

Chapitre 02 – Cours

Structures algébriques : groupes, anneaux et corps

Dans ce chapitre, tu vas apprendre à :

- Vérifier une loi et ses propriétés
- Utiliser le critère de sous-groupe
- Distinguer anneau et corps

1. Lois de composition

Une loi interne sur un ensemble E associe à chaque couple d'éléments de E un élément de E .

Avant d'examiner ses propriétés, on vérifie qu'elle est bien définie et interne.

Une loi est associative si le parenthésage de trois termes ne change pas le résultat ; elle est commutative si leur ordre peut être échangé.

Ces propriétés sont différentes.

Le produit matriciel est associatif mais n'est généralement pas commutatif.

2. Groupes

Un groupe possède une loi associative, un élément neutre et un inverse pour chaque élément.

Si la loi est commutative, le groupe est dit abélien.

Dans une notation additive, l'inverse s'appelle l'opposé.

Le neutre et l'inverse sont uniques : les propriétés de la loi permettent de le démontrer.

Les entiers avec l'addition forment un groupe ; avec la multiplication, ils n'en forment pas un, car 2 n'a pas d'inverse entier.

3. Sous-groupes et morphismes

Une partie H d'un groupe additif est un sous-groupe si elle est non vide et stable par différence.

Cette formulation rassemble neutre, somme et opposés en un test efficace.

Un morphisme respecte la loi : $f(x + y) = f(x) + f(y)$.

Son noyau est l'ensemble des éléments envoyés sur le neutre, son image l'ensemble des valeurs atteintes.

Le noyau réduit au neutre caractérise l'injectivité ; l'image entière caractérise la surjectivité.

Il faut conserver les ensembles de départ et d'arrivée dans ces affirmations.

4. Anneaux

Un anneau possède une addition de groupe abélien et une multiplication associative, distributive par rapport à l'addition.

Dans les exemples de ce cours, on travaille avec un élément unité.

Un anneau peut être commutatif ou non.

Un élément est inversible s'il possède un inverse multiplicatif ; les inversibles forment un groupe pour la multiplication.

Un diviseur de zéro non nul est un élément qui annule un autre élément non nul.

Dans un anneau comportant de tels éléments, la règle « produit nul » des nombres réels ne se transpose pas sans précaution.

5. Corps et congruences

Un corps est un anneau commutatif où tout élément non nul est inversible.

Les rationnels, réels et complexes sont des corps.

Pour $m \geq 2$, l'anneau $\mathbb{Z}/m\mathbb{Z}$ est un corps exactement lorsque m est premier.

Pour m composé, une décomposition $m=ab$ fournit des classes non nulles dont le produit est nul.

Si m est premier, Bézout fournit l'inverse de chaque classe non nulle.

6. Rédiger une vérification

On annonce l'ensemble, la loi et le neutre envisagé ; on vérifie chaque axiome au lieu de conclure par ressemblance avec un exemple connu.

Pour montrer qu'une structure échoue, un seul axiome réfuté suffit : non-stabilité, absence de neutre ou d'inverse, défaut de distributivité.

Les exemples concrets précèdent l'abstraction et servent à tester les hypothèses.

Ce chapitre est un approfondissement MPSI ; il ne faut pas l'imposer comme un programme autonome identique dans toutes les PCSI ou L1.

Neutre additif et unité multiplicative

Définition – Deux lois, deux rôles

Dans un anneau unitaire, 0 est le neutre de l'addition et 1 celui de la multiplication. Les inverses additifs existent pour tous les éléments ; les inverses multiplicatifs peuvent manquer. Pour parler d'un corps, on exige $0 \neq 1$ et l'inversibilité de tout élément non nul.

Exemple résolu – 1. Un sous-groupe concret

Montrons que $H = \{(x, y) \in \mathbb{Z}^2 : x + y \text{ est pair}\}$ est un sous-groupe de $(\mathbb{Z}^2, +)$.

1. Le couple $(0, 0)$ appartient à H : l'ensemble est non vide. La loi de départ est l'addition coordonnée par coordonnée.
2. Si $u = (x, y)$ et $v = (x', y')$ sont dans H , alors la somme des coordonnées de $u - v$ vaut $(x + y) - (x' + y')$, différence de deux entiers pairs.
3. Ainsi $u - v \in H$, et le critère de stabilité par différence conclut. L'ensemble n'est pas tout $\mathbb{Z}^2$, puisque $(1, 0)$ n'y appartient pas.

On a utilisé un critère de sous-groupe à l'intérieur d'un groupe déjà connu, sans vérifier son associativité.

Exemple résolu – 2. Comparer deux anneaux de classes

Comparons les modules 5 et 6.

1. Modulo 5, les quatre classes non nulles ont pour inverses respectifs 1, 3, 2, 4 : les produits valent tous 1 modulo 5.
2. L'anneau $\mathbb{Z}/5\mathbb{Z}$ est donc un corps. Le calcul illustre le théorème général utilisant la primalité du module et Bézout.
3. Modulo 6, les classes de 2 et 3 sont non nulles mais leur produit est nul. La classe de 2 ne peut être inversible : multiplier $2 \times 3 = 0$ par un inverse imposerait $3 = 0$.

La règle « un produit nul impose un facteur nul » exige donc une hypothèse supplémentaire sur l'anneau.

Un morphisme vers les classes modulo deux

$$\begin{array}{ccc} \boxed{\text{entiers pairs } 2k} & \xrightarrow{q} & \boxed{\bar{0}} \\ \boxed{\text{entiers impairs } 2k + 1} & \xrightarrow{q} & \boxed{\bar{1}} \\ q(a + b) = q(a) + q(b) \end{array}$$

La réduction $q : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ est surjective et son noyau est $2\mathbb{Z}$. Chaque classe regroupe tous les entiers ayant le même reste ; le morphisme conserve l'addition, mais n'est pas injectif puisque $q(0) = q(2)$.

À retenir – Bilan

Une structure dépend d'un ensemble et de lois précises. Vérifier la stabilité avant les axiomes, puis distinguer les propriétés de l'addition et de la multiplication. Les exemples de classes modulo un entier montrent pourquoi les règles des corps ne s'étendent pas automatiquement à tous les anneaux.
