

.  
. .  
. .  
. .



# Cours de Structures algébriques



.  
. .  
. .

**Mathias K.KOUAKOU**

**Université F.H.B de Cocody Abidjan (Côte d'Ivoire)**

- Lois de composition internes
- Groupes
- Anneaux
- Polynômes et fractions rationnelles à une variable
- Espaces vectoriels sur un corps

# Chapitre 1

## LOIS DE COMPOSITION INTERNES

### 1.1 Définitions et exemples

Soit  $E$  un ensemble non vide. On appelle loi de composition interne *l.c.i* sur  $E$  toute application  $f$  de  $E \times E$  dans  $E$ . Avec une loi de composition interne sur  $E$ , on a une règle de base pour calculer dans  $E$ .

Par exemple si :

$$E = \{ \bigcirc, \triangle, \square \}$$

Une loi de composition interne sur  $E$  est une application  $f$  de  $E \times E \longrightarrow E$ . Une telle application peut être définie par un tableau

*	$\bigcirc$	$\square$	$\triangle$
$\bigcirc$	$\square$	$\triangle$	$\bigcirc$
$\square$	$\bigcirc$	$\triangle$	$\triangle$
$\triangle$	$\bigcirc$	$\square$	$\bigcirc$

en convenant que  $f(X, Y)$  est l'élément du tableau se trouvant sur la ligne  $X$  et la colonne  $Y$ .

On pose  $X * Y = f(X, Y)$

On a alors

$$\bigcirc * \bigcirc = \square$$

$$\bigcirc * \triangle = \bigcirc$$

$$\triangle * \bigcirc = \bigcirc$$

$$\triangle * \triangle = \bigcirc$$

$$(\triangle * \square) * \bigcirc = \square * \bigcirc = \bigcirc$$

$$\triangle * (\square * \bigcirc) = \triangle * \bigcirc = \bigcirc$$

**Exemples classiques**

- 1.
- $E = \mathbb{R}$
- ou
- $E = \mathbb{C}$

$$(x, y) \mapsto x + y ; (x, y) \mapsto x \times y$$

2. si
- $A \neq \emptyset$
- , on pose
- $E = \mathcal{F}(A)$
- l'ensemble de toutes les applications de
- $A$
- dans
- $A$

$$(f, g) \mapsto f \circ g$$

3. La réunion "
- $\cup$
- " l'intersection "
- $\cap$
- " définissent sur
- $\mathcal{P}(A)$
- des lois de compositions internes.

**Notation :** Une loi de composition interne  $f : E \times E \rightarrow E$  est en général désignée explicitement par un symbole :  $\bullet, +, *, \top, \perp, \circ, \Delta, \dots$ , etc et  $f(x, y)$  est noté  $x \bullet y, x + y, x * y, \dots$ , etc La notation  $x + y$  est dite additive, alors que toutes les autres,  $x \bullet y, x * y, \dots$  sont dites multiplicatives.

**1.2 Parties stables**

Soient  $*$  une loi de composition interne sur  $E$  et  $A$  une partie **non vide** de  $E$ . On dit que  $A$  est stable pour la loi  $*$ , si

$$\forall (a, b) \in A^2, \text{ on a } a * b \in A$$

**Exemples :**

- Dans  $\mathbb{R}$  muni de l'addition,  $\{0\}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, [1, +\infty[, ]-\infty, -1], \dots$ , etc sont stables.

- Dans  $\mathbb{R}$  muni de la multiplication,

$$\{0\}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, [1, +\infty[, [0, 1], [-1, 1], \mathbb{R}_+, \mathbb{R}^*, \{1\}, \{1, -1\}, \dots, \text{ etc}$$

sont stables.

- Dans  $\mathcal{F}(A)$  muni de la composition des applications, le sous ensemble des applications injectives, celui des applications surjectives, et celui des applications bijectives sont stables.

**Remarques :** • Si  $A$  est une partie stable pour la loi  $*$ , alors l'application

$$f' : A \times A \longrightarrow A, (x, y) \mapsto x * y \text{ est bien définie.}$$

C'est donc une loi de composition interne sur  $A$ .

**On dit  $*$  induit naturellement une l.c.i sur  $A$ .**

• Notons bien que  $E$  est stable, et c'est la plus grande partie (au sens de l'inclusion  $\subseteq$ ) stable de  $(E, *)$

**1.3 Lois associatives**

Une loi de composition interne  $*$  sur  $E$  est dite **associative** si

$$\forall (x, y, z) \in E^3, \text{ on a } x * (y * z) = (x * y) * z$$

**Exemples et contre - exemples**

- l'addition et la multiplication dans  $\mathbb{C}$  sont associatives
- La composition des application est associative
- $\cap$  et  $\cup$  sont associatives dans  $\mathcal{P}(A)$
- Sur  $\mathbb{R}$ , la loi  $*$  définie par :  $x * y = x.y + 2$  n'est pas associative :  
**on a**  $((1 * 2) * 0 = 2$  **alors que**  $1 * (2 * 0) = 4)$

**Produit fini d'éléments de  $E$  .**

Soit  $E$  un ensemble non vide muni d'une loi de composition interne  $*$  et soit  $(x_1, x_2, \dots, x_n) \in E^n$  (où  $n \geq 3$ ). Le produit de la suite finie d'éléments de  $E$  :  $(x_1, x_2, \dots, x_n)$  est défini par le produit de la suite finie d'éléments de  $E$  :  $(x_1, x_2, \dots, x_n)$  est défini inductivement par

$$x = x_1 * x_2 * \dots * x_n = x = (x_1 * x_2 * \dots * x_{n-1}) * x_n$$

**Proposition** Si la loi de composition  $*$  est associative, alors

$$x = (x_1 * \dots * x_i) * (x_{i+1} * \dots * x_n) \quad \text{pour tout } 1 \leq i < n$$

**Preuve** : Par récurrence sur  $n$ .

- Pour  $n = 3$ , c'est la définition de l'associativité
- à l'ordre  $n + 1$

$$\begin{aligned} & (x_1 * \dots * x_i) * (x_{i+1} * \dots * x_{n+1}) \\ &= (x_1 * \dots * x_i) * [(x_{i+1} * \dots * x_n) * x_{n+1}] \text{ par définition} \\ &= [(x_1 * \dots * x_i) * (x_{i+1} * \dots * x_n)] * x_{n+1} \text{ par associativité} \\ &= [x_1 * \dots * x_i * x_{i+1} * \dots * x_n] * x_{n+1} \text{ par H.R} \\ &= [x_1 * \dots * x_i] * x_{i+1} * \dots * x_n * x_{n+1} \text{ par H.R} \end{aligned}$$

Le produit  $\underbrace{x * x * \dots * x}_{n \text{ fois}}$  est noté  $x^n$ .

Avec une loi additive  $+$ , la somme  $\underbrace{x + x + \dots + x}_{n \text{ fois}}$  est notée  $nx$

**1.4 Lois commutatives**

Soit  $*$  une loi de composition interne sur  $E$ . On dit que deux éléments  $a$  et  $b$  de  $E$  sont permutables pour la loi  $*$  si

$$a * b = b * a$$

On dit que la loi  $*$  est commutative si,

$$\forall (x, y) \in E^2, \text{ on a } x * y = y * x.$$

( En d'autres termes, les éléments de  $E$  sont permutables 2 à 2 ).

**Remarques :**

- (1) Tout élément  $x \in E$  permute avec lui même.
- (2) Si  $*$  est associative, tout  $x$  permute avec  $x^n$  ( $n \in \mathbb{N}^*$ ).

**Exemples et contre exemples**

- $+$  et  $\times$  sont des lois commutatives dans  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .
- $\cap$  et  $\cup$  sont commutatives
- La composition des applications " $\circ$ " n'est pas commutative.

**Remarque :** Il y a des lois commutatives qui ne sont pas associatives, et des lois associatives qui ne sont pas commutatives.

## 1.5 Élément neutre

Soit  $E$  un ensemble muni d'une loi de composition  $*$  un élément  $a \in E$  est dit neutre pour la loi  $*$  si,

$$\forall x \in E, \text{ on a } x * a = x \quad \text{et} \quad a * x = x$$

**Exemples**

- 0 est élément neutre de  $+$  dans  $\mathbb{R}$
- 1 est élément neutre de  $\times$  dans  $\mathbb{R}$
- $A$  est élément neutre de  $\cap$  dans  $\mathcal{P}(A)$
- Le vide  $\emptyset$  est élément neutre de  $\cup$  dans  $\mathcal{P}(A)$
- $id_A$  est élément neutre de  $\circ$  dans  $\mathcal{F}(A)$

Il y a cependant des lois qui n'ont pas d'élément neutre. Par exemples

- La loi  $*$  définie sur  $\mathbb{R}$  par  $x * y = x \cdot y + 2$  n'a pas d'élément neutre
- La loi  $\top$  définie sur  $\mathbb{R}$  par :  $x \top y = x^2 \cdot y$  n'a pas d'élément neutre
- La multiplication  $\times$  définie sur  $[2, +\infty[$  n'a pas d'élément neutre.

**Théorème 2 :** Si une loi de composition interne admet un élément neutre, cet élément est unique.

**REMARQUE :** Si  $a$  est l'élément neutre de la loi  $*$ , alors  $a$  commute avec tous les éléments de  $E$ .

## 1.6 Éléments symétriques

Soient  $E$  un ensemble non vide muni d'une loi de composition interne  $*$  admettant " $a$ " comme élément neutre.

- Un élément  $x \in E$  admet un symétrique s'il existe un  $y \in E$  tel que  $x * y = y * x = a$

Dans ce cas on dit que  $y$  est un symétrique de  $x$ .

**Exemples :**

- Dans  $\mathbb{R}$  muni de  $+$ , tout élément  $x \in \mathbb{R}$  admet  $-x$  pour symétrique
- Dans  $\mathbb{R}$  muni de  $\times$ , tout les éléments  $x \in \mathbb{R}^*$  admet  $\frac{1}{x}$  pour symétrique
- Dans  $\mathcal{P}(A)$  muni de la loi  $\Delta$

$$X\Delta Y = (X \cap \bar{Y}) \cup (\bar{X} \cap Y)$$

L'ensemble vide  $\emptyset$  est élément neutre de  $\Delta$ , et tout élément  $X \in \mathcal{P}(A)$  s'admet lui-même pour symétrique

**Théorème 3 :** Si  $E$  est un ensemble non vide muni d'une loi de composition interne associative, admettent un élément neutre, alors tout  $x \in E$  admet au plus un symétrique.

**Notation :** Si  $x \in E$  admet un symétrique, ce symétrique est unique, on le note  $x^{-1}$  (en notation multiplicative) et  $-x$  (en notation additive).

**Proposition 4 :** Si  $x$  et  $y$  sont deux éléments de  $E$  admettant chacun symétrique, alors  $x * y$  admet  $y^{-1} * x^{-1}$  pour symétrique

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

**Preuve :** Calculer  $(x * y) * (y^{-1} * x^{-1})$  puis  $(y^{-1} * x^{-1})$

**Corollaire 5 :** Si  $x$  admet un symétrique, alors pour tout  $n \in \mathbb{N}^*$ ,  $x^n$  admet  $(x^{-1})^n$  pour symétrique :

$$(x^n)^{-1} = (x^{-1})^n$$

**REMARQUES :**

- Si  $a$  est l'élément neutre de la loi  $*$ , alors  $a$  est son propre symétrique.
- Si  $y$  est le symétrique de  $x$ , alors  $x$  est le symétrique de  $y$ .
- $x$  commute avec son symétrique  $y$ .

## 1.7 Homomorphismes

**Définition :** Soient  $E, F$  deux ensembles munis respectivement des lois de compositions internes  $*$  et  $\bullet$

On dit qu'une application  $f : E \longrightarrow F$  est un homomorphisme si

$$\forall (x, x') \in E^2, \text{ on a } f(x * x') = f(x) \bullet f(x')$$

**Exemples**

1.  $id_E : E \longrightarrow E$  est un homomorphisme
2. si la loi  $\bullet$  admet  $\varepsilon \in F$  comme élément neutre, alors l'application constante  $h : E \longrightarrow F, x \longmapsto \varepsilon$  est un homomorphisme.
3.  $\ln : \mathbb{R}_+^* \longrightarrow \mathbb{R}$  est un homomorphisme si on considère la multiplication dans  $\mathbb{R}_+^*$  et l'addition dans  $\mathbb{R}$
4.  $b : \mathbb{C} \longrightarrow \mathbb{C}; z \longmapsto \bar{z}$  est un endomorphisme de  $(\mathbb{C}, +)$
5.  $f : \mathbb{R}^2 \longrightarrow \mathbb{R}, (a, b) \longmapsto 2a + b$  est un homomorphisme avec  $\mathbb{R}$  muni de l'addition usuelle et  $\mathbb{R}^2$  muni de l'addition suivante :

$$(a, b) + (a', b') = (a + a', b + b')$$

**Définitions :**

- un homomorphisme bijectif est appelé isomorphisme.
- Un homomorphisme de  $(E, *)$  dans  $(E, *)$  est appelé endomorphisme.

**Proposition 6 :** Soient  $f : E \longrightarrow F$  et  $g : F \longrightarrow G$  deux homomorphismes, alors  $g \circ f$  est un homomorphisme.

**Preuve :**  $(E, *)$  ,  $(F, \bullet)$  ,  $(G, \perp)$

**Proposition 7 :** Si  $f : E \longrightarrow F$  est un isomorphisme, alors la bijection réciproque  $f^{-1}$  est un isomorphisme.

**Exercice 1**

Soit  $f : E \longrightarrow F$  un homomorphisme

1. Montrer que si  $A$  est une partie stable de  $E$ , alors  $f(A)$  est une partie stable de  $F$ . (En partie en particulier  $Im f$  est une partie stable de  $F$ )
2. Montrer que si  $B$  est une partie stable de  $E$ , alors  $f^{-1}(B)$  est une partie stable de  $E$ .

**Exercice 2** Soient  $E$  et  $F$  deux ensembles munis respectivement des lois de composition internes  $*$  et  $\bullet$

1. Montrer que sur  $E \times F$ , les lois  $*$  et  $\bullet$  induisent une loi de composition interne  $\top$  :

$$(x, y) \top (x', y') = (x * x', y \bullet y')$$

2. Montrer que si  $A$  et  $B$  sont respectivement des parties stables de  $E$  et de  $F$ , alors  $A \times B$  est une partie stable pour  $E \times F$  pour la loi  $\top$



# Chapitre 2

## GROUPE

### 2.1 Définitions et exemples

On appelle groupe un ensemble non vide  $E$  muni d'une loi de composition interne  $*$  possédant les propriétés suivantes :

- i)  $*$  est associative.
- ii)  $*$  admet un élément neutre dans  $E$ .
- iii) Tout élément de  $E$  admet un symétrique.

Si de plus la loi  $*$  est commutative, le groupe  $E$  est dit commutatif. Les groupes commutatifs sont appelés groupes abéliens.

#### Exemples classiques

1.  $\mathbb{Z}$  muni de l'addition  $+$  est un groupe abélien.  
 $\mathbb{Z}$  muni de la multiplication  $\times$  n'est pas un groupe.
2.  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  sont des groupes abélien avec l'addition  $+$ , mais ne sont pas des groupes avec la multiplication  $\times$ .
3.  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}^*$  sont des groupes avec la multiplication.
4. Soit  $A$  un ensemble non vide.  
 $\mathcal{S}(A) = \{f \in \mathcal{F}(A) : f \text{ bijective}\}$  est une partie stable par la composition des applications  $\circ$ .  
 $\circ$  définit donc une loi de composition interne sur  $\mathcal{S}(A)$ , et muni de cette loi,  $\mathcal{S}(A)$  est un groupe non abélien.  
Pour  $A = \{1, 2, \dots, n\}$ .  
 $\mathcal{S}(A)$  est noté simplement  $S_n$  et est appelé groupe des permutations de  $n$  éléments  $\text{Card}(\mathcal{S}_n) = n!$
5.  $\mathcal{P}(\mathcal{A})$  avec la différence symétrique  $\Delta$  est un groupe abélien fini.
6. Le produit cartésien de deux groupes  $(E, *)$  et  $(F, \bullet)$  est un groupe avec la loi cartésienne  $\top$  :

$$(e, f) \top (e', f') = (e * e', f \bullet f').$$

En particulier  $E^2$ , est un groupe avec la loi cartésienne notée encore  $*$

$$(a, a') * (b, b') = (a * b, a' * b')$$

Plus généralement  $E^n$  est un groupe avec la loi cartésienne  $*$

$$(x_1, \dots, x_n) * (y_1, \dots, y_n) = (x_1 * y_1, \dots, x_n * y_n).$$

Exemple :  $\mathbb{R}^2, \mathbb{R}^3, \dots, \mathbb{R}^n$  sont des groupes abéliens avec la loi cartésienne  $+$ .

## 2.2 Sous-groupes d'un groupe

Soient  $(G, *)$  un groupe, d'élément neutre  $e$  et  $H$  une partie de  $G$ . On dit que  $H$  est un sous-groupe de  $(G, *)$  si les 3 propriétés suivantes sont vérifiées :

- i)  $e \in H$
- ii)  $\forall (x, y) \in H^2, x * y \in H$
- iii)  $\forall x \in H, x^{-1} \in H$

### Exemples

- $G$  lui-même et  $\{e\}$  sont des sous-groupes de  $(G, *)$ . Ces deux sous-groupes sont dits triviaux.
- $\mathbb{Z}$  est un sous groupe de  $(\mathbb{Q}, +)$
- $\mathbb{Q}$  est un sous groupe de  $(\mathbb{R}, +)$
- $\mathbb{R}$  est un sous groupe de  $(\mathbb{C}, +)$
- $\mathbb{R}_+^*, \{-1, 1\}$  sont des sous-groupes de  $(\mathbb{R}^*, \times)$
- $U_n = \{z \in \mathbb{C} : z^n = 1\}$  est un sous-groupe de  $n$  éléments de  $(\mathbb{C}^*, \times)$
- Pour tout  $a \in \mathbb{Z}$ , l'ensemble des multiples de  $a$ , noté  $a\mathbb{Z}$  est un sous groupe de  $(\mathbb{Z}, +)$ .
- Plus généralement, si  $(G, *)$  est un groupe et  $g \in G$ , alors l'ensemble des puissances de  $a : \{g^n, n \in \mathbb{Z}\}$  est un sous-groupe de  $(G, *)$ .

$$a^0 = e, a^{-2} = (a^{-1})^{-2}, a^{-3} = (a^{-1})^3$$

### Remarques :

1. Un sous-groupe  $H$  n'est pas vide.
2. Si  $H$  est un sous-groupe de  $(G, *)$  alors  $H$  est stable pour la loi  $*$  et  $*$  induit une loi de composition interne sur  $H$ .  $H$  muni de cette loi est un groupe d'où la terminologie "sous – groupe"
3. Très souvent pour montrer qu'un ensemble muni d'une loi de composition interne (l.c.i) est un groupe, on essaie de voir cet ensemble comme un sous-groupe d'un ensemble plus grands.

**Théorème 1 : (Caractérisation des sous-groupes de  $(\mathbb{Z}, +)$ )** Soit  $H$  un sous-groupe de  $(\mathbb{Z}, +)$ . Alors il existe  $a \in \mathbb{N}$  tel que  $H = a\mathbb{Z}$

**Preuve :** A faire en exo

**Corollaire 2 : (Egalité de Bézout)**

a) Soient  $a, b \in \mathbb{Z}$  et  $d = \text{pgcd}(a, b)$ . Alors

$$\exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = d \quad (d > 0)$$

b)  $a$  et  $b$  deux entiers sont premiers entre eux

$$\iff \exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1$$

**Preuve :**

a) On considère l'ensemble  $\{am + bn, (m, n) \in \mathbb{Z}^2\}$  qu'on note  $a\mathbb{Z} + b\mathbb{Z}$ .

Il est clair que  $a\mathbb{Z} + b\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ , donc  $\exists c \in \mathbb{N}$  tel que

$$a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$$

Par ailleurs,  $a\mathbb{Z} \subset d\mathbb{Z}$  et  $b\mathbb{Z} \subset d\mathbb{Z}$  donc  $c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$ . En particulier  $c$  est un multiple de  $d$  et  $(c \geq d)$ .

L'égalité  $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$  montre que  $c$  divise à la fois  $a$  et  $b$ , donc  $\text{pgcd}(a, b) = d \geq c$  finalement on a  $c = d$ .

b)  $\Rightarrow$ ) est clair

$\Leftarrow$ ) si  $au + bv = 1$ , alors tout diviseur de  $a$  et  $b$  divise  $au + bv$ , donc divise 1.

### 2.2.1 Intersection et sous-groupes d'un même groupe

Soient  $H_1$  et  $H_2$  deux sous-groupes d'un même groupe  $(G, *)$ ;  $H_1 \cap H_2$  est un sous groupe de  $(G, *)$  Plus généralement, si  $\{H_i\}_{i \in I}$  est une famille de sous-groupes d'un même groupe  $(G, *)$ , alors  $\bigcap_{i \in I} H_i$  est un sous groupe de  $(G, *)$ .

Soit  $A$  une partie de  $G$ . On appelle sous groupe engendré par  $A$  l'intersection de tous les sous-groupes de  $G$  contenant  $A$ . Ce sous-groupe est le plus petit (au sens de l'inclusion) sous-groupe de  $(G, *)$  contenant  $A$ .

Exemples : si  $A = \emptyset$ ,  $\langle \emptyset \rangle = \{e\}$ ;  $A = \{x\}$ ,  $\langle x \rangle = \{x^n, n \in \mathbb{Z}\}$ .

### 2.2.2 Réunions de sous-groupes

La réunion de deux sous-groupes d'un même groupe  $G$  n'est pas un sous groupe (en général). Par exemple  $2\mathbb{Z} \cup 3\mathbb{Z}$  n'est pas un sous groupe de  $\mathbb{Z}$

## 2.3 Classes d'équivalence suivant un sous-groupe

Soient  $(G, *)$  un groupe d'élément neutre  $e$  et  $H$  un sous-groupe de  $(G, *)$ .  $H$  permet de définir sur  $G$  la relation binaire  $\mathcal{R}_H$  suivant :

$$\text{pour tout } (x, y) \in G^2, \quad x \mathcal{R}_H y \text{ si } x^{-1} * y \in H$$

On a le théorème suivant :

**Théorème 3 (de Lagrange)**

- i)  $\mathcal{R}_H$  est une relation d'équivalence.
- ii) La classe d'équivalence d'un point  $a \in G$  est  $\bar{a} = \{a * h, h \in H\}$  qu'on note  $a * H$ .
- iii) Il y a une bijection entre  $\bar{e} = H$  et  $\bar{a} = a * H$ .
- iv) Si  $G$  est un groupe fini, on a

$$\text{Card}(G) = \text{Card}(H) \cdot \text{Card}\left(\frac{G}{\mathcal{R}_H}\right)$$

**Preuve :**

- i) à faire en exercice
- ii)  $a^{-1} * (a * h) = h \in H$ , donc  $(a * h)\mathcal{R}a$
- iii)  $\varphi : H \longrightarrow aH, h \longmapsto a * h$  est une application bijective.
- iv) Comme  $G$  est fini, l'ensemble des classes d'équivalence est aussi fini on a

$$G = H \cup (x_1 * H) \cup (x_2 * H) \cup \dots \cup (x_k * H)$$

d'où  $\text{Card}(G) = \text{Card}(H) + \text{Card}(x_1 * H) + \dots + \text{Card}(x_k * H)$ . Comme  $\text{Card}(x_i * H) = \text{Card}(H)$  on a  $\text{Card}(G) = \text{Card}(H) \cdot \text{Card}\left(\frac{G}{\mathcal{R}_H}\right)$

**Remarque**  $H$  Permet de définir une autre relation binaire  $\mathcal{R}'_H$  sur  $G$  par :

$$x\mathcal{R}'_Hy \quad \text{si } x * h^{-1} \in H$$

$\mathcal{R}'_H$  a toutes les propriétés dans le théorème de lagrange, sauf que la classe d'équivalence de  $a \in G$  est  $H * a = \{h * a, h \in H\}$ .

Très souvent, on a  $a * H \neq H * a$

### 2.3.1 Sous-groupes distingués dans $(G, *)$

Un sous-groupe  $H$  de  $(G, *)$  est dit distingué dans  $G$  si on a :

$$\forall x \in G, \forall h \in H, \text{ on a } x * h * x^{-1} \in H$$

**Par exemple**

- 1)  $\{e\}$  et  $G$  les deux sous groupes triviaux sont distingués.
- 2) Tout sous-groupe d'un groupe abélien est distingué.

**Théoreme :** Soient  $(G, *)$  et  $(F, \bullet)$  deux groupes d'éléments neutre  $e$  et  $\epsilon$ , et  $f : G \longrightarrow F$  un homomorphisme (de groupe). Alors

- $f^{-1}(\{\epsilon\})$  est un sous-groupe distingué de  $(G, *)$
- $\text{Im}f$  est un sous-groupe de  $(F, \bullet)$ .

**Preuve :** Comme  $e * e = e$ , On a  $f(e) \bullet f(e) = f(e)$  d'où

$f(e) = \epsilon$  c'est à dire  $e \in f^{-1}(\{\epsilon\})$ .

Si  $a, b \in f^{-1}(\{\epsilon\})$  alors  $f(a * b) = f(a) \bullet f(b) = \epsilon \bullet \epsilon = \epsilon$  alors  $a * b \in f^{-1}(\epsilon)$ .

Comme  $x * x^{-1} = e = x^{-1} * x$ ,  $f(x) \bullet f(x^{-1}) = \epsilon = f(x^{-1}) \bullet f(x)$  d'où

$$f(x^{-1}) = (f(x))^{-1}$$

si donc  $a \in \ker f = f^{-1}(\{\epsilon\})$  on a  $(a^{-1}) = (f(a))^{-1} = \epsilon^{-1} = \epsilon$

d'où  $a^{-1} \in f^{-1}(\{\epsilon\})$ .

## 2.4 Groupe quotient

**Proposition 5 :**

a)  $\mathcal{R}_H = \mathcal{R}'_H$

b)  $\mathcal{R}_H$  est compatible avec la loi  $*$  c'est à dire si  $a\mathcal{R}_H b$  et  $x\mathcal{R}_H y$ , alors  $(a * x)\mathcal{R}_H(b * y)$

**Preuve :**

a) Il faut montrer que  $a\mathcal{R}_H b \iff a\mathcal{R}'_H b$

Soit  $(a, b) \in G^2$  tel que  $a\mathcal{R}_H b$ .

Alors  $a^{-1} * b \in H$ . Comme  $H$  est distingué dans  $G$ ,  $a * (a^{-1} * b) * a^{-1} \in H$ . c'est à dire  $b * a^{-1} \in H$ , donc  $b\mathcal{R}'_H a$  et  $a\mathcal{R}'_H b$  (puisque  $\mathcal{R}'_H$  est symétrique)

○ Réciproquement, si  $a\mathcal{R}'_H b$ , alors  $a * b^{-1} \in H$ ,  $H$  étant distingué dans  $G$ , on  $b^{-1}(a * b^{-1}) * b \in H$ , donc  $b^{-1} * a \in H$  et  $a\mathcal{R}_H b$ .

b) Soient  $(a, b) \in G^2$ ,  $(x, y) \in G^2$  tels que  $a\mathcal{R}_H b$  et  $x\mathcal{R}_H y$ . on a :

$$(a * x)^{-1} * (b * y) = x^{-1} * (a^{-1} * b) * y$$

$$(a * x)^{-1} * (b * y) = (x^{-1} * (a^{-1} * b) * x) * (x^{-1} * y) \in H$$

**Notation :** Si  $H$  est distingué, l'ensemble quotient  $\frac{G}{\mathcal{R}_H}$  est noté  $\frac{G}{H}$ .

**Proposition 6 :** La loi  $*$  induit une loi de composition interne sur  $\frac{G}{H}$  par

$$(a, b) \longmapsto a * b$$

$\frac{G}{H}$  muni de cette loi (encore notée  $*$ ) est un groupe. (appelé groupe quotient).

**Exemple :**  $G = \mathbb{Z}$  avec l'addition  $+$  et  $H = 4\mathbb{Z}$

$\frac{\mathbb{Z}}{4\mathbb{Z}}$  est un groupe avec l'addition  $\bar{a} + \bar{b} = \overline{a + b}$

Ecrire la table de  $+$  de  $\frac{\mathbb{Z}}{4\mathbb{Z}}$



# Chapitre 3

## Anneaux

### 3.1 Définitions et exemples

On appelle anneau un ensemble  $A$  non vide muni de deux lois de composition interne, une addition  $(x, y) \mapsto x + y$  et une multiplication  $(x, y) \mapsto x \cdot y$  telles que :

- i) L'addition définit sur  $A$  une structure de groupe abélien.  
 $(A, +)$  est un groupe abélien.
- ii) La multiplication est associative

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall (a, b, c) \in A^3$$

- iii) La multiplication est distributive à gauche et à droite par rapport à l'addition

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (y + z) \cdot x &= y \cdot x + z \cdot x \end{aligned} \quad \forall (a, b, c) \in A^3$$

- Si de plus la multiplication est commutative, on dit que  $A$  est un anneau commutatif.
- L'anneau  $A$  est dit unitaire si la multiplication admet un élément neutre.

#### Notations

- L'élément neutre de  $+$  de  $A$  est noté  $0_A$  et pour tout  $x \in A$ , le symétrique de  $x$  par rapport à la loi  $+$  est noté  $-x$ .  
(on dit que  $-x$  est l'opposé de  $x$ )
- Si l'anneau  $A$  est unitaire, l'élément neutre de la multiplication "  $\cdot$  " dans  $A$  est noté  $1_A$ .  
Un élément  $x \in A$  sera dit inversible, s'il admet un symétrique par rapport à la multiplication, dans ce cas le symétrique de  $x$  est noté  $x^{-1}$ .  
On note  $\mathcal{U}(A)$  l'ensemble de tous les éléments inversibles de  $A$ .  $\mathcal{U}(A)$  est stable pour la multiplication et  $(\mathcal{U}(A), \cdot)$  est un groupe.
- Pour tout  $a \in A$ , et pour tout  $n \in \mathbb{N}^*$  on pose :

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ fois}} \quad \text{et} \quad na = \underbrace{a + a + \dots + a}_{n \text{ fois}}$$

**Exemples**

1.  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , munis de l'addition  $+$  et de la multiplication  $\cdot$  sont des anneaux commutatifs et unitaires.

2. Soit  $(G, +)$  un groupe abélien.

Une application  $f : G \rightarrow G$  est dite endomorphisme si :

$$f(x + x') = f(x) + f(x')$$

Par exemple  $Id_G$  est endomorphisme de  $G$ . On note  $End(G)$  l'ensemble de tous les endomorphismes de  $G$ .

Si  $f, g \in End(G)$ , alors  $f + g : x \mapsto f(x) + g(x)$  appartient à  $End(G)$ , et  $f \circ g \in End(G)$ .

Muni de ces deux lois de composition internes,  $(End(G), +, \circ)$  est un anneau unitaire non commutatif.

3. On appelle matrice carrée d'ordre 2 à coefficients dans  $\mathbb{R}$  tout tableau de la forme

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

On note  $\mathcal{M}_2(\mathbb{R})$  l'ensemble des matrices carrées d'ordre 2 à coefficients dans  $\mathbb{R}$

On pose :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' + b \cdot c' & a \cdot b' + b \cdot d' \\ c \cdot a' + d \cdot c' & c \cdot b' + d \cdot d' \end{pmatrix}$$

Montrer que  $(\mathcal{M}_2(\mathbb{R}), +, \bullet)$  est un anneau unitaire non commutatif.

4. Si  $A$  et  $A'$  sont 2 anneaux, il y a sur  $A \times A'$  une structure naturelle d'anneau

$$\begin{cases} (a, a') + (b, b') = (a + b, a' + b') \\ (a, a') \cdot (b, b') = (a \cdot b, a' \cdot b') \end{cases}$$

En particulier  $\mathbb{Z}^2, \mathbb{Z}^3, \mathbb{Z}^n, \dots, \mathbb{C}^2, \mathbb{C}^3, \dots$  sont des anneaux

5. Si  $A$  est un anneau et  $X$  est un ensemble quelconque non vide ;  
L'ensemble de toutes les applications  $f : X \rightarrow A$  noté  $A^X$  est un anneau avec les lois suivantes :

$$f, g \in A^X, \quad \begin{aligned} f + g : x &\mapsto f(x) + g(x) \\ f \cdot g : x &\mapsto f(x) \cdot g(x) \end{aligned}$$

**Propriétés remarquables dans l'anneau**

i)  $0_A \cdot x = 0_A, x \cdot 0_A = 0_A$  pour tout  $x \in A$

ii)  $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$  pour tout  $x, y \in A$

iii) Si  $A$  est un anneau unitaire, on a  $(-1_A) \cdot x = -x$

iv) Si  $x$  et  $y$  commutent (par rapport à " $\cdot$ ") c'est à dire  $x \cdot y = y \cdot x$  alors

$$(x \cdot y)^2 = x^2 y^2, (x \cdot y)^3, \dots, (x \cdot y)^n = x^n \cdot y^n \quad \forall n \in \mathbb{N}^*$$

$$(x + y)^2 = x^2 + 2(xy) + y^2$$



$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

Plus généralement

$$(x + y)^n = x^n + C_n^1 xy^{n-1} + C_n^2 x^2 y^{n-2} + \dots + C_n^k x^k y^{n-k} + \dots + C_n^{n-1} x^{n-1} y + y^n$$

**Exercice :** Calculer  $(1_A + a)^6$

### Définitions

- Un anneau  $A$  est dit intègre, si la partie  $A \setminus \{0_A\}$  est stable pour le produit.

Par exemple :  $(\mathbb{Z}, +, \bullet)$  est intègre,  $\mathcal{M}_2(\mathbb{R})$  n'est pas intègre.

- un anneau unitaire  $A$  est appelé corps, si  $\mathcal{U}(A)$ , l'ensemble des éléments inversibles de  $A$  est égal à  $A \setminus \{0\}$ .

$$\mathcal{U}(A) = A \setminus \{0\}$$

exemples :  $\mathbb{R}, \mathbb{C}, \mathbb{Q}$  sont des corps.

## 3.2 Sous-anneaux, Idéaux

Soient  $A$  un anneau commutatif unitaire et  $B$  une partie de  $A$ .

- On dit que  $B$  est un sous-anneau de  $A$  si :

- $B$  est un sous-groupe de  $(A, +)$
- $B$  contient  $1_A$  et  $B$  est stable par le produit  $\forall b, b' \in B, bb' \in B$

Par exemple :

- $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Q}$
- $\mathbb{R}$  est un sous-anneau de  $\mathbb{C}$
- $\mathbb{Q}$  est un sous-anneau de  $\mathbb{R}$

**Remarque :** L'intersection de sous-anneaux d'un même anneau est un sous-anneau.

- On dit que  $B$  est un idéal de  $A$  si

- $B$  est un sous-groupe de  $(A, +)$
- $\forall a \in A, \forall b \in B, on a ab \in B$

### Exemples

- $\{0_A\}, A$  sont des idéaux de  $A$  (dits triviaux)
- $aA$  l'ensemble des multiples de  $a$  dans  $A$  est un idéal (dit principal).
- Les idéaux de l'anneau  $\mathbb{Z}$  sont de la forme  $n\mathbb{Z}$ , où  $n \in \mathbb{N}$
- l'intersection d'idéaux d'un même anneau est un idéal
- la réunion d'idéaux est pas un idéal en général.

### 3.3 Anneaux quotients

**Proposition: 1.** Si  $I$  est un idéal de  $A$ , alors les lois " + " et " · " sont compatibles avec la relation d'équivalences (de Lagrange)

$$a \mathcal{R} b \text{ si } b - a \in I$$

**Proposition: 2.** L'ensemble quotient  $\frac{A}{I}$  muni des lois de composition internes

$$\bar{a} + \bar{b} = \overline{a + b}$$

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

est un anneau commutatif unitaire

**Exercice**

- Ecrire la tables de l'addition et de la multiplicattion de l'anneau quotient  $\frac{\mathbb{Z}}{6\mathbb{Z}}$ .
- Trouver  $\mathcal{U}(A)$

### 3.4 L'anneau quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Soit  $n \in \mathbb{N}^*$ . On considère l'anneau quotient  $\frac{\mathbb{Z}}{n\mathbb{Z}}$

**Lemme :** (La division euclidienne dans  $\mathbb{Z}$ )

Soient  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(s, r) \in \mathbb{Z} \times \mathbb{N}$  tel que

- $0 \leq r < b$
- $a = sb + r$

**Corollaire** L'anneau  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  a exeactement  $n$  éléments :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

**Preuve :** Soit  $a \in \mathbb{Z}$  la division euclidienne de  $a$  par  $n$  s'écrit :  $a = sn + r$  avec  $r \in \{0, 1, \dots, n-1\}$

On a  $a - r = s \cdot n \in n\mathbb{Z}$ , donc  $a \mathcal{R} r$  et  $\bar{a} = \bar{r}$

par ailleurs, si  $i \neq j$  et  $i, j \in \{0, 1, \dots, n-1\}$  on a  $\bar{i} \neq \bar{j}$  car  $0 \neq |i - j|$  et  $|i - j| < n$  donc  $j - i \notin n\mathbb{Z}$

**Proposition: 3.** – L'anneau  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  est un commutatif unitaire, d'élément unité  $\bar{1}$

- un élément  $\bar{a}$  de  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  est inversible si et seulement si  $\text{pgcd}(a, n) = 1$
- l'anneau  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  est un corps si et seulement si  $n$  est premier.

preuve

- $\bar{a}$  est inversible  $\Leftrightarrow \exists \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$  tel que  $\bar{b} = \bar{1}$ 
  - $\Leftrightarrow \exists b \in \mathbb{Z} : \bar{a}b = 1$
  - $\Leftrightarrow \exists b \in \mathbb{Z}, \exists k \in \mathbb{Z} : ab - kn = 1$
  - $\Leftrightarrow \text{pgcd}(a, b) = 1$  (Théorème de Bezout)
- $\frac{\mathbb{Z}}{n\mathbb{Z}}$  est un corps  $\Leftrightarrow \mathcal{U}(\frac{\mathbb{Z}}{n\mathbb{Z}}) = \frac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\bar{0}\}$ 
  - $\Leftrightarrow \bar{1}, \bar{2}, \dots, \overline{n-1}$  sont inversibles
  - $\Leftrightarrow 1, 2, \dots, n-1$  sont tous premiers avec  $n$
  - $\Leftrightarrow n$  n'a pas de diviseur premier autre que 1 et  $n$

### 3.5 Homomorphisme d'anneaux

Soient  $A$  et  $B$  deux anneaux unitaires et  $f : A \longrightarrow B$  une application. On dit que  $f$  est un homomorphisme d'anneau si :

- i)  $f(a + a') = f(a) + f(a')$
- ii)  $f(a \cdot a') = f(a) \cdot f(a')$
- iii)  $f(1_A) = 1_B$
- On note qu'un morphisme d'anneaux est un homomorphisme de groupes.
- si  $f$  est un homomorphisme d'anneaux, on appelle noyau de  $f$  et on le note  $\ker f$  l'ensemble

$$\ker f = \{a \in A : f(a) = 0_B\}$$

Exemples

1.  $\text{id}_A : A \longrightarrow A$  est un homomorphisme
2. Si  $I$  est un idéal de l'anneau  $A$ , la surjection canonique  $\pi : A \longrightarrow \frac{A}{I}$  est un homomorphisme.
3. L'application constante  $\mathcal{C} : A \longrightarrow B, x \longmapsto 0_B$  n'est pas un homomorphisme, car la troisième condition (iii) n'est pas vérifiée.

**Théorème 6 : (Chinois)** Soient  $p$  et  $q$  deux entiers premiers entre eux.

Alors l'homomorphisme  $\varphi : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}} ; n \longmapsto (\bar{n}, \bar{n})$  est surjectif.

**Preuve :** Comme  $\text{pgcd}(p, q) = 1$ , par Bézout il existe  $(a, b) \in \mathbb{Z}^2$  tel que

$$ap + bq = 1$$

On vérifie que  $\varphi(bx + ay) = (\bar{x}, \bar{y})$ , pour tout  $(\bar{x}, \bar{y}) \in \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$ .

**Exercice** Soit  $f : A \longrightarrow B$  un homomorphisme d'anneaux

- a) Montrer que  $f(0_A) = 0_B$
- b) Montrer que  $\ker f$  est un idéal de  $A$ ,  $\text{Im} f$  est un sous anneau de  $B$
- c) Montrer que la relation d'équivalence de Lagrange définie par  $\ker f$  est la même que celle définie par les images de  $f$ .
- d) Montrer que l'anneau quotient  $\frac{A}{\ker f}$  est isomorphe à  $\text{Im} f$

# Chapitre 4

## Polynômes et fractions rationnelles à une variable

### 4.1 Polynômes à une variable

#### 4.1.1 Définitions

Un polynôme à une variable  $X$ , à coefficients dans un anneau  $A$ , s'écrit formellement :

$$a_0 + a_1X + \cdots + a_nX^n \quad \text{où } n \in \mathbb{N}, a_i \in A$$

- $a_0$  est appelé terme constant du polynôme
- $X$  est aussi appelé l'indéterminée.
- $a_iX^i$  est appelé monôme de degré  $i$  et de coefficient  $a_i$ .

Soit

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

- Si  $\{i : a_i \neq 0_A\} \neq \emptyset$ , on appelle degré de  $P(X)$  et on note  $\deg(P(X))$  l'entier :

$$\max\{i : a_i \neq 0_A\}$$

- Si  $\{i : a_i \neq 0_A\} \neq \emptyset$ , on appelle valuation de  $P(X)$  et on note  $\text{val}(P(X))$  l'entier :

$$\min\{i : a_i \neq 0_A\}$$

Par exemple :

si  $P(X) = 2X + 0X^2 + 3X^4 + 8X^5 + 0X^6$

alors  $\deg(P(X)) = 5$  et  $\text{val}(P(X)) = 1$ .

On convient que

$$\deg(0 + 0X + \cdots + 0X^n) = -\infty$$

$$\text{val}(0 + 0X + \cdots + 0X^n) = +\infty$$

Seul  $0 + 0X + \cdots + 0X^n$  est de degré  $-\infty$  (seul polynôme de degré strictement négatif) et de valuation  $+\infty$

Egalité de deux polynômes

Deux polynômes  $P(X) = \sum_{i=0}^n a_i X^i$ ,  $Q(X) = \sum_{i=0}^m b_i X^i$  sont égaux si

$$\deg(P(X)) = \deg(Q(X)) \text{ et } a_i = b_i \quad \forall 0 \leq i \leq \deg(Q(X))$$

**Notation :** On note  $A[X]$  l'ensemble de tous les polynômes en  $X$  à coefficients dans l'anneau  $(A, +, \cdot)$ .

**4.1.2 Additions et multiplication dans  $A[X]$** 

**Addition** .

$$\sum_{i=0}^n a_i X^i + \sum_{i=0}^m b_i X^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i$$

où  $a_i + b_i$  est défini dans l'anneau  $A$ . La convention que  $a_i = 0_A$  si  $i > n$  et  $b_i = 0_A$  si  $i > m$ .

On voit alors que  $(A[X], +)$  est un groupe abélien d'élément neutre, le polynôme  $0 + 0X + \cdots + 0X^n$  (polynôme nul).

**La multiplication** .

$$\left(\sum_{i=0}^n a_i X^i\right) \bullet \left(\sum_{i=0}^m b_i X^i\right) = \sum_{k=0}^{n+m} (c_k) X^k$$

où  $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k$ .

**Proposition 1**

1.  $(A[X], +, \bullet)$  est un anneau unitaire. Si  $A$  est commutatif, alors  $A[X]$  aussi.
2. Si  $A$  est un anneau intègre, alors  $A[X]$  est aussi intègre.  
On a pour tout  $(P, Q) \in (A[X])^2$ ,
  - $\deg(P \bullet Q) = \deg(P) + \deg(Q)$  ;  $\text{val}(P \bullet Q) = \text{val}(P) + \text{val}(Q)$ .
  - $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$  ;  $\text{val}(P + Q) \geq \min(\text{val}(P), \text{val}(Q))$ .

**Exemple de calcul dans  $A[X]$**

$$(1 + X + 2X^3)(X + X^3) =$$

$$(1 - X)(1 + X + X^2) =$$

**Remarque :** Si  $A$  est un anneau intègre, l'anneau  $A[X]$  est intègre et un polynôme non constant  $P(X)$  n'est pas inversible.

### 4.1.3 Division euclidienne et division suivant les puissances croissantes)

Dès maintenant, on suppose que  $A = K$  est un corps commutatif.

**Proposition 2 : (Division euclidienne)** .

Soient  $P$  et  $Q$  deux polynômes de  $K[X]$  tels que  $Q \neq 0$ . Il existe un unique couple de polynômes  $(S, R)$  tel que :

$$\deg(R) < \deg(Q) \quad \text{et} \quad P = SQ + R \quad (*)$$

preuve :

- La formule précédente  $(*)$  est appelée division euclidienne de  $P$  par  $Q$ .
- $S$  et  $R$  sont respectivement appelés quotient et reste de la division euclidienne de  $P$  par  $Q$ .
- Si  $R = 0$ , on dit que  $Q$  divise  $P$  ou que  $P$  est un multiple de  $Q$  (dans  $A[X]$ ). On a  $P = SQ$ .

**Exemples :** Effectuer la division euclidienne de  $X^3 - 1$  par  $1 + X + X^2$  et

$$X^4 + 4X^3 - X^2 - X + 8 \text{ par } X^2 - X + 1$$

**Proposition 3 : (Division suivant les puissances croissantes)** . Soient  $P$ ,  $Q$  deux polynômes de  $K[X]$  tels que  $\text{val}(Q) = 0$  et  $n \in \mathbb{N}$ . Il existe un unique couple de polynômes  $(S, R)$  tel que :

$$\deg(Q) < n \quad \text{et} \quad P = SQ + X^n R \quad (**)$$

### 4.1.4 Polynômes irréductibles

Un polynôme non constant  $P$  est dit irréductible s'il n'a pas de diviseur propre, c'est à dire un diviseur  $Q$  tel que  $1 \leq \deg(Q) < \deg(P)$ . Par exemple, tout polynôme de degré 1 est irréductible.

**Proposition 4** Dans l'anneau  $K[X]$ , tout polynôme non constant  $P(X)$  s'écrit de façon unique comme un produit fini de polynômes irréductibles

$$P = P_1 \cdot P_2 \cdots P_r$$

où  $P_i$  irréductible.

- les  $P_i$  sont les facteurs irréductibles de  $P$ .
- On peut parler de pgcd et de ppcm d'un couple de polynômes  $(P, Q)$ .
- Le calcul de  $\text{pgcd}(P, Q)$  se fait avec l'algorithme d'euclide.
- Dans  $\mathbb{C}[X]$  tout polynôme s'écrit  $\lambda(\lambda - \alpha_1)^{m_1} \cdots (\lambda - \alpha_p)^{m_p}$

### 4.1.5 Racines d'un polynôme

Soit

$$P(X) = a_0 + a_1X + \cdots + a_nX^n \in k[X]$$

On dit que  $\alpha \in K$  est racine de  $P(X)$  si :

$$P(\alpha) = a_0 + a_1\alpha + \cdots + a_n(\alpha)^n = 0_K$$

**Lemme 5 :**  $\alpha \in K$  est racine de  $P(X)$  ssi  $X - \alpha$  divise  $P(X)$ .

**Preuve :**  $P(X) = (X - \alpha)S(X) + \alpha$

### 4.1.6 Dérivée formelle d'un polynôme et racines multiples

On appelle dérivée formelle d'un polynôme

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

le polynôme

$$P'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

On retrouve les propriétés classiques de la dérivation :

$$(P(X) + Q(X))' = P'(X) + Q'(X)$$

$$(\lambda P(X))' = \lambda P'(X)$$

$$(P(X)Q(X))' = P'(X)Q(X) + P(X)Q'(X)$$

$\alpha \in K$  est dit racine d'ordre  $m \in \mathbb{N}^*$  de  $P(X)$  si :

$$P(\alpha) = 0, P'(\alpha) = 0, \dots, P^{(m-1)}(\alpha) = 0, P^{(m)}(\alpha) \neq 0$$

$P^{(i)}(X)$  étant la  $i$ -ème dérivée formelle successive de  $P(X)$ .

**Proposition 6 :**  $\alpha \in K$  est une racine d'ordre  $m$  de  $P(X)$  ssi  $(X - \alpha)^m$  divise  $P(X)$  et  $(X - \alpha)^{m+1}$  ne divise pas  $P(X)$ .

**Remarque :** Si  $\alpha$  est une racine d'ordre  $m$  de  $P(X)$  et  $\beta$  est une autre racine d'ordre  $p$  de  $P(X)$  alors  $(X - \alpha)^m(X - \beta)^p$  divise  $P(X)$

### 4.1.7 Polynômes scindés de $K[X]$

Un polynôme  $P(X) = a_0 + a_1X + \cdots + a_nX^n \in k[X]$  de degré  $n$  (c-a-d  $a_n \neq 0$ ) est dit scindé, s'il existe  $(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n$  tel que

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

Par exemple, tout polynôme de  $\mathbb{C}[X]$  est scindé, alors que dans  $\mathbb{R}[X]$  il y a des polynômes non scindés ( $X^3 + X$ ).



Si  $P(X)$  est scindé, ses coefficients et ses racines sont liés par les  $n$  relations suivantes.

$$\left\{ \begin{array}{rcl} -a_n(\alpha_1 + \alpha_2 + \cdots + \alpha_n) & = & a_{n-1} \\ +a_n(\alpha_1\alpha_2 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n) & = & a_{n-2} \\ & \vdots & \\ (-1)^k a_n(\alpha_1\alpha_2 \cdots \alpha_k + \cdots + \alpha_{n-1}\alpha_{n-k+1} \cdots \alpha_n) & = & a_{n-k} \\ & & \\ (-1)^n a_n \alpha_1 \alpha_2 \cdots \alpha_n & = & 0 \end{array} \right.$$

(Somme de tous les produits de  $k$  racines d'indices distincts, il y en a  $\mathcal{C}_n^k$  exactement).

Exemple pour  $n = 4$

$$\left\{ \begin{array}{rcl} -a_4(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) & = & a_3 \\ +a_4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) & = & a_2 \\ -a_4(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) & = & a_1 \\ +a_4\alpha_1\alpha_2\alpha_3\alpha_4 & = & a_0 \end{array} \right.$$

.

**Thérème 7 : (de D'Alambert-Gauss)** Tout polynôme non-constant  $P(X)$  de  $\mathbb{C}[X]$  admet au moins une racine dans  $\mathbb{C}$ . En particulier, tous les polynômes de  $\mathbb{C}[X]$  non-constants sont scindés.

#### 4.1.8 Les polynômes de $\mathbb{R}[X]$

Soit

$$P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$$

**Lemme 8 :** Si  $z_0 \in \mathbb{C}$  est racine de  $P(X)$ , alors le conjugué  $\bar{z}_0$  est aussi racine de  $P(X)$ . En particulier  $(X^2 - 2\text{Re}(z_0)X + |z_0|^2)$  divise  $P(X)$ .

**Corollaire 8 :** Les polynômes irréductibles de  $\mathbb{R}[X]$  sont soit du 1<sup>er</sup> degré soit du second degré  $aX^2 + bX + c$  avec  $b^2 - 4ac < 0$ .

## 4.2 Fractions rationnelles à une variable

$K$  sera un corps commutatif dans toute la suite .

### 4.2.1 Définition

Une fraction rationnelle à une variable  $X$ , est un quotient de polynômes en  $X$ , elle s'écrit sous la forme  $\frac{P(X)}{Q(X)}$ , où  $P(X) \in K[X]$  et  $Q(X) \in K[X] \setminus \{0\}$ .

Deux fractions rationnelles  $\frac{P(X)}{Q(X)}$  et  $\frac{S(X)}{R(X)}$  sont égales si on a l'égalité

$$P(X)R(X) = S(X)Q(X) \text{ dans l'anneau } K[X].$$

En particulier si

$$H(X) \neq 0, \quad \frac{P(X)}{Q(X)} = \frac{P(X)H(X)}{Q(X)H(X)}$$

On note  $K(X)$  l'ensemble des fractions rationnelles.

On identifie un polynôme  $P(X)$  à la fraction rationnelle  $\frac{P(X)}{1}$ , on a ainsi l'inclusion  $K[X] \subsetneq K(X)$ . On pose :

$$\deg\left(\frac{P(X)}{Q(X)}\right) = \deg P(X) - \deg Q(X)$$

### 4.2.2 L'addition et la multiplication dans $K(X)$

**L'addition** Soient  $\frac{P}{Q}, \frac{S}{R} \in K(X)$ . On pose

$$\frac{P}{Q} + \frac{S}{R} = \frac{PR + QS}{QR}$$

**La multiplication** On pose

$$\frac{P}{Q} \cdot \frac{S}{R} = \frac{PS}{QR}$$

On a les résultats suivants :

**propositions** Avec cette addition et cette multiplication,  $K(X)$  est un corps et  $K[X]$  est un anneau de  $K(X)$ .

**propositions** Soient  $\frac{P}{Q}, \frac{R}{S} \in K(X)$  on a :

$$\begin{aligned} i) \quad \deg\left(\frac{P}{Q} \cdot \frac{R}{S}\right) &= \deg\frac{P}{Q} + \deg\frac{R}{S} \\ ii) \quad \deg\left(\frac{P}{Q} + \frac{R}{S}\right) &\leq \max\left(\deg\left(\frac{P}{Q}\right), \deg\left(\frac{R}{S}\right)\right) \end{aligned}$$

### 4.2.3 Décomposition en éléments simples d'une fraction rationnelle

**propositions** [Partie entière d'une fraction rationnelle]

Soit  $\frac{P}{Q} \in K(X)$ .

Il existe un unique polynôme  $E(X)$  et une unique fraction rationnelle  $\frac{R}{S}$  tels que :

$$\deg\left(\frac{R}{S}\right) < 0 \text{ et } \frac{P}{Q} = E(X) + \frac{R}{S}$$

**Preuve**

$$P = E.Q + R \text{ avec } \deg(K) < \deg Q \implies \frac{P}{Q} = E(X) + \frac{R}{Q}$$

$E(X)$  est appelé partie entière de  $\frac{P}{Q}$

**Exemples :**

$$\frac{X^2}{X+1} = X - 1 + \frac{1}{X+1}, \quad \frac{2X^5}{3X^5+X} = \frac{2}{3} - \frac{X}{X+1}, \quad \frac{X^3}{X^4+1} = 0 + \frac{x^3}{X^4+1}$$

**Théorème** Soit  $\frac{P}{Q}$  où  $Q = \lambda(X - \alpha)^n(X - \beta)^m \cdots (X - \gamma)^p$  Alors  $\frac{P}{Q}$  s'écrit de façon unique comme somme de sa partie entière et de fractions à degré strictement négatif comme suit :

$$\begin{aligned} \frac{P}{Q} = E(X) &+ \frac{a_n}{(X - \alpha)^n} + \cdots + \frac{a_1}{(X - \alpha)} \\ &+ \frac{b_m}{(X - \beta)^m} + \cdots + \frac{b_1}{(X - \beta)} \\ &+ \frac{c_p}{(X - \gamma)^p} + \cdots + \frac{a_1}{(X - \gamma)} \end{aligned}$$

Soit  $\frac{P}{Q} \in R(X)$  où  $Q = \lambda(X - \alpha)^n \cdots (X - \gamma)^m (X^2 + aX + b)^s \cdots (X^2 + cX + d)$ .  
Ainsi  $\frac{P}{Q}$  s'écrit de façon unique comme somme d'une partie entière de fonctions.

**Théorème 5** Soit  $\frac{P}{Q} \in K(X)$ , avec la décomposition en facteurs irréductibles de  $Q = A^n \cdot B^m \cdots C^r$ . La fraction  $\frac{P}{Q}$  s'écrit de façon unique comme suit :

$$\frac{P}{Q} = E + \frac{F_n}{A^n} + \cdots + \frac{F_1}{A} + \frac{H_m}{B^m} + \cdots + \frac{H_1}{B} + \frac{T_r}{C^r} + \cdots + \frac{T_1}{C}$$

où  $E$  est partie entière, et  $\deg(F_i) < \deg(A)$ ,  $\deg(H_i) < \deg(B)$ ,  $\deg(T_i) < \deg(C)$ .

Cette décomposition est unique et elle est appelée décomposition en éléments simples de la fraction  $\frac{P}{Q}$ .

Décomposition d'une fraction de  $\mathbb{C}(X)$  .

$$\frac{P}{Q} \in \mathbb{C}(X) \text{ avec}$$

$$Q = \lambda(X - a)^n \cdot (X - b)^m \cdots (X - c)^r$$

$$\frac{P}{Q} = E + \frac{\alpha_n}{(X-a)^n} + \cdots + \frac{\alpha_1}{(X-a)} + \frac{\beta_m}{(X-b)^m} + \cdots + \frac{\beta_1}{(X-b)} + \frac{\gamma_r}{(X-c)^r} + \cdots + \frac{\gamma_1}{(X-c)}$$

où  $E$  est la partie entière de  $\frac{P}{Q}$ ,  $\alpha_i, \beta_i, \gamma_i \in \mathbb{C}$

Décomposition d'une fraction de  $\mathbb{R}(X)$  .

$$\frac{P}{Q} \in R(X) \text{ avec}$$

$$Q = \lambda (X-a)^n \cdots (X-b)^m (X^2 + cX + d)^r \cdots (X^2 + eX + f)^s$$

$$\frac{P}{Q} = E + \left( \frac{\alpha_n}{(X-a)^n} + \cdots + \frac{\alpha_1}{(X-a)} \right)$$

+

$\vdots$

+

$$\left( \frac{\beta_m}{(X-b)^m} + \cdots + \frac{\beta_1}{(X-b)} \right)$$

+

$$\left( \frac{h_r X + r_r}{(X^2 + cX + d)^r} + \cdots + \frac{h_1 X + r_1}{(X^2 + cX + d)} \right)$$

+

$\vdots$

+

$$\left( \frac{u_s X + v_s}{(X^2 + eX + f)^s} + \cdots + \frac{u_1 X + v_1}{(X^2 + eX + f)} \right)$$

Où  $E$  est la partie entière et  $\alpha_i, \beta_i, \gamma_i, h_i, e_i, u_i, v_i \in \mathbb{R}$

# Chapitre 5

## Espaces vectoriels sur un corps

### 5.1 Lois de composition externes

Soient  $E$  un ensemble non vide. On appelle loi de composition externe l.c.e sur  $E$  toute application  $f$  de  $K \times E$  dans  $E$ .

**Exemple :** Une application  $g : \mathbb{N}^* \times E \longrightarrow E ; (n, e) \longmapsto ne$  est le model de lois externe le plus connu.

**Remarque :** Avec une loi de composition externe sur  $E$ , on a une règle de base pour multiplier les éléments de  $E$  par les éléments de  $K$ .

### 5.2 Espaces vectoriels sur un corps

Soit  $K$  un un corps commutatif. Un espace vectoriel sur  $K$  est un groupe abélien  $E$  (dont la loi est notée  $+$ ) muni d'une application :

$$\varphi : K \times E \longrightarrow E; (a, x) \longmapsto ax$$

vérifiant les quatre propriétés suivantes :

- i)  $(a + b)x = ax + bx$
- ii)  $(x + y)a = ax + ay$
- iii)  $a(bx) = (ab)x$
- iv)  $1_K x = x$

pour tout  $a, b \in K$  ; et pour tout  $x, y \in E$

**Remarques**

1. Si  $K = \mathbb{R}$ ,  $E$  est appelé espace vectoriel réel.
2. Si  $K = \mathbb{C}$ ,  $E$  est appelé espace vectoriel complexe.

**Exemples d'espaces vectoriels**

1. Le corps  $K$  est un espace vectoriel sur lui-même.
2. Si  $E_1$  et  $E_2$  sont deux espaces vectoriels sur  $K$  alors le produit cartésien  $E_1 \times E_2$  est un espace vectoriel sur  $K$  avec les lois cartésiennes.
3. Ainsi  $\mathbb{R}^2, \mathbb{R}^3, \dots, \mathbb{R}^n$  sont des espaces vectoriels sur  $\mathbb{R}$ .  $\mathbb{C}^2, \mathbb{C}^3, \dots, \mathbb{C}^n$  sont des espaces vectoriels sur  $\mathbb{C}$ .
4. Plus généralement,  $K^n$  est un espace vectoriel sur  $K$ .
5. L'anneau des polynômes  $K[X]$  son corps de fractions rationnelles  $K(X)$  sont des  $K$ -espaces vectoriels.

**Remarque :** Si  $E$  est un espace vectoriel sur  $\mathbb{C}$ , alors  $E$  est un espace vectoriel sur  $\mathbb{R}$ .

**5.3 Sous-espaces vectoriels**

Soient  $E$  un espace vectoriel sur  $K$  et  $V$  un sous-ensemble de  $E$ .

On dit que  $V$  est un sous-espace vectoriel de  $E$  si

- $V$  est un sous-groupe de  $(E, +)$
- et  $\forall x \in V, \forall a \in K$  on a  $ax \in V$

**Exemples :**  $\{0_E\}$  et  $E$  sont des sous-espaces vectoriels de  $E$ , ils sont dits triviaux.

**Proposition :** Si  $V_1$  et  $V_2$  sont deux sous-espaces vectoriels de  $E$ , alors

$$V_1 \cap V_2 \text{ et } V_1 + V_2$$

sont des sous-espaces vectoriels de  $E$ .

**5.4 Applications linéaires ou Homomorphismes d'espaces vectoriels**

Soient  $E$  et  $F$  deux espaces vectoriels sur un corps  $K$ . Une application  $v : E \longrightarrow F$  est un homomorphisme ou  $K$ -linéaire si :

- i)  $v(ax) = av(x)$
- ii)  $v(x + x') = v(x) + v(x') \quad \forall x, x' \in E \text{ et } \forall a \in K$

**Exemples :**

- $id_E$  est une application linéaire
- $C : E \longrightarrow F ; x \longmapsto 0_F$
- $p : E \times F \longrightarrow F ; (x, y) \longmapsto y$
- $f : \mathbb{R}^2 \longrightarrow \mathbb{R} ; (x, y) \longmapsto x + y$

**Proposition :** Soit  $v : E \longrightarrow F$  une application linéaire. Alors  $\ker v$  le noyau de  $v$  et  $\text{Im} v$  l'image de  $v$  sont respectivement sous-espace vectoriel de  $E$  et de  $F$ .

Les notions de monomorphisme ; d'épimorphisme, d'endomorphisme et d'isomorphisme sont laissées au lecteur.

## 5.5 Espaces vectoriels quotients

Soient  $E$  un espace vectoriel sur  $K$  et  $V$  un sous-espace vectoriel de  $E$ . Sur le groupe quotient  $\frac{E}{V}$  on peut définir une l.c.e comme suit :

$$\phi : K \times \frac{E}{V} \longrightarrow \frac{E}{V} ; (a, \bar{x}) \longmapsto \overline{ax}$$

$\phi$  est bien définie et avec  $\phi$  le groupe quotient  $\frac{E}{V}$  est un espace vectoriel sur  $K$ .

**N.B :** La structure d'espace vectoriel sera approfondie plus tard.