# Structures

Martin Andrieux

## 1 Groupes

**Définition**

Un *groupe* est un couple $(G, \cdot)$ où :

- $G$ est un ensemble
- $\cdot$ est une loi de composition interne sur $G$
- $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Il extiste un neutre (noté $1$) pour $\cdot$
- Tout élément possède un symétrique

Un groupe est dit *abélien* s'il est commutatif.

**Définition**

Un *morphisme* de groupe est une application $f : (G, \cdot) \to (H, \cdot)$ telle que :

- $(G, \cdot)$ et $(H, \cdot)$ sont deux groupes
- $\forall a, b \in G,\ f(a \cdot b) = f(a) \cdot f(b)$

$f$ est un *isomorphisme* de groupe si $f$ et $f^{-1}$ sont des morphismes bijectifs.

**Définition**

Soit $H \subset G$, $H$ est un *sous-groupe* de $G$ si :

- $H \neq \emptyset$
- $H$ est stable par $\cdot$
- $1 \in H$
- $\forall a \in H,\ a^{-1} \in H$

**Théorèmes**

- Les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$
- Tout groupe fini de cardinal $n$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$
- L'intersection de deux sous-groupes est un sous-groupe.

**Définition**

Pour $A \subset G$, il existe un plus petit sous-groupe de $G$ contenant $A$, c'est le sous-groupe *engendré* par $A$, noté $\langle A \rangle$.

**Théorème de Lagrange**

Le cardinal de tout sous-groupe divise le cardinal du groupe.

En particulier, pour $x$ dans $G$, le cardinal de $\langle x \rangle$, aussi appelé *ordre* de $x$, divise le cardinal de $G$.

## 2 Anneaux

**Définition**

Un *anneaux* est un triplet $(A, +, \cdot)$ où :

- $(A, +)$ est un groupe abélien
- $\cdot$ est une loi de composition interne associative pour $A$
- $\cdot$ est distributif par rapport à la somme
- $\cdot$ possède un neutre noté $1$ et $1 \neq 0$

**Définition**

Un *morphisme* d'anneaux est une application $f : A \to B$ telle que pour $x, y, z$ dans $A$ :

- $f(x + z) = f(x) + f(z)$

- $f(xy) = f(x)f(y)$
- $f(1) = 1$

$f$ est un *isomorphisme* d'anneaux di $f$ et $f^{-1}$ sont des morphismes bijectifs.

**Définition**

Soit $B \subset A$, $B$ est un *sous-anneau* de $A$ si :

- $B \neq \emptyset$
- $B$ est stable par $\cdot$ et $+$
- $1 \in B$

**Définition**

Un *corps* est un anneau dans lequel tous les éléments non nuls sont inversibles.
Soit $A$ un anneau, on note $A^*$ l'ensemble des éléments inversibles de $A$. $A^*$ est un groupe pour la loi $\cdot$.

**Définition**

Soit $A$ un anneau, on dit que $x$ et $y$ sont des *diviseurs de* $0$ si $x \neq 0$, $y \neq 0$ et $xy = 0$.
Si $A$ ne possède pas de diviseur de $0$, il est dit *intègre*.