Lois de compostions, groupes

R1.07 - Outils mathématiques

monnerat@u-pec.fr

10 novembre 2023

IUT de Fontainebleau

Loi de composition

Loi de composition

Défintion

Définition

loi de composition interne

Une loi de composition interne $*$ sur un ensemble E est une application de $E \times E$ dans E.

Notations

- Plutôt que de noter $f(x, y)$ l'image du couple (x, y), on note $x * y$, xTy, $u + v$, $u.v$, etc... (notation infixée).
- On parle souvent d'opération, ou de loi.
- On note $(E, *)$ un ensemble muni d'une loi de composition $*$.

Exemples :

- Les lois $\cup$, $\cap$, Δ sur $\mathcal{P}(E)$.
- La loi $\circ$ (composition) sur E^E (application de E dans E).
- Les lois $+$ et $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
- Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (ou sur tout ensemble totalement ordonné), les lois min et max notées (notation préfixée) $\min(x, y)$ et $\max(x, y)$.
- La "différence" est une loi sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, mais pas sur $\mathbb{N}$.
- L'implication logique sur l'ensemble $\{0, 1\}$.

Si $*$ est une opération sur F, on munit F^E de la loi notée encore $*$ en posant pour $f, g \in F^E$: $\forall x \in E,\ (f * g)(x) = f(x) * g(x)$.

Partie stable

Partie stable

On dit que $F \subset E$ est stable pour la loi $*$ définie sur E ssi

$$\forall (x, y) \in F^2, \quad x * y \in F$$

La restriction à $F \times F$ de $*$ définit donc une loi (induite) notée encore $*$.

Exemples :

- $\mathbb{R}_+$ et $\mathbb{R}_-$ sont stables pour la loi $+$.
- pour la loi $\times$, $\mathbb{R}_+$ est stable, mais pas $\mathbb{R}_-$.
- $[-1, 1]$ est stable pour la loi $\times$.

Homomorphismes

Soient E et F deux ensembles munis des lois $*$ et T. On dit que $f \in F^E$ est un homomorphisme (ou morphisme) de $(E, *)$ dans (F, T) ssi

$$\forall (x, y) \in E^2, \quad f(x * y) = f(x) T f(y)$$

Cas particuliers :

- Un morphisme de $(E, *)$ dans lui-même s'appelle un endomorphisme.
- Un morphisme bijectif de $(E, *)$ dans (F, T) est un isomormhisme.
- Un isomorphisme de $(E, *)$ dans lui-même est un automorphisme.

Si f est un isomorphisme de $(E, *)$ dans $(F, *)$, alors f^{-1} est un isomorphisme de (F, T) dans $(E, *)$.

- "le complémentaire" est un isomorphisme de $(\mathcal{P}(E), \cup)$ dans $(\mathcal{P}(E), \cap)$. Isomorphisme réciproque ?
- $x \to exp(x)$ est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.
- $x \to \ln(x)$ est un isomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

Loi de composition

Propriétés

Propriétés

Propriétés

Commutativité : $\forall (x, y) \in E^2,\ x * y = y * x$

Associativité : $\forall (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z$

Exemples :

- Les lois $+$ et $\times$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont commutatives et associatives.
- Idem pour les lois min et max sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- Idem pour $\cap, \cup, \Delta$ sur $\mathcal{P}(E)$.
- La loi $-$ (sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) n'est ni commutative, ni associative.
- La loi $\circ$ sur E^E est associative, mais pas commutative.
- $\to$ n'est ni associative, ni commutative sur $\{0, 1\}$.

Remarques :

- Lorsque la loi est associative, l'écriture $a * b * \ldots * x * y$ est définie sans ambiguité. On note alors

$$a^n = \underbrace{a * a * \ldots * a}_{n \text{ fois}}$$

- On note également $\min(x, y, z, \ldots)$.

Distributivité

Distributivité

Soit E un ensemble muni de deux lois $*$ et T. On dit que la loi $*$ est distributive par rapport à la loi T ssi $\forall (x,y,z) \in E^3$:

$$\begin{cases} x*(yTz) &= (x*y)T(x*z) & \text{distributivité à gauche} \\ (xTy)*z &= (x*z)T(y*z) & \text{distributivité à droite} \end{cases}$$

Exemples :

- Dans $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une sur l'autre.
- Dans $\mathcal{P}(E)$, la loi $\cap$ est distributive par rapport à Δ. En revanche, la loi Δ n'est pas distributive par rapport à $\cup$.
- Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, la loi $\times$ est distributive par rapport à $+$.
- La distributivité de $*$ par rapport à T permet d'écrire :

$$(aTb)*(cTd) = [(a*c)T(b*c)]T[(a*d)T(b*d)]$$

Elément neutre

Élement neutre

Soit E un ensemble muni d'une loi $*$. $e \in E$ est dit élément neutre ssi il vérifie

$$\forall x \in E,\ x * e = e * x = x$$

Unicité : Si e existe, il est unique. S'il y en avait deux, e et e', on aurait :

$$\left.\begin{array}{l} e * e' = e \\ e * e' = e' \end{array}\right\} \Rightarrow e = e'$$

Exemples :

- Dans $\mathcal{P}(E)$: $\emptyset$ est le neutre de $\cup$ et Δ, E est le neutre pour $\cap$.
- Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$: 0 est le neutre pour $+$, et 1 pour $\times$.
- Dans E^E : id_E est le neutre pour $\circ$.
- Dans $\mathbb{N}$: 0 est le neutre pour la loi max, pas de neutre pour min.
- Dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$: min et max n'ont pas de neutre.

Groupe

Groupe

Monoïde

Structure de monoïde

Monoïde

Soit E muni de la loi $*$. On dit que $(E, *)$ est un monoïde ssi $*$ est associative **et** posséde un élément neutre.

Exemples :

- $(\mathcal{P}(E), \cap)$, $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \Delta)$ sont des monoïdes.
- $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes.
- $(E^E, \circ)$ est un monoïde.
- Les chaînes de caractères avec la concaténation (cf module Langages).

Éléments symétrisables

Notion de symétrique

Soit $(E, *)$ un monoïde d'élément neutre e et $x \in E$. x est dit :

- symétrisable à gauche s'il existe $x' \in E$ tel que $x' * x = e$.
- symétrisable à droite s'il existe $x' \in E$ tel que $x * x' = e$.
- symétrisable s'il existe $x' \in E$ tel que $x * x' = x' * x = e$.

Si x est symétrisable, x' est unique. On l'appelle le symétrique ou l'inverse de x (noté x^{-1}).

Soient x' et x'' deux inverses de x. Par associativité,

$$\begin{aligned} x' * x * x'' &= (x' * x*) * x'' = e * x'' = x'' \\ &= x' * (x * x'') = x' * e = x' \end{aligned}$$

Propriétés et remarques

- L'élément neutre e est son propre inverse.
- Pour x inversible : $(x^{-1})^{-1} = x$.
- Quand x est symétrisable, on peut étendre la notation x^n aux entiers négatifs : $x^{-n} = (x^{-1})^n$. ($x^0 = e$)
- Si x et y sont inversibles, alors $x * y$ est inversible, d'inverse $y^{-1} * x^{-1}$.
- Si a est symétrisable, l'équation $a * x = b$ admet une unique solution, $x = a^{-1} * b$. (l'application $x \to a * x$ est bijective)
- Exemples :
  - Dans $(\mathbb{N}, +)$, seul 0 est symétrisable, mais tous les éléments de $(\mathbb{Z}, +), \ldots, (\mathbb{R}, +)$ le sont.
  - Les éléments symétrisables de $(\mathbb{Z}, \times)$ sont -1 et 1, et ceux de $(\mathbb{R}, \times)$ sont les réels non nuls.
  - Tout élément de $(\mathcal{P}(E), \Delta)$ est symétrisable.

Notations

	notation multiplicative	notation additive
monoïde	$(E, .)$	$(E, +)$
neutre	1_E	0_E
symétrique	x^{-1}	$-x$
composition	x^n	nx

Groupe

Groupe

Structure de Groupe

Groupe

Soit G un ensemble muni d'une loi $*$. On dit que $(G, *)$ est un groupe ssi :

- $(G, *)$ est un monoïde. ($*$ associative et il y a un neutre)
- Tout élément de G admet un symétrique.

Si la loi est commutative, on dit que le groupe est commutatif, ou Abélien.

Si G est fini, le cardinal $|G|$ s'appelle l'ordre du groupe.

Exemples et remarques :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sont des groupes abéliens.
- $(\{-1, 1\}, \times)$, $(\mathbb{Q}^*, \times)$,$(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ sont des groupes abéliens.
- Si E est un ensemble,

  $$(\sigma(E), \circ)$$

  (ensemble des bijections de $E \to E$ muni de la composition) est un groupe non commutatif (dès que $|E| \geq 3$).
- Si E est fini, quel est l'ordre de $\sigma(E)$?

Table d'un groupe ou d'une loi

Quand l'ensemble est fini on peut représenter la loi sous la forme d'une table. Si $G = \{a_1, \ldots, a_n\}$, on donne sous forme d'un tableau $n \times n$ les composés $a_i * a_j$ pour tous les couples (i, j) en ligne i et colonne j.

Exemple : soit la loi de groupe sur $A = \{1, 2, 3, 4, 5, 6\}$ définie par

$x * y = (x \times y) \mod 7$

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- $2 * (4 * 6) = 2 * 3 = 6$.
- $*$ est commutative.
- 1 est le neutre.
- $2^{-1} = 4$, $4^{-1} = 2$.
- $3^{-1} = 5$, $5^{-1} = 3$.
- $6^{-1} = 6$.

On remarque que chaque élément apparaît une et une seule fois sur chaque ligne et colonne. Pourquoi ?

Sous-groupe

Définition : Soit $(G, *)$ un groupe et $H \subset G$. On dit que H est un sous groupe de G ssi :

- H est stable pour la loi $*$.
- muni de la loi induite, $(H, *)$ est lui-même un groupe.

Caractérisation : Soit $(G, *)$ un groupe et $H \subset G$. Alors H est un sous-groupe de G ssi :

- H est non vide.
- $\forall (x, y) \in H^2,\ x * y^{-1} \in H$. (stabilité par produit et inversion)

Remarque : Dans un sous-groupe, il y a toujours l'élément neutre.

Exemples

- $\{e\}$ et G sont des sous groupes de $(G, *)$.
- Soit $n \in \mathbb{N}$. On note $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Alors $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Sous-Groupes de $(\mathbb{Z}, +)$

Théorème

les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

On a déjà vu que les $n\mathbb{Z}$ sont des sous-groupes. Réciproquement, soit $G \subset \mathbb{Z}$ un sous groupe :

Si $G = \{0\}$, $G = 0\mathbb{Z}$, et c'est fini.

Sinon, $G \cap \mathbb{N}_+^*$ est non vide (il y a un élément non nul **et** son opposé dans G

Soit $n > 0$ le minimum de $G \cap \mathbb{N}_+^*$.

Puisque $n \in G$, on a $n\mathbb{Z} \subset G$, puisque G stable par produit et opposé.

Soit $x \in G$. La **division euclidienne** de x par n donne $x = q.n + r$, avec $0 \leq r < n$.

Mais $r = x - q.n \in G$, puisque G est un sous-groupe. Si $r \neq 0$, on aurait donc $r \in G \cap \mathbb{N}_+^*$ avec $r < n$, ce qui contredit le statut de n. Donc $r = 0$.

D'où $G \subset n\mathbb{Z}$. Finallement $G = n\mathbb{Z}$.

Groupe

Groupe fini

Groupe fini

Théorème de Lagrange

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

Preuve :

- On considère la relation d'équivalence (le vérifier)

$$x \mathcal{R} y \Leftrightarrow y \in x.H$$

- Toutes les classes ont le même cardinal, celui de H.
- L'ensemble des classes forment une partition, le cardinal de G est donc un multiple de celui de H.

Par exemple, si $|G| = 6$, et H un sous groupe de G, les ordres possibles pour H sont $1, 2, 3, 6$

Ordre d'un élément

Ordre d'un élément : Soit $x \in (G, *)$ fini de cardinal n. Alors :

Il existe des entiers $k > 0$ tels que $x^k = e$.

- L'ensemble $\{e, x^1, \ldots, x^n\}$ est inclus dans G. D'après le principe des tiroirs, il existe deux entiers $i < j$ tels que $x^i = x^j$
- D'où $x^{j-i} = e$ avec $j - i > 0$.

Ordre d'un élément

On appelle ordre de x le plus petit entier $l > 0$ tel que $x^l = e$. on le note $ord(x)$ où $|x|$.

Groupe engendré par un élément

Groupe en engendré par x

$$gr(x) =< x >= \{e, x, x^2, \ldots, x^{ord(x)-1}\}$$

est un sous groupe (cyclique) de G (groupe engendré par x, noté $< x >$ ou $gr(x)$). C'est le plus petit sous groupe de G contenant x.

En particulier

$$x^{-1} = x^{ord(x)-1} \text{ et } x^n = e \Leftrightarrow ord(x) \text{ divise } n$$

L'ordre du groupe $gr(x)$ est l'ordre de x : $|gr(x)| = ord(x)$.

D'après le théorème de Lagrange, $|gr(x)|$ divise $|G|$, on a donc toujours

$$x^{|G|} = e$$

Exemple 1 : $(\mathbb{Z}/6\mathbb{Z}, +)$

loi de groupe $(x + y) \mod 6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	1	0
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- 1 est d'ordre 6.
  $gr(\{1\}) = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}/6\mathbb{Z}$.
- 2 est d'ordre 3. $gr(\{2\}) = \{0, 2, 4\}$.
- 3 est d'ordre 2. $gr(\{3\}) = \{0, 3\}$.
- 4 est d'ordre 3. $gr(\{4\}) = \{0, 4, 2\}$.
- 5 est d'ordre 6.
  $gr(\{5\}) = \{0, 5, 2, 4, 3, 2, 1\} = \mathbb{Z}/6\mathbb{Z}$.

1 et 5 sont générateurs de $\mathbb{Z}/6\mathbb{Z}$.

Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $(n > 0)$, 1 est toujours générateur.

On dit que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, ou monogène.

Exemple 2 : $(\mathbb{Z}/10\mathbb{Z}, .)^*$

.	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

- Les éléments inversibles sont : 1, 3, 7, 9.
- $|(\mathbb{Z}/10\mathbb{Z})^*| = 4$
- On vérifie le théorème de Lagrange : $1^4 = 3^4 = 7^4 = 9^4 = 1$.
- 1 est d'ordre 1.
- 3 et 7 sont d'ordre 4. $(\mathbb{Z}/10\mathbb{Z})^*$ est donc cyclique.
- 9 est d'ordre 2.

Exemple 3 : $\mathfrak{S}_3$

Groupe $\mathfrak{S}_3$

$$t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \; t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \; t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \; i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$\circ$	i	σ_1	σ_2	t_1	t_2	t_3
i	i	σ_1	σ_2	t_1	t_2	t_3
σ_1	σ_1	σ_2	i	t_3	t_1	t_2
σ_2	σ_2	i	σ_1	t_2	t_3	t_1
t_1	t_1	t_2	t_3	i	σ_1	σ_2
t_2	t_2	t_3	t_1	σ_2	i	σ_1
t_3	t_3	t_1	t_2	σ_1	σ_2	i

- i est d'ordre 1.
- t_1, t_2, t_3 sont d'ordre 2.
- σ_1, σ_2 sont d'ordre 3.
- $\{i, \sigma_1, \sigma_2\}$ est un sous groupe d'ordre 3.
- $\sigma_1^{-1} = \sigma_2$ et $\sigma_2^{-1} = \sigma_1$.
- $\mathfrak{S}_3$ n'est pas cyclique.