Chapitre 5

Structures algébriques

Un groupe ne possède qu'une seule loi. Or les ensembles de nombres en portent deux, une addition et une multiplication, liées entre elles par la distributivité. Ce chapitre enrichit donc progressivement la structure : à l'anneau, qui autorise le calcul algébrique ordinaire, succède le corps, dans lequel la division devient possible. Chaque axiome ajouté restreint la famille des exemples, mais accroît la puissance des résultats.

5.1 Anneaux

5.1.1 Définition

Définition : Soit G un ensemble muni de deux lois de composition interne $\cdot$ et $*$. On dit que $*$ est **distributive** sur $\cdot$ lorsque, pour tout $(x\,;y\,;z) \in G^3$:

$$x * (y \cdot z) = (x * y) \cdot (x * z) \qquad \text{et} \qquad (y \cdot z) * x = (y * x) \cdot (z * x)$$

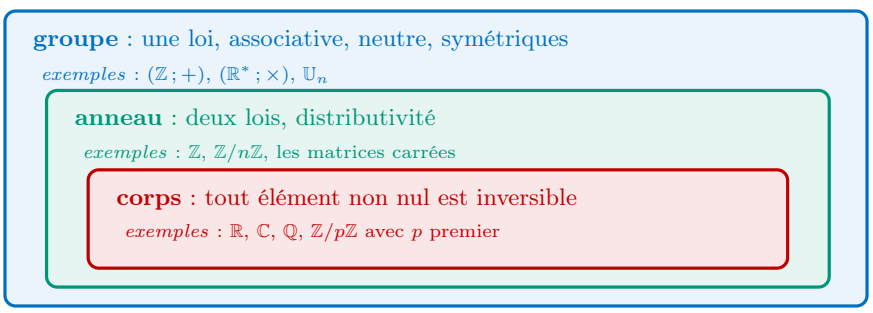
Remarque : Les deux égalités sont nécessaires tant que $*$ n'est pas supposée commutative : c'est la distributivité *à gauche* puis *à droite*. Sur $\mathbb{R}$, elles se confondent avec la règle de développement bien connue $a(b+c) = ab + ac$.

Définition : On appelle **anneau** tout triplet $(A\,;+\,;\times)$ où A est un ensemble muni de deux L.C.I. vérifiant :

- **N** : A contient un **neutre** 1_A pour $\times$, différent du neutre 0_A pour $+$;
- **A** : $(A\,;+)$ est un groupe **abélien** ;
- **D** : la loi $\times$ est **distributive** sur la loi $+$;
- **A** : la loi $\times$ est **associative**.

L'anneau est dit **commutatif** lorsque $\times$ est commutative. Une partie B de A est un **sous-anneau** lorsque la restriction des deux lois à B en fait un anneau.

Remarque : Notez l'asymétrie entre les deux lois : l'addition doit faire de A un groupe *abélien*, alors que la multiplication n'a besoin que d'être associative et de posséder un neutre. Aucun inverse n'est exigé pour $\times$, et c'est précisément ce que la structure de corps ajoutera en section 5.3.



Chaque structure est un cas particulier de la précédente, obtenu en ajoutant des axiomes : plus l'on descend, plus les exemples se raréfient, mais plus les théorèmes deviennent puissants.

Exemple : Quelques anneaux usuels :

- $(\mathbb{Z}\,;+\,;\times)$ est un anneau commutatif : c'est l'exemple fondateur ;
- $(\mathbb{R}^{\mathbb{R}}\,;+\,;\times)$, l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni des opérations point par point, est un anneau commutatif de neutres la fonction nulle et la fonction constante égale à 1 ;
- l'ensemble des matrices carrées de taille $n \geqslant 2$, muni de l'addition et du produit matriciel, est un anneau *non commutatif*.

Remarque : Dans un anneau, on dispose des règles de calcul habituelles, à une exception près de taille : un produit peut être nul sans qu'aucun facteur ne le soit. On parle alors de **diviseurs de zéro**. Dans $\mathbb{R}^{\mathbb{R}}$, par exemple, le produit de deux fonctions non nulles peut très bien être la fonction nulle, si leurs supports sont disjoints.

Nous en verrons un exemple numérique frappant en section 5.2, et cette anomalie disparaîtra dans les corps.

5.1.2 Sous-anneaux

Propriété 1 (caractérisation des sous-anneaux) : Soit $(A\,;+\,;\times)$ un anneau et B une partie de A. Alors :

$$B \text{ est un sous-anneau de } A \iff \begin{cases} 1_A \in B \\ \forall (x\,;y) \in B^2,\ x-y \in B \ \text{ et } \ xy \in B \end{cases}$$

∘ *Démonstration :* Le sens direct est immédiat, puisqu'un sous-anneau contient le neutre multiplicatif et est stable par les deux lois.

Réciproquement, supposons les deux conditions vérifiées. La première assure que B n'est pas vide, et la stabilité par $x-y$ signifie exactement, d'après le chapitre 3, que $(B\,;+)$ est un sous-groupe de $(A\,;+)$: il est donc un groupe abélien, la commutativité étant héritée. La stabilité par produit fait de $\times$ une L.C.I. sur B, associative et distributive puisqu'elle l'est déjà sur A. Enfin $1_A \in B$ fournit le neutre multiplicatif. □

Méthode : Pour montrer qu'une partie B est un sous-anneau de A :

1. On vérifie que $B \subset A$ et que $1_A \in B$.
2. On prend $(x\,;y) \in B^2$ quelconque et l'on montre que $x-y \in B$.
3. On montre, pour le même couple, que $xy \in B$.

Aucune vérification d'associativité ou de distributivité n'est nécessaire : ces propriétés sont héritées de A.

Exemple : Montrons que $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2} \;\middle|\; (a\,;b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $\mathbb{R}$.

D'abord $1 = 1+0\sqrt{2}$ appartient à cet ensemble. Soient ensuite $x = a+b\sqrt{2}$ et $y = c+d\sqrt{2}$ avec a, b, c, d entiers. Alors :

$$x-y = (a-c)+(b-d)\sqrt{2}$$

qui est bien de la forme voulue. Quant au produit, en développant et en utilisant $\left(\sqrt{2}\right)^2 = 2$:

$$xy = ac+ad\sqrt{2}+bc\sqrt{2}+2bd = \underbrace{(ac+2bd)}_{\in\mathbb{Z}} + \underbrace{(ad+bc)}_{\in\mathbb{Z}}\sqrt{2}$$

Les deux conditions sont vérifiées : $\mathbb{Z}\left[\sqrt{2}\right]$ est un sous-anneau de $\mathbb{R}$.

5.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

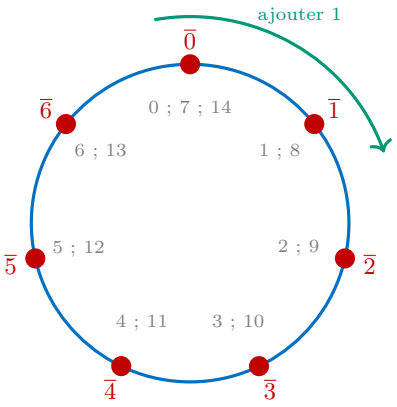
Définition : Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$. On appelle **classe d'équivalence de x pour la congruence modulo n** l'ensemble :

$$\overline{x} = \{y \in \mathbb{Z} \mid y \equiv x\ [n]\}$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalence.

Remarque : Deux entiers appartiennent à la même classe lorsqu'ils ont le même reste dans la division euclidienne par n. Les classes forment donc une **partition** de $\mathbb{Z}$ en exactement n paquets, représentés par $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$.

Un même paquet possède une infinité de noms : dans $\mathbb{Z}/7\mathbb{Z}$, on a $\overline{12} = \overline{5} = \overline{-2}$. C'est pourquoi toute définition portant sur les classes réclamera une précaution, comme on le verra à la proposition 2.



Compter dans $\mathbb{Z}/7\mathbb{Z}$, c'est tourner sur ce cadran : après $\overline{6}$, on revient à $\overline{0}$. C'est exactement le principe des jours de la semaine ou des heures sur une horloge.

Propriété 2 : Les opérations suivantes définissent deux L.C.I. sur $\mathbb{Z}/n\mathbb{Z}$:

$$\overline{x} + \overline{y} = \overline{x+y} \qquad \text{et} \qquad \overline{x} \times \overline{y} = \overline{xy}$$

de neutres respectifs $\overline{0}$ et $\overline{1}$. Muni de ces deux lois, $(\mathbb{Z}/n\mathbb{Z}\,;+\,;\times)$ est un **anneau commutatif**.

∘ *Démonstration :* Le point délicat, et le seul qui mérite attention, est de vérifier que ces définitions ont un *sens* : le résultat ne doit pas dépendre des représentants choisis.

Soient donc $x' \in \overline{x}$ et $y' \in \overline{y}$. Il existe alors deux entiers k et k' tels que $x' = x + kn$ et $y' = y + k'n$, d'où :

$$x' + y' = (x+y) + (k+k')n \qquad \text{et} \qquad x'y' = xy + \big(xk' + yk + kk'n\big)n$$

Ces deux résultats sont congrus à $x+y$ et xy modulo n : les classes obtenues sont bien les mêmes. Les axiomes d'anneau se transportent alors de $\mathbb{Z}$ à $\mathbb{Z}/n\mathbb{Z}$ sans difficulté. □

Exemple : Dans $\mathbb{Z}/7\mathbb{Z}$, on calcule sur les représentants avant de réduire :

$$\overline{6} \times \overline{5} = \overline{6 \times 5} = \overline{30} = \overline{2}$$

puisque $30 = 4 \times 7 + 2$.

Remarque : Voici l'anomalie annoncée en section 5.1. Dans $\mathbb{Z}/6\mathbb{Z}$:

$$\overline{2} \times \overline{3} = \overline{6} = \overline{0}$$

Deux classes non nulles ont donc un produit nul : ce sont des **diviseurs de zéro**. On ne peut par conséquent pas y simplifier une égalité comme on le ferait dans $\mathbb{R}$.

5.3 Corps

Définition : On appelle **corps** tout anneau commutatif non nul dont *tout élément non nul* est **inversible** pour la seconde loi. Autrement dit, $(A\,;+\,;\times)$ est un corps si et seulement si :

- ▷ $(A\,;+)$ est un groupe **abélien** ;
- ▷ $\big(A\setminus\{0_A\}\,;\times\big)$ est un groupe **abélien** ;
- ▷ la loi $\times$ est **distributive** sur la loi $+$.

Exemple : Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de leurs opérations usuelles, sont des corps.

En revanche $\mathbb{Z}$ n'en est pas un : c'est un anneau, mais 2 n'y admet pas d'inverse, puisque $\frac{1}{2}\notin\mathbb{Z}$. Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1.

Remarque : Attention à une erreur fréquente : $\mathbb{R}^n$ muni des opérations *coordonnée par coordonnée* n'est **pas** un corps dès que $n\geqslant 2$. En effet, dans $\mathbb{R}^2$:

$$(1\,;0)\times(0\,;1)=(0\,;0)$$

Deux éléments non nuls y ont un produit nul, ce qui interdit à l'un comme à l'autre d'être inversible. C'est un anneau, mais avec diviseurs de zéro.

De façon générale, **un corps ne possède jamais de diviseurs de zéro** : si $xy=0$ avec $x\neq 0$, il suffit de multiplier par x^{-1} pour obtenir $y=0$.

Théorème 1 : Corps $\mathbb{Z}/n\mathbb{Z}$:
Pour tout entier $n\in\mathbb{N}^*$:

$$(\mathbb{Z}/n\mathbb{Z}\,;+\,;\times)\text{ est un corps}\quad\Longleftrightarrow\quad n\text{ est premier}$$

∘ *Démonstration :* Sens direct : supposons que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Tout élément non nul y est inversible : pour $\overline{x}$ non nul, il existe $\overline{y}$ tel que $xy\equiv 1\ [n]$, c'est-à-dire qu'il existe $k\in\mathbb{Z}$ vérifiant :

$$xy=1+kn\qquad\text{soit}\qquad xy-kn=1$$

D'après le théorème de Bézout, x et n sont donc premiers entre eux. En prenant pour x chacun des représentants de $[\![1\,;n-1]\!]$, on obtient que n est premier avec tous les entiers qui lui sont inférieurs : n est premier.

Réciproque : supposons n premier, et soit $\overline{x}$ non nul, de représentant $x\in[\![1\,;n-1]\!]$. Comme n est premier et ne divise pas x, ces deux entiers sont premiers entre eux, et le théorème de Bézout fournit $(u\,;v)\in\mathbb{Z}^2$ tels que :

$$xu+nv=1$$

En passant modulo n, il vient $\overline{x}\times\overline{u}=\overline{1}$: la classe $\overline{x}$ est inversible, d'inverse $\overline{u}$. □

Les deux tables de multiplication ci-dessous illustrent ce théorème. À gauche $n=5$, qui est premier ; à droite $n=6$, qui ne l'est pas.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Dans $\mathbb{Z}/5\mathbb{Z}$, chaque ligne non nulle contient le neutre $\overline{1}$, en vert : tout élément est inversible, c'est un corps. Dans $\mathbb{Z}/6\mathbb{Z}$, les lignes de $\overline{2}$, $\overline{3}$ et $\overline{4}$ n'atteignent jamais $\overline{1}$ et produisent des zéros, en rouge : ces classes ne sont pas inversibles, et ce n'est pas un corps — ce que le théorème prévoyait, puisque $6=2\times 3$.

5.4 Morphismes d'anneaux

Définition : Soient $(A\,;+\,;\times)$ et $(B\,;\oplus\,;\otimes)$ deux anneaux. On appelle **morphisme d'anneaux** toute application $\varphi : A \to B$ qui est un morphisme pour les lois additives et vérifie de plus, pour tout $(x\,;y) \in A^2$:

$$\varphi(x \times y) = \varphi(x) \otimes \varphi(y) \qquad \text{et} \qquad \varphi(1_A) = 1_B$$

Remarque : La condition $\varphi(1_A) = 1_B$ doit être exigée explicitement, alors que $\varphi(0_A) = 0_B$ était automatique au chapitre 4. La raison en est simple : $(A\,;+)$ est un groupe, ce qui permettait de simplifier, alors que $(A\,;\times)$ n'en est pas un — sans inverse disponible, l'argument tombe.

Exemple : Trois morphismes d'anneaux :

- la conjugaison $z \mapsto \overline{z}$ de $\mathbb{C}$ dans lui-même, puisqu'elle respecte somme et produit et fixe 1 ;
- la **réduction modulo** n, qui à un entier associe sa classe :

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto \overline{x} \end{aligned}$$

  C'est un morphisme surjectif, précisément par définition des deux lois de la proposition 2 ;
- l'évaluation en un point a, qui à une fonction de $\mathbb{R}^{\mathbb{R}}$ associe $f(a)$, à valeurs dans $\mathbb{R}$.

Remarque : Le noyau d'un morphisme d'anneaux, défini comme au chapitre 4 par $\operatorname{Ker}\varphi = \{x \in A \mid \varphi(x) = 0_B\}$, n'est en général *pas* un sous-anneau : il ne contient pas 1_A, sauf cas dégénéré. Il possède en revanche une propriété plus forte, l'absorption par produit :

$$\forall x \in \operatorname{Ker}\varphi,\ \forall a \in A, \quad ax \in \operatorname{Ker}\varphi$$

Une telle partie s'appelle un **idéal** de A. Pour la réduction modulo n, le noyau est $n\mathbb{Z}$, et l'on retrouve la notation $\mathbb{Z}/n\mathbb{Z}$ — qui se lit désormais : le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.