# Structures Algébriques

Aubin SIONVILLE

MPI Clemenceau - 2021-2023

## Ensembles et relations

### Applications

| | | |
|---|---|---|
| $f$ est injective | $\iff$ | $f(x)$ a au maximum 1 antécédent |
| $f$ est surjective | $\iff$ | $f(x)$ a au minimum 1 antécédent |
| $f$ est bijective | $\iff$ | $f(x)$ a exactement 1 antécédent |

| | |
|---|---|
| Image directe : | $f(A) = \{f(a) \mid a \in A\}$ |
| Image réciproque : | $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$ |

### Relations binaires

**Relation d'équivalence :**

| | |
|---|---|
| Reflexivité : | $\forall x \in E, x \sim x$ |
| Symétrie : | $\forall x, y \in E, x \sim y \implies y \sim x$ |
| Transitivité : | $\forall x, y, z \in E, \begin{cases} x \sim y \\ y \sim z \end{cases} \implies x \sim z$ |

**Relation d'ordre :**

| | |
|---|---|
| Reflexivité : | $\forall x \in E, x \leq x$ |
| Antisymétrie : | $\forall x, y \in E, \begin{cases} x \leq y \\ y \leq x \end{cases} \implies x = y$ |
| Transitivité : | $\forall x, y, z \in E, \begin{cases} x \leq y \\ y \leq z \end{cases} \implies x \leq z$ |

# Groupes

## Définition

$$\boxed{(G,+) \text{ est un groupe si } \begin{cases} + \text{ est associative} & \forall x,y,z \in G, (x+y)+z = x+(y+z) \\ + \text{ a un neutre } e \in G & \forall x \in G, x+e = e+x = x \\ \forall x \in G, x \text{ a un opposé dans } G & \exists y \in G \text{ tel que } x+y = y+x = e \end{cases}}$$

On dit que c'est un groupe **commutatif** / **abélien** si $+$ est commutative.

## Sous-groupe

$$\boxed{(H,+) \text{ est un sous-groupe de } (G,+) \text{ si } \begin{cases} H \text{ est stable par } + & \forall x,y \in H, x+y \in H \\ \text{Le neutre de } + \text{ est dans } H & e \in H \\ \forall x \in H, x \text{ a un opposé dans } H & -x \in H \end{cases}}$$

## Sous-goupe engendré

Soit $G$ un groupe et $A \subseteq G$.

$$\boxed{\bigcap_{\substack{H \text{ sous-g de } G \\ A \subseteq H}} H = \langle A \rangle}$$

C'est le plus petit (par inclusion) sous-groupe de $G$ qui contient $A$.

## Groupe monogène

$$\boxed{(G,+) \text{ est un groupe monogène si } \exists a \in G, G = \langle a \rangle}$$

(Engendré par un élément unique)

## Groupe produit

Avec $(G_1,+), (G_2,+)$ des groupes :

$(G_1 \times G_2, +)$ le groupe produit

## Morphismes de groupes

Soit $(G,\times)$ et $(H,*)$ deux groupes.
$f : G \to H$ est un morphisme de groupes si :

$$\boxed{\forall (x,y) \in G, f(x \times y) = f(x) * f(y)}$$

## Conjugaison

Soit $g \in G$.

$$\boxed{\begin{array}{cccc} c_g & : & G & \to & G \\ & & x & \mapsto & gxg^{-1} \end{array} \text{ est la conjugaison par } g}$$

# Anneaux

## Définition

$$(A,+,\times) \text{ est un anneau si } \begin{cases} (A,+) \text{ est un groupe abélien de neutre } 0_A & \\ (A,\times) \text{ est un monoïde} & \begin{cases} \times \text{ est associative} \\ \times \text{ a un neutre } 1_A \in A \end{cases} \\ + \text{ et } \times \text{ sont distributives à gauche et à droite} & \forall x,y,z \in A, \begin{cases} x(y+z) = xy+xz \\ (y+z)x = yx+zx \end{cases} \end{cases}$$

On dit que $0_A$ est **absorbant**.

## Sous-anneau

$$(B,+,\times) \text{ est un sous-anneau de } (A,+,\times) \text{ si } \begin{cases} (B,+) \text{ est un sous-groupe de } (A,+) & \\ B \text{ est stable par } \times & \forall x,y \in B, x\times y \in B \\ \text{Le neutre de } \times \text{ est dans } B & 1_B \in B \end{cases}$$

## Commutativité

Avec $(A,+,\times)$ un anneau, si $(a,b) \in A^2$ commutent,

$$\boxed{(a+b)^b = \sum_k = 0^n \binom{n}{k} a^k b^{n-k}}$$

$$\boxed{(a-b)^n = (a-b)\sum_{k=0}^{n-1} \binom{n}{k} a^k b^{n-1-k}}$$

On peut faire de l'arithmétique dans les anneaux (Attention aux anneaux non commutatifs)

## Anneau intègre

$(A,+,\times)$ est un anneau intègre si

$$\boxed{\forall (a,b) \in A^2, (a\times b = 0_A \iff a = 0_A \text{ ou } b = 0_A)}$$

## Anneau nul

$(A,+,\times)$ est nul ($A = \{0_A\}$) si

$$\boxed{1_A = 0_A}$$

## Morphismes d'anneaux

Soit $(A,+,\times)$ et $(B,\oplus,\cdot)$ deux anneaux.
$f : A \to B$ est un morphisme d'anneaux si :

$$\begin{cases} \forall (a,b) \in A^2, f(a+b) = f(a) \oplus f(b) \\ \forall (a,b) \in A^2, f(a\times b) = f(a)\cdot f(b) \\ f(1_A) = 1_B \end{cases}$$

# Corps

## Définition

$$(\mathbb{K},+,\times) \text{ est un corps si } \begin{cases} (\mathbb{K},+) \text{ est un groupe abélien} \\ (\mathbb{K},\times) \text{ est un monoïde commutatif} \\ \times \text{ a un neutre } 1_{\mathbb{K}} \in \mathbb{K} \\ 0_{\mathbb{K}} \neq 1_{\mathbb{K}} \end{cases}$$

## Sous-corps

$$(\mathbb{L},+,\times) \text{ est un sous-corps de } (\mathbb{K},+,\times) \text{ si } \begin{cases} \forall(x,y \in \mathbb{L}, x-y \in \mathbb{L}) \\ \forall(x,y \in \mathbb{L}, x \times y^{-1} \in \mathbb{L}) \end{cases}$$

## $\mathbb{Z}/n\mathbb{Z}$

$$\boxed{(\mathbb{Z}/n\mathbb{Z},+,\times) \text{ est un corps} \iff n \text{ est premier}}$$

## Nombre de zéros

Avec $\mathbb{K}$ un corps et $P$ un polynôme de degré $n$,
$P(x) = 0_{\mathbb{K}}$ a au plus $n$ solutions dans $\mathbb{K}$.

## Morphismes de corps

Soit $(\mathbb{K}_1,+,\times)$ et $(\mathbb{K}_2,\oplus,\cdot)$ deux corps.
$f : \mathbb{K}_1 \to \mathbb{K}_2$ est un morphisme de corps si :

$$\begin{cases} \forall(a,b) \in \mathbb{K}_1^2, f(a+b) = f(a) \oplus f(b) \\ \forall(a,b) \in \mathbb{K}_1^2, f(a \times b) = f(a) \cdot f(b) \end{cases}$$