

# Structures algébriques

## 1. Loïs de composition

### Définitions

- Soit  $E$  un ensemble.  
Une loi de composition interne sur  $E$  est une application de  $E \times E$  dans  $E$ .
- Soient  $E$  et  $F$  deux ensembles.  
Une loi de composition externe à gauche (resp. à droite) sur  $E$  à domaine d'opérateurs  $F$  est une application de  $F \times E$  dans  $E$  (resp.  $E \times F$  dans  $E$ ).

### Notation

Si  $T$  est une loi de composition interne sur  $E$ , on note  $xTy$  pour  $T(x,y)$ .  
De même, on note  $a \perp x$  pour  $\perp(a,x)$  dans le cadre d'une loi  $\perp$  externe.

### Définition

On appelle magma tout ensemble muni d'une loi de composition interne.

### Remarque

Hormi les cas concernant les lois usuelles, on précisera toujours la loi considérée pour le magma.

### Exemples et contre exemples

- Soit  $\mathcal{P}$  l'ensemble des points du plan.  
Soit  $T$  l'application qui, à tout couple de points  $(A,B)$ , associe le milieu de segment  $[A,B]$ .  
 $(\mathcal{P},T)$  est un magma.
- Soit  $E = \{ \text{fonctions numériques définies sur } \mathbb{R} \text{ à valeurs dans } \mathbb{R}_+^* \}$ .  
Soit  $T$  l'application qui, à tout couple de fonctions  $(f,g)$  de  $E \times E$ , associe la fonction  $h$  définie par  $h(x) = (\ln f(x))^2 + (\ln g(x))^2 + 1$ .  
 $(E,T)$  est un magma.
- Soit  $\mathbb{N}$  l'ensemble des entiers naturels.  
Soit l'application  $\text{exp} : (n,p) \mapsto n^p$ .  
 $(\mathbb{N},\text{exp})$  est un magma.
- Le produit scalaire sur les vecteurs du plan ou de l'espace n'est pas une loi de composition interne.
- Soit  $E$  l'ensemble des fonctions numériques définies sur  $[0,1]$ .  
Soit  $F$  l'ensemble des entiers pairs.  
Soit  $\perp$  l'application qui, au couple  $(a,f)$  de  $F \times E$ , associe la fonction  $h$  définie par  $h(x) = af(x) + 2$ .  
 $\perp$  est une loi de composition externe sur  $E$  à domaine d'opérateurs  $F$ .

- On peut aussi définir une loi de composition interne par un tableau. Par exemple,  $\perp : \{a,b,c\} \rightarrow \{a,b,c\}$  définie par

$\perp$	$a$	$b$	$c$
$a$	$c$	$a$	$c$
$b$	$b$	$a$	$c$
$c$	$b$	$c$	$a$

## 2. Monoïdes

### Définitions

On dit qu'un magma  $(E, T)$  est unifié ou qu'il admet un élément neutre si  $\exists e \in E / \forall x \in E, x T e = x T e = x$ .  
 On dit qu'un magma  $(E, T)$  est associatif si,  $\forall x, y, z \in E, x T (y T z) = (x T y) T z$ .

Un magma unifié associatif est appelé un monoïde.

### Exemples

Les magmas suivants sont des monoïdes :

- $(\mathbb{N}, +)$  où  $+$  est l'addition usuelle.
- $(\mathbb{N}, \times)$  où  $\times$  est la multiplication usuelle.
- $(\mathcal{P}(E), \cup)$  où  $E$  est un ensemble,  $\mathcal{P}(E)$  l'ensemble des parties de  $E$  et  $\cup$  la réunion usuelle.
- $(\mathcal{P}(E), \cap)$  où  $E$  est un ensemble,  $\mathcal{P}(E)$  l'ensemble des parties de  $E$  et  $\cap$  l'intersection usuelle.
- $(E, o)$  où  $E$  est l'ensemble des fonctions numériques définies sur  $\mathbb{R}$  et  $o$  la composition usuelle des fonctions.
- De façon plus générale,  $(F, o)$  où  $F = E^E = \mathcal{N}(E, E)$  est l'ensemble des applications de  $E$  dans  $E$  et  $o$  la composition usuelle des fonctions.

### Propriété

L'élément neutre d'un magma unifié est unique.

### Démonstration

Soit  $(E, T)$  un magma. On suppose qu'il existe deux éléments neutres  $e$  et  $e'$ .

On a  $e T e' = e$  car  $e'$  est un élément neutre  
 $e T e' = e'$  car  $e$  est un élément neutre d'où le résultat.

### Définitions

On dit que deux éléments  $x$  et  $y$  d'un magma  $(E, T)$  commutent ou sont permutables si et seulement si  $x T y = y T x$ .

On dit qu'un magma  $(E, T)$  est commutatif si et seulement si tous les éléments de  $E$  sont deux à deux permutables.

### Exemples

Les quatre premiers cas de l'exemple précédent sont des monoïdes commutatifs; mais c'est faux pour les deux derniers.

## 2. Groupes

### Définition

Un magma  $(G,*)$  est un groupe s'il vérifie les trois conditions suivantes :

- i) La loi  $*$  est associative c'est-à-dire  $\forall x,y,z \in G, x * (y * z) = (x * y) * z$ .
  - ii) La loi  $*$  admet un élément neutre c'est-à-dire  $\exists e \in G / \forall x \in G, x * e = e * x = x$ .
  - iii) Tout élément est symétrisable c'est-à-dire,  $\forall x \in G, \exists x' \in G / x * x' = x' * x = e$ .
- Si, de plus, la loi est commutative, on dit que le groupe est commutatif ou abélien.

### Exemples et contre-exemples

Les magmas suivants sont des groupes :

- $(\mathbb{Z}, +)$  où  $+$  est l'addition usuelle.
- $(\mathbb{C}^*, \times)$  où  $\times$  est la multiplication usuelle.
- Soit  $E$  un ensemble et soit  $S(E) = \{\text{bijections de } E \text{ dans } E\} = \{\text{permutations de } E\}$   
 $(S(E), \circ)$  est un groupe appelé groupe symétrique de  $E$ .
- $(E, +)$  où  $E = \{\text{fonctions numériques définies sur } \mathbb{R}\}$  et  $+$  est la somme usuelle des fonctions.  
C'est-à-dire,  $f$  et  $g$  étant deux éléments de  $E$ ,  $f + g$  est définie, pour tout réel  $x$ , par :  
 $(f + g)(x) = f(x) + g(x)$ .
- $\{0,1\}$  muni d'une loi  $+$  défini par le tableau suivant :

	+	0	1
0	0	0	1
1	1	0	0

Les magmas suivants ne sont pas des groupes :

- $(\mathbb{Z}, \times)$  où  $\times$  est la multiplication usuelle.
- $(\mathbb{R}, \times)$  où  $\times$  est la multiplication usuelle.

### Remarques

- Rappel : L'élément neutre d'un groupe est unique. En particulier, un groupe est toujours non vide.  
Le symétrique d'un élément d'un groupe est unique.  
Tout élément d'un groupe est simplifiable.
- *Notation additive de la loi d'un groupe* :  $(G, *) = (G, +)$ .  
On note  $0_G$  l'élément neutre de  $G$ .  
On parle d'opposé à la place de symétrique et on note  $-x$  le symétrique d'un élément  $x$  i.e.  
l'élément qui vérifie  $x + (-x) = (-x) + x = e = 0_G$ . Par convention, on pose  $0_G \cdot x = 0_G$ ,  $1 \cdot x = x$  et, pour tout entier  $n \geq 2$ ,  $n \cdot x = x + x + \dots + x$  ( $n$  fois) et  $(-n)x = -(n \cdot x)$ .
- *Notation multiplicative de la loi d'un groupe* :  $(G, *) = (G, \times)$ .  
On note  $1_G$  l'élément neutre de  $G$ .  
On parle d'inverse à la place de symétrique et on note  $x^{-1}$  le symétrique d'un élément  $x$  i.e.  
l'élément qui vérifie  $x \times x^{-1} = x^{-1} \times x = e = 1_G$ . Par convention, on pose  $x^0 = 1_G$ ,  $x^1 = x$  et, pour tout entier  $n \geq 2$ ,  $x^n = x \times x \times \dots \times x$  ( $n$  fois) et  $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ .
- La notation additive est plus souvent utilisée pour les groupes commutatifs.  
Dans le reste du cours, nous utiliserons de préférence la notation multiplicative.  
Dans ce cas, nous noterons  $xy$  la composition de deux éléments  $x$  et  $y$  d'un groupe  $(G, \times)$ .

### Propriété

Soit  $(G,*)$  un groupe et soit  $x$  un élément de  $G$ .

Le symétrique de  $x$  est unique.

## Démonstration

On suppose qu'il existe deux symétriques à  $x$  :  $x'$  et  $x''$

$$\begin{aligned} x' * x * x'' &= (x' * x) * x'' = e * x'' = x'' \\ &= x' * (x * x'') = x' * e = x' \end{aligned}$$

## Remarques

- Si une loi  $*$  est commutative, pour vérifier qu'un élément  $e$  est l'élément neutre, il suffit uniquement de vérifier l'une des deux relations,  $x * e = x$  ou  $e * x = x$  pour tout  $x \in G$ . L'autre relation étant obtenue par la commutativité. De même, pour vérifier qu'un élément  $x'$  est le symétrique de  $x$ , il suffit que l'on ait soit  $x * x' = e$  soit  $x' * x = e$ .
- Si  $(G, *)$  est juste un magma, on a :

$$\begin{array}{ccc} a = b & \text{et} & a = b \\ \Rightarrow a * c = b * c & & \Rightarrow c * a = c * b. \end{array}$$

Si, de plus,  $(G, *)$  un groupe, on a alors la réciproque.

$$\begin{aligned} \text{car } a * c = b * c &\Rightarrow (a * c) * c' = (b * c) * c' \text{ où } c' \text{ est le symétrique de } c \\ &\Rightarrow a * (c * c') = b * (c * c') \\ &\Rightarrow a = b \end{aligned}$$

$$\begin{aligned} \text{De même : } c * a = c * b &\Rightarrow c' * (c * a) = c' * (c * b) \text{ où } c' \text{ est le symétrique de } c \\ &\Rightarrow (c' * c) * a = (c' * c) * b \\ &\Rightarrow a = b \end{aligned}$$

- On a :  $(\mathbb{R}, +)$  est un groupe et  $a + c = b + c \Leftrightarrow a = b$ .  
On a :  $(\mathbb{R}, \times)$  n'est pas un groupe (car 0 n'est pas inversible) et donc  $a * c = b * c \not\Rightarrow a = b$ .

## Propriété

Soit  $(G, *)$  un groupe. Pour tous les éléments  $a$  et  $b$  de  $G$ , on a :  $(a * b)^{-1} = b^{-1} * a^{-1}$

## Démonstration

$(a * b)^{-1}$  est par définition l'unique élément de  $G$  qui vérifie  $(a * b)^{-1} * (a * b) = (a * b) * (a * b)^{-1} = e$ .

$$\text{Or } (b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$$

$$\text{et } (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

## Remarque

Dans le cadre de lois non commutatives, les définitions d'élément neutre, de symétrique, d'élément simplifiable (et autres) peut être données en séparant les cas à gauche et à droite.

Par exemple :  $a * c = b * c \Leftrightarrow a = b$  signifie que  $c$  est simplifiable à droite.

## Propriété

Soit  $(G, \times)$  un groupe.  $\forall n, p \in \mathbb{Z}, \forall x \in G, x^{n+p} = x^n \times x^p$  et  $x^{n \times p} = (x^n)^p$ .

## Démonstration

- $n$  et  $p$  strictement positifs :  $x^n \times x^p = \underbrace{(x \times x \times \dots \times x)}_{n \text{ fois}} \times \underbrace{(x \times x \times \dots \times x)}_{p \text{ fois}} = x^{n+p}$ .

- $n$  et  $p$  strictement négatifs :  $x^n \times x^p = \underbrace{((x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1}))}_{n \text{ fois}} \times \underbrace{(x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1})}_{p \text{ fois}} = x^{n+p}$ .

- $n$  positif et  $p$  négatif avec :
  - $n = p$   $x^n \times x^p = \underbrace{x \times x \times \dots \times x}_{n \text{ fois}} \times \underbrace{(x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1})}_{n \text{ fois}} = e = 1_G = x^0$
  - $n > p$   $x^n \times x^p = \underbrace{x \times x \times \dots \times x}_{n \text{ fois}} \times \underbrace{(x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1})}_{p \text{ fois}} = \underbrace{x \times x \times \dots \times x}_{n-p \text{ fois}} = x^{n-p}$
  - $n < p$   $x^n \times x^p = \underbrace{x \times x \times \dots \times x}_{n \text{ fois}} \times \underbrace{(x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1})}_{p \text{ fois}} = \underbrace{(x^{-1}) \times (x^{-1}) \times \dots \times (x^{-1})}_{p-n \text{ fois}} = x^{n-p}$
- $n$  négatif et  $p$  positif : idem.

## Remarque

En notation additive, cela donne :

$$\forall n, p \in \mathbb{Z}, \forall x \in G, (n + p)x = (nx) + (px) \text{ et } (n \times p)x = n(px).$$

## Définition

Soit  $(G, *)$  un groupe. Soit  $H \subset G$  et  $H \neq \emptyset$ .

On dit que  $H$  est un sous-groupe de  $(G, *)$  si et seulement si  $H$  est un groupe pour la loi  $*$  induite.

## Exemples

- $(\mathbb{Z}, +)$  est un sous-groupe de  $(\mathbb{R}, +)$ .
- $2\mathbb{Z} = \{2k ; k \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .
- $(\mathbb{Z}^*, \times)$  n'est pas un sous-groupe de  $(\mathbb{R}^*, \times)$ .

## Propriété

Soit  $(G, )$  un groupe noté multiplicativement. Soit  $H \subset G$ .

Les propriétés suivantes sont équivalentes :

- (1)  $H$  est un sous-groupe de  $G$ .
- (2)  $H \neq \emptyset$ ,  $H$  est stable par la loi de  $G$  et  $\forall x \in H$ , on a  $x^{-1} \in H$ .
- (3)  $H \neq \emptyset$  et  $\forall x, y \in H$ , on a  $xy^{-1} \in H$ .

## Démonstration

- (1)  $\Rightarrow$  (2) évident
- (2)  $\Rightarrow$  (3) évident
- (3)  $\Rightarrow$  (1) Associativité : découle de celle de  $G$ .  
 Élément neutre :  $\forall x \in H, xx^{-1} \in H \Rightarrow e \in H$ .  
 Symétrique :  $\forall x \in H, ex^{-1} \in H \Rightarrow x^{-1} \in H$ .  
 Loi de composition interne :  $\forall x, y \in H$ , on a  $y^{-1} \in H$  et donc  $xy = x(y^{-1})^{-1} \in H$ .

## Remarques

- Soit  $H$  un sous-groupe de  $G$ .  
L'élément neutre de  $H$  et le même que celui de  $G$ .  
Le symétrique d'un élément de  $H$  est le même dans  $H$  que dans  $G$ .
- Si la loi de  $G$  est une loi notée additivement, on a :
  - (2')  $H \neq \emptyset$ ,  $H$  est stable par la loi de  $G$  et  $\forall x \in H$ , on a  $-x \in H$ .
  - (3')  $H \neq \emptyset$ ,  $\forall x, y \in H$ , on a  $x - y \in H$ .

## Exemples importants

Soit  $G$  un groupe. Les ensembles  $\{e\}$  et  $G$  sont des sous-groupes de  $G$ .  
Tous les autres sous-groupes sont dits propres.

## Propriété

Si  $(K,*)$  est un sous-groupe de  $(H,*)$  et si  $(H,*)$  est un sous-groupe de  $(G,*)$  alors  $(K,*)$  est un sous-groupe de  $(G,*)$ .

## Exemple

Soit  $\mathcal{P}$  l'ensemble des points du plan.

L'ensemble  $T$  des transformations (bijections du plan) du plan muni de la loi de composition usuelle des fonctions est un groupe.

L'ensemble  $I$  des isométries est un sous-groupe de  $T$ .

L'ensemble des translations est un sous-groupe de  $I$ .

L'ensemble des rotations d'un centre commun est un sous-groupe de  $I$ .

L'ensemble des déplacements (conserve les angles orientés) est un sous-groupe de  $I$ .

## Démonstration

Trivial + remarque sur la loi.

## Propriété

Soit  $G$  un groupe et soit  $(H_i)_{i \in I}$  une famille non vide de sous-groupes de  $G$ .

Alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

## Démonstration

- $\forall i \in I (\neq \emptyset), e \in H_i$  donc  $e \in \bigcap_{i \in I} H_i$  donc  $\bigcap_{i \in I} H_i \neq \emptyset$ .
- Soit  $x$  et  $y$  deux éléments de  $\bigcap_{i \in I} H_i$ .  $\forall i \in I, x$  et  $y \in H_i$  donc  $xy^{-1} \in H_i$ . D'où  $xy^{-1} \in \bigcap_{i \in I} H_i$ .

## Remarque

En général, la réunion de 2 sous-groupes n'est pas un sous-groupe.

Par exemple, on a  $2\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z},+)$  et  $3\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z},+)$ .

Si  $2\mathbb{Z} \cup 3\mathbb{Z}$  était un sous-groupe de  $(\mathbb{Z},+)$ , on devrait avoir  $2 + 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ .

Or 5 n'étant ni un multiple de 2, ni un multiple de 3, n'appartient pas à  $2\mathbb{Z} \cup 3\mathbb{Z}$ .

## Propriété

Soit  $G$  un groupe et soit  $a$  un élément de  $G$ . Il existe un plus petit sous-groupe de  $G$  contenant  $a$ . Ce sous-groupe est appelé groupe engendré par  $a$  et est noté  $\text{gr}(a)$ .

## Démonstration

Soit  $(H_i)_{i \in I}$  l'ensemble des sous-groupes de  $G$  qui contiennent  $a$ .

Cette famille n'est pas vide car  $G$  appartient à cette famille et  $\text{gr}(a) = \bigcap_{i \in I} H_i$

## Propriété

Soit  $G$  un groupe dont la loi est notée multiplicativement et soit  $a$  un élément de  $G$ .

On a  $\text{gr}(a) = \{ \dots, a^{-2}, a^{-1}, 1, a, a^2, \dots \} = \{ a^i \text{ où } i \in \mathbb{Z} \}$ .

## Démonstration

- ( $\subset$ ) On pose  $E = \{ \dots, a^{-2}, a^{-1}, 1, a, a^2, \dots \}$ . Il suffit de montrer que  $E$  est un sous-groupe de  $G$ .
- Puisque l'on a bien  $E$  qui contient  $a$ ,  $E \neq \emptyset$ .
  - $\forall x, y \in E, \exists n, p \in \mathbb{Z} / x = a^n$  et  $y = a^p$ . On a  $xy^{-1} = a^{n-p} \in E$ .
- ( $\supset$ ) Puisque  $\text{gr}(a)$  est un sous-groupe qui contient  $a$ ,  $\text{gr}(a)$  doit être stable par inverse et composition. Donc  $a^{-1} \in \text{gr}(a)$  et  $\forall n \in \mathbb{Z}, a^n \in \text{gr}(a)$ .

## Exemples

- $(2\mathbb{Z}, +)$  est le sous-groupe de  $(\mathbb{Z}, +)$  engendré par 2.
- $(\mathbb{Z}, +)$  est le sous-groupe de  $(\mathbb{R}, +)$  engendré par 1.
- Dans  $(\mathbb{C}^*, \times)$ ,  $\text{gr}(i) = \{ 1, i, -1, -i \}$ .

## Remarque

On peut généraliser cette définition à une partie  $A$  quelconque d'un groupe  $G$  : il existe un plus petit sous-groupe de  $G$  contenant  $A$ .

Ce sous-groupe est appelé groupe engendré par  $A$  et est noté  $\text{gr}(A)$ .

## Propriété

Soit  $G$  un groupe dont la loi est notée multiplicativement et soit  $A$  une partie de  $G$ .

On note  $A^{-1} = \{ x^{-1} \text{ où } x \in A \}$ . On a  $\text{gr}(A) = \{ a_1 a_2 \dots a_n \text{ où } n \in \mathbb{N} \text{ et } a_i \in A \cup A^{-1} \}$ .

## Démonstration

- ( $\subset$ ) On pose  $E = \{ a_1 a_2 \dots a_n \text{ où } n \in \mathbb{N} \text{ et } a_i \in A \cup A^{-1} \}$ .  
Il suffit de montrer que  $E$  est un sous-groupe de  $G$ .
- Puisque l'on a bien  $E$  qui contient  $a$ ,  $E \neq \emptyset$ .
  - $\forall x, y \in E, \exists n, p \in \mathbb{N}$  et  $\exists a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_p \in A \cup A^{-1}$  tels que :  
 $x = a_1 a_2 \dots a_n$  et  $y = b_1 b_2 \dots b_p$ .  
D'où  $xy^{-1} = a_1 a_2 \dots a_n b_p^{-1} b_{p-1}^{-1} \dots b_1^{-1}$ .  
On a bien  $xy^{-1} \in E$  car  $b_i^{-1} \in A \cup A^{-1} \forall i = 1, n$ .
- ( $\supset$ ) Puisque  $\text{gr}(A)$  est un sous-groupe qui contient  $a$ ,  $\text{gr}(A)$  doit être stable par inverse et composition. Donc  $A^{-1} \subset \text{gr}(A)$ ,  $A \cup A^{-1} \subset \text{gr}(A)$  et  $\forall n \in \mathbb{Z}, a_1 a_2 \dots a_n \in \text{gr}(A)$  si  $a_i \in A \cup A^{-1}$ .

## Exemple

Dans  $(\mathbb{Z}, +)$ , on considère  $A = \{ 2, 3 \}$ . On a  $\text{gr}(A) = \mathbb{Z}$ .

## Définition

Soit  $G$  un groupe et soit  $A$  une partie de  $G$ .

On dit que  $A$  est une partie génératrice de  $G$  si et seulement si  $\text{gr}(A) = G$ .

En particulier, on dit que le groupe est monogène si, de plus, on a  $\text{card}(A) = 1$ .

## Exemple

$(\mathbb{Z}, +)$  est monogène car  $\text{gr}(1) = \mathbb{Z}$ .

## Définition

Un groupe est dit cyclique si et seulement si il est monogène et de cardinal fini.

## Exemples

- $(\{1, i, -1, -i\}, \times)$  est cyclique.
- $\mathbb{Z}/p\mathbb{Z}$  est cyclique.
- Soit  $p$  un entier non nul. Dans le plan cartésien muni d'un repère orthonormal  $(O, \vec{i}, \vec{j})$ , l'ensemble des rotations de centre  $O$  et d'angle  $\frac{2k\pi}{p}$  ( $k \in \mathbb{Z}$ ) muni de la loi de composition usuelle des fonctions est un groupe cyclique.

## Remarque

Un groupe cyclique est donc un ensemble de la forme  $\{1, a, a^2, \dots, a^p\}$  où  $a$  est un élément du groupe.

## Définition

Soit  $(G, *)$  un groupe d'élément neutre 1 et soit  $x$  un élément de  $G$ .

On définit l'ordre de  $x$  (noté  $\text{ordre}(x)$ ) par : si  $\forall n \in \mathbb{N}^*, x^n \neq 1$  alors  $\text{ordre}(x) = +\infty$   
sinon  $\text{ordre}(x)$  est le plus petit entier non nul  $p$  tel que  $x^p = 1$ .

## Exemples

- Dans  $(\{1, i, -1, -i\}, \times)$ ,  $\text{ordre}(1) = 1$ ,  $\text{ordre}(-1) = 2$ ,  $\text{ordre}(i) = 4$  et  $\text{ordre}(-i) = 4$ .
- Dans  $(\mathbb{Z}, +)$ ,  $\text{ordre}(1) = +\infty$ ,  $\text{ordre}(3) = +\infty$  et  $\text{ordre}(0) = 1$ .

## Définition

Soient  $(G, *)$  et  $(G', *')$  deux groupes.

On dit qu'une application  $f$  de  $G$  vers  $G'$  est un morphisme de groupes si et seulement si :

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

## Exemples

- $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \times)$   
 $x \mapsto \exp x$
- $g : (\mathbb{R}^*, \times) \rightarrow (\mathbb{R}, +)$   
 $x \mapsto \ln |x|$
- $h : (\mathbb{C}^*, \times) \rightarrow (\mathbb{C}^*, \times)$   
 $z \mapsto \bar{z}$
- Soient  $(G, *)$  et  $(G', *')$  deux groupes d'éléments neutres respectifs  $e$  et  $e'$ .  
 $i : (G, *) \rightarrow (G', *')$   
 $x \mapsto e'$

## Remarques

Un morphisme d'un ensemble dans lui-même est appelé un endomorphisme.

Un morphisme bijectif est appelé un isomorphisme.

Un endomorphisme bijectif est appelé un automorphisme.

Deux groupes sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre.

## Exemples fondamentaux

- Soit  $(G, *)$  un groupe noté multiplicativement et soit  $x$  un élément de  $G$ .

$$f_x : (\mathbb{Z}, +) \rightarrow (G, *)$$
$$n \rightarrow \begin{cases} x^n & \text{si } n > 0 \\ 1 & \text{si } n = 0 \\ (x^{-1})^{-n} & \text{si } n < 0 \end{cases} \quad \text{on vérifie que } f_x \text{ est un bien un homomorphisme de groupe.}$$

- Soit  $(G, *)$  un groupe noté additivement et soit  $x$  un élément de  $G$ .

$$f_x : (\mathbb{Z}, +) \rightarrow (G, *)$$
$$n \rightarrow \begin{cases} nx & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ (-n)(-x) & \text{si } n < 0 \end{cases} \quad \text{on vérifie que } f_x \text{ est un bien un homomorphisme de groupe.}$$

## Remarque

On pourra parler aussi de morphismes de magmas ou de monoïdes.

Par exemple, si  $E$  est un ensemble, l'application  $f : (\mathcal{P}(E), \cup) \rightarrow (\mathcal{P}(E), \cap)$  est un morphisme de monoïde.

$$X \mapsto C_E X$$

## Propriété

Soient  $(G, *)$  et  $(G', *)$  deux groupes d'éléments neutres respectif  $e$  et  $e'$ .

Soit  $f$  un morphisme de groupe de  $G$  vers  $G'$ .

Alors  $f(e) = e'$ .

## Démonstration

$$\begin{aligned} f(x) &= f(x * e) = f(x) *' f(e) \\ &= f(e * x) = f(e) *' f(x) \end{aligned}$$

C'est-à-dire  $f(e) = e'$  à cause de l'unicité de l'élément neutre.

## Propriété

Soient  $(G, *)$  et  $(H, \nabla)$  deux groupes.

Soit  $f$  un morphisme de groupe de  $G$  vers  $H$ . Alors on a :

- $\forall x \in G, f(x^{-1}) = [f(x)]^{-1}$
- $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = [f(x)]^n$

## Démonstration

- $e' = f(x * x^{-1}) = f(x) \nabla f(x^{-1})$   
 $= f(x^{-1} * x) = f(x^{-1}) \nabla f(x)$

C'est-à-dire  $f(x^{-1}) = [f(x)]^{-1}$  à cause de l'unicité du symétrique.

- 1ère étape : si  $n \geq 0$ , on utilise une démonstration par récurrence :
  - vrai au rang 0 : par convention  $x^0 = e$
  - on suppose vrai au rang  $n$
$$f(x^{n+1}) = f(x^n * x) = f(x^n) * f(x) = [f(x)]^n \nabla f(x) = [f(x)]^{n+1}$$
- 2ème étape : si  $n < 0$ 

$$f(x^n) = f[(x^{-1})^{-n}] = [f(x^{-1})]^{-n} = [f(x)^{-1}]^{-n} = [f(x)]^n$$

## Remarque

En notation additive, cela donne :

- $\forall x \in G, f(-x) = -f(x).$
- $\forall x \in G, \forall n \in \mathbb{Z}, \text{ on a } f(nx) = nf(x).$

## Propriété

La composée de deux morphismes est un morphisme.

La composée de deux isomorphismes est un isomorphisme.

## Démonstration

Soient  $(G_1, *_1), (G_2, *_2)$  et  $(G_3, *_3)$  trois groupes.

Soit  $f$  un morphisme de groupe de  $G_1$  vers  $G_2$ .

Soit  $g$  un morphisme de groupe de  $G_2$  vers  $G_3$ .

$$\begin{aligned} \forall a, b \in G_1, (f \circ g)(a *_1 b) &= f[g(a *_1 b)] \\ &= f[g(a) *_2 g(b)] && \text{car } g \text{ est un morphisme} \\ &= f[g(a)] *_3 f[g(b)] && \text{car } f \text{ est un morphisme} \end{aligned}$$

## Définition

Soit  $(G_1, *_1)$  un groupe d'élément neutre  $e_1$  et soit  $(G_2, *_2)$  un groupe d'élément neutre  $e_2$ .

Soit  $f$  un morphisme de groupe de  $G_1$  vers  $G_2$ .

On appelle image de  $f$  et on note  $\text{Im } f$  l'ensemble image de  $f$  c'est-à-dire :

$$f(G_1) = \text{Im } f = \{y \in G_2 / \exists x \in G_1; y = f(x)\}.$$

On appelle noyau de  $f$  et on note  $\text{Ker } f$  l'image réciproque de  $\{e_2\}$  c'est-à-dire :

$$\text{Ker } f = \{x \in G_1 / f(x) = e_2\}.$$

## Exemples

- $f: (\mathbb{Z}, +) \rightarrow (\{0,1\}, +)$ 

$$\begin{aligned} p \mapsto 0 & \text{ si } p = 2k & k \in \mathbb{Z} \\ p \mapsto 1 & \text{ si } p = 2k+1 & k \in \mathbb{Z} \end{aligned} \quad \text{Ker } f = 2\mathbb{Z}$$
- $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \times)$ 

$$x \mapsto \exp x \quad \text{Im } f = \mathbb{R}_+^*$$

## Propriété

Soit  $(G_1, *_1)$  un groupe d'élément neutre  $e_1$  et soit  $H_1$  un sous-groupe de  $G_1$ .

Soit  $(G_2, *_2)$  un groupe d'élément neutre  $e_2$  et soit  $H_2$  un sous-groupe de  $G_2$ .

Soit  $f$  un morphisme de groupe de  $G_1$  vers  $G_2$ .

Alors  $f(H_1)$  est un sous-groupe de  $G_2$  et  $f^{-1}(H_2)$  est un sous-groupe de  $G_1$ .

En particulier,  $\text{Im } f$  est un sous-groupe de  $G_2$  et  $\text{Ker } f$  est un sous-groupe de  $G_1$ .

## Démonstration

- ◇  $f(H_1)$  sous-groupe de  $G_2$ .
- $e_1 \in H_1$  donc  $f(e_1) = e_2 \in f(H_1)$ . Donc  $f(H_1) \neq \emptyset$ .
  - Soient  $b_1$  et  $b_2$  deux éléments de  $f(H_1)$ .  
 $\exists a_1 \in H_1 / b_1 = f(a_1)$  et  $\exists a_2 \in H_1 / b_2 = f(a_2)$   
 $b_1 *_2 (b_2)^{-1} = f(a_1) *_2 (f(a_2))^{-1}$   
 $= f(a_1) *_2 f(a_2^{-1})$   
 $= f(a_1 *_1 a_2^{-1})$   
 or  $a_1 *_1 a_2^{-1} \in H_1$  car  $H_1$  est un sous-groupe de  $G_1$ .  
 Donc  $b_1 *_2 (b_2)^{-1} \in f(H_1)$ .
- ◇  $f^{-1}(H_2)$  sous-groupe de  $G_1$ .
- $e_2 \in H_2$  et  $f(e_1) = e_2$  donc  $e_1 \in f^{-1}(H_2)$ . Donc  $f^{-1}(H_2) \neq \emptyset$ .
  - Soient  $a_1$  et  $a_2$  deux éléments de  $f^{-1}(H_2)$ .  
 $\exists b_1 \in H_2 / b_1 = f(a_1)$  et  $\exists b_2 \in H_2 / b_2 = f(a_2)$   
 $f(a_1 *_1 a_2^{-1}) = f(a_1) *_2 f(a_2^{-1})$   
 $= f(a_1) *_2 (f(a_2))^{-1}$   
 $= b_1 *_2 (b_2)^{-1}$   
 or  $b_1 *_2 (b_2)^{-1} \in H_2$  car  $H_2$  est un sous-groupe de  $G_2$ .  
 Donc  $a_1 *_1 a_2^{-1} \in f^{-1}(H_2)$ .

## 3. Anneaux et corps

### Définition

Soit  $A$  un ensemble muni de deux lois de composition interne  $T$  et  $\perp$ .

On dit que  $(A, T, \perp)$  est un anneau si et seulement si :

- $(A, T)$  est un groupe abélien.
- $(A, \perp)$  est un monoïde.
- La loi  $\perp$  est distributive par rapport à la loi  $T$ .  
 c'est-à-dire distributive à gauche:  $\forall x, y, z \in A, x \perp (y T z) = (x \perp y) T (x \perp z)$   
 et distributive à droite:  $\forall x, y, z \in A, (y T z) \perp x = (y \perp x) T (z \perp x)$ .

### Remarques

- Un anneau n'est jamais vide
- Généralement la loi donnant la structure de groupe est notée additivement et l'autre est notée multiplicativement.

### Exemples

- $(\mathbb{Z}, +, \times)$  où  $+$  et  $\times$  sont l'addition usuelle et la multiplication usuelle.
- $(\mathbb{D}, +, \times)$  où  $+$  et  $\times$  sont l'addition usuelle et la multiplication usuelle
- $(\{0, 1\}, +, \times)$  où  $+$  et  $\times$  sont les lois définis par les tableaux suivants :  

$$\begin{array}{cc} + & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{et} \quad \begin{array}{cc} \times & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$
- $(\{0\}, +, \times)$  où  $+$  et  $\times$  sont l'addition usuelle et la multiplication usuelle.  
 Cet anneau est appelé un anneau nul.

- Soit  $E = \{\text{fonctions numériques définies sur } \mathbb{R}\}$   
 $(E, +, \times)$  où  $+$  et  $\times$  sont les lois usuelles :  
 $(f + g)(x) = f(x) + g(x)$  et  
 $(f \times g)(x) = f(x) \times g(x)$  pour tout réel  $x$  ( $f$  et  $g$  étant deux éléments de  $E$ )  
 On pourrait déterminer les éléments neutres pour chacune des lois.....

## Notation

Soit  $(A, +, \times)$  un anneau.

On note généralement  $0$  ou  $0_A$  l'élément neutre de  $(A, +)$  et  $1$  ou  $1_A$  l'élément neutre de  $(A, \times)$ .

On parlera d'opposé pour le symétrique d'un élément pour la loi  $+$ .

On note  $A^* = A \setminus \{0_A\}$ .

## Exemple

Pour les matrices, on a dans  $(\mathcal{M}_3(\mathbb{R}), +, \times)$  :

$$1 = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } 0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

## Définition

Un anneau  $(A, +, \times)$  est dit commutatif si la loi  $\times$  est commutative.

## Exemples

- Les précédents exemples d'anneaux sont des anneaux commutatifs.
- Soit  $(G, +)$  un groupe abélien.  
 Soit  $\text{End}(G) = \{\text{endomorphismes de } G\}$ .  
 $+$  et  $\circ$  étant l'addition et la composition usuelle des fonctions.  
 $(\text{End}(G), +, \circ)$  est un anneau qui n'est généralement pas commutatif.
- $(\mathcal{M}_n(\mathbb{R}), +, \times)$  que nous verrons plus tard n'est pas non plus commutatif.

## Propriétés

Soit  $(A, +, \times)$  un anneau.

- $\forall x \in A, \quad 0 \times x = x \times 0 = 0.$
- $\forall x, y \in A \quad (-x) \times y = x \times (-y) = -(x \times y).$
- $\forall x, y \in A \quad (-x) \times (-y) = x \times y.$

## Conséquence

$0$  n'a de symétrique pour la loi  $\times$  que si  $1 = 0$ .

## Démonstration

- $\forall x \in A, \quad 0 \times x = (0 + 0) \times x$   
 $= 0 \times x + 0 \times x.$   
 Donc  $0 \times x = 0.$                       *Idem pour l'autre égalité.*

- b.  $\forall x, y \in A \quad 0 \times y = 0$   
 $0 \times y = (x + (-x)) \times y = x \times y + (-x) \times y = 0$  donc  $(-x) \times y$  est le symétrique de  $x \times y$ .  
 $x \times 0 = 0$   
 $x \times 0 = x \times (y + (-y)) = x \times y + x \times (-y) = 0$  donc  $x \times (-y)$  est aussi le symétrique de  $x \times y$ .
- c.  $\forall x, y \in A \quad (-x) \times (-y) = -(x \times (-y)) = -(-x \times y) = x \times y$ .

## Remarque importante

Soit  $(A, +, \times)$  un anneau.

Si l'élément neutre de la multiplication est le même que celui de l'addition c'est-à-dire  $1 = 0$  alors

$\forall x \in A, \quad 1 \cdot x = x$  car 1 élément neutre de la multiplication.

et  $1 \cdot x = 0 \cdot x = 0$  d'après la propriété précédente.

Donc  $\forall x \in A, \quad x = 0$  c'est-à-dire  $A$  anneau réduit à un seul élément.

Un tel anneau sera appelé un anneau nul.

Les autres anneaux seront dits unifères.

## Définition

Soit  $(A, +, \times)$  un anneau unifère.

On dit qu'un élément est inversible si et seulement si il admet un symétrique par rapport à la loi  $\times$  c'est-à-dire  $x \in A$  et  $x$  inversible  $\Leftrightarrow \exists x' \in A / x \times x' = x' \times x = 1$ .

On note  $u(A)$  l'ensemble des éléments inversibles de  $A$  (qui sont appelés aussi des unités).

## Exemple

- $u(\mathbb{Z}) = \{-1; 1\}$  et  $u(\mathbb{Q}) = \mathbb{Q}^*$ .
- $(E, +, \times)$  où  $E = \{\text{fonctions numériques définies sur } \mathbb{R}\}$ ,  $+$  et  $\times$  sont l'addition et la multiplication usuelles des fonctions.  
 $u(E) = \{\text{fonctions numériques qui ne s'annulent pas sur } \mathbb{R}\}$ .
- $(\text{End}(G), +, \circ)$  où  $(G, +)$  est un groupe  $+$  et  $\circ$  sont l'addition et la composition usuelles des fonctions.  
 $u(\text{End}(G)) = \text{Aut}(G) = \{\text{automorphismes de } G\}$ .

## Propriété

Soit  $(A, +, \times)$  un anneau unifère.

L'ensemble  $u(A)$  des unités est un groupe pour la loi  $\times$  de  $A$  (loi induite).

## Démonstration

- Stabilité : évident  $\forall x, y \in u(A) \quad xy(y^{-1}x^{-1}) = 1$
- Associativité : évident  $(A, \times)$  est un monoïde
- Élément neutre : évident  $1 \cdot 1 = 1$
- Symétrique : évident par définition de  $u(A)$

## Exemple

$(\mathbb{R}, +, \times)$  est un anneau dont les éléments inversibles sont les réels non nuls donc  $(\mathbb{R}^*, \times)$  est un groupe.

$(\mathbb{Z}, +, \times)$  est un anneau dont les éléments inversibles sont  $-1$  et  $1$  donc  $(\{-1; 1\}, \times)$  est un groupe.

## Définition

Soit  $(A, +, \times)$  un anneau unifié. Soit  $a, b \in A^*$ .

Si  $ab = 0$ , on dit que  $a$  est un diviseur de zéro à gauche et que  $b$  est un diviseur de zéro à droite.

## Exemples

- $(E, +, \times)$  où  $E = \{\text{fonctions numériques définies sur } \mathbb{R}\}$ ,  $+$  et  $\times$  sont l'addition et la multiplication usuelles des fonctions.

Soient  $f$  et  $g$  les fonctions de  $E$  définies par :

$$f(x) = \begin{cases} 0 & \text{si } x < 0 \\ 1 & \text{sinon} \end{cases} \quad g(x) = \begin{cases} 1 & \text{si } x < 0 \\ 0 & \text{sinon} \end{cases}$$

On a  $f \times g = 0$ .

- Dans  $\mathbb{Z}/6\mathbb{Z}$ , on a  $\bar{2} \times \bar{3} = \bar{0}$ .
- Dans  $\mathcal{M}_2(\mathbb{R})$ , on a  $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ .

## Définition

On dit qu'un anneau non nul est intègre si et seulement si il ne possède pas de diviseur de zéro.

## Exemples

- $(\mathbb{Z}, +, \times)$  est un anneau intègre.
- $(\mathbb{C}, +, \times)$  est un anneau intègre.
- $(\mathbb{Z}/5\mathbb{Z}, +, \times)$  est un anneau intègre ( $+$  et  $\times$  étant les lois quotients).
- De façon général,  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un anneau intègre si  $p$  est premier.

## Définition

Soit  $(A, +, \times)$  et  $(A', +, \times)$  deux anneaux.

On appelle morphisme d'anneaux toute application de  $A$  dans  $A'$  qui vérifie :

$$\forall x, y \in A, \quad f(x+y) = f(x) + f(y) \\ \text{et } f(x \times y) = f(x) \times f(y).$$

## Exemple

$$f: (\mathbb{C}, +, \times) \rightarrow (\mathbb{C}, +, \times) \\ z \mapsto \bar{z}$$

## Remarque

L'élément unité de  $A$  n'est pas forcément transformé en l'élément unité de  $A'$ .

- $f: A \rightarrow A'$   
 $x \mapsto 0$   $f$  est bien un morphisme d'anneaux et on a  $f(1) = 0$ .
- Soient  $A$  et  $B$  deux anneaux.  
 $i: A \rightarrow A \times B$   
 $x \mapsto (x, 0)$   $i$  est bien un morphisme d'anneaux et on a  $i(1) = (1, 0) \neq (1, 1)$ .

Si  $A$  et  $A'$  sont unifiés et que l'on a  $f(1) = 1$ , on dit que  $f$  est unitaire.

## Définition

Soit  $(A, +, \times)$  un anneau.

On dit qu'une partie  $B$  de  $A$  est un sous anneau de  $A$  si et seulement si :

- (i)  $(B, +)$  est un sous-groupe de  $A$ .
- (ii)  $B$  est stable pour la loi  $\times$  c'est-à-dire  $\forall x, y \in B, x \times y \in B$

## Exemples

- $(\mathbb{Z}, +, \times)$  est un sous anneau de  $(\mathbb{R}, +, \times)$ .
- $(2\mathbb{Z}, +, \times)$  est un sous anneau de  $(\mathbb{Z}, +, \times)$ .

## Remarques

- Soit  $(A, +, \times)$  un anneau et  $B$  un sous anneau de  $A$ .  
 $A$  unifié  $\not\Rightarrow B$  unifié. Par exemple,  $\{0_A\}$  est un sous anneau de tout anneau unifié.
- $(2\mathbb{Z}, +, \times)$  est un sous anneau de  $A$  mais ne possède pas d'élément neutre pour la multiplication..

## Définition

On dit qu'un sous anneau  $B$  d'un anneau  $A$  est unitaire s'il possède le même élément unité que  $A$ .

## Exemple

$\mathbb{Z}$  est le seul sous anneau unitaire de  $(\mathbb{Z}, +, \times)$ .

## Remarque

Pour Bourbaki et certains autres, il n'existe pas d'autre sous-anneaux que ceux qui sont unitaires et il n'existe pas d'autre morphisme que ceux qui sont unitaires.

## Propriété

Un sous-anneau unitaire d'un anneau est un anneau.

## Propriété

Soit  $(A, +, \times)$  un anneau.

Soit  $(B_i)_{i \in I}$  une famille non vide de sous anneaux (resp. sous anneaux unitaires) de  $A$ .

Alors  $\bigcap_{i \in I} B_i$  est un sous anneau (resp. sous anneau unitaire) de  $A$ .

## Démonstration

- $\forall i \in I, B_i$  est un sous-groupe de  $A$  donc  $\bigcap_{i \in I} B_i$  est un sous-groupe de  $A$ .
- Stable par multiplication  
 $x, y \in \bigcap_{i \in I} B_i \Leftrightarrow \forall i \in I, x \in B_i \text{ et } y \in B_i$   
 $\Rightarrow \forall i \in I, x \times y \in B_i \Rightarrow x \times y \in \bigcap_{i \in I} B_i$
- $\forall i \in I, 1_A \in I$ . Donc  $1_A \in \bigcap_{i \in I} B_i$ .

## Propriété

Soit  $(A, +, \times)$  un anneau et soit  $C$  une partie de  $A$ .

On appelle sous anneau engendré par  $C$ , le plus petit (en terme d'inclusion) sous anneau de  $A$  qui contient le sous-ensemble  $C$ .

## Démonstration

Soit  $(B_i)_{i \in I}$  l'ensemble des sous anneaux de  $A$  qui contiennent  $C$ .

Cette famille n'est pas vide car  $A$  appartient à cette famille.

$\bigcap_{i \in I} B_i$  est le plus petit sous anneau de  $A$  qui contient  $C$ .

## Propriété

Soient  $(A, +, \times)$  et  $(A', +, \times)$  deux anneaux.

Soit  $f$  un morphisme unitaire d'anneaux de  $A$  vers  $A'$ .

L'image directe d'un sous anneau (resp. unitaire) de  $A$  est un sous anneau (resp. unitaire) de  $A'$ .

L'image réciproque d'un sous anneau (resp. unitaire) de  $A'$  est un sous anneau (resp. unitaire) de  $A$ .

## Démonstration

- Sous-groupe déjà fait.
- Stabilité par multiplication évidente.

Dans la partie qui concerne les idéaux, nous considérerons uniquement des anneaux unifières commutatifs.

## Définition

Soit  $(A, +, \times)$  un anneau et soit  $I$  une partie de  $A$ .

On dit que  $I$  est un idéal de  $A$  si et seulement si

- (i)  $(I, +)$  est un sous-groupe de  $A$ .
- (ii)  $\forall x \in I, \forall a \in A, a \times x \in I$ .

## Exemples

- $(2\mathbb{Z}, +, \times)$  est un idéal de  $(\mathbb{Z}, +, \times)$
- De façon plus générale,  $(p\mathbb{Z}, +, \times)$  est un idéal de  $(\mathbb{Z}, +, \times)$  pour tout  $p \in \mathbb{N}$ .
- $A$  et  $\{0_A\}$  sont des idéaux de  $A$ .

## Remarques

- Tout idéal est un sous anneau.
- Si  $A$  est unifière le seul idéal de  $A$  qui contienne l'élément unité est  $A$  lui-même.
- $\mathbb{Z}$  est un sous anneau de  $(\mathbb{R}, +, \times)$  mais n'est pas un idéal de ce même anneau.

## Propriété

Soit  $(A, +, \times)$  un anneau et soit  $(I_j)_{j \in J}$  une famille non vide d'idéaux de  $A$ . Alors  $\bigcap_{j \in J} I_j$  est un idéal de  $A$ .

## Démonstration

- $\forall j \in J, I_j$  est un sous-groupe de  $A$  donc  $\bigcap_{j \in J} I_j$  est un sous-groupe de  $A$ .
- Stable par multiplication par un élément de  $A$   
$$x \in \bigcap_{j \in J} I_j \quad \Leftrightarrow \forall j \in J, x \in I_j \quad \Rightarrow \forall j \in J, x \times a \in I_j \quad \forall a \in A$$
$$\Rightarrow x \times a \in \bigcap_{j \in J} I_j.$$

## Propriété

Soit  $(A, +, \times)$  un anneau et soit  $C$  une partie de  $A$ .

On appelle idéal engendré par  $C$ , le plus petit (au sens de l'inclusion) idéal de  $A$  qui contient  $C$ .

## Démonstration

Soit  $(B_i)_{i \in I}$  l'ensemble des idéaux de  $A$  qui contiennent  $C$ . Cette famille n'est pas vide car  $A$  appartient à cette famille. L'ensemble  $\bigcap_{i \in I} B_i$  est le plus petit idéal de  $A$  qui contient  $C$ .

**Remarque** (Caractérisation d'un idéal engendré par une partie d'un anneau)

Soit  $C$  une partie non vide d'un anneau  $(A, +, \times)$ .

Soit  $E = \{c_1 a_1 + c_2 a_2 + \dots + c_n a_n \text{ où } n \in \mathbb{N}^* \text{ et } \forall i = 1, n \ c_i \in C \text{ et } a_i \in A\}$ .

1. Tout élément de  $E$  appartient à l'idéal engendré par  $C$  dans  $A$ .
2. On peut vérifier que  $E$  est un idéal de  $A$  qui contient  $C$ .

## Définition

Soit  $(A, +, \times)$  un anneau.

Soit  $I$  une partie de  $A$ .

On dit que  $I$  est un idéal principal de  $A$  si et seulement si  $I$  peut être engendré par un seul élément (pas nécessairement unique).

## Exemples

- $(2\mathbb{Z}, +, \times)$  est un idéal principal de  $(\mathbb{Z}, +, \times)$ .  
C'est le plus petit idéal de  $\mathbb{Z}$  qui contient 2.
- $I = \{(X+1)Q(X) \text{ où } Q \in \mathbb{R}[X]\}$  est un idéal principal de  $(\mathbb{R}[X], +, \times)$   
C'est le plus petit idéal de  $\mathbb{R}[X]$  qui contient  $X+1$ .

## Remarque

On dit qu'un anneau est principal si et seulement si tous ses idéaux sont principaux.

## Propriété

Soient  $(A, +, \times)$  et  $(A', +, \times)$  deux anneaux.

Soit  $f$  un morphisme d'anneaux de  $A$  vers  $A'$ .

L'image réciproque d'un idéal de  $A'$  est un idéal de  $A$ .

En particulier,  $\text{Ker } f$  est un idéal de  $A$ .

## Remarque

En général, l'image directe d'un idéal de  $A$  n'est pas un idéal de  $A'$  mais de  $f(A)$ .

## Démonstration

### 1. Image réciproque

- Sous-groupe déjà fait.
- Stabilité par multiplication par un élément de  $A$ .  
Soit  $I$  un idéal de  $A'$ ,  $x \in f^{-1}(I) \Leftrightarrow f(x) \in I$   
 $\forall a \in A, f(ax) = f(a)f(x)$  or  $f(a) \in A'$  et  $f(x) \in I$  donc  $f(a)f(x) \in I$ .  
C'est-à-dire  $ax \in f^{-1}(I)$ .

### 2. $\text{Ker}f = f^{-1}(\{0_{A'}\})$ .

$\{0_{A'}\}$  est bien un idéal de  $A'$ .

## Définition

Soit  $(A, +, \times)$  un anneau.

On définit l'indice d'un élément  $a$  de  $A$  (noté  $i(a)$ ) par :

Si  $\forall n \in \mathbb{N}^*, na \neq 0$  alors  $i(a) = +\infty$ .

Sinon  $i(a)$  est le plus petit entier non nul  $p$  tel que  $pa = 0$ .

## Exemple

Dans  $\mathbb{Z}/12\mathbb{Z}$ ,  $i(2) = 6$  et  $i(3) = 4$ .

## Définition

Soit  $(A, +, \times)$  un anneau.

Soit  $J$  l'ensemble des indices des éléments de  $A$ .

Si  $J$  est majoré, le ppcm de ces indices est appelé caractéristique de l'anneau  $A$  et est noté  $\chi(A)$ .

Si  $J$  est non majoré, on dit que l'anneau est de caractéristique nulle.

## Exemples

$$\chi(\mathbb{R}) = 0.$$

$$\chi(\mathbb{Z}/2\mathbb{Z}) = 2.$$

## Définition

On appelle corps tout anneau unifié dont tous les éléments non nuls sont inversibles.

C'est-à-dire, si  $(A, +, \times)$  est un anneau unifié, on a :  $A$  corps  $\Leftrightarrow (A^*, \times)$  est un groupe

Si de plus la loi  $\times$  est commutative, on dit que le corps est commutatif.

## Exemples

- $(\mathbb{Z}, +, \times)$  et  $(\mathbb{R}[X], +, \times)$  ne sont pas des corps.
- $(\mathbb{R}, +, \times)$  et  $(\mathbb{R}(X), +, \times)$  sont des corps.
- $\mathbb{Z}/5\mathbb{Z}$  est un corps.

## Propriété

Tout corps est intègre.

## Démonstration

Supposons  $ab = 0$  avec  $a \neq 0$  et  $b \neq 0$ .

Si  $a \neq 0$ , alors  $a$  est inversible  $\Rightarrow a^{-1}ab = a^{-1}0 \Rightarrow b = 0$  absurde.