

Structures algébriques usuelles et groupe symétrique (rappel MPSI)

Binyze Mohamed

MP 2025-2026

Sommaire

1	Structure de groupe	1
2	Structure d'anneau	3
3	Groupe symétrique	4

1 Structure de groupe

Groupe et sous-groupe

Définition 1.1.

vocabulaire sur les lois de composition internes

Soit E un ensemble. On appelle **loi de composition interne** (l.c.i.) sur E toute application de $E \times E$ dans E , notée $\star : E \times E \longrightarrow E$. L'élément $x \star y$ est appelé **composé** de x par y via la loi $\star$.

$$(x, y) \longmapsto x \star y$$

1. La loi $\star$ est dite **commutative** si : $\forall (x, y) \in E^2, x \star y = y \star x$.
2. La loi $\star$ est dite **associative** si : $\forall (x, y, z) \in E^3, x \star (y \star z) = (x \star y) \star z$.
3. Si $\top$ est une autre l.c.i. sur E , on dit que la loi $\star$ est **distributive** sur la loi $\top$ si :

$$\forall (x, y, z) \in E^3, x \star (y \top z) = (x \star y) \top (x \star z) \text{ et } (y \top z) \star x = (y \star x) \top (z \star x).$$

4. On dit qu'un élément e de E est **neutre**¹ pour la loi $\star$ si : $\forall x \in E, e \star x = x \star e = x$.
5. Lorsque E possède un neutre e , on dit qu'un élément $x \in E$ est **inversible** si : $\exists x' \in E, x \star x' = x' \star x = e$.
Si de plus la loi $\star$ est associative, x' est **unique** et appelé **l'inverse** de x . On le note souvent x^{-1} ou $-x$.

1. Lorsqu'un tel élément existe, il est **unique**.

Proposition 1.1.

inversibilité du produit de deux éléments inversibles

Soit $\star$ une l.c.i. sur un ensemble E associative et possédant un neutre e .

1. Si $x \in E$ est inversible, alors x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.
2. Si $x, y \in E$ sont inversibles, alors $x \star y$ l'est aussi et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Définition 1.2.

partie stable par une l.c.i.

Soit $\star$ une l.c.i. sur un ensemble E et $F \subset E$ non vide. On dit que F est stable par $\star$ si : $\forall (x, y) \in F^2, x \star y \in F$.

Définition 1.3.

groupe

On appelle **groupe** tout couple $(G, \star)$ formé d'un ensemble G et d'une l.c.i. $\star$ sur G vérifiant :

1. $\star$ est associative : $\forall (x, y, z) \in G^3, (x \star y) \star z = x \star (y \star z)$.
2. $\star$ possède un élément neutre : $\exists e \in G, \forall x \in G, x \star e = x = e \star x$.
3. Tout élément de G est inversible pour $\star$: $\forall x \in G, \exists y \in G, x \star y = e = y \star x$.

Si de plus la loi $\star$ est commutative, on parle de **groupe commutatif** (ou **abélien**).

■ Notations additives et multiplicatives dans un groupe G .

- Lorsque la loi de G est notée additivement $(G, +)$, l'élément neutre est noté 0_G et l'inverse (opposé) d'un élément x de G est noté $-x$. Pour $n \in \mathbb{Z}$, on définit la n -ième multiple, nx , de x par :

$$nx = \begin{cases} \underbrace{x + \dots + x}_{n \text{ fois}} & \text{si } n > 0 \\ 0_G & \text{si } n = 0 \\ \underbrace{(-x) + \dots + (-x)}_{n \text{ fois}} & \text{si } n < 0 \end{cases}$$

- Lorsque la loi de G est notée multiplicativement $(G, \times)$, l'élément neutre est noté 1_G et l'inverse d'un élément x de G est noté x^{-1} . Pour $n \in \mathbb{Z}$, on définit la puissance n -ième, x^n , de x par :

$$x^n = \begin{cases} \underbrace{x \times \dots \times x}_{n \text{ fois}} & \text{si } n > 0 \\ 1_G & \text{si } n = 0 \\ \underbrace{(x^{-1}) \times \dots \times (x^{-1})}_{n \text{ fois}} & \text{si } n < 0 \end{cases}$$

Proposition 1.2.

propriétés

Soient G un groupe, $x \in G$ et $(m, n) \in \mathbb{Z}^2$.

1. Lorsque la loi de G est notée additivement $(G, +)$, on a : $(m + n)x = mx + nx$ et $m(nx) = (mn)x$.
2. Lorsque la loi de G est notée multiplicativement $(G, \times)$, on a : $x^{m+n} = x^m x^n$ et $(x^m)^n = x^{mn}$.

Définition 1.4.

groupe des permutations d'un ensemble

Soit E un ensemble non vide. On note $\mathcal{S}_E$ l'ensemble des **permutations** de E (bijections de E vers lui-même). Le couple $(\mathcal{S}_E, \circ)$ forme un groupe de neutre Id_E , appelé **groupe des permutations** de E .

Théorème 1.1.

groupe produit

Soient $(G, \top)$ et $(H, \perp)$ deux groupes de neutres respectifs e_G et e_H . Soit $\star$ la l.c.i. définie sur $G \times H$ par :

$$\forall (g_1, g_2) \in G^2, \forall (h_1, h_2) \in H^2, (g_1, h_1) \star (g_2, h_2) \stackrel{\text{déf}}{=} (g_1 \top g_2, h_1 \perp h_2).$$

$(G \times H, \star)$ est un groupe de neutre (e_G, e_H) appelé ¹ **groupe produit**.

De plus, pour tout $(g, h) \in G \times H$, on a : $(g, h)^{-1} = (g^{-1}, h^{-1})$.

1. On définit de même le produit d'un nombre fini de groupes.

Définition 1.5.

sous-groupe

Soit $(G, \star)$ un groupe de neutre e .

On appelle **sous-groupe** de $(G, \star)$ toute partie H non vide de G telle que ¹ :

1. H est stable par $\star$: $\forall (x, y) \in H^2, x \star y \in H$.
2. H est stable par prise d'inverse : $\forall x \in H, x^{-1} \in H$.

1. La restriction à H de la l.c.i. sur G fait de H un groupe de même élément neutre que G .

Proposition 1.3.**caractérisation d'un sous-groupe**

Soit $(G, \star)$ un groupe de neutre e et H une partie de G .

$$H \text{ sous-groupe de } G \iff e \in H \text{ et } \forall (x, y) \in H^2, x \star y^{-1} \in H.$$

Morphisme de groupe**Définition 1.6.****morphisme de groupes, isomorphisme de groupes**

Soient $(G, \star)$, $(H, \top)$ deux groupes et $f : G \longrightarrow H$ une application.

1. On dit que f est un **morphisme de groupes** si : $\forall x, y \in G, f(x \star y) = f(x) \top f(y)$.
2. On dit que f est un **isomorphisme de groupes** si f est un morphisme de groupes bijectif.

Proposition 1.4.**propriétés**

1. Soient G, H deux groupes de neutres respectifs e_G, e_H et $f : G \longrightarrow H$ un morphisme de groupes.
 - a. $f(e_G) = e_H$.
 - b. Soit $x \in G$. Alors x est inversible si, et seulement si, $f(x)$ est inversible et on a : $(f(x))^{-1} = f(x^{-1})$.
2. La composée de morphismes (resp. isomorphismes) de groupes est un morphisme (resp. isomorphisme) de groupes.
3. L'application réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.
4. L'image directe et l'image réciproque de sous-groupes par un morphisme de groupes sont des sous-groupes.

Définition 1.7.**noyau et image d'un morphisme de groupe**

Soient G, H deux groupes de neutres respectifs e_G, e_H et $f : G \longrightarrow H$ un morphisme de groupes.

1. L'ensemble $\ker(f) \stackrel{\text{déf}}{=} f^{-1}(\{e_H\}) = \{x \in G, f(x) = e_H\}$ est un sous-groupe de G appelé le **noyau** de f .
2. L'ensemble $\text{Im}(f) \stackrel{\text{déf}}{=} f(G) = \{y \in H, \exists x \in G, y = f(x)\}$ est un sous-groupe de H appelé l'**image** de f .

Proposition 1.5.**caractérisation des morphismes injectifs et surjectifs**

Soient G, H deux groupes de neutres respectifs e_G, e_H et $f : G \longrightarrow H$ un morphisme de groupes.

1. f injectif $\iff \ker(f) = \{e_G\}$.
2. f surjectif $\iff \text{Im}(f) = H$.

2 Structure d'anneau**Anneau et sous-anneau****Définition 2.1.****anneau**

Soit A un ensemble non vide muni de deux l.c.i. notées $+$ et $\times$. On dit que $(A, +, \times)$ est un **anneau** lorsque :

1. $(A, +)$ est un groupe abélien, son neutre est noté 0 (ou 0_A).
2. $\times$ est associative et possède¹ un élément neutre, noté 1 (ou 1_A), appelé **élément unité** de A .
3. $\times$ est distributive sur $+$: $\forall (a, b, c) \in A^3, a \times (b + c) = a \times b + a \times c$ et $(b + c) \times a = b \times a + c \times a$.

Si de plus la loi $\times$ est commutative on dit que $(A, +, \times)$ est un **anneau commutatif**.

1. Par convention un anneau est unitaire c-à-d : la loi $\times$ admet un élément unité.

■ Lorsque $(A, +, \times)$ est un anneau, on note, pour tout $x, y \in A$, xy au lieu de $x \times y$.

calculs dans un anneau

1. Formule du binôme : pour tout $n \in \mathbb{N}$, on a :

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

2. Formule de factorisation : pour tout $n \in \mathbb{N}^*$, on a :

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

anneau intègre

On dit qu'un anneau commutatif A est *intègre* si : $A \neq \{0\}$ et $\forall (a,b) \in A^2, \quad ab=0 \implies a=0 \text{ ou } b=0$.

sous-anneau

Soit A un anneau et B une partie de A . On dit que B est un **sous-anneau** de A si¹ :

1. $1_A \in B$.
2. $(B, +)$ sous-groupe de $(A, +)$.
3. $\forall (x, y) \in B^2, \quad xy \in B$.

1. Ce qui équivaut à : $1_A \in B$ et $\forall (x, y) \in B^2, x - y \in B, xy \in B$

groupe des éléments inversibles

Soit A un anneau. On dit qu'un élément $a \in A$ est **inversible** si $\boxed{\exists b \in A, ab = ba = 1_A}$. L'élément b est unique, noté a^{-1} , et appelé l'inverse de a .

L'ensemble $\mathbb{U}(A)$ des éléments inversibles de A est un **groupe** pour la loi $\times$.

corps

On dit qu'un triplet $(K, +, \times)$ est un **corps** lorsque :

1. $(K, +, \times)$ anneau commutatif non nul.
2. Tout élément de $K \setminus \{0_K\}$ admet un inverse pour $\times$ dans K .

Morphisme d'anneaux

morphisme d'anneaux, isomorphisme d'anneaux

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux de neutres respectifs $0_A, 0_B$ et d'éléments unités respectifs $1_A, 1_B$. Soit $f : A \longrightarrow B$ une application.

1. On dit que f est un **morphisme d'anneaux** si :
 - a. $f(1_A) = 1_B$.
 - b. $\forall (a, a') \in A^2, \quad f(a + a') = f(a) + f(a') \quad \text{et} \quad f(a \times a') = f(a) \times f(a')$.
2. On dit que f est un **isomorphisme d'anneaux** si f est un morphisme d'anneaux bijectif.

propriétés

- 1.** Soient A, B deux anneaux de neutres respectifs $0_A, 0_B$ et $f: A \longrightarrow B$ un morphisme d'anneaux.

- a. $f(0_A) = 0_B$.
b. $\forall a \in A, f(-a) = -f(a)$.
c. $\forall a \in A, \forall n \in \mathbb{Z}, f(na) = nf(a)$.
d. $\forall a \in A, \forall n \in \mathbb{N}, f(a^n) = (f(a))^n$.
e. $\forall a \in A, a \in \mathbb{U}(A) \implies \begin{cases} f(a) \in \mathbb{U}(B) \\ (f(a))^{-1} = f(a^{-1}) \end{cases}$.

2. La composée de deux morphismes (resp. isomorphismes) d'anneaux est un morphisme (resp. isomorphisme) d'anneaux.
3. L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

3 Groupe symétrique

Permutation de $\{1, \dots, n\}$

Définition 3.1.

permutation de $\{1, \dots, n\}$

Une **permutation** de $\{1, \dots, n\}$ est une bijection de $\{1, \dots, n\}$ vers lui-même. Une permutation σ se note :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Par la bijectivité de σ , les éléments $1, 2, \dots, n$ figurent une fois et une seule sur la seconde ligne.

Définition 3.2.

support d'une permutation

On appelle **support** d'une permutation $\sigma \in \mathcal{S}_n$ l'ensemble des éléments de $\{1, \dots, n\}$ non invariants c-à-d :

$$\text{supp}(\sigma) = \{i \in \llbracket 1, n \rrbracket, \sigma(i) \neq i\}.$$

Théorème 3.1.

structure de $\mathcal{S}_n$

L'ensemble $\mathcal{S}_n$ des permutations de $\{1, \dots, n\}$ est un **groupe** pour la loi $\circ$ de composition et de neutre la permutation identité Id.

- Le groupe $\mathcal{S}_n$ possède $n!$ éléments et n'est pas commutatif dès que $n \geq 3$.
- Pour toute permutation $\sigma \in \mathcal{S}_n$ et tout entier $k \in \mathbb{Z}$, on note σ^k la permutation de $\mathcal{S}_n$ définie par :

$$\sigma^k \stackrel{\text{déf}}{=} \begin{cases} \text{Id} & \text{si } k = 0 \\ \sigma \circ \dots \circ \sigma \text{ (} k \text{ fois)} & \text{si } k \geq 1 \\ (\sigma^{-k})^{-1} & \text{si } k \leq -1 \end{cases}.$$

Définition 3.3.

groupe symétrique

Le groupe $\mathcal{S}_n$ est appelé **groupe symétrique** d'ordre n .

Cycles, transpositions

Définition 3.4.

cycle

Soit $p \geq 2$ un entier et $a_1, \dots, a_p$ des éléments deux à deux distincts de $\{1, \dots, n\}$.

Sur $\{1, \dots, n\}$, on définit une permutation c en posant :

$$\begin{cases} c(a_i) = a_{i+1} & \text{si } 1 \leq i \leq p-1 \\ c(a_p) = a_1 \\ c(x) = x & \text{si } x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_p\} \end{cases}.$$

On dit que c est un **cycle de longueur p** (ou encore un **p -cycle**). On le note $c = (a_1 \ a_2 \ \dots \ a_p)$.

- L'ensemble $\{a_1, \dots, a_p\}$ constitue le support du cycle c : $\text{supp}(c) = \{a_1, \dots, a_p\}$.
- Un cycle c de longueur p vérifie : $c^p = \text{Id}$. L'inverse d'un cycle est encore un cycle :

$$(a_1 \ a_2 \ \dots \ a_p)^{-1} = (a_p \ a_{p-1} \ \dots \ a_1).$$

- Soient σ et σ' deux cycles. La composée de σ et σ' est notée : $\sigma \circ \sigma' \stackrel{\text{déf}}{=} \sigma \sigma'$. Lorsque les supports sont disjoints, cette composée est **commutative** : $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset \implies \sigma \sigma' = \sigma' \sigma$.

Théorème 3.2.

décomposition d'une permutation en produit de cycles

Toute permutation σ de $\{1, \dots, n\}$ peut s'écrire comme un produit de cycles à supports disjoints. De plus, cette décomposition est **unique** à l'ordre près des facteurs.

Définition 3.5.**transposition**

On appelle **transposition** tout cycle de longueur 2.

- Pour $i, j \in \{1, \dots, n\}$ distincts, une transposition $\tau = (i \ j)$ a pour **seul effet d'échanger** i et j .
- Une transposition τ vérifie : $\tau^2 = \text{Id}$ et donc $\tau^{-1} = \tau$.

Théorème 3.3.**décomposition d'un cycle en produit de transpositions**

Tout cycle de longueur p peut s'écrire comme un produit de $p - 1$ transpositions :

$$(a_1 \ a_2 \ \dots \ a_p) = (a_1 \ a_2)(a_2 \ a_3) \dots (a_{p-1} \ a_p).$$

Corollaire 3.1.**décomposition d'une permutation en produit de transpositions**

Toute permutation de $\{1, \dots, n\}$ peut se décomposer en un produit de transpositions.

Signature**Théorème 3.4.****signature**

Il **existe** un **unique morphisme**¹ de groupes noté ε de $(\mathcal{S}_n, \circ)$ vers $(\{-1, 1\}, \times)$ tel que :

$$\varepsilon(\tau) = -1 \text{ pour toute transposition } \tau \text{ de } \mathcal{S}_n.$$

L'application ε est appelée **signature**.

1. $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ pour toutes permutations σ et σ' de $\mathcal{S}_n$.

Proposition 3.1.**signature d'un cycle et d'une permutation**

1. Si c est un cycle de longueur p , alors $\varepsilon(c) = (-1)^{p-1}$.
2. Si une permutation σ s'écrit comme produit de r transpositions, $\sigma = \tau_1 \dots \tau_r$, alors $\varepsilon(\sigma) = (-1)^r$.