Structures algébriques

Chapitre 10

Loi de composition interne

Définition
Une *loi de composition interne* sur un ensemble E est une application $* : E \times E \to E$, $(x, y) \mapsto x * y$.

Propriété — Propriétés possibles
- **Associativité** : $(x * y) * z = x * (y * z)$ pour tous x, y, z.
- **Commutativité** : $x * y = y * x$.
- **Élément neutre** : $e \in E$ tel que $e * x = x * e = x$ pour tout x.
- **Symétrique** de x : $x' \in E$ tel que $x * x' = x' * x = e$.

Exemple.
- $(\mathbb{R}, +)$: associative, commutative, neutre 0, symétrique $-x$.
- $(\mathbb{R}, \times)$: associative, commutative, neutre 1, symétrique $\frac{1}{x}$ pour $x \neq 0$.
- $(\mathbb{N}, +)$: associative, commutative, neutre 0, mais pas de symétrique général.

Groupes

Définition
Un *groupe* $(G, *)$ est un ensemble G muni d'une loi $*$ telle que :
1. $*$ est associative ;
2. $*$ a un élément neutre e ;
3. tout élément de G a un symétrique pour $*$.

Si $*$ est commutative, on parle de *groupe abélien* (ou commutatif).

Exemple.
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{R}^*, \times)$ sont abéliens.
- $(\mathbb{N}, +)$ n'est pas un groupe (pas de symétrique).
- Rotations du plan (avec composition) : groupe non abélien (plusieurs dimensions), mais les rotations de même centre sont abéliennes.

Sous-groupes

Définition
Une partie $H \subseteq G$ est un *sous-groupe* de $(G, *)$ si :
1. H est non vide (contient e) ;
2. $\forall x, y \in H, x * y \in H$;
3. $\forall x \in H, x^{-1} \in H$ (symétrique dans H).

Théorème — Caractérisation
H est un sous-groupe de G ssi $H \neq \emptyset$ et $\forall x, y \in H, x * y^{-1} \in H$.

Exemple. $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$.

Morphismes de groupes

Définition
Soient $(G, *)$ et $(G', \star)$ deux groupes. Une application $f : G \to G'$ est un *morphisme* de groupes si :

$$\forall x, y \in G, f(x * y) = f(x) \star f(y).$$

- *Isomorphisme* : morphisme bijectif.
- *Endomorphisme* : morphisme $G \to G$.
- *Automorphisme* : endomorphisme bijectif.

Propriété
Soit $f : G \to G'$ un morphisme. Alors :
- $f(e_G) = e_{G'}$.
- $f(x^{-1}) = f(x)^{-1}$.
- $\mathrm{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$ est un sous-groupe de G.
- $\mathrm{Im}(f) = f(G)$ est un sous-groupe de G'.

Anneaux (introduction)

Définition
Un *anneau* $(A, +, \times)$ est un ensemble muni de deux lois telles que :
1. $(A, +)$ est un groupe abélien (neutre 0) ;
2. $\times$ est associative avec élément neutre 1 ;
3. Distributivité de $\times$ par rapport à $+$.

Si $\times$ est commutative, l'anneau est *commutatif*. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ sont des anneaux commutatifs.

Corps

Définition
Un *corps* est un anneau commutatif K tel que $(K \setminus \{0\}, \times)$ soit un groupe (c'est-à-dire, tout élément non nul est inversible).

Exemples : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. $\mathbb{Z}$ n'est pas un corps (2 n'a pas d'inverse dans $\mathbb{Z}$). $\frac{\mathbb{Z}}{p}\mathbb{Z}$ est un corps ssi p est premier.