Chapitre 3

Groupes

Additionner des entiers, composer des applications, multiplier des matrices : ces opérations n'ont rien à voir entre elles, et pourtant elles obéissent aux mêmes règles. Plutôt que de refaire dix fois les mêmes raisonnements, l'algèbre choisit d'isoler ces règles communes et de les étudier une fois pour toutes. C'est la démarche **structurale**, dont le **groupe** est la première et la plus simple des structures.

3.1 Lois de composition interne

3.1.1 Définition

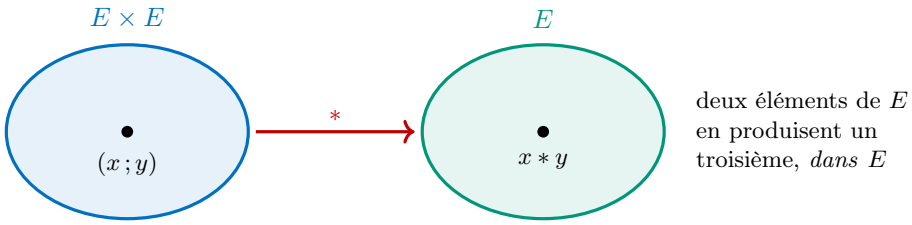
Définition : Soit E un ensemble. On appelle **loi de composition interne** sur E, en abrégé **L.C.I.**, toute application :

$$\Phi : E \times E \longrightarrow E$$

Pour $(x\,;y) \in E^2$, l'image $\Phi(x\,;y)$ se note selon les situations :

$$x * y \qquad x \cdot y \qquad x + y \qquad x \circ y \qquad x \perp y$$

Remarque : Le mot *interne* porte toute la définition : le résultat doit rester *dans* E. Ainsi la soustraction est une L.C.I. sur $\mathbb{Z}$, mais pas sur $\mathbb{N}$, puisque $3 - 5$ en sort.



Définition : Soit $*$ une L.C.I. sur E. On dit qu'elle est :

- **commutative** si $\forall (x\,;y) \in E^2,\ x * y = y * x$;
- **associative** si $\forall (x\,;y\,;z) \in E^3,\ (x * y) * z = x * (y * z)$.

Dans ce dernier cas, et dans ce cas seulement, on peut écrire $x * y * z$ sans parenthèses.

Un élément $e \in E$ est un **élément neutre** pour $*$ lorsque :

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

Remarque : Aucune de ces trois propriétés n'est automatique. La composition des applications de E dans E n'est en général pas commutative, et l'on rencontrera des lois non associatives, comme la soustraction sur $\mathbb{Z}$:

$$(5 - 3) - 1 = 1 \qquad \text{tandis que} \qquad 5 - (3 - 1) = 3$$

Propriété 1 : Si une L.C.I. admet un élément neutre, alors celui-ci est **unique**.

∘ *Démonstration :* Supposons que e et e' soient deux éléments neutres, et calculons $e * e'$ de deux façons. Comme e' est neutre, $e * e' = e$; comme e est neutre, $e * e' = e'$. Ces deux calculs portant sur le même élément, on en déduit $e = e'$. □

3.1.2 Symétrique

Définition : Soit $*$ une L.C.I. sur E admettant un neutre e. On appelle **symétrique** d'un élément x tout élément $y \in E$ tel que :

$$x * y = y * x = e$$

Propriété 2 : Si la loi $*$ est *associative*, alors le symétrique d'un élément, lorsqu'il existe, est **unique**.

∘ *Démonstration :* Soient y et y' deux symétriques de x, et calculons $y * x * y'$ de deux façons, ce que l'associativité autorise :

$$\left.\begin{array}{rcccl} (y * x) * y' & = & e * y' & = & y' \\ y * (x * y') & = & y * e & = & y \end{array}\right\} \implies y = y'$$

□

Remarque : Quelques conventions et conséquences :

- le neutre est toujours son propre symétrique, puisque $e * e = e$;
- pour une loi notée **additivement**, le neutre se note 0 et le symétrique de x se note $-x$, appelé son **opposé** ;
- pour une loi notée **multiplicativement**, le neutre se note 1 et le symétrique se note x^{-1}, appelé son **inverse**. Les éléments qui en admettent un sont dits **inversibles**.

3.1.3 Un catalogue d'exemples

Exemple : Passons en revue quelques lois usuelles. Le tableau ci-dessous se lit ligne par ligne, et servira de réservoir d'exemples pour tout le chapitre.

Loi	Commutative	Associative	Neutre	Éléments symétrisables
$+$ sur $\mathbb{N}$	oui	oui	0	0 seulement
$\times$ sur $\mathbb{N}$	oui	oui	1	1 seulement
$+$ sur $\mathbb{Z}$	oui	oui	0	tous
$\circ$ sur E^E	non	oui	Id_E	les bijections
$\cap$ sur $\mathcal{P}(E)$	oui	oui	E	E seulement
$\cup$ sur $\mathcal{P}(E)$	oui	oui	$\varnothing$	$\varnothing$ seulement

La dernière colonne est la plus intéressante : elle mesure à quel point la loi est *réversible*. Sur $\mathbb{N}$, l'addition ne se défait pas, et c'est précisément pour y remédier que l'on construit $\mathbb{Z}$.

Remarque : Lorsque E est fini, on décrit commodément une L.C.I. par sa **table**, dite **table de Cayley** : on y lit à l'intersection de la ligne x et de la colonne y le résultat $x * y$. Voici celle de la multiplication sur $\{1\,;\mathrm{i}\,;-1\,;-\mathrm{i}\}$.

$\times$	1	i	-1	$-$i
1	1	i	-1	$-$i
i	i	-1	$-$i	1
-1	-1	$-$i	1	i
$-$i	$-$i	1	i	-1

Trois lectures immédiates : la table est *symétrique* par rapport à sa diagonale, donc la loi est commutative ; la première ligne reproduit l'en-tête, donc 1 est neutre ; le neutre apparaît *une fois dans chaque ligne*, en vert, donc tout élément admet un symétrique.

3.2 Groupes

3.2.1 Définition et exemples

Définition : On appelle **groupe** tout couple $(G\,;*)$ vérifiant les quatre conditions suivantes :

I : G est un ensemble et $*$ est une L.C.I. sur G ;

A : $*$ est associative ;

N : il existe un neutre dans G pour $*$;

S : tout élément de G admet un symétrique pour $*$.

Si de plus $*$ est commutative, le groupe est dit **abélien**.

Remarque : L'acronyme **IANS** donne l'ordre de vérification, et il faut s'y tenir : il est vain de chercher un symétrique avant d'avoir établi l'existence du neutre, et vain de chercher un neutre avant de savoir que la loi est bien interne. Notez que la commutativité *ne figure pas* dans la liste : la plupart des groupes intéressants ne sont pas abéliens.

Exemple : Reprenons le catalogue précédent à la lumière de cette définition.

- $(\mathbb{Z}\,;+)$, $(\mathbb{Q}\,;+)$, $(\mathbb{R}\,;+)$ sont des groupes abéliens, de neutre 0 ;
- $(\mathbb{N}\,;+)$ n'en est pas un : l'axiome **S** échoue, car 3 n'a pas d'opposé dans $\mathbb{N}$;
- $(\mathbb{R}\,;\times)$ n'en est pas un non plus : 0 n'admet pas d'inverse. En revanche $(\mathbb{R}^*\,;\times)$ est un groupe abélien de neutre 1 ;
- l'ensemble des *bijections* de E dans E, muni de $\circ$, est un groupe, appelé **groupe symétrique** de E. Il n'est pas abélien dès que E possède au moins trois éléments.

3.2.2 Premières propriétés

Propriété 3 : Soit $(G\,;\times)$ un groupe. Alors, pour tout couple $(x\,;y) \in G^2$:

$$(x \times y)^{-1} = y^{-1} \times x^{-1}$$

$\circ$ *Démonstration :* Il suffit de vérifier que $y^{-1} \times x^{-1}$ se comporte comme l'inverse de $x \times y$, dans les deux sens :

$$\left.\begin{array}{rcl} (x \times y) \times (y^{-1} \times x^{-1}) & = & x \times \underbrace{y \times y^{-1}}_{=e} \times x^{-1} = x \times x^{-1} = e \\ (y^{-1} \times x^{-1}) \times (x \times y) & = & y^{-1} \times \underbrace{x^{-1} \times x}_{=e} \times y = y^{-1} \times y = e \end{array}\right\}$$

L'unicité du symétrique, établie à la proposition 2, permet alors de conclure. □

Remarque : L'**inversion renverse l'ordre**. L'image est parlante : pour défaire l'action « enfiler ses chaussettes puis ses chaussures », il faut retirer les chaussures *d'abord*, puis les chaussettes. Dans un groupe abélien, cette précaution est superflue, mais elle devient essentielle pour les matrices ou les permutations.

Propriété 4 (groupe produit) : Soient $(G\,;\cdot)$ et $(H\,;*)$ deux groupes. Posons, pour tous $\big((x\,;y)\,;(x'\,;y')\big) \in (G\times H)^2$:

$$(x\,;y)\perp(x'\,;y') = (x\cdot x'\,;\, y*y')$$

Alors $(G\times H\,;\perp)$ est un groupe, appelé **groupe produit** de G et H.

∘ *Démonstration :* On vérifie les quatre axiomes, chacun *composante par composante*. La loi est interne puisque $x\cdot x'\in G$ et $y*y'\in H$. Elle est associative, car elle l'est sur chaque composante. Le couple $(e_G\,;e_H)$ est neutre, et le symétrique de $(x\,;y)$ est $(x^{-1}\,;y^{-1})$. □

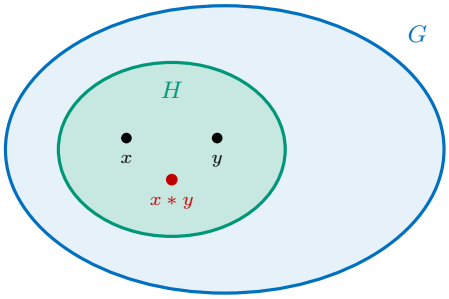
Exemple : Le plan $\mathbb{R}^2$, muni de l'addition $(x\,;y)+(x'\,;y') = (x+x'\,;y+y')$, est le groupe produit de $(\mathbb{R}\,;+)$ par lui-même. C'est exactement l'addition des vecteurs du plan.

3.3 Sous-groupes

Définition : Soit $(G\,;*)$ un groupe et H une partie de G. On dit que H est un **sous-groupe** de G lorsque :

- H contient l'élément neutre e de G ;
- H est **stable par la loi** : $\forall(x\,;y)\in H^2,\ x*y\in H$;
- H est **stable par passage au symétrique** : $\forall x\in H,\ x^{-1}\in H$.

Remarque : Un sous-groupe est alors lui-même un groupe pour la loi de G, et c'est tout l'intérêt de la notion : plutôt que de revérifier les quatre axiomes, il suffit d'en vérifier trois, dont deux sont de simples stabilités. L'associativité, elle, est héritée gratuitement.



le produit de deux éléments de H ne *sort pas* de H

Propriété 5 (caractérisation des sous-groupes) : Soit $(G\,;\cdot)$ un groupe et H une partie de G. Alors :

$$H \text{ est un sous-groupe de } G \iff \begin{cases} H\neq\varnothing \\ \forall(x\,;y)\in H^2,\ xy^{-1}\in H \end{cases}$$

∘ *Démonstration :* Sens direct : si H est un sous-groupe, il contient e donc n'est pas vide, et pour $(x\,;y)\in H^2$, on a $y^{-1}\in H$ puis $xy^{-1}\in H$ par stabilité.

Réciproque : supposons les deux conditions vérifiées. Comme H n'est pas vide, il contient un élément a ; en appliquant la seconde condition au couple $(a\,;a)$, on obtient $aa^{-1}=e\in H$. Soit alors $x\in H$: le couple $(e\,;x)$ donne $ex^{-1}=x^{-1}\in H$, d'où la stabilité par symétrique. Enfin, pour $(x\,;y)\in H^2$, on sait désormais que $y^{-1}\in H$, et le couple $(x\,;y^{-1})$ donne $x(y^{-1})^{-1}=xy\in H$. □

Méthode : Pour démontrer qu'une partie H est un sous-groupe de G :

1. On vérifie que $H\subset G$, ce qui est souvent immédiat mais doit être écrit.
2. On montre que $H\neq\varnothing$, en exhibant un élément — presque toujours le neutre.
3. On prend $(x\,;y)\in H^2$ quelconque et l'on montre que $xy^{-1}\in H$.

Cette caractérisation en deux points est bien plus rapide que le retour à la définition, et c'est elle que l'on utilise en pratique.

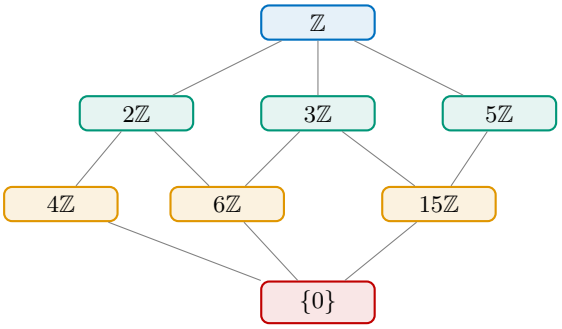
Exemple : Montrons que $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}\,;+)$.

D'abord $2\mathbb{Z} \subset \mathbb{Z}$, et $0 = 2\times 0$ appartient à $2\mathbb{Z}$, qui n'est donc pas vide. Soient ensuite x et y dans $2\mathbb{Z}$: il existe k et k' entiers tels que $x = 2k$ et $y = 2k'$. Comme la loi est notée additivement, le symétrique de y est $-y$, et :

$$x - y = 2k - 2k' = 2(k - k')$$

avec $k - k' \in \mathbb{Z}$. Donc $x - y \in 2\mathbb{Z}$, et $2\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.

Remarque : Le même raisonnement montre que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour tout entier n, et l'on démontre — c'est un résultat important de l'arithmétique — que ce sont là *les seuls* sous-groupes de $(\mathbb{Z}\,;+)$.



chaque trait indique une inclusion : $6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$

Les inclusions entre ces sous-groupes reflètent exactement la divisibilité : $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. Le groupe $\mathbb{Z}$ tout entier correspond à $n = 1$, et le sous-groupe trivial $\{0\}$ à $n = 0$.