrow a = b$$

On dit que x est **régulier** lorsqu'il l'est à gauche et à droite.

Propriété 2 : Régularité d'un inversible

Tout élément inversible de $(E, \star)$ est régulier.

Corollaire 1 : Régularité dans un groupe

Si $(G, \star)$ est un groupe, alors tout élément de G est régulier.

Corollaire 2 : Bijectivité des translations

Si $(G, \star)$ est une groupe et $a \in G$ fixé.

Les applications $\varphi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \end{array}\right.$ *et* $\psi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{array}\right.$ *(appelées translations à gauche et à droite) sont bijectives.*

Corollaire 3

Si $(G, \star)$ est une groupe et $a \in G$ fixé.

$$G = \{a \star x,\ x \in G\} = \{x \star a,\ x \in G\}.$$

1. On dit que $(E, \star)$ est un **monoïde**.

IV Groupe produit (MP2I)

Propriété 3 : Groupe produit

Soit $(G,\star)$ et (H,Δ) des groupes.
Pour tout (g,h) et (g',h') dans $G\times H$, on pose

$$(g,h)\top(g',h') = (g\star g', h\Delta h').$$

Alors $(G\times H,\top)$ a une structure de groupe.
Si, de plus, les lois $\star$ et Δ sont commutatives, alors $\top$ l'est.

V Sous-groupes

1 Définition et caractérisation (MP2I)

Définition 4 : Sous-groupe

Soit $(G,\star)$ groupe. On note $\star|_{H^2}$ la restriction à H^2 de la loi $\star$.
On dit que H est un **sous-groupe** de $(G,\star)$ si $H\subset G$ et $(H,\star|_{H^2})$ est un groupe.

Propriété 4 : Sous-groupes triviaux

*Soit $(G,\star)$ groupe. G et $\{e_G\}$ sont des sous-groupes de $(G,\star)$ appelés **sous-groupes triviaux**.*

Propriété 5

Soit H un sous-groupe de $(G,\star)$.

(i) $(H,\star)$ possède le même élément neutre que $(G,\star)$.

(ii) Si $x\in H$, alors x a même inverse dans $(H,\star)$ et dans $(G,\star)$.

Propriété 6 : caractérisation des sous-groupes

Soit $(G,\star)$ un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

(i) H est un sous-groupe de $(G,\star)$

(ii)
$$\begin{cases} H\subset G \\ H\neq\varnothing \quad (e_G\in H) \\ H \text{ est stable par } \star : \ \forall x,y\in H,\ x\star y\in H \\ H \text{ est stable par inverse } \forall x\in H,\ x^{-1}\in H \end{cases}$$

(iii)
$$\begin{cases} H\subset G \\ H\neq\varnothing \quad (e_G\in H) \\ \forall x,y\in H,\ x\star y^{-1}\in H \end{cases}$$

2 Intersection et réunion (MPI)

Propriété 7 : Intersection de sous-groupes

Soit $(G,\star)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,\star)$. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G,\star)$.

3 Sous-groupes de $(\mathbb{Z},+)$ (MPI)

Notation 2

Pour tout $a\in\mathbb{Z}$, on note $a\mathbb{Z} = \{ak,\ k\in\mathbb{Z}\}$.

Propriété 8 : Sous-groupes de $(\mathbb{Z},+)$

Les sous-groupes G de $(\mathbb{Z},+)$ sont exactement les $a\mathbb{Z}$ pour $a\in\mathbb{N}$.
De plus, si $G\neq\{0\}$, $a=\min(G\cap\mathbb{N}^*)$.

4 Sous-groupes de $(\mathbb{R},+)$ (HP)

Théorème 1 : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R},+)$.
Alors G est soit dense dans $\mathbb{R}$, soit discret (de la forme $\alpha\mathbb{Z}$).

VI Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

1 Congruences (MP2I)

Définition 5 : Rappel : Congruence

Soit $n\in\mathbb{N}^*$. On dit que $a,b\in\mathbb{Z}$ sont **congrus modulo** n et on note $a\equiv b\ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k\in\mathbb{Z}$ tel que $a=b+kn$.

Propriété 9 : Rappel : Relation d'équivalence

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété 10 : Rappel : Nombre d'entiers modulo n

$\forall\, a \in \mathbb{Z},\ \exists !\, r \in [\![0, n-1]\!],\ a \equiv r\ [n]$. *$r$ est le reste de la division euclidienne de a par n.*

Ainsi, la relation d'équivalence $\cdot \equiv \cdot\ [n]$ possède exactement n classes d'équivalences.

Propriété 11 : Rappel : Compatibilité de $+$

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$.

Alors $a + c \equiv b + d\ [n]$.

2 Le groupe $\mathbb{Z}/n\mathbb{Z}$ (MPI)

Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$ fixé.

Définition 6 : $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble (quotient) des n classes d'équivalences de $\cdot \equiv \cdot\ [n]$, notées $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Ainsi

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

Définition 7 : Surjection canonique

L'application surjective $\left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}\right.$ est appelée **surjection canonique**.

Lemme 1 : Compatibilité avec $+$

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors $\overline{a+b} = \overline{c+d}$.

Définition 8 : Loi $+$

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$, ce qui définit une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 12 : Structure de groupe additif

$\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe commutatif isomorphe à $\left(\mathbb{U}_n, \times\right)$.

VII Morphismes (MP2I)

1 Définition

Définition 9 : Morphisme de groupe

Soient $(G, \star)$ et $(G', \bullet)$ deux groupes.

$f : (G, \star) \to (G', \bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall\, (x, y) \in G^2,\ f(x \star y) = f(x) \bullet f(y)$$

Lorsque $(G, \star) = (G', \bullet)$, on parle d'**endomorphisme** de groupes.

Lorsque f est bijective, on parle d'**isomorphisme**.

Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont **isomorphes.**

Lorsque f est bijective et $G = G'$, on parle d'**automorphisme**.

Propriété 13 : Image du neutre et du symétrique par un morphisme de groupes

Si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f\left(\mathrm{sym}(x)\right) = \mathrm{sym}(f(x))$.

Propriété 14 : Image d'une itérée

En notation multiplicative, si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, pour tout $x \in G$ et pour tout $k \in \mathbb{Z}$, $f\left(x^k\right) = f(x)^k$.

Propriété 15 : Composée de morphismes

Si $f : (G, \star) \to (G', \bullet)$ et $g : (G', \bullet) \to (G'', \Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

2 Noyau et image

Définition 10 : Image et noyau d'un morphisme

Soit $f : (G,\star) \to (G',\bullet)$ un morphisme de groupes.

- On appelle **noyau** de f l'ensemble

$$\operatorname{Ker} f = f^{(-1)}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\} \subset G.$$

Ainsi, $x \in \operatorname{Ker} f \iff f(x) = e_{G'}$.

- On appelle **image** de f l'ensemble

$$\operatorname{Im} f = f(G) = \{f(x),\ x \in G\} \subset G'.$$

Ainsi, $y \in \operatorname{Im} f \iff \exists\, x \in G,\ \ y = f(x)$.

Propriété 16 : Caractérisations de l'injectivité et de la surjectivité

Soit $f : (G,\star) \to (G',\bullet)$ un morphisme de groupe.

- *f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

Propriété 17 : Images directe et réciproque d'un sous-groupe

Soit $f : (G,\star) \to (G',\bullet)$ un morphisme de groupes.

(i) Si H est un sous-groupe de $(G,\star)$, alors $f(H)$ est un sous-groupe de $(G',\bullet)$

(ii) Si H' est un sous-groupe de $(G',\bullet)$, $f^{(-1)}(H')$ est un sous-groupe de $(G,\star)$.

Corollaire 4 : Cas particulier du noyau et de l'image

Soit $f : (G,\star) \to (G',\bullet)$ un morphisme de groupes.
Alors $\operatorname{Ker} f$ est un sous-groupe de $(G,\star)$ et $\operatorname{Im} f$ est un sous-groupe de $(G',\bullet)$.

3 Isomorphismes

Propriété 18 : Réciproque d'un isomorphisme

Soit $f : (G,\star) \to (G',\bullet)$ un isomorphisme de groupes.
Alors f^{-1} est un isomorphisme du groupe $(G',\bullet)$ sur le groupe $(G,\star)$.

VIII Groupes monogènes (MPI)

1 Sous-groupes engendré par une partie

Définition 11 : Groupe engendré par une partie

Soit $(G,*)$ un groupe, A partie non vide de G.
On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A\rangle$.
On dit alors que A est une **partie génératrice** de $\langle A\rangle$.

Propriété 19 : Éléments de $\langle A\rangle$

Les éléments de $\langle A\rangle$ sont exactement les produits (pour $*$) d'éléments de A ou de A^{-1}.
Autrement dit, $x \in \langle A\rangle$ si et seulement s'il existe $k \in \mathbb{N}$, $(a_1,\dots,a_k) \in A^k$ et $(\varepsilon_1,\dots,\varepsilon_k) \in \{-1,1\}^k$ tel que

$$x = a_1^{\varepsilon_1} * \cdots * a_k^{\varepsilon_k}.$$

2 Groupes monogènes et cycliques

Propriété 20 : Sous-groupe engendré par un élément

*Soit $a \in G$. Le sous-groupe **engendré par** a noté $\langle a\rangle$ plutôt que $\langle\{a\}\rangle$ est*

$$\langle a\rangle = \{a^k,\ k \in \mathbb{Z}\}$$

*On dit que a en est un **générateur**.*

Définition 12 : Groupe monogène

Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \langle a\rangle$.
Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

Propriété 21 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique, dont les générateurs sont exactement les $\overline{k}$ avec $k \wedge n = 1$.

3 Ordre d'un élément dans un groupe

$(G,*)$ est un groupe d'élément neutre e.

Définition 13 : Ordre d'un élément

On dit que $a \in G$ est **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.

Dans ce cas, on appelle **ordre de** a le plus petit $k \in \mathbb{N}^*$ tel que $a^k = e$.

Propriété 22 : de l'ordre d'un élément

Soit a un élément de G d'ordre fini m.

- *Si $k \in \mathbb{Z}$, $a^k = e$ si et seulement si $k \in m\mathbb{Z}$ ie m divise k.*
- *$\langle a \rangle = \{a^k, k \in [\![0, m-1]\!]\}$ et $|\langle a \rangle| = m$.*

Propriété 23 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.

Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à $(\mathbb{U}_n,+)$ et à $(\mathbb{Z}/n\mathbb{Z},+)$

Théorème 2 : de Lagrange (HP mais très classique)

Soit $(G,*)$ un groupe fini, H un sous-groupe de G. Alors $|H|$ divise $|G|$.

Propriété 24 : de l'ordre

Soit $(G,*)$ un groupe fini de neutre e.

(i) Tout élément de G est d'ordre fini.

(ii) L'ordre de tout élément de G divise le cardinal de G.

(iii) Pour tout $a \in G$, $a^{|G|} = e$.

IX GROUPES SYMÉTRIQUES (MP2I)

1 Définition, structure

Définition 14 : Permutation, groupe symétrique

Si E est un ensemble, on appelle **permutation** de E toute bijection de E dans E. On note $\mathfrak{S}(E)$ leur ensemble.

Si $E = [\![1,n]\!]$ où $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n$ appelé **groupe symétrique d'ordre n (ou de degré n)** cet ensemble.

Si $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & 3 \cdots\cdots n \\ \sigma(1) & \sigma(2) & \sigma(3) \cdots\cdots \sigma(n) \end{pmatrix}$.

Propriété 25 : Structure

$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre (ie *de cardinal*) *$n!$, non abélien dès que $n \geqslant 3$.*

Définition 15 : Orbites

Soit $\sigma \in \mathfrak{S}_n$. La relation binaire définie sur $[\![1,n]\!]$ par

$$x \sim y \iff \exists\, k \in \mathbb{Z},\ \ y = \sigma^k(x)$$

est une relation d'équivalence dont les classes d'équivalence sont les **orbites** de σ.

Si $x \in [\![1,n]\!]$,

$$\mathcal{O}(x) = \left\{\sigma^k(x),\ k \in \mathbb{Z}\right\}.$$

Propriété 26 : Description d'une orbite

Soit $\sigma \in \mathfrak{S}_n$, $x \in [\![1,n]\!]$. Alors il existe $\ell \in \mathbb{N}$ tel que $\mathcal{O}(x) = \{x, \sigma(x), \ldots, \sigma^{\ell-1}(x)\}$ (deux à deux distincts).

Définition 16 : Support

Si $\sigma \in \mathfrak{S}_n$, son **support** est l'ensemble des éléments de $[\![1,n]\!]$ qui **ne sont pas** invariants par σ.

Propriété 27 : Commutation de permutations à supports disjoints

(i) Le support d'une permutation est stable par cette permutation.

(ii) Deux permutations à supports disjoints commutent.

2 Cycles

Définition 17 : Transposition, cycle

- Une **transposition** τ est une permutation qui échange deux éléments i et j de $[\![1,n]\!]$, et laisse les autres invariants ie dont le support est $\{i,j\}$.
  On la note $\tau = (i\ j)$ ou parfois $\tau_{i,j}$.
  $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et si $k \notin \{i,j\}$, $\tau_{i,j}(k) = k$.

- Soit $p \in \mathbb{N}$ tel que $2 \leqslant p \leqslant n$.
  On appelle **p-cycle** une permutation c de $\mathfrak{S}_n$ qui permute circulairement p éléments $i_1, i_2, \ldots, i_p$ de $[\![1,n]\!]$ et laisse les autres invariants ie dont le support est $\{i_1, \ldots, i_p\}$ et telle que

$$c(i_1) = i_2\,;\ c(i_2) = i_3\,;\ \cdots\ ;\ c(i_{p-1}) = i_p\,;\ c(i_p) = i_1$$

  p est la **longueur** du cycle c. On note $c = (i_1\ i_2\ \cdots\ i_p)$.

Propriété 28 : Ordre d'un cycle

Un p-cycle est d'ordre p.

Théorème 3 : Unique décomposition en produit de cycles à supports disjoints

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

Corollaire 5 : Décomposition en produit de transpositions (non unique)

Toute permutation se décompose en produit (composée) de transpositions.

Voici deux propositions adaptables à tout cycle :

$$\begin{aligned}(1 \quad 2 \quad \cdots \quad p) &= (1 \quad p)\,(1 \quad p-1)\,\cdots\,(1 \quad 2)\\ &= (1 \quad 2)\,(2 \quad 3)\,\cdots\,(p-1 \quad p)\end{aligned}$$

3 Signature

Définition 18 : Inversions, signature

Soit $\sigma \in \mathfrak{S}_n$. On appelle **inversion** par σ tout couple (i,j) tel que $i < j$ et $\sigma(i) > \sigma(j)$.
On note $I(\sigma)$ le nombre d'inversions par σ.
On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1,1\}$.
On vérifie que $\varepsilon(\sigma) = \prod_{1\leqslant i<j\leqslant n} \dfrac{\sigma(j)-\sigma(i)}{j-i}$.
Une permutation σ est dite **paire** lorsque $I(\sigma)$ est pair et donc $\varepsilon(\sigma) = 1$. Elle est dite **impaire** dans le cas contraire.

Théorème 4 : Morphisme de signature

Soit $n \geqslant 2$. L'application

$$\varepsilon : \left| \begin{array}{ccc} (\mathfrak{S}_n, \circ) & \longrightarrow & (\{-1,1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{array} \right.$$

est un morphisme de groupe, ie si $\sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

Propriété 29 : de la signature

(i) *Si $\sigma \in \mathfrak{S}_n$ se décompose en produit de N transpositions, $\varepsilon(\sigma) = (-1)^N$.*
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.

(ii) *Si c est un p-cycle, $\varepsilon(c) = (-1)^{p-1}$.*

(iii) *Si $\sigma \in \mathfrak{S}_n$, $\varepsilon\left(\sigma^{-1}\right) = \varepsilon(\sigma)$.*

4 Groupe alterné (HP)

Définition 19 : Groupe alterné

Le sous-groupe $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon)$ des permutations paires de $\mathfrak{S}_n$ est appelé ***groupe alterné d'ordre n (ou de degré n)***.

Propriété 30

Pour tout $n \geqslant 2$, $|\mathfrak{A}_n| = \dfrac{n!}{2}$.