Algèbre abstraite

Loi binaire

Soit A un ensemble, une **loi binaire sur** A est une fonction $A \times A \to A$. Les lois binaires sont souvent écrites avec une *notation infixe* : si $*$ est le symbole de la loi, on écrira $a * b$ plutôt que $*(a, b)$.

On dit qu'une loi $* : A \times A \to A$ est

- **Associative**: si pour tout $a, b, c \in A$ on a $(a * b) * c = a * (b * c)$;
- **Commutative**: si pour tout $a, b \in A$ on a $a * b = b * a$.

Exemples

- L'addition et la multiplication (d'entiers, de réels, …) sont des lois binaires.

Groupes

Un **groupe** est un ensemble G muni d'une loi binaire $*$ tels que :

- $*$ est **associative** ;
- il existe un élément $e \in G$, dit **élément neutre**, tel que pour tout $a \in G$ on a $e * a = a * e = a$;
- pour tout $a \in G$ il existe un $b \in G$, dit l'**inverse de** a, tel que $a * b = b * a = e$.

Si en plus $*$ est commutative, le groupe G est dit commutatif, ou **abélien**.

Notation

Souvent on se dispense de noter le symbole de la loi, on écrit alors ab pour $a * b$. Dans ce cas on dit que la loi de groupe est *notée multiplicativement*. On peut parfois noter $a \cdot b$ lorsque la lecture serait ambiguë.

Pour une loi multiplicative, on note a^{-1}, ou parfois $1/a$, l'inverse de a ; on note a^n l'élément

$$a^n = \underbrace{aa \cdots a}_{n \text{ fois}}.$$

Lorsque la loi de groupe est notée $+$, on dit qu'elle *notée additivement*. L'usage veut qu'on utilise la notation additive *uniquement pour les lois coummutatives*. On note alors $-a$ l'inverse de a (et on l'appelle parfois *opposé*) ; on note na, ou $n \cdot a$, ou encore $[n]a$ l'élément

$$na = \underbrace{a + a + \cdots + a}_{n \text{ fois}}.$$

Exemples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont tous des groupes abéliens.
- $(\mathbb{N}, +)$ n'est pas un groupe : tous les éléments n'ont pas d'opposé.
- $(\mathbb{Z}, \times)$ n'est pas un groupe : tous les éléments n'ont pas d'inverse.
- $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes, mais si on leur enlève le 0 ils deviennent des groupes abéliens.
- $(\mathcal{S}_n, \circ)$, l'ensemble des permutations sur n éléments muni de l'opération de composition, est un groupe **non-abélien**.

Anneaux, corps

Un **anneau** est un ensemble A muni de deux lois binaires, notées $+$ et $\cdot$, telles que :

- $(A, +)$ est un **groupe abélien**, dont on notera 0 l'élément neutre ;
- $\cdot$ est **associative** ;
- il existe un élément de A, noté 1, tel que pour tout $a \in A$ on a $1 \cdot a = a \cdot 1 = a$;
- $\cdot$ distribue sur $+$, c'est à dire que pour tout $a, b, c \in A$ on a $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Un anneau tel que $\cdot$ est commutative est dit un **anneau commutatif**.

Un **corps** est un anneau commutatif dont tous les éléments, à l'exception de 0, ont un inverse multiplicatif.

Exemples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs. Parmi eux, $\mathbb{Z}$ est le seul qui ne soit pas aussi un corps.

- L'ensemble $\mathcal{M}_n(\mathbb{Z})$ des matrices carrées $n \times n$ à coefficients dans $\mathbb{Z}$ est un anneau **non-commutatif**. Les matrices carrées à coefficients dans $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$ forment aussi des anneaux non-commutatifs.

Anneaux d'entiers modulaires

Pour un entier n, l'ensemble $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ est noté $\mathbb{Z}/n\mathbb{Z}$. Par la suite, pour ne pas alourdir la notation, on désignera chaque classe d'équivalence $\bar{a}$ par un de ses représentants. Par défaut, on choisit le représentant canonique (l'unique représentant compris entre 0 et $n-1$ et ayant comme reste a), et on écrira alors cet ensemble comme $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$.

On va munir cet ensemble de deux opérations, l'addition $+$ et la multiplication $\times$:

- $+$ Pour tout $a, b \in \mathbb{Z}/n\mathbb{Z}$, $a + b := a + b \mod n$
- $\times$ Pour tout $a, b \in \mathbb{Z}/n\mathbb{Z}$, $a \times b := a \times b \mod n$

On peut vérifier que $\mathbb{Z}/n\mathbb{Z}$ a une structure d'anneau et que cet anneau est commutatif. Il est un corps si et seulement si n est premier.
