

**Université Paris-Dauphine**  
**DUMI2E**  
**Année 2017-2018**

**ALGÈBRE LINÉAIRE 1**

**Denis Pasquignon**

Ce polycopié reprend en grande partie celui écrit par Yannick Viossat pour l'année universitaire 2010-2011 sur ce même cours.



# Table des matières

<b>1</b>	<b>Éléments de logique</b>	<b>7</b>
1.1	Les propositions	7
1.1.1	Equivalence logique	7
1.1.2	Négation	8
1.1.3	Sens de "et", "ou"	8
1.1.4	Implication	9
1.2	Les quantificateurs "pour tout" et "il existe"	10
1.2.1	Définitions	10
1.2.2	Enoncés avec plusieurs quantificateurs	11
1.2.3	Négation	11
1.3	Quelques formes de raisonnement	12
1.3.1	Par contre-exemple	12
1.3.2	Par contraposée	12
1.3.3	Par l'absurde	13
1.3.4	Par récurrence	13
<b>2</b>	<b>Calcul algébrique</b>	<b>15</b>
2.1	Somme et produit	15
2.2	Formules à connaître	18
<b>3</b>	<b>Un peu de théorie des ensembles</b>	<b>19</b>
3.1	Définitions	19
3.2	Union et intersection de deux ensembles	20
3.3	Différence de deux parties, complémentaire d'une partie	21
3.4	Produit cartésien	23
3.5	Union et intersection d'un nombre quelconque d'ensembles	24
3.6	Partitions d'un ensemble	25
3.6.1	Définition	25
3.6.2	Relations d'équivalence	25
<b>4</b>	<b>Applications</b>	<b>27</b>
4.1	Généralités	27
4.2	Antécédents, image directe, image réciproque	28
4.3	Applications injectives, surjectives, bijectives	31
4.4	Application réciproque d'une application bijective	32
4.5	Prolongements et restrictions	34

<b>5</b>	<b>Ensembles finis, ensembles dénombrables</b>	<b>35</b>
5.1	Ensembles finis . . . . .	35
5.2	Ensembles dénombrables . . . . .	37
<b>6</b>	<b>Les nombres complexes</b>	<b>41</b>
6.1	Définitions élémentaires . . . . .	41
6.2	Conjugué d'un nombre complexe . . . . .	44
6.3	Module d'un nombre complexe . . . . .	45
6.4	Argument d'un nombre complexe . . . . .	46
6.5	Racines $n$ èmes d'un nombre complexe . . . . .	49
6.6	Equation du second degré dans $\mathcal{C}$ . . . . .	51
6.7	Géométrie dans le plan complexe . . . . .	52
<b>7</b>	<b>Les nombres entiers et les nombres rationnels</b>	<b>53</b>
7.1	Le principe de récurrence . . . . .	53
7.2	La division euclidienne . . . . .	55
7.3	Le ppcm d'une famille d'entiers . . . . .	56
7.4	Le pgcd d'une famille d'entiers . . . . .	57
7.5	Nombres premiers entre eux . . . . .	60
7.6	Nombres premiers . . . . .	63
7.7	Décomposition d'un entier en facteurs premiers . . . . .	64
<b>8</b>	<b>Les polynômes</b>	<b>67</b>
8.1	Définitions et vocabulaire . . . . .	67
8.2	Division euclidienne . . . . .	69
8.3	Le ppcm d'une famille de polynômes . . . . .	70
8.4	Le pgcd d'une famille de polynômes . . . . .	71
8.5	Polynômes premiers entre eux . . . . .	74
8.6	Polynômes premiers . . . . .	77
8.7	Décomposition d'un polynôme en facteurs premiers . . . . .	77
8.8	Racine d'un polynôme . . . . .	78
8.9	Dérivée d'un polynôme et formule de Taylor . . . . .	81
8.10	Multiplicité d'une racine . . . . .	83
8.11	Applications aux fractions rationnelles . . . . .	84
<b>9</b>	<b>Matrices</b>	<b>87</b>
9.1	Définitions et terminologie . . . . .	87
9.1.1	Définitions et notations . . . . .	87
9.1.2	Matrices particulières . . . . .	87
9.2	Opérations sur les matrices . . . . .	89
9.2.1	Egalité de deux matrices . . . . .	89
9.2.2	Somme de deux matrices de $M_{n,p}$ . . . . .	89
9.2.3	Multiplication d'une matrice de $M_{n,p}$ par un scalaire . . . . .	90
9.2.4	Produit de deux matrices . . . . .	91
9.2.5	Transposée d'une matrice . . . . .	95
9.3	Les matrices carrées . . . . .	96
9.3.1	Quelques matrices carrées particulières . . . . .	96
9.3.2	Opérations dans $M_n$ . . . . .	97
9.3.3	Puissances d'une matrice carrée . . . . .	97
9.3.4	Matrices inversibles . . . . .	99

<b>10 systèmes linéaires</b>	<b>101</b>
10.1 Définitions et écriture matricielle . . . . .	101
10.2 Systèmes faciles à résoudre . . . . .	102
10.2.1 Systèmes triangulaires . . . . .	102
10.2.2 Systèmes échelonnés . . . . .	103
10.3 Opérations élémentaires sur les lignes . . . . .	104
10.3.1 Définition et propriété . . . . .	104
10.3.2 Disposition pratique des calculs . . . . .	105
10.4 Méthode de Gauss . . . . .	106
10.4.1 Exposé de la méthode . . . . .	106
10.4.2 Réduite de Gauss d'une matrice $A$ . . . . .	107
10.4.3 Exemples . . . . .	107
10.4.4 Choix des pivots . . . . .	109
10.4.5 Cas général : résolution du système . . . . .	111
10.4.6 Solutions d'un système linéaire quelconque . . . . .	112
10.5 Matrices et systèmes linéaires . . . . .	113
10.5.1 Interprétation matricielle des opérations élémentaires . . . . .	113
10.5.2 Calcul de l'inverse d'une matrice par la méthode du pivot . . . . .	115

### Notations

Dans toute le polycopié, nous utiliserons les notations suivantes :

- $\mathbb{N}$  désigne l'ensemble des entiers naturels,  $\mathbb{N}^*$  l'ensemble des entiers naturels non nuls,
- $\mathbb{Z}$  désigne l'ensemble des entiers relatifs,  $\mathbb{Z}^*$  l'ensemble des entiers relatifs non nuls,
- $\mathbb{Q}$  désigne l'ensemble des rationnels,  $\mathbb{Q}^*$  l'ensemble des rationnels non nuls,
- $\mathbb{R}$  désigne l'ensemble des réels,  $\mathbb{R}^*$  l'ensemble des réels non nuls,
- $\mathbb{C}$  désigne l'ensemble des nombres complexes,  $\mathbb{C}^*$  l'ensemble des nombres complexes non nuls,
- $\mathbb{R}[X]$  désigne l'ensemble des polynômes à coefficients réels,
- $\mathbb{C}[X]$  désigne l'ensemble des polynômes à coefficients complexes.
- Si  $z$  est un nombre complexe,  $\mathcal{R}e(z)$  désigne sa partie réelle tandis que  $\mathcal{I}m(z)$  désigne sa partie imaginaire.

### Quelques lettres grecques fréquemment utilisées en mathématiques :

	Minuscule	Majuscule
alpha	$\alpha$	$A$
bêta	$\beta$	$B$
gamma	$\gamma$	$\Gamma$
delta	$\delta$	$\Delta$
epsilon	$\epsilon$	$E$
zéta	$\zeta$	$Z$
éta	$\eta$	$N$
théta	$\theta$	$\Theta$
kappa	$\kappa$	$K$
lambda	$\lambda$	$\Lambda$
mu	$\mu$	$M$
nu	$\nu$	$N$
xi	$\xi$	$\Xi$
pi	$\pi$	$\Pi$
rhô	$\rho$	$R$
sigma	$\sigma$	$\Sigma$
tau	$\tau$	$T$
phi	$\phi$	$\Phi$
khi	$\chi$	$X$
psi	$\psi$	$\Psi$
omega	$\omega$	$\Omega$

# Chapitre 1

## Eléments de logique

### 1.1 Les propositions

Une proposition est un énoncé mathématique complet qui est soit vrai soit faux. Par exemple, " $2^3 \geq 10$ " est une proposition fautive; "Dans tout triangle rectangle, le carré de l'hypothénuse est égal à la somme des carrés des deux autres côtés" est une proposition vraie. Un axiome est une proposition dont on admet qu'elle est vraie. Un théorème est une proposition dont on démontre qu'elle est vraie, à l'aide des axiomes, des théorèmes déjà démontrés, et des règles de logique que nous allons étudier.

A partir de propositions existantes et d'expressions comme "non", "et", "ou", "implique", ..., on peut former de nouvelles propositions. Dans la suite, les lettres P, Q, R désignent des propositions.

#### 1.1.1 Equivalence logique

**Définition 1.1.1** Les propositions  $P$  et  $Q$  sont équivalentes si elles sont vraies simultanément et fausses simultanément et on note

$$P \Leftrightarrow Q.$$

On dit que  $P$  est vraie si et seulement si  $Q$  est vraie.

On dit que deux propositions équivalentes sont deux propositions ayant les mêmes valeurs de vérité. Pour prouver que  $P$  et  $Q$  sont équivalentes, on construit un tableau appelé table de vérité dans lequel on fait apparaître les différentes valeurs de vérité possibles pour le couple  $(P, Q)$  (Vrai et Vrai, Vrai et Faux, ...) et, en correspondance, les valeurs de vérité de la proposition  $P \Leftrightarrow Q$ . Ainsi, la table de vérité de l'équivalence logique  $P \Leftrightarrow Q$  est :

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

La première ligne de ce tableau signifie que si les propositions  $P$  et  $Q$  sont vraies, la proposition  $P \Leftrightarrow Q$  est vraie. La deuxième ligne signifie que si  $P$  est vraie et  $Q$  fautive alors la proposition  $P \Leftrightarrow Q$  est fautive.

**Exemple 1.1.2** Pour tout réel  $x$ ,

$$x^2 \leq 4 \Leftrightarrow |x| \leq 2 \Leftrightarrow -2 \leq x \leq 2.$$

### 1.1.2 Négation

**Définition 1.1.3** La proposition "non $P$ ", appelée négation de  $P$ , veut dire : " $P$  est fausse". La proposition "non $P$ " est fausse si  $P$  est vraie, et vraie si  $P$  est fausse. La table de vérité de non $P$  est

$P$	non $P$
$V$	$F$
$F$	$V$

**Proposition 1.1.4** Soit  $P$  une proposition, on a

$$P \Leftrightarrow \text{non}(\text{non}P).$$

**preuve :** Il est clair que  $P$  et  $\text{non}(\text{non}P)$  ont les mêmes valeurs de vérité. ■

**Exemple 1.1.5** Soit  $x$  un réel, la négation de  $x > 3$  est  $x \leq 3$ .

### 1.1.3 Sens de "et", "ou"

**Définition 1.1.6** La proposition " $P$  et  $Q$ " est vraie si et seulement si les propositions  $P$  et  $Q$  sont toutes les deux vraies.

La proposition " $P$  ou  $Q$ " est vraie si et seulement si au moins l'une des propositions  $P$  et  $Q$  est vraie.

Les tables de vérité de "et" et du "ou" :

$P$	$Q$	$P$ et $Q$	$P$ ou $Q$
$V$	$V$	$V$	$V$
$V$	$F$	$F$	$V$
$F$	$V$	$F$	$V$
$F$	$F$	$F$	$F$

A noter : en mathématiques, " $P$  ou  $Q$ " ne veut pas dire "soit  $P$ , soit  $Q$ " (comme dans "fromage ou dessert" ) mais "soit  $P$ , soit  $Q$ , soit les deux" . On dit que le "ou" est inclusif.

On peut combiner plusieurs de ces expressions. Par exemple, la proposition " $(\text{non}P)$  ou  $Q$ " veut dire : " $\text{non}P$  est vraie ou  $Q$  est vraie", c'est à dire : " $P$  est fausse ou  $Q$  est vraie". Elle est vraie dans les trois cas suivants : " $P$  fausse,  $Q$  fausse", " $P$  fausse,  $Q$  vraie" et " $P$  vraie,  $Q$  vraie". Elle est fausse dans le quatrième et dernier cas possible : " $P$  vraie,  $Q$  fausse".

On prouve avec des tables de vérité les propositions suivantes :

**Proposition 1.1.7 Lois de Morgan** Soit  $P$  et  $Q$  deux propositions, on a

$$\text{non}(P \text{ ou } Q) \Leftrightarrow (\text{non } P \text{ et non } Q)$$

et

$$\text{non}(P \text{ et } Q) \Leftrightarrow (\text{non } P \text{ ou non } Q).$$

**Proposition 1.1.8 commutativité, associativité et distributivité** Soit  $P$ ,  $Q$  et  $R$  trois propositions, on a

- $(P \text{ et } Q) \Leftrightarrow (Q \text{ et } P)$
- $(P \text{ ou } Q) \Leftrightarrow (Q \text{ ou } P)$
- $((P \text{ et } Q) \text{ et } R) \Leftrightarrow (P \text{ et } (Q \text{ et } R))$
- $((P \text{ ou } Q) \text{ ou } R) \Leftrightarrow (P \text{ ou } (Q \text{ ou } R))$
- $((P \text{ et } Q) \text{ ou } R) \Leftrightarrow ((P \text{ ou } R) \text{ et } (Q \text{ ou } R))$
- $((P \text{ ou } Q) \text{ et } R) \Leftrightarrow ((P \text{ et } R) \text{ ou } (Q \text{ et } R))$

**Remarque 1.1.9** En général, la place des parenthèses est importante. Par exemple, " $\text{non}P$  ou  $Q$ " ne veut pas dire la même chose que " $\text{non}(P \text{ ou } Q)$ " : si  $P$  et  $Q$  sont toutes les deux vraies, la première proposition est vraie, mais la seconde est fausse.

**Exemple 1.1.10** Soit  $P$  un polynôme de  $\mathbb{R}[X]$ ,

$$\text{non}(P(0) = 0 \text{ ou } P(1) = 0) \Leftrightarrow P(0) \neq 0 \text{ et } P(1) \neq 0.$$

#### 1.1.4 Implication

**Définition 1.1.11** Soit  $P$  et  $Q$  deux propositions, la proposition  $P$  implique  $Q$ , notée  $P \Rightarrow Q$ , est définie par sa table de vérité

$P$	$Q$	$P \Rightarrow Q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$V$
$F$	$F$	$V$

L'implication  $P \Rightarrow Q$  exprime que si  $P$  est vraie alors  $Q$  est vraie. On dit que  $Q$  est une **condition nécessaire** pour que  $P$  soit vraie et  $P$  est une **condition suffisante** pour que  $Q$  soit vraie.

**Proposition 1.1.12** Soit  $P$  une proposition, on a

$$\text{non}(P \Rightarrow Q) \Leftrightarrow (P \text{ et non } Q).$$

**preuve :**  $P \Rightarrow Q$  est fausse dans l'unique cas où  $P$  est vraie et  $Q$  fausse c'est-à-dire  $P$  est vraie et non  $Q$  vraie.



Avec des tables de vérité, on prouve la proposition suivante :

**Proposition 1.1.13** *Soit  $P$ ,  $Q$  et  $R$  trois propositions, on a*

1. **transitivité de l'implication**

$$((P \Rightarrow Q) \text{ et } (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R).$$

2. **équivalence**

$$((P \Rightarrow Q) \text{ et } (Q \Rightarrow P)) \Leftrightarrow (P \Leftrightarrow Q).$$

3. **contraposée**

$$(P \Rightarrow Q) \Leftrightarrow (\text{non } Q \Rightarrow \text{non } P).$$

## 1.2 Les quantificateurs “pour tout” et “il existe”

### 1.2.1 Définitions

Soit  $x$  un réel, on définit une proposition qui dépend de  $x$  et on la note  $P(x)$ . Par exemple, on considère la proposition  $P(x)$  qui est  $x^2 + x + 1 \geq 0$ . Cette proposition peut être vraie que pour certains réels  $x$ , ou pour tous ou aucun. Pour exprimer que  $P(x)$  est vraie pour tout réel  $x$ , on utilise un quantificateur “pour tout”, noté  $\forall$ , on écrit alors

$$\forall x \in \mathbb{R}, x^2 + x + 1 \geq 0$$

Après  $\forall$ , la virgule se lit “on a” ou ne se lit pas.

De même, pour exprimer qu’il existe un réel  $x$  tel que  $P(x)$  soit vraie, on utilise un quantificateur “il existe”, noté  $\exists$ , on écrit alors

$$\exists x \in \mathbb{R}, x^2 + x + 1 \geq 0$$

Après  $\exists$ , la virgule se lit “tel que”.

Plus généralement, soit  $E$  un ensemble et  $P(x)$  un énoncé qui, pour toute valeur donnée à  $x$  dans  $E$  est soit vrai soit faux.

**Définition 1.2.1** *On a*

— La proposition : « Pour tous les éléments  $x$  de  $E$ , la proposition  $P(x)$  est vraie » s’écrit :

$$\forall x \in E, P(x).$$

— La proposition : « il existe au moins un élément  $x$  de  $E$  tel que la proposition  $P(x)$  est vraie » s’écrit :

$$\exists x \in E, P(x).$$

— La proposition : « il existe un et un seul élément  $x$  de  $E$  tel que la proposition  $P(x)$  est vraie » s’écrit :

$$\exists! x \in E, P(x).$$

$\forall$  s’appelle le quantificateur universel et  $\exists$  s’appelle le quantificateur existentiel.

**Exemple 1.2.2**

$\forall x \in \mathbb{R}, x^2 + x + 1 \geq 0$  est une proposition vraie

tandis que la proposition suivante est fausse

$$\forall x \in \mathbb{R}, (x - 1)(x - 3) \geq 0,$$

puisque pour  $x = 2$ ,  $(2 - 1)(2 - 3) = -1$  est négatif. Mais

$$\exists x \in \mathbb{R}, (x - 1)(x - 3) \geq 0 \text{ est une proposition vraie}$$

puisque pour  $x = 4$ , l'inégalité est vérifiée.

**1.2.2 Énoncés avec plusieurs quantificateurs**

Importance de l'ordre : dans un énoncé comprenant plusieurs quantificateurs, l'ordre dans lequel ils interviennent est important. Considérons les deux propositions suivantes :

$$P1 : \forall x \in \mathbb{R}, \exists n \in \mathbb{N}, x \leq n.$$

$$P2 : \exists n \in \mathbb{N}, \forall x \in \mathbb{R}, x \leq n.$$

La première proposition est vraie : pour n'importe quel réel donné, on peut trouver un entier naturel qui est plus grand que ce réel. En revanche, la seconde proposition est fausse : il n'existe pas d'entier naturel qui soit plus grand que tous les réels (si je fixe un entier naturel  $n$ , il y aura toujours des réels  $x$  tels que  $x > n$ , par exemple  $x = n + 1$ ). Le problème vient du fait que dans la première proposition,  $n$  peut dépendre de  $x$ , alors que dans la deuxième proposition, le  $n$  ne dépend pas de  $x$ .

**1.2.3 Négation**

**Proposition 1.2.3** On a

— La négation de “Pour tout élément  $x$  de  $E$ ,  $P(x)$  est vraie” est : “Il existe un élément  $x$  de  $E$  tel que  $P(x)$  est fausse” soit

$$\text{non}(\forall x \in E, P(x)) \Leftrightarrow (\exists x \in E, \text{non}(P(x))).$$

— La négation de “Il existe un élément  $x$  de  $E$  tel que  $P(x)$  est vraie” est “Pour tout élément  $x$  de  $E$ ,  $P(x)$  est fausse” soit

$$\text{non}(\exists x \in E, P(x)) \Leftrightarrow (\forall x \in E, \text{non}(P(x))).$$

**Exemple 1.2.4** La négation de

$$\forall x \in \mathbb{R}, x^2 + x + 1 \geq 0$$

est

$$\exists x \in \mathbb{R}, x^2 + x + 1 < 0.$$

Pour former la négation d'une proposition comportant plusieurs quantificateurs, il suffit d'appliquer les règles précédentes plusieurs fois de suite. En pratique, cela revient à appliquer la règle suivante : pour former la négation d'une proposition comportant un ou plusieurs quantificateurs, on inverse les quantificateurs et on nie la conclusion. Inverser les quantificateurs veut

dire changer les "pour tout" en "il existe" et les "il existe" en "pour tout". Si la proposition est écrite de manière formelle (avec  $\exists$ ,  $\forall$ , etc.), on change les  $\forall$  en  $\exists$ , les  $\exists$  en  $\forall$ , et on nie la conclusion.

**Exemple 1.2.5** Soit  $P1 : \forall x \in \mathbb{R}, \exists n \in \mathbb{N}, x \leq n$ . la négation de  $P1$  est

$$\exists x \in \mathbb{R}, \forall n \in \mathbb{N}, x > n.$$

**Exemple 1.2.6** soit  $P$  la proposition suivante (qui affirme l'existence du quotient et du reste dans la division euclidienne d'un entier naturel par un entier naturel non nul; la division euclidienne est celle qu'on vous a apprise en primaire) :

$$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^*, \exists q \in \mathbb{N}, \exists r \in \mathbb{N}, (a = bq + r \text{ et } r < b)$$

La négation de  $P$  est :

$$\exists a \in \mathbb{N}, \exists b \in \mathbb{N}^*, \forall q \in \mathbb{N}, \forall r \in \mathbb{N}, \text{non}(a = bq + r \text{ et } r < b)$$

ce qui donne finalement

$$\exists a \in \mathbb{N}, \exists b \in \mathbb{N}^*, \forall q \in \mathbb{N}, \forall r \in \mathbb{N}, (a \neq bq + r \text{ ou } r \geq b)$$

## 1.3 Quelques formes de raisonnement

### 1.3.1 Par contre-exemple

On utilise un contre-exemple pour infirmer une propriété présentée comme générale. Par exemple soit  $P$  la proposition

$$\forall (x, y) \in \mathbb{R}^+, \sqrt{x+y} = \sqrt{x} + \sqrt{y}.$$

Cette proposition est fautive puisque pour  $x = 4$  et  $y = 9$ ,  $\sqrt{x} + \sqrt{y} = 5$  et  $\sqrt{x+y} = \sqrt{13}$ .

### 1.3.2 Par contraposée

Soient  $P$  et  $Q$  deux propositions. Pour montrer la proposition " $P \Rightarrow Q$ ", il suffit de montrer " $(\text{Non } Q) \Rightarrow (\text{Non } P)$ " : en effet les propositions " $P \Rightarrow Q$ " et " $(\text{Non } Q) \Rightarrow (\text{Non } P)$ " sont équivalentes.

$$(P \Rightarrow Q) \iff ((\text{Non } Q) \Rightarrow (\text{Non } P)).$$

**Exemple 1.3.1** On veut montrer que pour tout entier naturel  $n$ , si  $n^2$  est pair, alors  $n$  est pair. La contraposée donne : pour entier naturel  $n$ , si  $n$  est impair, alors  $n^2$  est impair. Or il se trouve que la contraposée est très simple à prouver, en effet soit  $n$  un entier naturel, si  $n$  est impair, alors  $n = 2p + 1$  où  $p$  est un entier naturel. On en déduit que  $n^2 = 2(2p^2 + 2p) + 1$  donc  $n^2$  est impair.

**Exemple 1.3.2** Soit  $x$  un réel fixé, on considère la proposition

$$(\forall \epsilon > 0, |x| < \epsilon) \Rightarrow x = 0.$$

On note  $P$  la proposition  $\forall \epsilon > 0, |x| < \epsilon$  et  $Q$  la proposition  $x = 0$ . La négation de  $P$  est  $\exists \epsilon > 0, |x| \geq \epsilon$  et la négation de  $Q$  est  $x \neq 0$ . La contraposée de  $P \Rightarrow Q$  est

$$x \neq 0 \Rightarrow (\exists \epsilon > 0, |x| \geq \epsilon).$$

Or si  $x$  est non nul,  $|x|$  est strictement positif. On pose  $\epsilon = |x|$ , ce réel  $\epsilon$  est strictement positif et on a bien l'inégalité donc non  $Q$  est vraie. La contraposée est vraie donc  $P \Rightarrow Q$  est vraie.

### 1.3.3 Par l'absurde

Pour montrer qu'une proposition  $P$  est vraie, on suppose que  $P$  est fausse, et on cherche à aboutir à une contradiction.

**Exemple 1.3.3** Soit  $P$  la proposition

$$\forall n \in \mathbb{N}^*, n^2 + 1 \text{ n'est pas le carré d'un entier.}$$

Pour prouver que  $P$  est vraie, on suppose que la négation est vraie soit

$$\exists n \in \mathbb{N}^*, \exists p \in \mathbb{N}, n^2 + 1 = p^2.$$

On note  $n_0 \geq 1$  et  $p_0$  tels que

$$n_0^2 + 1 = p_0^2,$$

ce qui s'écrit

$$(p_0 - n_0)(p_0 + n_0) = 1.$$

On a un produit d'entiers naturels égal à 1 donc les deux facteurs sont égaux à 1 soit

$$p_0 - n_0 = p_0 + n_0 = 1.$$

La première égalité donne  $n_0 = 0$  ce qui contredit  $n_0$  non nul. Par conséquent si la négation de  $P$  est vraie, alors on aboutit à une contradiction donc la proposition  $P$  est vraie.

**Exemple 1.3.4** Soit la proposition  $P =$  "il y a une infinité de nombre premiers". On veut montrer que  $P$  est vraie, pour cela on raisonne par l'absurde en supposant que  $P$  est fausse c'est-à-dire que  $\text{non}P$  est vraie. On suppose donc qu'il existe un nombre fini de nombres premiers".

Soit alors  $p$  le plus grand nombre premier. Définissons  $q$  comme étant le nombre  $q = p! + 1 = 1 \times 2 \times \dots \times p + 1$ . Puisque  $q$  est strictement supérieur à  $p$ ,  $q$  n'est pas un nombre premier, il admet donc un diviseur premier  $r > 1$ . Puisque  $r$  est un nombre premier,  $r$  est inférieur à  $p$  et donc  $r$  divise  $p!$ . Ainsi  $r$  divise  $q$  et  $p!$  donc  $q - p! = 1$  donc  $r = 1$  ce qui contredit  $r > 1$ . Par conséquent si la négation de  $P$  est vraie, cela conduit à une contradiction, donc la négation de  $P$  est fausse soit  $P$  est vraie.

### 1.3.4 Par récurrence

On se sert du raisonnement par récurrence pour montrer qu'une famille de propositions  $P(n)$ , indexée par des entiers naturels  $n \in \mathbb{N}$ , est vraie pour tout entier  $n \geq n_0$ . Le principe est le suivant :

1. Initialisation : on montre que  $P(n_0)$  est vraie,
2. Hérité : Soit un entier  $n \geq n_0$ , on montre que si  $P(n)$  est vraie (hypothèse de récurrence), alors  $P(n+1)$  est vraie également.

Si l'on arrive à montrer que (1) et (2) sont vraies, alors la méthode de récurrence permet d'affirmer que  $P(n)$  est vrai pour tout entier  $n \geq n_0$ .

**Exemple 1.3.5** on veut montrer que la somme  $S_n$  des  $n$  premiers entiers naturels est égale à  $n(n+1)/2$ . Appelons  $P(n)$  cette proposition.

1. Initialisation : on vérifie directement que  $P(1)$  est vraie :  $S_1 = 1 = 1(1+1)/2$ .

2. *Hérédité* : Supposons que  $P(n)$  soit vrai pour un certain  $n \geq 1$  (hypothèse de récurrence), et montrons que  $P(n+1)$  l'est aussi. Comme  $S_{n+1} = S_n + (n+1)$ , on a, par hypothèse de récurrence,

$$S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)((n+1) + 1)}{2}$$

Donc  $P(n+1)$  est vrai.

D'après le principe du raisonnement par récurrence, on en déduit que  $P(n)$  est vrai pour tout  $n$ , c'est-à-dire que  $S_n = \frac{n(n+1)}{2}$  pour tout  $n \in \mathbb{N}^*$ .

**Exemple 1.3.6** Dans cet exemple, nous montrons que l'hérédité ne suffit pas c'est-à-dire on peut avoir  $P(n)$  implique  $P(n+1)$  vrai pour tout entier  $n$  et pourtant  $P(n)$  est fausse. On considère la propriété

$$\forall n \in \mathbb{N}, P(n) : 3 \text{ divise } 4^n + 1.$$

Soit un entier  $n$ , on suppose que  $P(n)$  est vrai. On a

$$4^{n+1} + 1 = 4 \times 4^n + 4 - 3 = 4(4^n + 1) + 3,$$

or par hypothèse de récurrence, 3 divise  $4^n + 1$  donc  $4(4^n + 1) + 3$  donc  $P(n+1)$  est vraie. Par contre  $P(0)$  est fausse car 3 ne divise pas 5. On peut montrer que pour tout entier  $n$ ,  $P(n)$  est fausse.

## Chapitre 2

# Calcul algébrique

L'objectif de ce chapitre est essentiellement pratique : savoir calculer avec des formules contenant des indices utilisant les symboles  $\Sigma$  pour somme et  $\Pi$  pour produit.

### 2.1 Somme et produit

L'écriture

$$\sum_{k=0}^5 2^k$$

se lit " somme pour  $k$  allant de 0 à 5 de  $2^k$  " ce qui revient à

$$\sum_{k=0}^5 2^k = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5.$$

La lettre  $k$  est un indice de sommation, on peut choisir  $i$  comme indice sans modifier la valeur de la somme, on dit que  $k$  est une variable muette :

$$\sum_{i=0}^5 2^i = \sum_{k=0}^5 2^k = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5.$$

On rappelle que par convention,  $a^0 = 1$  pour tout réel  $a$ .

Le nombre de termes de cette somme est  $5 - 0 + 1 = 6$ , on reconnaît la somme des termes d'une suite géométrique donc

$$\sum_{k=0}^5 2^k = 1 \times \frac{1 - 2^6}{1 - 2} = 63.$$

On peut aussi écrire une somme allant de  $k = 0$  à  $k = n$  où  $n$  est un entier naturel quelconque, on a

$$\sum_{k=0}^n 2^k = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^n.$$

Le nombre de terme de cette somme est  $n + 1$  et on a

$$\sum_{k=0}^n 2^k = 1 \times \frac{1 - 2^{n+1}}{1 - 2} = 2^{n+1} - 1.$$

Lorsque la quantité à sommer ne dépend pas de l'indice de sommation, le calcul de la somme revient à compter les termes de la somme, ainsi pour tout réel  $a$  :

$$\sum_{k=1}^{10} a = a + a + \cdots + a = 10 \times a$$

Par contre

$$\sum_{k=0}^{10} a = 11 \times a.$$

Cet exemple montre que la valeur d'une somme dépend de l'indice de départ et de celui d'arrivée.

Dans certaine somme, il peut être astucieux de faire un changement d'indice, par exemple on pose  $i = k - 1$  et on obtient

$$\sum_{k=1}^3 2^k = \sum_{k=0}^2 2^{k+1} = 2 \sum_{k=0}^2 2^k = 2(1 + 2 + 2^2) = 14$$

Considérons le cas d'une somme double

$$S = \sum_{i=0}^2 \sum_{j=0}^1 2^{ij}.$$

On a

$$S = \sum_{i=0}^2 (1 + 2^i) = (1 + 1) + (1 + 2) + (1 + 4) = 10.$$

Cette opération revient à additionner tous les termes  $2^{ij}$  lorsque  $i$  varie de 0 à 2 et  $j$  de 0 à 1. On peut disposer ces valeurs dans un tableau

$i/j$	0	1	
0	1	1	<b>2</b>
1	1	2	<b>3</b>
2	1	4	<b>5</b>
	<b>3</b>	<b>7</b>	<b>S = 10</b>

Sur ce tableau, pour calculer  $S$  on peut soit additionner les termes par lignes puis additionner les résultats ou encore additionner les colonnes puis additionner les résultats. Ainsi

$$S = (1 + 1 + 1) + (1 + 2 + 4) = \sum_{j=0}^1 \sum_{i=0}^2 2^{ij}.$$

On a ainsi réalisé une interversion des deux sommes.

De manière générale, on a toujours pour  $n$  et  $p$  deux entiers et  $(a_{ij})$   $np$  réels ou complexes

$$\sum_{i=0}^n \sum_{j=0}^p a_{ij} = \sum_{j=0}^p \sum_{i=0}^n a_{ij}.$$

Une situation plus difficile apparaît lorsque les indices  $i$  et  $j$  sont liés, par exemple on impose  $j \leq i$  alors intervertir les deux sommes nécessite de respecter cette condition

$$\sum_{0 \leq j \leq i \leq n} a_{ij} = \sum_{i=0}^n \sum_{j=0}^i a_{ij} = \sum_{j=0}^n \sum_{i=j}^n a_{ij}.$$

Par exemple

$$\begin{aligned}
 \sum_{1 \leq i \leq j \leq 5} \frac{i}{j} &= \sum_{i=1}^5 \sum_{j=i}^5 \frac{i}{j} = \sum_{j=1}^5 \sum_{i=1}^j \frac{i}{j}, \\
 &= \sum_{j=1}^5 \frac{1}{j} \sum_{i=1}^j i, \\
 &= \sum_{j=1}^5 \frac{1}{j} \frac{j(j+1)}{2}, \\
 &= \frac{1}{2} \sum_{j=1}^5 j+1, \\
 &= \frac{1}{2} \left( \sum_{j=1}^5 j + \sum_{j=1}^5 1 \right), \\
 &= \frac{1}{2} (15 + 5) = 10.
 \end{aligned}$$

Pour comprendre l'interversion, on dispose les nombres  $i/j$  dans un tableau

$i/j$	1	2	3	4	5
1	<b>1</b>	<b>1/2</b>	<b>1/3</b>	<b>1/4</b>	<b>1/5</b>
2	2	<b>1</b>	<b>2/3</b>	<b>2/4</b>	<b>2/5</b>
3	3	3/2	<b>1</b>	<b>3/4</b>	<b>3/5</b>
4	4	2	4/3	<b>1</b>	<b>4/5</b>
5	5	5/2	5/3	5/4	<b>1</b>

Dans ce tableau, les cases qui vérifient la condition  $i \leq j$  correspondent aux nombres au dessus de la diagonale de 1, c'est-à-dire aux nombres représentés en gras. La double somme signifie que l'on additionne tous les nombres en gras. Or il y a deux façons de faire : Dans la première double somme écrite, on somme sur  $i$  ce qui signifie que l'on fixe une ligne  $i$  puis on additionne tous les termes en gras de cette ligne, puis tous ces termes sont additionnés. Mais on peut aussi fixer  $j$  c'est-à-dire fixer une colonne puis sommer tous les nombres en gras de cette colonne, puis tous ces termes sont additionnés. Ces deux méthodes donnent bien entendu le même résultat.

On procède de la même manière pour les produits, on a

$$\prod_{k=1}^n a_k = a_1 \times \cdots \times a_n.$$

Par exemple, on a par définition du factoriel d'un entier.

$$\prod_{k=1}^n k = n!.$$

et aussi

$$\prod_{k=1}^n 2 = 2 \cdot \cdots \cdot 2 = 2^n.$$

## 2.2 Formules à connaître

**Somme des  $n$  premiers entiers.** Pour tout entier  $n$ , on a

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}.$$

**Somme des termes d'une suite géométrique de raison  $q$ .** Pour tout entier  $n$ ,

$$\sum_{k=0}^n q^k = \begin{cases} \frac{1-q^{n+1}}{1-q} & \text{si } q \neq 1, \\ n+1 & \text{si } q = 1. \end{cases}.$$

**Formule du binôme de Newton.** Pour tout entier  $n$ , pour tout complexe  $a$  et  $b$

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

# Chapitre 3

## Un peu de théorie des ensembles

### 3.1 Définitions

**Définition 3.1.1** *Un ensemble est une collection d'objets. Ces objets sont appelés éléments de l'ensemble.*

*L'ensemble qui n'a aucun élément s'appelle ensemble vide. On le note  $\emptyset$ .*

*Pour dire que  $x$  est un élément de l'ensemble  $E$ , on écrit  $x \in E$ . Pour dire que  $x$  n'est pas un élément de  $E$ , on écrit  $x \notin E$ .*

*Deux ensembles  $A$  et  $B$  sont égaux s'ils ont les mêmes éléments. On note alors  $A = B$ .*

**Exemple 3.1.2**  $\{n \in \mathbb{N}, n \leq 5\}$  se lit : "l'ensemble des  $n$  de  $\mathbb{N}$  tel que  $n \leq 5$ ". On peut aussi écrire  $\{n \in \mathbb{N} \mid n \leq 5\}$ , et  $\{n \in \mathbb{N} : n \leq 5\}$ .

**Exemple 3.1.3** Les ensembles de nombres :  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{R}_+$ ,  $\mathbb{N}^*$ ,  $\{1, 2, 3\}$ .

#### Définition 3.1.4 Inclusion

*Soit  $A$  et  $B$  deux sous ensemble de  $E$ . On dit que l'ensemble  $A$  est inclus dans l'ensemble  $B$  si tout élément de  $A$  est un élément de  $B$ . On note alors  $A \subset B$  :*

$$[A \subset B] \Leftrightarrow [\forall x \in E, x \in A \Rightarrow x \in B].$$

*En particulier l'ensemble vide est inclus dans tout ensemble et tout ensemble est inclus dans lui-même.*

La méthode la plus courante pour montrer que deux ensembles sont égaux est de procéder par "double inclusion", c'est à dire de montrer d'abord que  $A$  est inclus dans  $B$ , puis que  $B$  est inclus dans  $A$ .

**Proposition 3.1.5** *Deux ensembles  $A$  et  $B$  sont égaux si et seulement si  $A$  est inclus dans  $B$  et  $B$  est inclus dans  $A$  :*

$$[A = B] \Leftrightarrow [A \subset B \text{ et } B \subset A]$$

**Définition 3.1.6 Ensemble des parties**

L'ensemble des parties de  $B$  se note  $\mathcal{P}(B)$ .

**Exemple 3.1.7** soit  $B = \{1, 2, 3\}$ . Quels sont les parties de  $B$  ? Ce sont les ensembles inclus dans  $B$ . C'est à dire :  $\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}$ , et  $\{1, 2, 3\} = B$ . On a donc :

$$\mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\}$$

**3.2 Union et intersection de deux ensembles**

Dans tout ce qui suit,  $A$  et  $B$  désignent des ensembles.

**Définition 3.2.1 Union, Intersection**

L'union des ensembles  $A$  et  $B$  est l'ensemble des éléments qui appartiennent à  $A$  ou à  $B$ . On la note  $A \cup B$ . Formellement,

$$[x \in A \cup B] \Leftrightarrow [x \in A \text{ ou } x \in B].$$

L'intersection des ensembles  $A$  et  $B$  est l'ensemble des éléments qui appartiennent à la fois à  $A$  et à  $B$ . On la note  $A \cap B$ . Formellement,

$$[x \in A \cap B] \Leftrightarrow [x \in A \text{ et } x \in B].$$

**Exemple 3.2.2**  $A = \{2, 5, 7\}$  et  $B = \{1, 5, 7, 9\}$ , on a  $A \cup B = \{1, 2, 5, 7, 9\}$ , et  $A \cap B = \{5, 7\}$ .

**Proposition 3.2.3 Commutativité, associativité, distributivité**

Soit  $A, B, C$  des ensembles quelconques. On a

—  $A \cup B = B \cup A$  et  $A \cap B = B \cap A$ . On dit que l'union et l'intersection sont des opérations commutatives.

$$A \cup (B \cup C) = (A \cup B) \cup C \quad \text{et} \quad A \cap (B \cap C) = (A \cap B) \cap C$$

On dit que l'union et l'intersection sont des opérations associatives.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{et} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

On dit que l'union est distributive sur l'intersection et que l'intersection est distributive sur l'union.

**preuve** On démontre la commutativité et l'associativité de l'union (respectivement, de l'intersection) en utilisant la commutativité et l'associativité du OU (respectivement, du ET). De même, on prouve que l'union est distributive sur l'intersection, et que l'intersection est distributive sur l'union, en utilisant la distributivité du OU sur le ET, et la distributivité du ET sur le OU.

■

**Remarque 3.2.4** Une conséquence de l'associativité de l'union et de l'intersection est que les expressions  $A \cup B \cup C$  et  $A \cap B \cap C$  ne sont pas ambiguës (on n'a pas besoin de parenthèses). La

première désigne l'ensemble des éléments qui appartiennent à au moins l'un des trois ensemble  $A$ ,  $B$ ,  $C$ . La seconde désigne l'ensemble des éléments qui appartiennent aux trois ensembles à la fois.

**Exercice 1** Soient  $A = \{2, 5, 7\}$ ,  $B = \{1, 5, 7, 9\}$  et  $C = \{2, 7, 9, 10\}$ . Donner la liste des éléments de  $A \cup B \cup C$  et de  $A \cap B \cap C$ .

**Exercice 2** Soit  $E$  un ensemble et  $A$  et  $B$  deux ensembles inclus dans  $E$ , montrer que

$$A \subset B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A.$$

*solution : nous allons prouver les implications suivantes*

$$A \subset B \Rightarrow A \cup B = B \Rightarrow A \cap B = A \Rightarrow A \subset B.$$

on suppose que  $A \subset B$ , alors on utilise une double inclusion pour prouver l'égalité  $A \cup B = B$  :

- Par définition de l'union :  $B \subset A \cup B$ ,
- réciproquement, soit  $x$  un élément de  $A \cup B$ , donc  $x \in A$  ou  $x \in B$ . Si  $x \in A$ , alors comme  $A$  est inclus dans  $B$ ,  $x \in B$ . Donc dans tous les cas,  $x \in B$ . Ainsi  $A \cup B \subset B$ .

Par conséquent  $A \cup B = B$ . On a donc prouvé que

$$A \subset B \Rightarrow A \cup B = B.$$

On suppose que  $A \cup B = B$ , on utilise une double inclusion pour prouver l'égalité  $A \cap B = A$  :

- Par définition de l'intersection :  $A \cap B \subset A$ ,
- réciproquement, soit  $x$  un élément de  $A$ , donc  $x \in A \cup B$ , or  $A \cup B = B$  donc  $x \in B$  et  $x \in A$ , donc  $x \in A \cap B$ . Ainsi  $A \subset A \cap B$ .

Par conséquent  $A \cap B = A$ . On a donc prouvé que

$$A \cup B = B \Rightarrow A \cap B = A.$$

Il reste la dernière implication, on suppose que  $A \cap B = A$ . Soit  $x$  un élément de  $A$ , alors  $x$  appartient à  $A \cap B$  donc à  $B$ . Par conséquent  $A \subset B$ .

En conclusion les trois implications donnent les équivalences demandées.

### 3.3 Différence de deux parties, complémentaire d'une partie

#### Définition 3.3.1 Ensemble "A moins B"

Soient  $A$  et  $B$  deux ensembles. On appelle "A moins B", et on note  $A \setminus B$ , l'ensemble des éléments de  $A$  qui ne sont pas dans  $B$ . On a donc :

$$x \in A \setminus B \Leftrightarrow (x \in A \text{ et } x \notin B)$$

**Exemple 3.3.2** si  $A = \{2, 5, 7\}$  et  $B = \{1, 5, 7, 9\}$ , on a  $A \setminus B = \{2\}$  et  $B \setminus A = \{1, 9\}$ .

**Proposition 3.3.3** Pour tout ensemble  $A$ , on a  $A \setminus \emptyset = A$ , et  $A \setminus A = \emptyset$ . De plus, pour tous ensembles  $A$  et  $B$ , on a  $A \subset B \Leftrightarrow A \setminus B = \emptyset$ .

**Définition 3.3.4 Complémentaire** Soit  $E$  un ensemble. Si  $A$  est une partie de  $E$ , l'ensemble  $E \setminus A$  s'appelle aussi complémentaire de  $A$  dans  $E$ . On le note  $C_E(A)$ . Quand il n'y a pas d'ambiguïté sur  $E$ , on le note plus simplement  $A^c$  ou  $\bar{A}$ . D'une manière générale on a

$$[x \in C_E(A)] \Leftrightarrow [x \in E \text{ et } x \notin A].$$

**Exemple 3.3.5** Soit  $E = \{1, 2, 3, 4, 5\}$ . Soit  $A = \{2, 3\}$ . On a  $C_E(A) = \{1, 4, 5\}$ . Soit  $B = C_E(A)$ . On a  $C_E(B) = \{2, 3\} = A$ .

**Exemple 3.3.6** Soit  $E = \mathbb{R}$ . Soit  $A = [0, 1]$ . On a  $C_{\mathbb{R}}(A) = \{x \in \mathbb{R}, x \notin [0, 1]\} = ]-\infty, 0[ \cup ]1, +\infty[$ . Soit  $B = C_E(A)$ . On a  $C_E(B) = [0, 1] = A$

**Proposition 3.3.7** Soit  $E$  un ensemble et  $A \subset E$ , on a

- Le complémentaire dans  $E$  de l'ensemble vide est l'ensemble  $E$  tout entier :  $C_E(\emptyset) = E$ .
- Le complémentaire dans  $E$  de  $E$  lui-même est l'ensemble vide :  $C_E(E) = \emptyset$ .
- le complémentaire du complémentaire de  $A$  est  $A$  :  $C_E(C_E(A)) = A$ .

**preuve**

- Puisque  $C_E(\emptyset) = E \setminus \emptyset = E$ , on en déduit le résultat.
- De même,  $C_E(E) = E \setminus E = \emptyset$ .
- On utilise une double implication, soit  $x \in C_E(C_E(A))$ , donc  $x \notin C_E(A)$  donc  $x \in A$ , d'où

$$C_E(C_E(A)) \subset A.$$

La réciproque suit le même chemin, si  $x \in A$  alors  $x \notin C_E(A)$  donc  $x \in C_E(C_E(A))$ . D'où l'inclusion réciproque. ■

**Proposition 3.3.8** Soit  $E$  un ensemble. Soient  $A$  et  $B$  des parties de  $E$ . On a alors :

$$[A \subset B] \Leftrightarrow [C_E(B) \subset C_E(A)]$$

**preuve** On raisonne par double implication

- Supposons  $A \subset B$ . Soit  $x$  dans  $C_E(B)$ . On a donc  $x \in E$  et  $x \notin B$ . Comme  $A \subset B$  et  $x \notin B$ , il s'ensuit que  $x \notin A$ . Donc  $x \in C_E(A)$ . Par conséquent

$$C_E(B) \subset C_E(A).$$

- Réciproquement, supposons  $C_E(B) \subset C_E(A)$ . Notons  $A' = C_E(B)$  et  $B' = C_E(A)$ .  $A'$  et  $B'$  sont deux parties de  $E$  telles que  $A' \subset B'$ . D'après la démonstration qui vient d'être faite, on a donc  $C_E(B') \subset C_E(A')$ . Or  $C_E(B') = C_E(C_E(A)) = A$  et de même  $C_E(A') = B$ . Donc  $A \subset B$ . ■

**Remarque 3.3.9** Il est possible de démontrer ce résultat en utilisant l'équivalence entre une implication et sa contraposée. On a les équivalences suivantes

$$\begin{aligned} C_E(B) \subset C_E(A) &\Leftrightarrow \forall x \in E, x \notin B \implies x \notin A, \\ &\Leftrightarrow \forall x \in E, x \in A \implies x \in B, \\ &\Leftrightarrow A \subset B. \end{aligned}$$

**Proposition 3.3.10 Complémentaire de l'union, complémentaire de l'intersection.**

Soient  $E$  un ensemble, et  $A$  et  $B$  deux sous-ensembles de  $E$ . On a :

1.  $C_E(A \cup B) = C_E(A) \cap C_E(B)$ .
2.  $C_E(A \cap B) = C_E(A) \cup C_E(B)$

Ainsi le complémentaire de l'union est l'intersection des complémentaires et le complémentaire de l'intersection est l'union des complémentaires.

**preuve** On a l'équivalence suivante

$$\forall x \in E, x \in A \cup B \iff x \in A \text{ ou } x \in B.$$

Par négation, on obtient

$$\forall x \in E, x \notin A \cup B \iff x \notin A \text{ et } x \notin B.$$

Donc

$$\forall x \in E, x \in C_E(A \cup B) \iff x \in C_E(A) \cap C_E(B).$$

d'où la première égalité  $C_E(A \cup B) = C_E(A) \cap C_E(B)$ .

Pour la deuxième, on pose  $A' = C_E(A)$  et  $B' = C_E(B)$ , on applique la propriété (1) à  $A'$  et  $B'$ , on obtient

$$C_E(A' \cup B') = C_E(A') \cap C_E(B') = A \cap B.$$

On applique le complémentaire d'où

$$A' \cup B' = C_E(A \cap B),$$

soit la deuxième égalité  $C_E(A \cap B) = C_E(A) \cup C_E(B)$ . ■

**Remarque 3.3.11** Il y a des liens entre les expressions utilisées en logique (et, ou, etc.) et les opérations sur les ensembles (intersection, union, etc.), mais il ne faut pas mélanger. Les expressions "et", "ou", "implique", etc. sont à placer entre des propositions, pas entre des ensembles. Les signes  $\cap$ ,  $\cup$ ,  $\subset$ , etc. sont à placer entre des ensembles, pas entre des propositions. En d'autres termes, si  $P$  et  $Q$  sont des propositions, " $P$  et  $Q$ " a un sens, mais " $P \cap Q$ " n'en a pas. Si  $A$  et  $B$  sont des ensembles, " $A \cap B$ " a un sens, mais " $A$  et  $B$ " n'en a pas.

## 3.4 Produit cartésien

Un couple est la donnée de deux objets dans un certain ordre. Bien noter que dans un couple, l'ordre compte :  $(1, 3) \neq (3, 1)$ . Un triplet (resp. quadruplet, quintuplet) est la donnée de trois (resp. quatre, cinq) objets dans un certain ordre. Soit  $n$  un entier naturel non nul, un  $n$ -uplet est la donnée de  $n$  objets dans un certain ordre.

**Définition 3.4.1 Produit Cartésien** On considère un nombre fini d'ensembles  $A_1, A_2, \dots, A_n$ , le produit cartésien des ensembles  $A_1, A_2, \dots, A_n$ , noté  $A_1 \times A_2 \times \dots \times A_n$ , est constitué des  $n$ -uplets  $(a_1, a_2, \dots, a_n)$  tels que  $a_i \in A_i$  pour tout  $i$  dans  $\{1, 2, \dots, n\}$ .

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n), \text{ tel que } a_i \in A_i \text{ pour tout } 1 \leq i \leq n\}$$

Cas particulier :  $A \times A$  se note  $A^2$ ,  $\underbrace{A \times \dots \times A}_{n \text{ fois}}$  se note  $A^n$ .

**Exemple 3.4.2** si  $A = \{1, 2, 3\}$  et  $B = \{1, 7\}$ , alors

$$A \times B = \{(1, 1), (1, 7), (2, 1), (2, 7), (3, 1), (3, 7)\}$$

et

$$B \times A = \{(1, 1), (1, 2), (1, 3), (7, 1), (7, 2), (7, 3)\}$$

**Exemple 3.4.3** si  $A = \{\text{saumon}, \text{poulet}\}$  et  $B = \{\text{banane}, \text{orange}\}$ , alors

$$A \times B = \{(\text{saumon}, \text{banane}), (\text{saumon}, \text{orange}), (\text{poulet}, \text{banane}), (\text{poulet}, \text{orange})\}$$

**Exemple 3.4.4** on note  $\mathbb{N}^2$  l'ensemble des couples d'entiers naturels et  $\mathbb{R}^2$  l'ensemble des couples de réels.

**Exercice 3** Soient  $A$  et  $B$  les intervalles :  $A = [0, 1]$  et  $B = [2, 5]$ . Dessiner dans le plan  $\mathbb{R}^2$  les ensembles  $A \times B$  et  $B \times A$ . Bien noter que  $A \times B \neq B \times A$ .

### 3.5 Union et intersection d'un nombre quelconque d'ensembles

**Définition 3.5.1** Soit  $I$  est un ensemble quelconque (en particulier, pas forcément fini, et pas forcément un sous-ensemble de  $\mathbb{N}$ ), et si pour tout  $i \in I$ ,  $A_i$  est un ensemble,

$$\bigcup_{i \in I} A_i$$

désigne l'ensemble des éléments qui appartiennent à au moins l'un des ensembles  $A_i$  :

$$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i \in I, x \in A_i.$$

De même,  $\bigcap_{i \in I} A_i$  désigne l'ensemble des éléments qui appartiennent à tous les  $A_i$  :

$$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i \in I, x \in A_i.$$

**Remarque 3.5.2** La variable  $i$  est muette : les ensembles  $\bigcup_{1 \leq i \leq n} A_i$  et  $\bigcup_{1 \leq k \leq n} A_k$  sont les mêmes.

**Proposition 3.5.3** si  $I$  est un ensemble d'indices quelconque et pour tout  $i$  dans  $I$ ,  $B_i$  est un ensemble :

$$A \cup \left( \bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cup B_i) \quad \text{et} \quad A \cap \left( \bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i)$$

De même, si  $E$  est un ensemble et pour tout  $i$  dans  $I$ ,  $A_i \subset E$  :

$$C_E \left( \bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} C_E(A_i) \quad \text{et} \quad C_E \left( \bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} C_E(A_i)$$

**Remarque 3.5.4** L'union des ensembles  $A_1, A_2, \dots, A_n$  peut aussi s'écrire  $\bigcup_{1 \leq i \leq n} A_i$  ou  $\bigcup_{i=1}^n A_i$ .  
Les mêmes notations sont utilisées pour l'intersection.

## 3.6 Partitions d'un ensemble

### 3.6.1 Définition

**Définition 3.6.1** Soit  $E$  un ensemble. On appelle partition de  $E$  une famille finie ou non  $(A_i)_{i \in I}$  de parties de  $E$  telles que

- $\forall i \in I, A_i \neq \emptyset$ ,
- $\forall i \neq j, A_i \cap A_j = \emptyset$ ,
- $\bigcup_{i \in I} A_i = E$ .

La notion de partition est liée à celle de relation d'équivalence.

### 3.6.2 Relations d'équivalence

**Définition 3.6.2** Une relation binaire  $\mathcal{R}$  est définie par un ensemble  $E$  et par une partie  $G$  de  $E \times E$ . On dit alors que  $\mathcal{R}$  est une relation binaire sur  $E$ . On dit que  $x$  est en relation avec  $y$  et on note  $x \mathcal{R} y$  si et seulement si  $(x, y) \in G$ .

En pratique, une relation est en général définie par une propriété commune aux couples  $(x, y)$ , par exemple la relation  $\mathcal{R}$  sur  $\mathbb{R}$  telle que :  $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x \mathcal{R} y \Leftrightarrow x - y = 1$ .

Nous ne nous intéresserons ici qu'aux relations d'équivalence (les relations d'ordre, qui forment une autre grande classe de relations, sont hors programme).

**Définition 3.6.3** Une relation  $\mathcal{R}$  sur un ensemble  $E$  est une relation d'équivalence si elle vérifie les trois propriétés suivantes :

- réflexivité : pour tout  $x$  de  $E$ ,  $x \mathcal{R} x$  ; on dit que  $\mathcal{R}$  est réflexive ;
- symétrie : pour tous  $x$  et  $y$  de  $E$ , si  $x \mathcal{R} y$  alors  $y \mathcal{R} x$  ; on dit que  $\mathcal{R}$  est symétrique ;
- transitivité : pour tous  $x, y$  et  $z$  de  $E$ , si  $x \mathcal{R} y$  et  $y \mathcal{R} z$ , alors  $x \mathcal{R} z$  ; on dit que  $\mathcal{R}$  est transitive.

**Exemple 3.6.4** Sur  $\mathbb{Z}$ , la relation de congruence modulo  $n$  (où  $n \in \mathbb{N}^*$ ) : si  $p, q$  et  $n$  sont des entiers relatifs, on dit que  $p$  est congru à  $q$  modulo  $n$  si  $p - q$  est un multiple de  $n$ . C'est une relation d'équivalence.

**Exemple 3.6.5** Soit  $E$  et  $F$  des ensembles, et  $f : E \rightarrow F$  une application. Soit  $\mathcal{R}$  la relation sur  $E$  définie par, pour tous  $x$  et  $y$  dans  $E$ ,  $x \mathcal{R} y$  si et seulement si  $f(x) = f(y)$ . C'est une relation d'équivalence.

**Définition 3.6.6** *Classes d'équivalence.* Une relation d'équivalence permet de regrouper les éléments d'un ensemble en classes d'équivalence ; la classe de l'élément  $a$ , notée  $cl(a)$  ou  $\bar{a}$ , est l'ensemble de tous les éléments  $x$  tels que  $x \mathcal{R} a$  ; ces éléments sont dits équivalents à  $a$ .

**Proposition 3.6.7** *Lorsque  $\mathcal{R}$  est une relation d'équivalence sur un ensemble  $E$ , l'ensemble des classes d'équivalences est appelé ensemble quotient de  $E$  par  $\mathcal{R}$ , et noté  $E/\mathcal{R}$ .*

*L'ensemble  $E/\mathcal{R}$  possède trois propriétés remarquables :*

- aucune classe d'équivalence n'est vide,
- deux classes distinctes sont disjointes,
- l'union de toutes les classes d'équivalence est l'ensemble  $E$ .

*Les classes d'équivalence forment donc une partition de  $E$ .*

# Chapitre 4

## Applications

### 4.1 Généralités

Notations : dans tout le chapitre,  $E$ ,  $F$ ,  $G$  et  $H$  désignent des ensembles non vides.

**Définition 4.1.1** Une application  $f$  est la donnée d'un ensemble de départ non vide, d'un ensemble d'arrivée non vide, et d'une règle de calcul qui associe à tout élément  $x$  de l'ensemble de départ un unique élément de l'ensemble d'arrivée, noté  $f(x)$  et appelé image de  $x$  par  $f$ . La règle de calcul est notée  $x \mapsto f(x)$ .  
L'ensemble des applications de  $E$  dans  $F$  se note  $\mathcal{F}(E, F)$  ou  $F^E$ .

**Définition 4.1.2** **Egalité de deux applications.** Si  $E, E', F, F'$  sont des ensembles non vides, deux applications  $f : E \rightarrow F$  et  $g : E' \rightarrow F'$  sont égales si et seulement si elles ont même ensemble de départ ( $E = E'$ ), même ensemble d'arrivée ( $F = F'$ ) et même règle de calcul ( $f(x) = g(x)$  pour tout  $x$  dans  $E$ ).

**Exemple 4.1.3** Soient  $f_1, f_2, f_3, f_4$  les applications suivantes :

$$\begin{array}{cccccc} f_1 : \mathbb{R} & \rightarrow & \mathbb{R} & f_2 : \mathbb{R}_+ & \rightarrow & \mathbb{R} & f_3 : \mathbb{R} & \rightarrow & \mathbb{R}_+ & f_4 : \mathbb{R}_+ & \rightarrow & \mathbb{R}_+ \\ x & \mapsto & x^2 & x & \mapsto & x^2 & x & \mapsto & x^2 & x & \mapsto & x^2 \end{array}$$

Bien qu'elles aient en commun la règle de calcul  $x \mapsto x^2$ , ces applications sont toutes différentes. Par exemple,  $f_1$  et  $f_2$  sont différentes car elles n'ont pas le même ensemble de départ ;  $f_1$  et  $f_3$  sont différentes, car elles n'ont pas le même ensemble d'arrivée. Ces applications n'ont d'ailleurs pas les mêmes propriétés. Par exemple,  $f_2$  et  $f_4$  sont croissantes, alors que  $f_1$  et  $f_3$  ne le sont pas.

**Exemple 4.1.4** Soient  $f, g$  et  $h$  définies par

$$\begin{array}{ccc} f : \mathbb{R} & \rightarrow & \mathbb{R} & g : \mathbb{R}^* & \rightarrow & ]0, +\infty[ & h : [1, 2] & \rightarrow & [0, 5] \\ x & \mapsto & 1/x & x & \mapsto & 1/x & x & \mapsto & x^2 \end{array}$$

On dit que  $f$  n'est pas une application bien définie ce qui signifie que  $f$  n'est pas une application car 0 appartient à l'ensemble de départ, mais  $f(0)$  n'est pas défini. De même  $g$  n'est pas bien définie puisque par exemple,  $-2$  appartient à l'ensemble de départ, mais  $1/(-2)$  n'appartient pas à l'ensemble d'arrivée. En revanche,  $h$  est une application bien définie.

**Définition 4.1.5 Graphe** : Soit  $f : E \rightarrow F$  une application. Le graphe de  $f$  est l'ensemble des couples  $(x, f(x))$ , c'est une partie de  $E \times F$ .

**Définition 4.1.6 Composition** : soient  $E, F, F'$  et  $G$  des ensembles. Soient  $f : E \rightarrow F$  et  $g : F' \rightarrow G$  des applications. Si  $F \subset F'$ , on peut définir la composée de  $f$  et  $g$ , notée  $g \circ f$  ("g rond f"). C'est l'application de  $E$  dans  $G$  telle que  $g \circ f(x) = g(f(x))$  pour tout  $x$  dans  $E$ .

**Exemple 4.1.7** Soient

$$f : \begin{array}{l} ]2, +\infty[ \rightarrow \mathbb{R} \setminus \{5\} \\ x \mapsto x^2 + 1 \end{array} \quad \text{et} \quad g : \begin{array}{l} \mathbb{R} \setminus \{5\} \rightarrow \mathbb{R} \\ x \mapsto \frac{1}{x-5} \end{array}$$

Pour tout  $x$  dans  $]2, +\infty[$ ,  $f(x) \in \mathbb{R} \setminus \{5\}$ . On peut donc définir  $g \circ f$  et on a, pour tout  $x$  dans  $]2, +\infty[$  :

$$g \circ f(x) = \frac{1}{(x^2 + 1) - 5} = \frac{1}{x^2 - 4}$$

**Proposition 4.1.8** Soient  $f : E \rightarrow F$ ,  $g : F \rightarrow G$ , et  $h : G \rightarrow H$  des applications. On a  $h \circ (g \circ f) = (h \circ g) \circ f$  (on dit que la composition des applications est une opération associative).

**preuve** Les applications  $h \circ (g \circ f)$  et  $(h \circ g) \circ f$  sont toutes deux égales à l'application de  $E$  dans  $H$  qui à  $x$  associe  $h(g(f(x)))$ . ■

**Définition 4.1.9 Application identité** : soit  $E$  un ensemble. On note  $Id_E$  et on appelle application identité de  $E$  l'application :

$$Id_E : \begin{array}{l} E \rightarrow E \\ x \mapsto x \end{array}$$

**Proposition 4.1.10** Pour toute application  $f : E \rightarrow F$ , on a  $Id_F \circ f = f = f \circ Id_E$ .

**preuve** Ces trois applications vont de  $E$  dans  $F$ . De plus, pour tout  $x$  dans  $E$ ,  $Id_F \circ f(x) = Id_F(f(x)) = f(x)$  et  $f \circ Id_E(x) = f(Id_E(x)) = f(x)$ . ■

## 4.2 Antécédents, image directe, image réciproque

**Définition 4.2.1 Antécédents** : soit  $f : E \rightarrow F$  une application. Soient  $x \in E$  et  $z \in F$ . Si  $z$  est l'image de  $x$  par  $f$  (i.e.  $f(x) = z$ ), on dit que  $x$  est un antécédent de  $z$  par  $f$ .

**Remarque 4.2.2** Un élément de l'ensemble de départ a exactement une image. En revanche, un élément de l'ensemble d'arrivée peut avoir 0, 1 ou plusieurs antécédents.

**Exemple 4.2.3** Soit  $f_1 : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $x^2$ . Le réel  $-1$  n'a pas d'antécédents par  $f_1$ , 0 en a exactement un (lui-même), et 3 en a deux :  $\sqrt{3}$  et  $-\sqrt{3}$ .

Soit  $f_2 : \mathbb{R}_+ \rightarrow \mathbb{R}$  qui à  $x$  associe  $x^2$ . Le réel 3 a un unique antécédent par  $f_2$  :  $\sqrt{3}$ , car  $-\sqrt{3}$  n'appartient pas à l'ensemble de départ de  $f_2$ .

Soit  $g : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $g(x) = \sin x$ . Les réels n'appartenant pas à l'intervalle  $[-1, 1]$  n'ont pas d'antécédents par  $g$ . Les réels appartenant à  $[-1, 1]$  en ont une infinité.

**Remarque 4.2.4** Dans le cas des applications de  $\mathbb{R}$  dans  $\mathbb{R}$ , l'image et les antécédents d'un réel se lisent facilement sur le graphe.

**Définition 4.2.5 Image directe et image réciproque**

Soit  $f : E \rightarrow F$  une application. Soient  $A \subset E$  et  $B \subset F$ .

**L'image (directe)** de  $A$  par  $f$  est la partie de  $F$  formée des images de tous les éléments de  $A$ . On la note  $f(A)$ . On a donc :

$$f(A) = \{f(x), x \in A\} = \{y \in F, \exists x \in A, y = f(x)\}$$

**L'image réciproque** de  $B$  par  $f$  est l'ensemble des éléments de  $E$  dont l'image est dans  $B$ . En d'autres termes, c'est l'ensemble des antécédents des éléments de  $B$ . On la note  $f^{-1}(B)$ . On a donc

$$f^{-1}(B) = \{x \in E, f(x) \in B\} = \{x \in E, \exists z \in B, f(x) = z\}$$

**Exemple 4.2.6** Le tableau suivant donne des exemples d'images directes par les applications  $f_1, \dots, f_4$  de l'exemple 3.1.3. Pour mémoire, ces applications ont toutes la règle de calcul  $x \mapsto x^2$  mais différent par leurs ensembles de départ et d'arrivée. Ces derniers sont rappelés sur la première ligne du tableau. "ND" veut dire "Non défini".

	$\mathbb{R} \rightarrow \mathbb{R}$	$\mathbb{R}_+ \rightarrow \mathbb{R}$	$\mathbb{R} \rightarrow \mathbb{R}_+$	$\mathbb{R}_+ \rightarrow \mathbb{R}_+$
$A$	$f_1(A)$	$f_2(A)$	$f_3(A)$	$f_4(A)$
$\{2\}$	$\{4\}$	$\{4\}$	$\{4\}$	$\{4\}$
$\{-2, 2\}$	$\{4\}$	ND	$\{4\}$	ND
$[-1, 3]$	$[0, 9]$	ND	$[0, 9]$	ND
$[-1, 0] \cup [1, 3]$	$[0, 9]$	ND	$[0, 9]$	ND
$\mathbb{R}_+$	$\mathbb{R}_+$	$\mathbb{R}_+$	$\mathbb{R}_+$	$\mathbb{R}_+$
$\mathbb{R}$	$\mathbb{R}_+$	ND	$\mathbb{R}_+$	ND

La raison pour laquelle, par exemple,  $f_2(\mathbb{R})$  n'est pas défini, est que  $\mathbb{R}$  n'est pas inclus dans l'ensemble de départ de  $f_2$ .

Le tableau suivant donne des exemples d'images réciproques pour les mêmes applications. On remarquera que l'image réciproque d'un ensemble non vide peut être vide.

	$\mathbb{R} \rightarrow \mathbb{R}$	$\mathbb{R}_+ \rightarrow \mathbb{R}$	$\mathbb{R} \rightarrow \mathbb{R}_+$	$\mathbb{R}_+ \rightarrow \mathbb{R}_+$
$B$	$f_1^{-1}(B)$	$f_2^{-1}(B)$	$f_3^{-1}(B)$	$f_4^{-1}(B)$
$\{2\}$	$\{-\sqrt{2}, \sqrt{2}\}$	$\{\sqrt{2}\}$	$\{-\sqrt{2}, \sqrt{2}\}$	$\{\sqrt{2}\}$
$\{-1, 2\}$	$\{-\sqrt{2}, \sqrt{2}\}$	$\{\sqrt{2}\}$	ND	ND
$[0, 3]$	$[-\sqrt{3}, \sqrt{3}]$	$[0, \sqrt{3}]$	$[-\sqrt{3}, \sqrt{3}]$	$[0, \sqrt{3}]$
$[-1, 3]$	$[-\sqrt{3}, \sqrt{3}]$	$[0, \sqrt{3}]$	ND	ND
$[-1, 0] \cup [1, 3]$	$\{0\} \cup [-\sqrt{3}, -1] \cup [1, \sqrt{3}]$	$\{0\} \cup [1, \sqrt{3}]$	ND	ND
$\mathbb{R}_+$	$\mathbb{R}$	$\mathbb{R}_+$	$\mathbb{R}$	$\mathbb{R}_+$
$\mathbb{R}_-^*$	$\emptyset$	$\emptyset$	ND	ND
$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R}_+$	ND	ND

La raison pour laquelle, par exemple, l'image réciproque de  $\mathbb{R}$  par  $f_3$  n'est pas définie est que  $\mathbb{R}$  n'est pas inclus dans l'ensemble d'arrivée de  $f_3$ .

**Exercice 4** Soit  $f : E \rightarrow F$  une application. Soient  $A$  et  $A'$  des parties de  $E$ , et  $B$  et  $B'$  des parties de  $F$ . Montrer que

1. Si  $A \subset A'$  alors  $f(A) \subset f(A')$ .
2. Si  $B \subset B'$ , alors  $f^{-1}(B) \subset f^{-1}(B')$ .
3.  $A \subset f^{-1}(f(A))$
4.  $f(f^{-1}(B)) \subset B$
5.  $f(A \cup A') = f(A) \cup f(A')$
6.  $f(A \cap A') \subset f(A) \cap f(A')$
7.  $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$
8.  $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$

Etudier les réciproques.

solution :

1. Soit  $y$  un élément de  $f(A)$ , alors il existe  $x \in A$ , tel que  $y = f(x)$ . Or  $A \subset A'$ , donc  $x \in A'$  donc  $y \in f(A')$ . On a ainsi l'inclusion. La réciproque est fautive. Il suffit de prendre la fonction  $f(x) = x^2$  définie de  $\mathbb{R}$  dans  $\mathbb{R}$ ,  $A = \{1\}$  et  $A' = \{-1\}$ .
2. Soit  $x \in f^{-1}(B)$ , alors il existe  $y \in B$  tel que  $f(x) = y$ . Or  $B \subset B'$ , donc  $y \in B'$  d'où  $x \in f^{-1}(B')$ . on a ainsi l'inclusion. La réciproque est fautive. Il suffit de prendre la fonction  $f(x) = x^2$  définie de  $\mathbb{R}$  dans  $\mathbb{R}$ ,  $B = \{1, -1\}$  et  $B' = \{1, -2\}$ .
3. Soit  $x \in A$ . Posons  $B = f(A)$ . On a  $f(x) \in B$  donc  $x \in f^{-1}(B) = f^{-1}(f(A))$ .
4. Soit  $y \in f(f^{-1}(B))$ . Posons  $A = f^{-1}(B)$ . On a  $y \in f(A)$ , donc il existe  $x \in A$  tel que  $f(x) = y$ . Comme  $x \in A = f^{-1}(B)$ , on a  $f(x) \in B$ . Donc  $y \in B$ . Donc  $f(f^{-1}(B)) \subset B$ . La réciproque est fautive, en effet on considère l'application  $f : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $x^2$ . Posons  $B = \mathbb{R}_-$  donc  $f^{-1}(B) = \emptyset$  et donc  $f(f^{-1}(B)) = \emptyset$ .
5. Par double inclusion. Montrons tout d'abord  $f(A \cup A') \subset f(A) \cup f(A')$ . Soit  $y \in f(A \cup A')$ . Il existe  $x \in A \cup A'$  tel que  $f(x) = y$ . Comme  $x \in A \cup A'$ , on a  $x \in A$  ou  $x \in A'$ . Si  $x \in A$ ,  $f(x) \in f(A)$  donc  $y \in f(A)$  donc  $y \in f(A) \cup f(A')$ . Sinon,  $x \in A'$ , et de même  $y \in f(A) \cup f(A')$ . Donc  $f(A \cup A') \subset f(A) \cup f(A')$ . Montrons maintenant  $f(A) \cup f(A') \subset f(A \cup A')$ . On a  $A \subset A \cup A'$  donc  $f(A) \subset f(A \cup A')$ . De même,  $f(A') \subset f(A \cup A')$ . Donc  $f(A) \cup f(A') \subset f(A \cup A')$ , et par double inclusion on a l'égalité.

6.  $A \cap A' \subset A$  donc  $f(A \cap A') \subset f(A)$ . De même  $f(A \cap A') \subset f(A')$ , donc  $f(A \cap A') \subset f(A) \cap f(A')$ . L'égalité est fautive, en effet on considère l'application  $f : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $x^2$ . Posons  $A = \mathbb{R}_-$  et  $A' = \mathbb{R}_+$ , donc  $A \cap A' = \{0\}$ , et  $f(A) = f(A') = \mathbb{R}_+$ .
7. Soit  $x \in E$ . On a :  $x \in f^{-1}(B \cup B')$  ssi  $f(x) \in B \cup B'$  donc ssi ( $f(x) \in B$  ou  $f(x) \in B'$ ), donc ssi ( $x \in f^{-1}(B)$  ou  $x \in f^{-1}(B')$ ), donc ssi  $x \in f^{-1}(B) \cup f^{-1}(B')$ . Donc  $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$ .
8. Identique à la preuve précédente en remplaçant  $\cup$  par  $\cap$ , et "ou" par "et".

### 4.3 Applications injectives, surjectives, bijectives

**Définition 4.3.1** Soit  $f$  une application.

- $f$  est injective si tout élément de l'ensemble d'arrivée a au plus un antécédent par  $f$ .
- $f$  est surjective si tout élément de l'ensemble d'arrivée a au moins un antécédent.
- $f$  est bijective si tout élément de l'ensemble d'arrivée a un unique antécédent.

Une application injective (respectivement surjective, bijective) est aussi appelée une injection (respectivement surjection, bijection).

**Exemple 4.3.2** Soient  $f_1 : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f_2 : \mathbb{R}_+ \rightarrow \mathbb{R}$ ,  $f_3 : \mathbb{R} \rightarrow \mathbb{R}_+$  et  $f_4 : \mathbb{R}_+ \rightarrow \mathbb{R}_+$  qui à  $x$  associent  $x^2$ . L'application  $f_1$  n'est ni injective ni surjective;  $f_2$  est injective mais pas surjective;  $f_3$  est surjective mais pas injective;  $f_4$  est bijective.

**Exemple 4.3.3** Soit  $E$  un ensemble. L'application identité de  $E$  est bijective.

**Proposition 4.3.4** Soit  $f : E \rightarrow F$  une application. On a

$$f \text{ est injective} \iff \forall (x, x') \in E^2, f(x) = f(x') \implies x = x'.$$

#### Preuve

On raisonne par double implication.

on suppose que  $f$  injective. Soient  $x$  et  $x'$  dans  $E$  tels que  $f(x) = f(x')$ . Soit  $z = f(x)$ . Si  $x \neq x'$ ,  $z$  a au moins deux antécédents distincts, ce qui est impossible car  $f$  est injective. Donc  $x = x'$ .

Réciproquement : soit  $z$  dans  $F$ . Si  $z$  a deux antécédents distincts  $x$  et  $x'$  alors  $x \neq x'$  mais  $f(x) = z = f(x')$ , ce qui implique  $x = x'$ . Donc  $z$  a au plus un antécédent, donc  $f$  est injective. ■

**Proposition 4.3.5** Soit  $f : E \rightarrow F$  une application.  $f$  est surjective si et seulement si

$$f(E) = F.$$

#### Preuve

$f(E)$  est l'ensemble des images des éléments de  $E$ . C'est donc l'ensemble des éléments de  $F$  qui ont au moins un antécédent. Donc  $f(E) = F$  ssi tout élément de  $F$  a au moins un antécédent par  $f$ , c'est à dire ssi  $f$  est surjective. ■

**Exercice 5** Soient  $f : E \rightarrow F$  et  $g : F \rightarrow G$  des applications. Montrer que

1. si  $f$  et  $g$  sont injectives, alors  $g \circ f$  est injective.
2. si  $f$  et  $g$  sont surjectives, alors  $g \circ f$  est surjective.
3. si  $g \circ f$  est injective, alors  $f$  est injective.
4. si  $g \circ f$  est surjective, alors  $g$  est surjective.

Montrer que les réciproques des assertions précédentes sont fausses.

solution :

1. Supposons  $f$  et  $g$  injectives. Soient  $x$  et  $x'$  dans  $E$  tels que  $g \circ f(x) = g \circ f(x')$ . On a  $g(f(x)) = g(f(x'))$  donc par injectivité de  $g$ ,  $f(x) = f(x')$ , donc par injectivité de  $f$ ,  $x = x'$ . L'application  $g \circ f$  est donc bien injective.
2. Supposons  $f$  et  $g$  surjectives. Soit  $z \in G$ . Comme  $g$  est surjective, il existe  $y \in F$  tel que  $z = g(y)$ . De plus, comme  $f$  est surjective, il existe  $x \in E$  tel que  $y = f(x)$ . On a donc  $z = g(f(x)) = g \circ f(x)$ , donc  $z$  a au moins un antécédent par  $g \circ f$ . Donc  $g \circ f$  est bien surjective.
3. Supposons  $g \circ f$  injective. Soient  $x$  et  $x'$  dans  $E$  tels que  $f(x) = f(x')$ . On a donc  $g(f(x)) = g(f(x'))$ , donc par injectivité de  $g \circ f$ ,  $x = x'$ . Donc  $f$  est injective.
4. Supposons  $g \circ f$  surjective. Soit  $z \in G$ . Comme  $g \circ f$  est surjective, il existe  $x$  dans  $E$  tel que  $z = g \circ f(x)$ . Posons  $y = f(x)$  (c'est à dire : appelons  $y$  l'image de  $x$  par  $f$ ). On a  $y \in F$  et  $z = g(y)$ , donc  $z$  a au moins un antécédent par  $g$ , donc  $g$  est surjective.

Montrons que les réciproques de 1) et 2) sont fausses : soit  $f : \mathbb{N} \rightarrow \mathbb{N}$  qui à tout entier naturel  $n$  associe  $n + 1$ . Soit  $g : \mathbb{N} \rightarrow \mathbb{N}$  qui à tout entier naturel  $n$  associe  $n - 1$  si  $n \neq 0$  et qui à  $0$  associe  $0$ . Pour tout entier naturel  $n$ , on a  $g \circ f(n) = g(n + 1) = (n + 1) - 1 = n$  (on a utilisé  $n + 1 \neq 0$  pour calculer  $g(n + 1)$ ). On a donc  $g \circ f = \text{Id}_{\mathbb{N}}$ . L'application  $g \circ f$  est donc bijective, donc injective et surjective. Pourtant  $f$  n'est pas surjective (car  $0$  n'a pas d'antécédents par  $f$ ) et  $g$  n'est pas injective (car  $0$  a deux antécédents par  $g : 1$  et  $0$ ).

Montrons maintenant que les réciproques de 3) et de 4) sont fausses. Soient  $f = \text{Id}_{\mathbb{R}}$  et  $g$  l'application de  $\mathbb{R}$  dans  $\mathbb{R}$  qui à tout réel  $x$  associe  $0$ . L'application  $g$  est donc constante. Pour tout réel  $x$ ,  $g \circ f(x) = g(x) = 0$ . L'application  $g \circ f$  n'est donc pas injective, bien que  $f$  le soit. Le lecteur vérifiera que, de même, l'application  $f \circ g$  n'est pas surjective, bien que  $f$  le soit.

**Exercice 6** Soit  $f : E \rightarrow F$  une application, soit  $b \in F$ , on veut résoudre dans  $E$  l'équation

$$f(x) = b.$$

1. Montrer que si  $b \notin f(E)$ , alors il n'y a pas de solutions dans  $E$ .
2. Montrer que si  $b \in f(E)$  et si  $f$  est injective, alors il existe une unique solution.

## 4.4 Application réciproque d'une application bijective

**Définition 4.4.1** Soit  $f : E \rightarrow F$  une application bijective. On appelle application réciproque de  $f$  l'application  $g : F \rightarrow E$  telle que pour tout  $y$  dans  $F$ ,  $g(y)$  est l'unique antécédent de  $y$  par  $f$ . On la note  $f^{-1}$ .

**Proposition 4.4.2** Soit  $f : E \rightarrow F$ . Si  $f$  est bijective, alors

$$\forall x \in E, \forall y \in F, (y = f(x)) \Leftrightarrow (x = f^{-1}(y)).$$

**Preuve**

Soit  $x \in E$  et  $y \in F$ . Si  $y = f(x)$  alors  $x$  est un antécédent de  $y$ . Mais  $f^{-1}(y)$  est l'unique antécédent de  $y$  par  $f$ , donc  $f^{-1}(y) = x$ . Réciproquement, si  $x = f^{-1}(y)$ , alors  $x$  est l'unique antécédent de  $y$  par  $f$ ; en particulier,  $x$  est un antécédent de  $y$ , donc  $f(x) = y$ .

■

**Proposition 4.4.3** Soit  $f : E \rightarrow F$  une application.

1. si  $f$  est bijective, alors  $f^{-1} \circ f = Id_E$  et  $f \circ f^{-1} = Id_F$ .
2. S'il existe une application  $g$  de  $F$  vers  $E$  telle que  $g \circ f = Id_E$  et  $f \circ g = Id_F$ , alors  $f$  est bijective et  $g = f^{-1}$ .
3. si  $f$  est bijective, alors sa réciproque  $f^{-1}$  aussi et  $(f^{-1})^{-1} = f$ .
4. Soit  $g : F \rightarrow G$ . Si  $f$  et  $g$  sont bijectives, alors  $g \circ f$  est bijective et  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

**Preuve**

1) Supposons  $f$  bijective. Soit  $x \in E$ . Posons  $y = f(x)$ . D'après la proposition 4.4.2,  $f^{-1}(y) = x$  donc  $f^{-1}(f(x)) = x$ , donc  $f^{-1} \circ f = Id_E$ . Le lecteur vérifiera que, de même,  $f \circ f^{-1} = Id_F$ .

2) Supposons  $g \circ f = Id_E$  et  $f \circ g = Id_F$ . On a donc  $g \circ f$  et  $f \circ g$  bijectives. En particulier,  $g \circ f$  est injective, donc  $f$  est injective d'après le point 3) de l'exercice 5. De même,  $f \circ g$  est surjective, donc  $f$  est surjective d'après le point 4) de l'exercice 5. L'application  $f$  est donc bijective, donc sa réciproque  $f^{-1}$  existe et d'après 1),  $f^{-1} \circ f = Id_E$ . En composant l'égalité  $f \circ g = Id_F$  par  $f^{-1}$ , on obtient  $f^{-1} \circ f \circ g = f^{-1} \circ Id_F = f^{-1}$ , donc  $g = Id_F \circ g = (f^{-1} \circ f) \circ g = f^{-1}$ .

3) Supposons  $f$  bijective. Pour mieux comprendre la façon dont nous allons utiliser le 2), posons  $g = f^{-1}$ ,  $\tilde{E} = F$  et  $\tilde{F} = E$ . On a d'après le 1),  $g \circ f = Id_{\tilde{F}}$  et  $f \circ g = Id_{\tilde{E}}$ . D'après le 2), on a donc  $g$  bijective et  $g^{-1} = f$ , c'est à dire  $f^{-1}$  bijective et  $(f^{-1})^{-1} = f$ .

4) Supposons  $f$  et  $g$  bijectives. Leur réciproques  $f^{-1}$  et  $g^{-1}$  existent donc. De plus,  $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ Id_E \circ g^{-1} = g \circ g^{-1} = Id_G$ . De même,  $(f^{-1} \circ g^{-1}) \circ (g \circ f) = Id_E$ , donc d'après le 2),  $g \circ f$  est bijective et  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

■

**Exercice 7** Soit  $f : E \rightarrow F$  une application. Supposons qu'il existe une application  $g : F \rightarrow E$  telle que, pour tout  $x$  dans  $E$  et tout  $y$  dans  $F$ ,  $y = f(x) \Leftrightarrow x = g(y)$ . Alors  $f$  est bijective et  $f^{-1} = g$ .

**Remarque 4.4.4** Si  $f$  n'est pas bijective, son application réciproque n'existe pas. La notation  $f^{-1}(B)$  ne désigne alors pas l'image de  $B$  par l'application  $f^{-1}$  (puisque cette application n'existe pas!), mais uniquement l'image réciproque de  $B$  par  $f$ . En particulier, ce n'est pas parce que la notation  $f^{-1}(B)$  apparaît dans un énoncé qu'on a supposé que  $f$  était bijective.

## 4.5 Prolongements et restrictions

**Proposition 4.5.1** Soit  $f : E \rightarrow F$  une application. Soit  $A \subset E$  et  $B \subset F$  tel que  $f(A) \subset B$ . On appelle restriction de  $f$  à  $A$  comme ensemble de départ et  $B$  comme ensemble d'arrivée, et on note  $f|_{A \rightarrow B}$ , l'application de  $A$  dans  $B$  qui à tout  $x$  dans  $A$  associe  $f(x)$ . Cette application a la même règle de calcul que  $f$ , seuls changent les ensembles de départ et d'arrivée.  
 Notation : quand on restreint uniquement l'ensemble de départ ( $B = F$  : cas courant), on utilise aussi la notation  $f|_A$  pour  $f|_{A \rightarrow F}$ .  
 Soient  $f$  et  $g$  des applications. On dit que  $f$  est un prolongement de  $g$  si  $g$  est une restriction de  $f$ .

**Exemple 4.5.2** Soit  $f : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $x^2$ . Soit  $g = f|_{\mathbb{R}^+ \rightarrow \mathbb{R}^+}$ , c'est à dire soit  $g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$  qui à  $x$  associe  $x^2$ . L'application  $g$  est une restriction de  $f$ . Elle a l'avantage d'être croissante et bijective, alors que  $f$  ne l'est pas.

**Exemple 4.5.3** Soit  $g : \mathbb{R}^* \rightarrow \mathbb{R}$  qui à  $x$  associe  $(\sin x)/x$ . Soit  $f : \mathbb{R} \rightarrow \mathbb{R}$  qui à  $x$  associe  $(\sin x)/x$  si  $x \neq 0$ , et qui à  $0$  associe  $1$ . L'application  $f$  est un prolongement de  $g$  (on a  $g = f|_{\mathbb{R}^*}$ ). De plus, on peut montrer que  $f$  est continue sur  $\mathbb{R}$ . On dit que  $f$  est le prolongement par continuité de  $g$ . L'avantage de considérer  $f$  plutôt que  $g$  est qu'on peut appliquer à  $f$  les théorèmes sur les fonctions continues sur  $\mathbb{R}$  tout entier (par exemple, avec  $f$  on peut utiliser le théorème des valeurs intermédiaires sur un intervalle contenant  $0$ , alors qu'on ne pourrait pas le faire avec  $g$ ).

**Proposition 4.5.4** Soit  $f : E \rightarrow F$  une application.

- La restriction de  $f$  à  $E$  comme ensemble de départ et  $f(E)$  comme ensemble d'arrivée est surjective.
- Si  $f$  est injective, toutes ses restrictions le sont.
- Si  $f$  est injective, la restriction de  $f$  à  $E$  comme ensemble de départ et  $f(E)$  comme ensemble d'arrivée est bijective (on dit que  $f$  induit une bijection de  $E$  sur  $f(E)$ ).

### Preuve

a) Notons  $g$  cette restriction ( $g = f|_{E \rightarrow f(E)}$ ). Soit  $y \in f(E)$ . Il existe  $x \in E$  tel que  $y = f(x)$ . Mais  $g(x) = f(x)$ . Donc  $g(x) = y$  et  $y$  a au moins un antécédent par  $g$ . Ceci est vrai pour tout  $y$  dans  $f(E)$ , donc pour tout  $y$  dans l'ensemble d'arrivée de  $g$ , donc  $g$  est surjective.

b) Supposons  $f$  injective. Soient  $A \subset E$  et  $B \subset F$  tels que  $f(A) \subset B$ . Soit  $g$  la restriction de  $f$  à  $A$  comme ensemble de départ et  $B$  comme ensemble d'arrivée. Soient  $x$  et  $x'$  dans  $A$ . Si  $g(x) = g(x')$  alors  $f(x) = f(x')$  par définition de  $g$ , donc  $x = x'$  par injectivité de  $f$ . Donc  $g$  est injective.

c) Conséquence directe de a) et b).

■

# Chapitre 5

## Ensembles finis, ensembles dénombrables

### 5.1 Ensembles finis

Pour tout entier  $n \geq 1$ , on note  $\llbracket 1, n \rrbracket$  l'intervalle des entiers compris entre 1 et  $n$ .

**Définition 5.1.1** *Un ensemble  $E$  est fini s'il est vide ou s'il existe un entier  $n \in \mathbb{N}^*$  et une bijection de  $E$  dans  $\llbracket 1, n \rrbracket$ .*

**Proposition 5.1.2** *Soit  $E$  un ensemble fini non vide, et  $n$  et  $p$  des entiers naturels. S'il existe une bijection de  $E$  dans  $\llbracket 1, n \rrbracket$  et une bijection de  $E$  dans  $\llbracket 1, p \rrbracket$  alors  $n = p$ . Le **cardinal d'un ensemble fini** est donc cet unique entier  $n$ .  
Par convention,  $\text{Card } \emptyset = 0$ .*

La démonstration de la proposition repose sur le lemme un peu technique suivant :

**Lemme 5.1.3** *Pour tout entier  $n \geq 1$ , s'il existe un entier  $p \in \mathbb{N}^*$  et une application injective de  $\llbracket 1, n \rrbracket$  dans  $\llbracket 1, p \rrbracket$ , alors  $n \leq p$ .*

**Preuve** Elle se fait par récurrence sur  $n$ .

La propriété est évidente pour  $n = 1$ .

Supposons maintenant que le résultat soit vrai pour  $n \geq 1$  : s'il existe une injection de  $\llbracket 1, n \rrbracket$  dans  $\llbracket 1, p \rrbracket$ , alors  $n \leq p$ . Soit  $f$  une injection de  $\llbracket 1, n+1 \rrbracket$  dans  $\llbracket 1, p \rrbracket$  où  $p$  est un entier non nul. Puisque  $f$  est injective,  $a = f(n+1)$  n'appartient pas à  $f(\llbracket 1, n \rrbracket)$  donc  $p \geq 2$ . On construit une nouvelle application  $g$  de  $\llbracket 1, n \rrbracket$  dans  $\llbracket 1, p-1 \rrbracket$  par

$$g: \llbracket 1, n \rrbracket \rightarrow \llbracket 1, p-1 \rrbracket$$
$$i \mapsto g(i) = \begin{cases} f(i) & \text{si } f(i) \leq p-1, \\ a & \text{si } f(i) = p. \end{cases}$$

Il est clair que  $g$  est injective donc d'après l'hypothèse de récurrence  $n \leq p-1$  soit  $n+1 \leq p$ .

■

**Preuve de la proposition 5.1.2** Si  $f$  est une bijection de  $E$  dans  $\llbracket 1, n \rrbracket$  et  $g$  une bijection de  $E$  dans  $\llbracket 1, p \rrbracket$ , alors  $g \circ f^{-1}$  est une bijection de  $\llbracket 1, n \rrbracket$  dans  $\llbracket 1, p \rrbracket$ . Donc  $n \leq p$  d'après le lemme précédent. De plus,  $f \circ g^{-1}$  est une bijection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, n \rrbracket$ , donc  $p \leq n$  toujours grâce au lemme. En conclusion,  $p = n$ . ■

La proposition suivante sera souvent utiliser pour déterminer le cardinal d'un ensemble fini  $E$  : plutôt que de construire une bijection de  $E$  sur un intervalle d'entier  $\llbracket 1, n \rrbracket$ , on met en évidence une bijection de  $E$  sur un ensemble  $F$  dont le cardinal est connu.

**Proposition 5.1.4** *Si  $E$  et  $F$  sont deux ensembles finis de même cardinal, alors il existe une bijection de  $E$  sur  $F$ . Réciproquement si  $E$  est un ensemble et si  $F$  est un ensemble fini en bijection avec  $E$ , alors  $E$  est un ensemble fini et  $\text{Card } E = \text{Card } F$ .*

**Preuve** On admet qu'il existe une bijection de l'ensemble vide sur lui-même. D'autre part, l'ensemble vide ne peut être en bijection avec un ensemble non vide donc on se limite au cas où  $E$  et  $F$  sont non vides. Soit  $n$  le cardinal de  $E$  et de  $F$ , il existe une bijection  $f$  de  $\llbracket 1, n \rrbracket$  dans  $E$  et  $g$  une bijection de  $\llbracket 1, n \rrbracket$  dans  $F$ , alors  $g \circ f^{-1}$  est une bijection de  $E$  dans  $F$ . Réciproquement, soit  $g$  une bijection de  $\llbracket 1, n \rrbracket$  dans  $F$  et  $f$  une bijection de  $F$  dans  $E$ . Alors l'application  $f \circ g$  est une bijection de  $\llbracket 1, n \rrbracket$  dans  $E$ , ce qui prouve que  $E$  est fini de cardinal  $n$ . ■

**Proposition 5.1.5** *Toute partie  $A$  d'un ensemble fini  $E$  est un ensemble fini et  $\text{Card } A \leq \text{Card } E$ . De plus  $\text{Card } A = \text{Card } E$  si et seulement si  $A = E$ .*

**Preuve** Si  $E$  est l'ensemble vide, le résultat est immédiat. On suppose  $E$  non vide, il existe un entier  $n \geq 1$  tel que  $\text{Card } E = n$ . On se place dans le cas où  $E = \llbracket 1, n \rrbracket$  et  $A$  est une partie de  $E$ . On raisonne par récurrence sur  $n$  :

- si  $n = 1$ ,  $A$  est soit vide soit  $\{1\}$  et la propriété est vraie.
- soit  $n \geq 1$  tel que la propriété soit vraie. Si  $A$  est strictement incluse dans  $E$ , il existe  $a$  de  $E$  qui n'appartient pas à  $A$ . On construit une application  $f$  telle que

$$f : \llbracket 1, n+1 \rrbracket \rightarrow \llbracket 1, n+1 \rrbracket$$

$$i \mapsto f(i) = \begin{cases} i & \text{si } i \neq a \text{ et } i \neq n+1, \\ n+1 & \text{si } i = a, \\ a & \text{si } i = n+1. \end{cases}$$

$f$  est une bijection et  $f(A) \subset \llbracket 1, n \rrbracket$ . On applique l'hypothèse de récurrence donc  $\text{Card } A = \text{Card } f(A) < n < n+1$ . L'égalité est impossible si  $A$  est strictement inclus dans  $E$ . Enfin si  $A = E$ , le résultat est immédiat.

Pour conclure dans le cas général, soit  $f$  une bijection de  $E$  dans  $\llbracket 1, n \rrbracket$ ,  $f(A)$  est en bijection avec  $A$  et c'est une partie de  $\llbracket 1, n \rrbracket$  d'où la conclusion. ■

**Remarque 5.1.6** *Un ensemble  $E$  de cardinal  $n \geq 1$  est un ensemble dont on peut numéroter les éléments de 1 à  $n$ ; en effet, si  $f$  est une bijection de  $\llbracket 1, n \rrbracket$  dans  $E$ , on pose*

$$\forall i \in \llbracket 1, n \rrbracket, \quad x_i = f(i).$$

On a donc

$$E = \{x_1, \dots, x_n\}.$$

Pour  $n \geq 2$ , la numérotation n'est pas unique.

**Proposition 5.1.7** Soient  $A$  et  $B$  deux parties finies disjointes d'un ensemble  $E$  alors

$$\text{Card } A \cup B = \text{Card } A + \text{Card } B.$$

On en déduit que

— si  $(A_i)_{1 \leq i \leq n}$  est une famille de parties deux à deux disjointes, alors

$$\text{Card } \bigcup_{i=1}^n A_i = \sum_{i=1}^n \text{Card } A_i,$$

— si  $\text{Card } E = n$ , alors

$$\text{Card } A^c = n - \text{Card } A,$$

— si  $B \subset A$ , alors

$$\text{Card } A \setminus B = \text{Card } A - \text{Card } B,$$

— si  $A$  et  $B$  sont deux parties d'un ensemble  $E$  alors

$$\text{Card } A \cup B = \text{Card } A + \text{Card } B - \text{Card } A \cap B.$$

**Preuve** On suppose que  $A$  et  $B$  sont deux parties disjointes. Si  $A$  ou  $B$  est vide, le résultat est évident. On étudie le cas où  $\text{Card } A = p \geq 1$  et  $\text{Card } B = q \geq 1$ , soit  $f$  une bijection de  $\llbracket 1, p \rrbracket$  dans  $A$  et  $g$  une bijection de  $\llbracket 1, q \rrbracket$ , on construit une application  $h$  par

$$h : \llbracket 1, p+q \rrbracket \rightarrow A \cup B$$

$$i \mapsto h(i) = \begin{cases} f(i) & \text{si } 1 \leq i \leq p, \\ g(i-p) & \text{si } p+1 \leq i \leq p+q, \end{cases}$$

$h$  est une bijection donc  $\text{Card } A \cup B = p + q$ .

On en déduit le premier résultat par récurrence sur  $n$ . Le deuxième est un cas particulier avec la famille  $(A, A^c)$ . enfin le troisième vient de l'égalité  $(A \setminus B) \cup B = A$ . Enfin le dernier point vient de  $A \cup B = (A \setminus A \cap B) \cup (B \setminus A \cap B) \cup (A \cap B)$ .

■

## 5.2 Ensembles dénombrables

Les ensembles dénombrables forment une classe particulière d'ensembles infinis :

**Définition 5.2.1** Un ensemble  $E$  est infini s'il n'est pas fini.

Un ensemble  $E$  est dénombrable s'il existe une bijection de  $\mathbb{N}$  dans  $E$ .

Un ensemble est au plus dénombrable s'il est fini ou dénombrable.

**Remarque 5.2.2** Dans quelques ouvrages, le mot dénombrable désigne un ensemble fini ou dénombrable et un ensemble dénombrable infini est appelé strictement dénombrable.

**Remarque 5.2.3** Un ensemble dénombrable est un ensemble dont on peut numéroter les éléments de 0 à l'infini. Soit  $f$  une bijection de  $\mathbb{N}$  dans  $E$ , on définit une suite  $(x_i)_{i \geq 0}$  dont tous les éléments sont distincts. On dira que les éléments d'un ensemble dénombrable peuvent être rangés dans une suite.

**Exemple 5.2.4** Les ensembles  $\mathbb{N}$ ,  $\mathbb{N}^*$  sont dénombrables ainsi que l'ensemble des entiers pairs ( $f(n) = 2n$ ) et l'ensemble des carrés parfaits ( $f(n) = n^2$ ). Ces exemples prouvent que contrairement à ce qui se passe pour les ensembles finis, il existe des parties strictes de  $\mathbb{N}$  en bijection avec  $\mathbb{N}$ .

**Proposition 5.2.5** Toute partie  $A$  de  $\mathbb{N}$  est au plus dénombrable. Plus précisément, si  $A \neq \emptyset$

- soit  $A$  est majorée, et alors  $A$  est finie,
- soit  $A$  n'est pas majorée, et alors  $A$  est dénombrable.

**Preuve** Si  $A$  est vide,  $A$  est finie par définition. On suppose  $A$  non vide.

- si  $A$  est majorée par  $n$ , alors  $A \subset \llbracket 1, n \rrbracket$  donc  $A$  est finie,
- si  $A$  n'est pas majorée, on construit une bijection  $f$  de  $\mathbb{N}$  dans  $A$  : comme  $A$  est une partie non vide de  $\mathbb{N}$ ,  $A$  admet un plus petit élément  $a_0$ . On pose  $f(0) = a_0$ . Soit  $A_1 = A \setminus \{a_0\}$ ,  $A_1$  est non vide sinon  $A = \{a_0\}$  serait majorée. On note  $a_1$  le plus petit élément de  $A_1$  et on pose  $f(1) = a_1 > f(0) = a_0$ . Par récurrence, suivant le même procédé, on va construire une suite strictement croissante  $(a_n)$  d'éléments de  $A$ . Si l'on a déjà déterminé

$$a_0 < a_1 < \dots < a_{n-1},$$

on pose

$$A_n = A \setminus \bigcup_{i=0}^{n-1} \{a_i\},$$

cet ensemble  $A_n$  est non vide sinon  $A$  serait majoré. On note  $a_n$  le plus petit élément de  $A_n$  et on pose  $f(n) = a_n$ . On définit ainsi une application de  $\mathbb{N}$  dans  $A$  strictement croissante donc injective. On montre que  $f$  est surjective : soit  $a \in A$ , on pose

$$K_a = \{n \in \mathbb{N}, a_n \geq a\},$$

comme pour tout entier  $n$ ,  $a_n \geq n$  ( par récurrence), on en déduit que  $K_a$  est non vide donc admet un plus petit élément  $p$ . On a

$$a_p \geq a > a_{p-1}.$$

Comme  $a > a_{p-1}$ ,  $a \in A \setminus \bigcup_{i=1}^{p-1} \{a_i\}$ , par définition de  $a_p$ ,  $a \geq a_p$  d'où  $a = a_p = f(p)$ . Par conséquent  $f$  est bijective donc  $A$  dénombrable. ■

**Remarque 5.2.6** On peut résumer ce théorème en disant que les ensembles dénombrables sont les plus petits ensembles infinis.

**Corollaire 5.2.7** Un ensemble  $E$  est au plus dénombrable si et seulement si il existe une injection de  $E$  dans  $\mathbb{N}$ .

**Preuve** On se limite au cas où  $E$  est non vide. Si  $E$  est au plus dénombrable, alors

- soit  $E$  est fini, on pose  $g = i_n \circ f^{-1}$  où  $f$  est une bijection de  $\llbracket 1, n \rrbracket$  dans  $E$  et  $i_n$  l'injection canonique de  $\llbracket 1, n \rrbracket$  dans  $\mathbb{N}$ . L'application  $g$  est une injection de  $E$  dans  $\mathbb{N}$ .
- soit  $E$  est dénombrable, alors il existe une bijection de  $E$  dans  $\mathbb{N}$  qui est aussi une injection.

Réciproquement si il existe une injection notée  $f$  de  $E$  dans  $\mathbb{N}$ . Alors  $E$  est en bijection avec  $f(E)$  qui est une partie de  $\mathbb{N}$ . D'après la proposition précédente,  $f(E)$  est soit finie soit dénombrable donc  $E$  est au plus dénombrable.

■

**Proposition 5.2.8**  $\mathbb{N} \times \mathbb{N}$  est dénombrable.

**Preuve** La démonstration la plus rapide de ce résultat repose sur l'arithmétique : on considère l'application  $f$  définie de  $\mathbb{N} \times \mathbb{N}$  dans  $\mathbb{N}$  par

$$\forall (n, p) \in \mathbb{N} \times \mathbb{N}, f(n, p) = 2^n 3^p.$$

Comme  $f$  est injective,  $\mathbb{N} \times \mathbb{N}$  est au plus dénombrable et comme  $\mathbb{N} \times \mathbb{N}$  est infini,  $\mathbb{N} \times \mathbb{N}$  est dénombrable.

■

**Proposition 5.2.9** Pour tout entier  $k$  non nul, le produit cartésien de  $k$  ensembles dénombrables est dénombrable.

**Preuve** Il suffit de faire la démonstration pour  $k = 2$ , puis on conclut par récurrence sur  $k$ . Soit  $E$  et  $F$  deux ensembles dénombrables, on note  $f$  une bijection de  $\mathbb{N}$  dans  $E$  et  $g$  une bijection de  $\mathbb{N}$  dans  $F$ , alors on définit l'application  $h$  de  $\mathbb{N} \times \mathbb{N}$  dans  $E \times F$  par

$$\forall (n, p) \in \mathbb{N} \times \mathbb{N}, h(n, p) = (f(n), g(p)).$$

Comme  $h$  est une bijection et comme  $\mathbb{N} \times \mathbb{N}$  est dénombrable,  $E \times F$  est dénombrable

■

**Proposition 5.2.10** Une réunion dénombrable d'ensembles dénombrables est dénombrable c'est-à-dire si  $I$  est un ensemble d'indices dénombrable, et si pour tout  $i$  dans  $I$ ,  $E_i$  est un ensemble dénombrable, alors  $E = \bigcup_{i \in I} E_i$  est dénombrable.

**Preuve** Nous ne donnons la démonstration que dans le cas où  $I$  est un ensemble fini. Pour cela, on raisonne par récurrence sur le cardinal de  $I$ . Donc on montre que l'union de deux ensembles dénombrables  $E$  et  $F$  est dénombrable, puis on conclut par récurrence. Pour commencer on se ramène à une union disjointe c'est-à-dire

$$E \cup F = E \cup F' \quad \text{où } F' = F \setminus E.$$

On définit une application  $h$  par

$$\forall x \in E \cup F, h(x) = \begin{cases} (1, f(x)) & \text{si } x \in E, \\ (2, g(x)) & \text{si } x \in F'. \end{cases}$$

où  $f$  et  $g$  sont des bijections respectivement de  $E$  et  $F$  sur  $\mathbb{N}$ . L'application  $h$  est à valeurs dans  $\{1, 2\} \times \mathbb{N}$  et est injective. Comme  $\{1, 2\} \times \mathbb{N}$  est dénombrable,  $E \cup F$  est au plus dénombrable. De plus  $E \cup F$  contient  $E$  un ensemble infini donc  $E \cup F$  est dénombrable.

■

**Proposition 5.2.11** *L'ensemble  $Q$  des rationnels est dénombrable.*

*Par contre l'ensemble  $E$  des suites de  $\{0, 1\}$  est non dénombrable.*

*De même l'ensemble des réels  $\mathbb{R}$  et  $\mathcal{P}(\mathbb{N})$ , l'ensemble des parties de  $\mathbb{N}$ , ne sont pas dénombrables.*

**Preuve** Tout rationnel strictement positif s'écrit de façon unique sous la forme  $\frac{p}{q}$  où  $p$  et  $q$  sont des entiers non nuls, ce qui revient à dire que l'application  $f$  définie de  $Q^{+*}$  dans  $\mathbb{N} \times \mathbb{N}$  est injective. On en déduit que  $Q^{+*}$  est dénombrable d'où  $Q = \{0\} \cup Q^{+*} \cup Q^{-*}$  est dénombrable.

Pour le deuxième point, on raisonne par l'absurde donc on suppose  $E$  dénombrable : soit  $f$  une bijection de  $\mathbb{N}$  dans  $E$ , alors pour tout entier  $i$ ,  $f(i)$  est une suite de 0 ou de 1. On construit une suite de  $E$  notée  $u = (u_n)_{n \in \mathbb{N}}$  définie par

$$u_n = \begin{cases} 1 & \text{si } f(n)_n = 0, \\ 0 & \text{si } f(n)_n = 1, \end{cases}$$

Comme  $f$  est bijective, il existe un entier  $k$  tel que  $u = f(k)$  ce qui est impossible car ces deux suites diffèrent à l'indice  $k$ . Donc l'ensemble  $E$  des suites de  $\{0, 1\}$  est non dénombrable.

On admet les résultats suivants : l'ensemble des réels  $\mathbb{R}$  et  $\mathcal{P}(\mathbb{N})$ , l'ensemble des parties de  $\mathbb{N}$ , ne sont pas dénombrables. ■

# Chapitre 6

## Les nombres complexes

### 6.1 Définitions élémentaires

**Définition 6.1.1** On appelle **nombre complexe** toute expression de la forme  $z = x + iy$ , où  $x$  et  $y$  sont des réels et où  $i$  est un nombre tel que  $i^2 = -1$ . L'écriture  $z = x + iy$  s'appelle l'écriture algébrique de  $z$ . La **partie réelle** de  $z$ , noté  $\operatorname{Re}(z)$ , est le nombre réel  $x$  et la **partie imaginaire** de  $z$ , noté  $\operatorname{Im}(z)$ , le nombre réel  $y$  :

$$\text{si } z = x + iy \quad \text{alors} \quad \operatorname{Re}(z) = x \quad \text{et} \quad \operatorname{Im}(z) = y.$$

Un nombre complexe est **imaginaire pur** si sa partie réelle est nulle. Un nombre complexe est dit **réel** si sa partie imaginaire est nulle. L'ensemble des nombres complexes est noté  $\mathbb{C}$ .

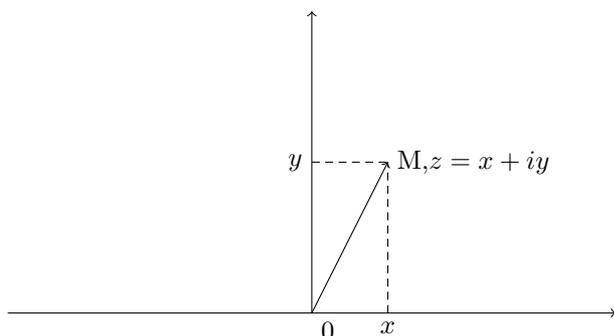
Nous donnons une interprétation géométrique des nombres complexes. On considère le plan muni d'une base orthonormée  $(O, \vec{i}, \vec{j})$ .

**Définition 6.1.2** Soit  $z = x + iy$  un nombre complexe.

- Le point d'affixe  $z$  est le point  $M$  du plan de coordonnées  $(x, y)$ .
- Le vecteur d'affixe  $z$  est le vecteur  $\vec{v}$  de coordonnées  $(x, y)$ .

Réciproquement,

- A tout point  $M$  du plan, de coordonnées  $(x, y)$ , on peut associer le nombre complexe  $z = x + iy$ . Le point  $M$  a alors pour affixe  $z$ .
- De même, à tout vecteur  $\vec{v}$  de coordonnées  $(x, y)$ , on peut associer le nombre complexe  $z = x + iy$ . Le vecteur  $\vec{v}$  a alors pour affixe  $z$ .



**Proposition 6.1.3** On dit que deux nombres complexes  $z = x + iy$  et  $z' = x' + iy'$  sont égaux si leurs parties réelles et leurs parties imaginaires sont égales :

$$z = z' \Leftrightarrow x = x' \text{ et } y = y'$$

**Définition 6.1.4 Somme et Produit de deux complexes.**

Dans  $\mathbb{C}$  on définit les opérations suivantes :

1. **Addition :** Si  $z = x + iy$  et  $z' = x' + iy'$  sont deux nombres complexes, la somme  $z + z'$  est le nombre complexe défini par

$$z + z' = (x + x') + i(y + y')$$

2. **Produit :** Si  $z = x + iy$  et  $z' = x' + iy'$  sont deux nombres complexes, le produit  $z.z'$  est le nombre complexe défini par

$$z.z' = (xx' - yy') + i(xy' + x'y)$$

Voici quelques propriétés élémentaires de l'addition :

**Proposition 6.1.5** Supposons que  $z$ ,  $z'$  et  $z''$  sont des nombres complexes. Alors

1. **Associativité :**  $z + (z' + z'') = (z + z') + z''$
2. **Commutativité :**  $z + z' = z' + z$
3. **Existence d'un élément neutre :** 0 est l'élément neutre pour l'addition :  $0 + z = z + 0 = z$ .
4. **Existence d'un opposé :** si  $z = x + iy$ , alors le nombre complexe  $(-z) = (-x) + i(-y)$  vérifie :  $z + (-z) = (-z) + z = 0$ .

Ces résultats sont de simples applications de résultats symétriques dans  $\mathbb{R}$ . Nous ne les démontrons donc pas.

**Interprétation de la somme de nombres complexes :**

- Si le vecteur  $\vec{v}_1$  a pour affixe  $z_1$  et le vecteur  $\vec{v}_2$  a pour affixe  $z_2$ , alors le vecteur  $\vec{v}_1 + \vec{v}_2$  a pour affixe  $z_1 + z_2$ .
- Si le point  $M_1$  a pour affixe  $z_1$  et le point  $M_2$  a pour affixe  $z_2$ , alors le vecteur  $\overrightarrow{M_1 M_2}$  a pour affixe  $z_2 - z_1$ .

Nous énonçons maintenant les propriétés élémentaires du produit :

**Proposition 6.1.6** *Supposons que  $z, z'$  et  $z''$  sont des nombres complexes.*

1. **Associativité** :  $z.(z'.z'') = (z.z').z''$
2. **Commutativité** :  $z.z' = z'.z$
3. **Distributivité** :  $(z + z').z'' = z.z'' + z'.z''$
4. **Existence d'un élément neutre** : le nombre complexe 1 est l'élément neutre pour le produit :  $1.z = z.1 = z$ .
5. **Existence d'un inverse** : tout nombre complexe **non nul**  $z$  admet un inverse pour le produit, noté  $\frac{1}{z}$ .
6. **0 est un élément absorbant** :  $0.z = z.0 = 0$ .

**Preuve** : Nous nous contentons de démontrer l'existence d'un inverse, le reste étant immédiat. Soit  $z = x + iy$  un complexe non nul. On prétend que le complexe  $z' = x' + iy'$  avec

$$x' = x/(x^2 + y^2) \text{ et } y' = -y/(x^2 + y^2)$$

est un inverse de  $z$ . En effet,

$$\begin{aligned} z.z' &= (xx' - yy') + i(xy' + yx') \\ &= (x^2/(x^2 + y^2) + y^2/(x^2 + y^2)) + i(xy/(x^2 + y^2) - xy/(x^2 + y^2)) = 1. \end{aligned}$$

Montrons maintenant qu'un tel inverse est unique. Si  $z_1$  et  $z_2$  sont deux inverses de  $z$ , alors on a  $z.z_1 = 1$ , ce qui entraîne, en multipliant par  $z_2$  à gauche, que

$$z_2 = z_2.1 = z_2.(z.z_1) = (z_2.z).z_1 = 1.z_1 = z_1.$$

Donc l'inverse est unique. ■

Une conséquence très importante de l'existence d'un inverse est la suivante :

**Corollaire 6.1.7** *Si  $z$  et  $z'$  sont deux nombres complexes, et si  $z.z' = 0$  alors soit  $z = 0$  soit  $z' = 0$ .*

*On dit que  $\mathbb{C}$  est intègre.*

**Preuve** : Il suffit de supposer par exemple que  $z$  est non nul, et de multiplier l'égalité  $z.z' = 0$  par  $1/z$ , ce qui donne  $z' = 0$ . Donc soit  $z = 0$ , soit  $z' = 0$ . ■

**Proposition 6.1.8 Formule du binôme de Newton.** *Supposons que  $z, z'$  sont des nombres complexes et  $n$  un entier naturel, on a*

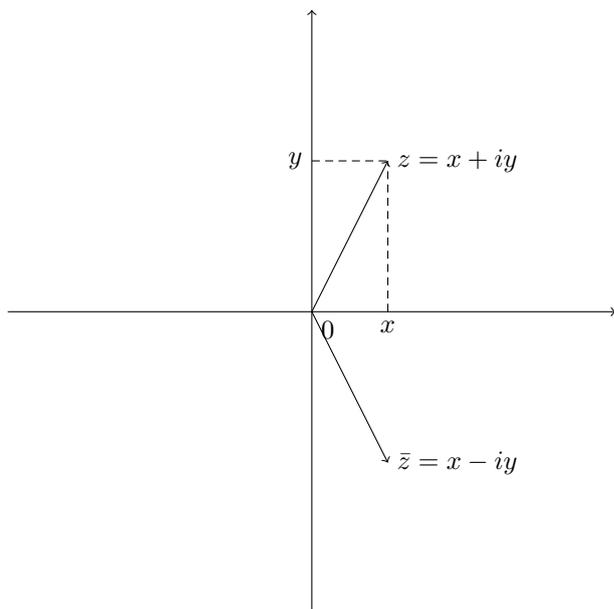
$$(z + z')^n = \sum_{k=0}^n \binom{n}{k} z^k z'^{n-k}.$$

## 6.2 Conjugué d'un nombre complexe

**Définition 6.2.1** Soit  $z = x + iy$  un nombre complexe. On appelle conjugué de  $z$  le nombre complexe noté  $\bar{z}$  de même partie réelle que  $z$  et de partie imaginaire opposée :

$$\text{si } z = x + iy, \quad \text{alors } \bar{z} = x - iy$$

Géométriquement, soit  $M$  le point d'affixe  $z$ , le point associé au conjugué de  $z$  est le symétrique de  $M$  par rapport à l'axe des abscisses.



**Proposition 6.2.2** Soient  $z$  et  $z'$  deux nombres complexes. Alors

1.  $\overline{\bar{z}} = z$
2.  $\overline{z + z'} = \bar{z} + \bar{z}'$
3.  $\overline{z \cdot z'} = \bar{z} \cdot \bar{z}'$
4.  $z$  est réel si et seulement si  $z = \bar{z}$
5.  $z$  est imaginaire pur si et seulement si  $\bar{z} = -z$ .
6.  $\operatorname{Re}(z) = \frac{z + \bar{z}}{2}$  et  $\operatorname{Im}(z) = \frac{z - \bar{z}}{2i}$ .

**Preuve :** La première assertion est évidente.

Montrons la troisième. Si  $z = x + iy$  et  $z' = x' + iy'$ , alors

$$\overline{z \cdot z'} = \overline{xx' - yy' + i(xy' + yx')} = xx' - yy' - i(xy' + yx'),$$

tandis que

$$\bar{z} \cdot \bar{z}' = (x - iy)(x' - iy') = xx' - yy' - i(xy' + yx'),$$

d'où l'égalité annoncée.

Nous laissons les assertions suivantes en exercice. ■

## 6.3 Module d'un nombre complexe

**Définition 6.3.1** Soit  $z = x + iy$  un nombre complexe. Le module de  $z$  est le réel, noté  $|z|$ , défini par

$$|z| = \sqrt{x^2 + y^2}.$$

On note  $U$  l'ensemble des complexes  $z$  de module 1.

Géométriquement, le module de  $z$  est la longueur du segment joignant l'origine au point d'affixe  $z$  et  $U$  est représenté par le cercle de centre l'origine et de rayon 1.

**Proposition 6.3.2** Soient  $z$  et  $z'$  deux nombres complexes. Alors

1.  $|z| \geq 0$  et on a l'équivalence :  $|z| = 0$  si et seulement si  $z = 0$ .
2.  $|z|^2 = z \cdot \bar{z}$  et, si  $z \neq 0$ ,  $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$
3.  $|z \cdot z'| = |z| |z'|$
4.  $|-z| = |z|$ ,  $|\bar{z}| = |z|$  et, si  $z \neq 0$ ,  $\left| \frac{1}{z} \right| = \frac{1}{|z|}$ .
5.  $|\operatorname{Re}(z)| \leq |z|$  et  $|\operatorname{Im}(z)| \leq |z|$
6. (Inégalité triangulaire)  $|z + z'| \leq |z| + |z'|$
7.  $||z| - |z'|| \leq |z - z'|$

**Preuve :** Dans toute la preuve on note  $z = x + iy$  et  $z' = x' + iy'$ .

1. Comme  $|z| = \sqrt{x^2 + y^2}$  et que, par définition, une racine est positive,  $|z| \geq 0$ .

Si  $z = 0$  alors il est clair que  $|z| = \sqrt{0^2 + 0^2} = 0$ . Réciproquement, si  $|z| = 0$ , alors on a  $x^2 + y^2 = 0$ . La somme du réel positif  $x^2$  et du réel positif  $y^2$  étant égale à zéro, on en déduit que  $x = y = 0$ . Donc  $z = 0$ .

2.  $z \cdot \bar{z} = (x + iy) \cdot (x - iy) = x^2 - i^2 y^2 = x^2 + y^2 = |z|^2$ .
3. On a, d'une part,

$$|z \cdot z'|^2 = (xx' - yy')^2 + (xy' + yx')^2 = x^2(x')^2 + y^2(y')^2 + x^2(y')^2 + y^2(x')^2$$

car les termes croisés se simplifient. D'autre part, on a

$$(|z| |z'|)^2 = (x^2 + y^2)((x')^2 + (y')^2) = x^2(x')^2 + y^2(y')^2 + x^2(y')^2 + y^2(x')^2.$$

D'où l'égalité désirée.

4. Laissez au lecteur en exercice
5. idem
6. On a

$$\begin{aligned} |z + z'|^2 &= (z + z') \cdot \overline{(z + z')} \\ &= (z + z') \cdot (\bar{z} + \bar{z}') \\ &= z \cdot \bar{z} + z \cdot \bar{z}' + \bar{z} \cdot z' + z' \cdot \bar{z}' \\ &= |z|^2 + 2\operatorname{Re}(z\bar{z}') + |z'|^2 \\ &\leq |z|^2 + 2|\operatorname{Re}(z\bar{z}')| + |z'|^2 \end{aligned}$$

car  $z \cdot \bar{z}' + \bar{z} \cdot z' = z \cdot \bar{z}' + \overline{z \cdot \bar{z}'}$ . Or

$$|\operatorname{Re}(z\bar{z}')| \leq |z\bar{z}'| = |z| |z'| = |z| |z'|.$$

Donc

$$|z + z'|^2 \leq |z|^2 + 2|z| |z'| + |z'|^2 = (|z| + |z'|)^2,$$

ce qui donne l'inégalité demandée.

7. On a  $|z| = |(z - z') + z'| \leq |z - z'| + |z'|$  d'après l'inégalité triangulaire. Donc  $|z| - |z'| \leq |z - z'|$ .  
En inversant les rôles de  $z$  et  $z'$ , on obtient de même que  $|z'| - |z| \leq |z - z'|$ . Ces deux inégalités impliquent le résultat désiré :  $||z| - |z' || \leq |z - z'|$ .

■

**Exercice 8** Montrer que  $U$  vérifie :

- i) si  $z$  et  $z'$  appartiennent à  $U$ , alors  $z.z'$  aussi,
- ii) si  $z$  appartient à  $U$ , alors  $z \neq 0$  et  $1/z$  appartient aussi à  $U$ .

**Exercice 9** Montrer que, si  $z \in \mathcal{C}$  avec  $z \neq 0$ , alors  $z/|z|$  appartient à  $U$ .

## 6.4 Argument d'un nombre complexe

**Définition 6.4.1 (Exponentielle complexe)** Pour tout nombre réel  $t$ , on note

$$e^{it} = \cos(t) + i \sin(t).$$

**Proposition 6.4.2** Soient  $z$  et  $z'$  deux nombres complexes. Alors, pour tout  $t \in \mathbb{R}$ , on a :

1.  $e^{it}$  appartient à  $U$ .
2.  $\frac{1}{e^{it}} = \overline{e^{it}} = e^{-it}$
3.  $e^{it} = 1$  si et seulement si il existe un entier relatif  $k$  tel que  $t = 2k\pi$ .
4. pour tout réel  $t'$ ,  $e^{i(t+t')} = e^{it} \cdot e^{it'}$
5. **Formule de Moivre** : pour tout entier relatif  $n$ , on a  $(e^{it})^n = e^{int}$
6. **formules d'Euler** :

$$\forall t \in \mathbb{R}, \cos(t) = \frac{e^{it} + e^{-it}}{2} \text{ et } \sin(t) = \frac{e^{it} - e^{-it}}{2i}.$$

**Remarque 6.4.3** Les propriétés précédentes expliquent, par analogie avec les propriétés de l'exponentielle dans  $\mathbb{R}$ , la notation  $e^{it}$ .

**Preuve de la proposition 6.4.2** : C'est une application directe des formules de trigonométrie.

1.  $|e^{it}| = \sqrt{\cos^2(t) + \sin^2(t)} = \sqrt{1} = 1$ .
2. Notons d'abord que  $e^{-it} = \cos(-t) + i \sin(-t) = \cos(t) - i \sin(t) = \overline{e^{it}}$  car  $\cos(-t) = \cos(t)$  et  $\sin(-t) = -\sin(t)$ . Montrons maintenant que  $e^{it} \cdot e^{-it} = 1$ , ce qui prouvera que  $e^{-it} = 1/e^{it}$ . En effet,  $e^{it} \cdot e^{-it} = e^{it} \overline{e^{it}} = |e^{it}|^2 = 1^2 = 1$ .
3.  $e^{it} = 1$  équivaut à  $\cos(t) = 1$  et  $\sin(t) = 0$ . Or il est bien connu que, si  $\cos(t) = 1$  et  $\sin(t) = 0$ , alors  $t = 0$  modulo  $2\pi$ , c'est-à-dire qu'il existe un entier relatif  $k$  tel que  $t = 2k\pi$ .
4. Calculons  $e^{it} \cdot e^{it'}$  :

$$e^{it} \cdot e^{it'} = (\cos(t) \cos(t') - \sin(t) \sin(t')) + i(\cos(t) \sin(t') + \sin(t) \cos(t')) = \cos(t+t') + i \sin(t+t') = e^{i(t+t')}.$$

5. Cela se démontre par récurrence, en utilisant le résultat précédent.
6. immédiat.

■

**Théorème 6.4.4** Pour tout nombre complexe  $z$  appartenant à  $U$ , il existe un réel  $t$  tel que

$$z = e^{it}$$

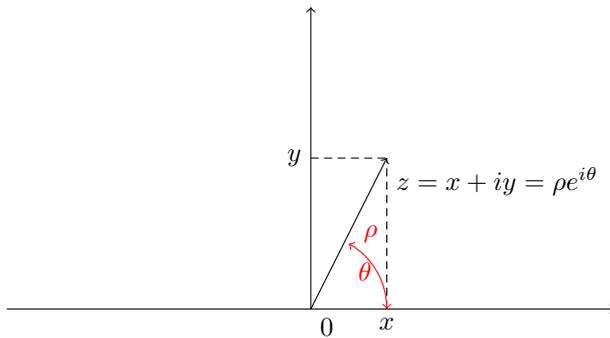
Ce théorème est admis. Autrement dit, l'application exponentielle, définie de  $\mathbb{R}$  dans  $U$  est surjective.

**Définition 6.4.5** Soit  $z$  un nombre complexe non nul. On appelle argument de  $z$  tout réel  $t$  tel que

$$\frac{z}{|z|} = e^{it}.$$

Tout argument de  $z$  est noté  $\arg(z)$ .

Dans le plan complexe, l'argument de  $z$  est l'angle entre l'axe des réels et le segment joignant l'origine au point d'affixe  $z$  orienté dans le sens inverse des aiguilles d'une montre.



**Remarque 6.4.6** Cette définition a bien un sens car nous avons vu dans un exercice ci-dessus que  $z/|z|$  appartient à  $U$ . Bien noter qu'il n'y a pas unicité de l'argument, puisque si  $t$  est un argument de  $z$ , alors  $t + 2k\pi$  est également un argument de  $z$  pour tout  $k \in \mathbb{Z}$ .

**Définition 6.4.7 Forme trigonométrique :** On dit qu'un nombre complexe non nul  $z$  est mis sous forme trigonométrique si on écrit  $z$  sous la forme :  $z = |z|e^{it}$ , avec  $t$  un argument de  $z$ .

**Proposition 6.4.8** Soient  $z$  un complexe non nul et  $t$  un argument de  $z$ . Alors un réel  $t'$  est un argument de  $z$  si et seulement s'il existe un entier relatif  $k$  tel que

$$t' = t + 2k\pi.$$

**Preuve :** Supposons d'abord que  $t'$  soit un argument de  $z$ . Alors, par définition de l'argument, on a

$$\frac{z}{|z|} = e^{it} = e^{it'}.$$

En divisant cette égalité par  $e^{it}$ , on obtient  $1 = e^{i(t'-t)}$ . Cette égalité implique l'existence d'un entier relatif  $k$  tel que  $t' = t + 2k\pi$  (cf. la proposition 6.4.2).

Réciproquement, s'il existe un entier relatif  $k$  tel que  $t' = t + 2k\pi$ , alors

$$e^{it'} = e^{it} = \frac{z}{|z|},$$

et  $t'$  est un argument de  $z$ . ■

**Proposition 6.4.9** Soient  $z$  et  $z'$  deux nombres complexes non nuls. Alors

1.  $\arg(-z) = \pi + \arg(z) \pmod{2\pi}$  et  $\arg(\bar{z}) = -\arg(z) \pmod{2\pi}$ ,
2.  $\arg(1/z) = -\arg(z) \pmod{2\pi}$ ,
3.  $\arg(z.z') = \arg(z) + \arg(z') \pmod{2\pi}$

**Preuve :**

1. Soit  $t$  un argument de  $-z$  et  $t'$  un argument de  $z$ . Montrons que  $t = \pi + t' \pmod{2\pi}$ . En effet, par définition de l'argument, on a :

$$e^{it} = \frac{-z}{|-z|} = -\frac{z}{|z|} = -e^{it'} = e^{i(t'+\pi)}.$$

Donc  $t' = t + \pi \pmod{2\pi}$  (cf. Proposition 6.4.2, 3).

Montrons que  $\arg(\bar{z}) = -\arg(z) \pmod{2\pi}$ . Soit  $t$  un argument de  $\bar{z}$  et  $t'$  un argument de  $z$ . Alors

$$e^{it} = \frac{\bar{z}}{|\bar{z}|} = \overline{\left(\frac{z}{|z|}\right)} = \overline{e^{it'}} = e^{-it'}$$

(on a utilisé le fait que  $|\bar{z}| = |z|$ ). Donc  $t = -t' \pmod{2\pi}$ .

2. Soit  $t$  un argument de  $1/z$  et  $t'$  un argument de  $z$ . Alors

$$e^{it} = \frac{1/z}{|1/z|} = \frac{1/z}{1/|z|} = \frac{1}{z/|z|} = \frac{1}{e^{it'}} = e^{-it'}$$

(on a utilisé le fait que  $|1/z| = 1/|z|$ ). Donc  $t = -t' \pmod{2\pi}$ .

3. Soient  $t$  un argument de  $z$ ,  $t'$  un argument de  $z'$  et  $t''$  un argument de  $z.z'$ . On a alors

$$e^{it''} = \frac{z.z'}{|z.z'|} = \frac{z}{|z|} \cdot \frac{z'}{|z'|} = e^{it} \cdot e^{it'} = e^{i(t+t')}$$

(on a utilisé le fait que  $|z.z'| = |z||z'|$ ). Donc  $t'' = t + t' \pmod{2\pi}$ . ■

**Définition 6.4.10 (Fonction Exponentielle)** Pour tout complexe  $z = x + iy$ , on note

$$e^z = e^x e^{iy}.$$

La fonction exponentielle ainsi définie sur  $\mathcal{C}$  prolonge la fonction exponentielle tout en conservant la propriété suivante :

**Proposition 6.4.11** Soient  $z$  et  $z'$  deux nombres complexes alors on a

$$e^z e^{z'} = e^{z+z'}.$$

## 6.5 Racines nièmes d'un nombre complexe

Dans toute cette partie,  $n$  désigne un entier naturel non nul.

**Définition 6.5.1** On dit qu'un nombre complexe  $z$  est une racine nième de l'unité (ou de 1) si  $z^n = 1$ .

**Exemple 6.5.2** Le nombre complexe  $i$  est racine quatrième de l'unité car  $i^4 = (-1)^2 = 1$ .

**Théorème 6.5.3** Il y a exactement  $n$  racines nièmes de l'unité. Ce sont les nombres complexes de la forme

$$\omega_k = e^{\frac{2ik\pi}{n}} = \omega_1^k \quad \text{où } k \in \{0, \dots, n-1\}.$$

**Preuve :** D'abord il est clair que les  $\omega_k$  définis ci-dessus sont des racines nièmes de l'unité. En effet,

$$\omega_k^n = \left( e^{\frac{2ik\pi}{n}} \right)^n = e^{2ik\pi} = 1.$$

Notons de plus que, si  $0 \leq k, k' \leq n-1$ , avec  $k \neq k'$ , alors  $\omega_k \neq \omega_{k'}$ . Il y a donc au moins  $n$  racines distinctes de l'unité.

Réciproquement, supposons qu'un nombre complexe  $z$  soit racine nième de l'unité. Montrons d'abord que  $z$  appartient à  $U$ . En effet, on a

$$1 = |z^n| = |z|^n.$$

Or le module est un nombre réel positif. Donc  $|z| = 1$ , i.e.,  $z \in U$ .

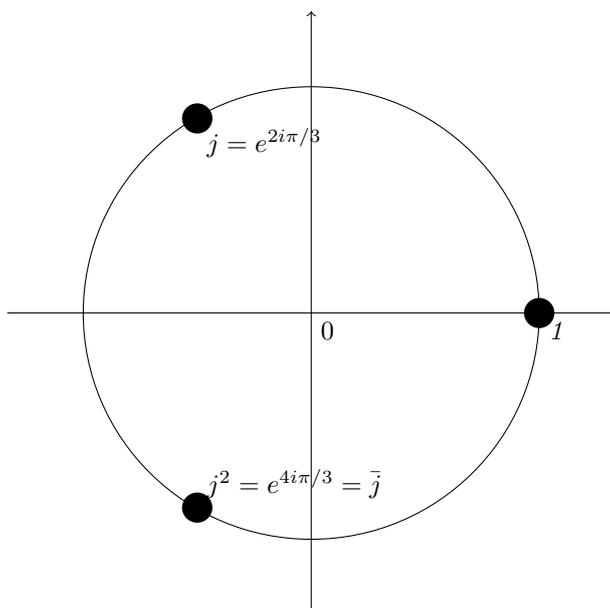
Comme  $z \in U$ , il existe un nombre réel  $t$  tel que  $z = e^{it}$ . Choisissons un entier  $k'$  tel que  $t + 2k'\pi$  soit positif. Notons que  $t' = t + 2k'\pi$  est un argument de  $z$ . Comme  $z$  est racine nième de l'unité, on a :  $z^n = 1 = e^{int'}$ . On déduit de la proposition 6.4.2 qu'il existe un entier relatif  $k$  tel que

$$nt' = 2k\pi.$$

Par conséquent, comme  $n \neq 0$ , cela donne  $t' = \frac{2k\pi}{n}$ . Comme  $t'$  est positif,  $k$  l'est aussi. Effectuons la division euclidienne de  $k$  par  $n$  : il existe deux entiers naturels  $p$  et  $r$ , tels que  $r \in \{0, \dots, n-1\}$  et  $k = pn + r$ . Alors, comme  $t' = 2p\pi + \frac{2r\pi}{n}$  est un argument de  $z$ , on déduit de la proposition 6.4.8 que  $\frac{2r\pi}{n}$  est un argument de  $z$ . D'où  $z = e^{\frac{2ir\pi}{n}}$  avec  $r \in \{0, \dots, n-1\}$ , ce qui est bien le résultat désiré. ■

**Exemple 6.5.4** Les racines cubiques de l'unité sont notées  $1$ ,  $j$  et  $j^2 = \bar{j}$  où

$$j = e^{\frac{2i\pi}{3}} \quad \text{et} \quad j^2 = e^{\frac{4i\pi}{3}}.$$



**Proposition 6.5.5** Somme des racines nièmes de l'unité. On a pour  $n \geq 2$

$$\sum_{k=0}^{n-1} \omega_k = 0.$$

Pour  $n = 3$ , on a  $1 + j + j^2 = 0$ .

**Preuve :** Il suffit d'appliquer le résultat sur la somme des termes d'une suite géométrique puisque  $\omega_1 \neq 1$

$$\sum_{k=0}^{n-1} \omega_k = \sum_{k=0}^{n-1} \omega_1^k = \frac{1 - \omega_1^n}{1 - \omega_1} = 0.$$

■

**Définition 6.5.6** Soit  $a$  un nombre complexe non nul. On dit qu'un nombre complexe  $z$  est une racine nième de  $a$  si  $z^n = a$ .

**Remarque 6.5.7** Dans le cas  $n = 2$  on parle de "racine carrée" ou même simplement de "racine" de  $a$ . Par contre, on n'écrit **jamais** cette racine sous la forme  $\sqrt{a}$  ni  $a^{\frac{1}{2}}$ .

**Corollaire 6.5.8** Pour tout nombre complexe non nul  $a$ , il existe exactement  $n$  racines nièmes de  $a$ . Ce sont les nombres complexes de la forme

$$z_k = |a|^{1/n} e^{\frac{it+2ik\pi}{n}} = |a|^{1/n} e^{\frac{it}{n}} \times \omega_k \quad \text{où } k \in \{0, \dots, n-1\},$$

et où  $t$  désigne un argument de  $a$ .

**Preuve :** Il est aisé de voir que, si  $z_k = |a|^{1/n} e^{\frac{it+2ik\pi}{n}}$  avec  $k \in \{0, \dots, n-1\}$ , alors  $z_k$  est une racine  $n$ ième de  $a$ .

Réciproquement, supposons que  $z$  soit une racine  $n$ ième de  $a$ . Alors le nombre complexe  $ze^{-it/n}/|a|^{\frac{1}{n}}$  est une racine  $n$ ième de l'unité, car

$$\left( \frac{ze^{-it/n}}{|a|^{\frac{1}{n}}} \right)^n = \frac{z^n e^{-it}}{|a|} = \frac{ae^{-it}}{|a|} = \frac{|a|e^{it}e^{-it}}{|a|} = 1,$$

car  $a = |a|e^{it}$  (forme trigonométrique). Donc, d'après le théorème 6.5.3, il existe un entier  $k \in \{0, \dots, n-1\}$  tel que

$$\frac{ze^{-it/n}}{|a|^{\frac{1}{n}}} = e^{\frac{2ik\pi}{n}}.$$

En multipliant l'égalité par  $e^{it/n}|a|^{\frac{1}{n}}$ , on obtient que  $z$  se met sous la forme désirée :

$$z = |a|^{1/n} e^{\frac{it+2ik\pi}{n}} \quad \text{où } k \in \{0, \dots, n-1\}.$$

■

## 6.6 Equation du second degré dans $\mathcal{C}$

On considère une équation du second degré dans  $\mathcal{C}$  :

$$(*) \quad az^2 + bz + c = 0$$

où  $a$ ,  $b$  et  $c$  sont des nombres complexes donnés avec  $a \neq 0$ , et  $z$  est l'inconnue.

**Théorème 6.6.1** Soit  $\Delta = b^2 - 4ac$ . Alors

— si  $\Delta \neq 0$ , alors l'équation (\*) admet exactement deux solutions distinctes  $z_1$  et  $z_2$  avec

$$z_1 = \frac{-b + \delta_1}{2a} \quad \text{et} \quad z_2 = \frac{-b + \delta_2}{2a},$$

où  $\delta_1$  et  $\delta_2$  sont les deux racines carrées du nombre complexe  $\Delta$ .

— si  $\Delta = 0$ , alors l'équation admet une solution unique  $z = \frac{-b}{2a}$ .

**Preuve :** Montrons d'abord qu'un nombre complexe  $z$  est solution de (\*) si et seulement si  $2az + b$  est une racine carrée de  $\Delta$ .

En effet, si  $z$  est solution de (\*), alors

$$(2az + b)^2 = 4a^2z^2 + 4abz + b^2 = 4a(az^2 + bz) + b^2 = 4a(-c) + b^2 = \Delta.$$

Réciproquement, si  $2az + b$  est une racine carrée de  $\Delta$ , alors

$$(2az + b)^2 = 4a^2z^2 + 4abz + b^2 = b^2 - 4ac,$$

ce qui implique, en simplifiant d'abord par  $b^2$  puis en divisant par  $4a$ , que

$$az^2 + bz + c = 0.$$

Donc  $z$  est bien solution de (\*).

Supposons maintenant que  $\Delta \neq 0$ . Alors il existe deux racines distinctes de  $\Delta$ , notées respectivement  $\delta_1$  et  $\delta_2$ . Un nombre complexe  $z$  est alors solution de (\*) si et seulement si  $2az + b$  est une racine carrée de  $\Delta$ , i.e., si et seulement si  $2az + b = \delta_j$  (avec  $j = 1$  ou  $j = 2$ ). En soustrayant  $b$  à cette égalité, puis en divisant par  $2a$  on obtient le résultat annoncé.

Si au contraire  $\Delta = 0$ , alors la seule racine carrée de  $\Delta$  est 0. Donc un nombre complexe  $z$  est solution de (\*) si et seulement si  $2az + b$  est nul. Ce qui donne bien une seule solution  $z = -b/2a$ .

■

**Exercice 10** Si  $a$ ,  $b$  et  $c$  sont des réels, alors si  $z$  est une solution,  $\bar{z}$  est aussi une solution.

## 6.7 Géométrie dans le plan complexe

**Théorème 6.7.1** Soit  $f$  une application de  $\mathbb{C}$  dans  $\mathbb{C}$ . On note  $F$  l'application du plan complexe dans lui-même qui au point d'affixe  $z$  associe le point d'affixe  $f(z)$ . Soit  $A$  un point du plan d'affixe  $z_A$ .

— **Translation** : L'application  $F$  est la translation du vecteur  $\overrightarrow{OA}$  si et seulement si

$$\forall z \in \mathbb{C}, f(z) = z + z_A.$$

— **Homothétie** : Soit  $\lambda$  un réel, l'application  $F$  est l'homothétie de centre  $A$  et de rapport  $\lambda$  si et seulement si

$$\forall z \in \mathbb{C}, f(z) = \lambda(z - z_A) + z_A.$$

— **Rotation** : Soit  $\theta$  un réel, l'application  $F$  est la rotation de centre  $A$  et d'angle  $\theta$  si et seulement si

$$\forall z \in \mathbb{C}, f(z) = e^{i\theta}(z - z_A) + z_A.$$

## Chapitre 7

# Les nombres entiers et les nombres rationnels

Nous supposons ici connues les règles de calcul sur  $\mathbb{N}$ ,  $\mathbb{Z}$  et  $\mathbb{Q}$ , ainsi que les propriétés de l'ordre sur ces ensembles.

Rappelons la propriété très importante suivante :  $\mathbb{N}$  (respectivement  $\mathbb{Z}$  ou  $\mathbb{Q}$ ) est **intègre** : si  $p_1$  et  $p_2$  appartiennent à  $\mathbb{N}$  (resp. à  $\mathbb{Z}$  ou à  $\mathbb{Q}$ ), et si  $p_1 p_2 = 0$ , alors  $p_1 = 0$  ou  $p_2 = 0$ .

### 7.1 Le principe de récurrence

**Définition 7.1.1** On dit qu'une partie non vide  $A$  de  $\mathbb{N}$  est **minorée** s'il existe un entier  $m$  tel que

$$\forall a \in A, m \leq a.$$

On dit que  $m$  est un **minorant** de  $A$ .

On dit qu'une partie non vide  $A$  de  $\mathbb{N}$  possède un **plus petit élément**  $\bar{a}$  si :

- i)  $\bar{a}$  appartient à  $A$ ,
- ii)  $\forall a \in A$ , on a :  $\bar{a} \leq a$ .

**Remarque 7.1.2** 1. Un tel élément, s'il existe, est nécessairement unique.

2. Si  $\bar{a}$  est le plus petit élément de  $A$ , alors

$$\forall a \in \mathbb{N}, \text{ avec } a < \bar{a}, \text{ on a } a \notin A.$$

Une propriété très importante de l'ensemble des entiers est la suivante :

**Théorème 7.1.3** Soit  $A$  une partie **non vide** de  $\mathbb{N}$ . Alors  $A$  possède un plus petit élément.

Ce théorème est admis.

**Définition 7.1.4** On dit qu'une partie non vide  $A$  de  $\mathbb{N}$  est **majorée** s'il existe un entier  $M$  tel que

$$\forall a \in A, a \leq M .$$

On dit que  $M$  est un **majorant** de  $A$ .

On dit qu'une partie non vide  $A$  de  $\mathbb{N}$  possède un **plus grand élément**  $\bar{a}$  si

i)  $\bar{a}$  appartient à  $A$ ,

ii)  $\forall a \in A$ , on a :  $\bar{a} \geq a$ .

**Corollaire 7.1.5** Toute partie non vide et majorée de  $\mathbb{N}$  possède un plus grand élément.

**Preuve :** Soit  $B$  le sous-ensemble de  $\mathbb{N}$  composé des majorants de  $A$  :

$$B = \{b \in \mathbb{N} \mid \forall a \in A, b \geq a\} .$$

Comme  $A$  est majoré,  $B$  est une partie non vide de  $\mathbb{N}$ . Donc, d'après le théorème 7.1.3,  $B$  possède un plus petit élément noté  $\bar{a}$ .

Montrons que  $\bar{a}$  est bien le plus grand élément de  $A$ . Pour cela, montrons d'abord que  $\bar{a}$  appartient à  $A$ . Raisonnons par l'absurde en supposant au contraire que  $\bar{a}$  n'appartient pas à  $A$ . Nous allons montrer qu'alors  $b = \bar{a} - 1$  appartient à  $B$ , ce qui contredit le fait que  $\bar{a}$  est le plus petit élément de  $B$ . En effet, comme  $\bar{a}$  appartient à  $B$ , on a : pour tout  $a \in A$ ,  $a \leq \bar{a}$ . Or  $\bar{a}$  n'appartient pas à  $A$ , donc en fait  $a < \bar{a}$ , ce qui montre que  $a \leq \bar{a} - 1 = b$ . On a donc prouvé que, pour tout  $a \in A$ ,  $a \leq b$ . Ceci montre que  $b$  appartient à  $B$ , et contredit le fait que  $\bar{a}$  est le plus petit élément de  $B$ .

Par conséquent, on a démontré que  $\bar{a}$  appartient à  $A$ . Comme  $\bar{a}$  appartient à  $B$ , il est clair que  $\bar{a}$  est un majorant de  $A$ . En conclusion,  $\bar{a}$  est bien le plus grand élément de  $A$ .

■

Voici le résultat le plus important de cette partie :

**Théorème 7.1.6 (Principe de récurrence)** Soit  $\mathcal{P} : \mathbb{N} \rightarrow \{0, 1\}$  une application possédant les propriétés suivantes :

a)  $\mathcal{P}(0) = 1$

b) pour tout  $n \in \mathbb{N}$ , si  $\mathcal{P}(n) = 1$ , alors  $\mathcal{P}(n+1) = 1$ .

Alors  $\mathcal{P}(n) = 1$  pour tout  $n \in \mathbb{N}$ .

**Remarque 7.1.7** En pratique,  $\mathcal{P}(n)$  désigne une propriété, dépendant de l'entier  $n$ , dont on veut montrer qu'elle est vraie pour tout entier  $n$ . L'expression  $\mathcal{P}(n) = 1$  signifie que la propriété est vraie, tandis que  $\mathcal{P}(n) = 0$  qu'elle est fausse.

**Preuve du théorème 7.1.6 :** On raisonne par l'absurde en supposant qu'il existe  $n_0 \in \mathbb{N}$  tel que  $\mathcal{P}(n_0) = 0$ . Soit

$$A = \{n \in \mathbb{N} \mid \mathcal{P}(n) = 0\} .$$

Par hypothèse,  $A$  est une partie non vide de  $\mathbb{N}$  car  $n_0$  appartient à  $A$ .

Donc  $A$  possède un plus petit élément  $\bar{a}$ . Notons que  $\bar{a}$  appartient à  $A$ , donc  $\mathcal{P}(\bar{a}) = 0$ , et que  $\bar{a} \geq 1$  car  $\mathcal{P}(0) = 1$  par hypothèse (a).

De plus, comme  $\bar{a}$  est le plus petit élément de  $A$ ,  $n = \bar{a} - 1$  (qui appartient à  $\mathbb{N}$ ) n'appartient pas à  $A$ . D'où  $\mathcal{P}(n) = 1$ . Mais l'hypothèse (b) implique alors que  $\mathcal{P}(n+1) = 1$ . On a trouvé une contradiction puisque  $n+1 = \bar{a}$ .

Ceci prouve que, pour tout  $n \in \mathbb{N}$ ,  $\mathcal{P}(n) = 1$ .

■

On montre exactement de la même façon le principe de récurrence généralisé, qui est souvent utile :

**Théorème 7.1.8 (Principe de récurrence généralisé)** Soit  $\mathcal{P} : \mathbb{N} \rightarrow \{0, 1\}$  une application possédant les propriétés suivantes :

a)  $\mathcal{P}(0) = 1$

b) pour tout  $n \in \mathbb{N}$ , si  $\{\forall k \leq n, \mathcal{P}(k) = 1\}$ , alors  $\mathcal{P}(n+1) = 1$ .

Alors  $\mathcal{P}(n) = 1$  pour tout  $n \in \mathbb{N}$ .

**Preuve :** Exercice.

## 7.2 La division euclidienne

**Définition 7.2.1** Soient  $a$  et  $b$  deux entiers relatifs. On dit que  $a$  divise  $b$  et on note  $a|b$  si

a)  $a$  n'est pas nul,

b) il existe un entier relatif  $k \in \mathbb{Z}$  tel que  $b = ka$ .

**Proposition 7.2.2** Soient  $a, b$  et  $c$  trois entiers relatifs.

1. si  $c \neq 0$ , alors  $a|b$  si et seulement si  $ac|bc$ ,
2. si  $a|b$ , alors  $(-a)|b$  et  $a|(-b)$ ,
3. si  $a|b$  et  $a|c$ , alors  $a|(b+c)$ .
4. si  $a|b$  et  $b|a$ , alors  $a = b$  ou  $a = -b$ .
5. si  $ab|c$  alors  $a|c$  et  $b|c$ .
6. si  $a \in \mathbb{N}^*$  et  $b \in \mathbb{N}$ , avec  $a|b$ , alors soit  $b = 0$  soit  $a \leq b$ .

**Preuve :** Cette proposition est une conséquence immédiate de la définition de la division. Nous la laissons en exercice. ■

**Théorème 7.2.3 (Division euclidienne)** Soient  $a$  et  $b$  deux entiers naturels, avec  $a$  non nul. Il existe alors un unique couple  $(q, r) \in \mathbb{N}^2$  tel que

$$b = qa + r \quad \text{et} \quad 0 \leq r < a .$$

$q$  est appelé **quotient** de la division euclidienne tandis que  $r$  s'appelle **le reste**.

**Preuve**

— **Preuve de l'unicité :** Montrons d'abord que le couple  $(q, r)$ , s'il existe, est unique. Pour cela, on suppose qu'il existe deux couples  $(q_1, r_1) \in \mathbb{N}^2$  et  $(q_2, r_2) \in \mathbb{N}^2$  tels que l'égalité suivante soit satisfaite : pour  $j = 1$  et  $j = 2$ ,

$$b = q_j a + r_j \quad \text{et} \quad 0 \leq r_j < a .$$

Sans perte de généralité, on peut supposer que  $r_1 \leq r_2$  (dans le cas contraire, on échange le rôle de  $(q_1, r_1)$  et  $(q_2, r_2)$ ). Comme

$$b = q_1 a + r_1 = q_2 a + r_2, \quad \text{on a : } r_2 - r_1 = a(q_1 - q_2).$$

Donc  $r_2 - r_1$  est un entier naturel divisible par  $a$ . Mais, d'autre part,  $r_2 - r_1 \leq r_2$  (car  $r_1 \geq 0$ ) et  $r_2 < a$ . Comme  $a > 0$ ,  $a|(r_2 - r_1)$  et  $a > (r_2 - r_1)$ , on a  $r_2 - r_1 = 0$ . Cette égalité, conjuguée avec l'égalité  $r_2 - r_1 = a(q_1 - q_2)$  et le fait que  $a \neq 0$  implique que  $q_1 = q_2$ . En conclusion, nous avons prouvé que, si le couple  $(q, r)$  existe, il est unique.

— **Preuve de l'existence :** Nous montrons maintenant son existence. Pour cela, on considère le sous-ensemble  $A$  de  $\mathbb{N}$  défini par

$$A = \{p \in \mathbb{N} \mid ap > b\}.$$

Notons d'abord que l'ensemble  $A$  n'est pas vide. En effet, le nombre entier  $b + 1$  appartient à  $A$  car  $a \geq 1$ , et donc  $a(b + 1) \geq b + 1 > b$ .

Par conséquent, l'ensemble  $A$  possède un plus petit élément  $\bar{p}$ . Posons  $q = \bar{p} - 1$  et  $r = b - aq$ . Comme  $0$  n'appartient pas à  $A$ , on a  $q \geq 0$ . Comme l'égalité  $b = aq + r$  est évidente d'après la définition de  $q$  et  $r$ , il reste à montrer que  $0 \leq r < a$ .

Notons d'abord que  $r \geq 0$ . En effet, comme  $\bar{p}$  est le plus petit élément de  $A$ ,  $q = \bar{p} - 1$  n'appartient pas à  $A$ , i.e.,  $aq \leq b$ . D'où  $r \geq 0$ .

Montrons enfin que  $r < a$ . En effet, comme  $\bar{p}$  appartient à  $A$ , on a  $a\bar{p} > b$ . D'où  $a(q + 1) > b$ , ce qui implique que  $r = b - aq < a$ .

■

### 7.3 Le ppcm d'une famille d'entiers

**Définition 7.3.1 (PPCM)** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . On appelle plus petit commun multiplicateur (ppcm) de  $\{a_1, \dots, a_n\}$  l'unique entier  $\mu \in \mathbb{N}^*$  tel que

a)  $\forall i = 1, \dots, n, a_i | \mu$ ,

b)  $\forall k \in \mathbb{N}^*,$  si  $\{\forall i = 1, \dots, n, a_i | k\}$ , alors  $\mu | k$ .

Le ppcm de  $\{a_1, \dots, a_n\}$  est noté  $\text{ppcm}\{a_1, \dots, a_n\}$ .

Montrons l'existence du  $\text{ppcm}\{a_1, \dots, a_n\}$ .

**Théorème 7.3.2** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . Le ppcm de  $\{a_1, \dots, a_n\}$  existe et est unique. C'est le plus petit multiple commun à  $a_1, \dots, a_n$ .

**Preuve :** Soit  $A$  l'ensemble des entiers naturels non nuls multiples communs à tous les  $a_i$  :

$$A = \{k \in \mathbb{N}^* \mid \forall i = 1, \dots, n, a_i | k\}.$$

L'ensemble  $A$  est non vide car il contient l'entier  $|a_1 \dots a_n|$ . Donc  $A$  possède un plus petit élément noté  $\mu$ . Montrons que  $\mu$  est bien le ppcm de  $\{a_1, \dots, a_n\}$ .

Comme  $\mu$  appartient à  $A$ ,  $\mu$  est non nul et vérifie la condition (a) de la définition. Pour montrer que  $\mu$  vérifie aussi (b), il suffit de montrer que  $\mu$  divise  $k$  pour tout  $k$  appartenant à  $A$ .

On raisonne par l'absurde en supposant qu'il existe  $k$  dans  $A$  qui n'est pas divisible par  $\mu$ . Soient  $q$  et  $r$  respectivement le quotient et le reste de la division euclidienne de  $k$  par  $\mu$ . On a  $k = q\mu + r$  et  $0 < r < \mu$ . Comme, pour tout  $i = 1, \dots, n$ ,  $a_i$  divise  $k$  et  $\mu$ ,  $a_i$  divise  $r$ . Donc  $r$  appartient à  $A$ , ce qui

contredit le fait que  $\mu$  est le plus petit élément de  $A$ . Donc  $\mu$  divise  $k$  pour tout  $k$  dans  $A$ . On a montré l'existence du ppcm de  $\{a_1, \dots, a_n\}$ .

Montrons l'unicité du ppcm. Si  $\mu_1$  et  $\mu_2$  sont deux ppcm de  $\{a_1, \dots, a_n\}$ , alors  $\mu_1$  divise  $\mu_2$  et  $\mu_2$  divise  $\mu_1$  (c'est la propriété (b) de la définition). Donc, d'après la proposition 7.2.2, on a  $\mu_1 = \mu_2$  ou  $\mu_1 = -\mu_2$ . Comme  $\mu_1$  et  $\mu_2$  sont strictement positifs, la seule égalité possible est  $\mu_1 = \mu_2$ . Le ppcm est donc unique. ■

Voici quelques propriétés du ppcm :

**Proposition 7.3.3**

i) Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$  et  $\alpha \in \mathbb{Z}^*$ . Alors

$$\text{ppcm}\{\alpha a_1, \dots, \alpha a_n\} = |\alpha| \text{ppcm}\{a_1, \dots, a_n\}.$$

ii) Si  $a$  et  $b$  sont deux entiers relatifs non nuls, avec  $a|b$ , alors

$$\text{ppcm}\{a, b\} = |b|.$$

**Preuve :** i) Appelons  $\mu$  le ppcm de  $\{a_1, \dots, a_n\}$ . Il faut montrer que  $|\alpha|\mu$  est le ppcm de  $\{\alpha a_1, \dots, \alpha a_n\}$ .

Comme, pour tout  $i = 1, \dots, n$ ,  $a_i$  divise  $\mu$ , on a que  $\alpha a_i$  divise  $|\alpha|\mu$ . Donc  $|\alpha|\mu$  vérifie le (a) de la définition du ppcm.

Soit  $k \in \mathbb{N}^*$  tel que, pour tout  $i = 1, \dots, n$ ,  $\alpha a_i$  divise  $k$ . Alors  $\alpha$  divise  $k$  (cf proposition 7.2.2), et donc  $|\alpha|$  divise aussi  $k$ . Posons  $k' = \frac{k}{|\alpha|}$ . Notons que  $k'$  appartient à  $\mathbb{N}^*$  car  $k \in \mathbb{N}^*$ .

Comme, pour tout  $i = 1, \dots, n$ ,  $\alpha a_i$  divise  $k = |\alpha|k'$ , on en déduit que  $a_i$  divise  $k'$ . De plus,  $\mu$  étant le ppcm de  $\{a_1, \dots, a_n\}$ , la propriété (b) de la définition du ppcm implique que  $\mu$  divise  $k'$ . Donc  $\alpha\mu$  divise  $k = |\alpha|k'$ . Par conséquent,  $|\alpha|\mu$  vérifie la condition (b) de la définition du ppcm.

ii) Pour montrer que  $\text{ppcm}\{a, b\} = |b|$ , posons  $\mu = |b|$ . Alors  $a$  et  $b$  divisent clairement  $\mu$ , qui vérifie (a) de la définition du ppcm.

Soit maintenant  $k$  tel que  $a$  et  $b$  divisent  $k$ . Alors  $\mu = |b|$  divise aussi  $k$ . D'où  $\mu$  vérifie le (b) de la définition du ppcm. ■

## 7.4 Le pgcd d'une famille d'entiers

**Définition 7.4.1 (PGCD)** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . On appelle plus grand commun diviseur (pgcd) de  $\{a_1, \dots, a_n\}$  l'unique entier  $\mu \in \mathbb{N}^*$  tel que

a)  $\forall i = 1, \dots, n, \mu|a_i$ ,

b)  $\forall k \in \mathbb{N}^*$ , si  $\{\forall i = 1, \dots, n, k|a_i\}$ , alors  $k|\mu$ .

Le pgcd de  $\{a_1, \dots, a_n\}$  est noté  $\text{pgcd}\{a_1, \dots, a_n\}$

**Théorème 7.4.2** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . Le pgcd de  $\{a_1, \dots, a_n\}$  existe et est unique.

**Preuve de l'unicité :** L'unicité du pgcd est claire puisque, si  $\mu_1$  et  $\mu_2$  sont deux pgcd de  $\{a_1, \dots, a_n\}$ , alors  $\mu_1$  et  $\mu_2$  se divisent l'un l'autre, et, étant positifs, sont donc égaux. ■

Le lemme suivant montre l'existence du pgcd :

**Lemme 7.4.3** Soient  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$  et  $\mathcal{I}$  le sous-ensemble de  $\mathbb{N}^*$  défini par

$$\mathcal{I} = \{m \in \mathbb{N}^* \mid \exists (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \text{ tels que } m = \alpha_1 a_1 + \dots + \alpha_n a_n\}.$$

Alors  $\mathcal{I}$  est non vide, et le plus petit élément de  $\mathcal{I}$  est le pgcd de  $\{a_1, \dots, a_n\}$ .

**Preuve :** L'ensemble  $\mathcal{I}$  est non vide car, par exemple  $a_1^2$  appartient à  $\mathcal{I}$  (prendre  $\alpha_1 = a_1$ ,  $\alpha_2 = \dots = \alpha_n = 0$ ). Notons  $\mu$  le plus petit élément de la partie  $\mathcal{I}$ .

Comme  $\mu$  appartient à  $\mathcal{I}$ , il existe  $\alpha_1, \dots, \alpha_n$  tels que  $\mu = \alpha_1 a_1 + \dots + \alpha_n a_n$ . Vérifions que  $\mu$  satisfait (a) de la définition du pgcd. Pour cela, on raisonne par l'absurde en supposant qu'il existe  $i \in \{1, \dots, n\}$  tel que  $\mu$  ne divise pas  $a_i$ . Soit  $q$  et  $r$  respectivement le quotient et le reste de la division euclidienne de  $a_i$  par  $\mu$  :  $a_i = q\mu + r$  et  $0 < r < \mu$ . Alors  $r$  appartient à  $\mathcal{I}$  car  $r \in \mathbb{N}^*$  et

$$r = a_i - q\mu = (-\alpha_1 q)a_1 + \dots + (-\alpha_{i-1} q)a_{i-1} + (1 - \alpha_i q)a_i + (-\alpha_{i+1} q)a_{i+1} + \dots + (-\alpha_n q)a_n.$$

Mais d'autre part  $\mu > r$  et  $\mu$  est le plus petit élément de  $\mathcal{I}$ . On a donc trouvé une contradiction. Par conséquent  $\mu$  divise tous les  $a_i$ ,  $i = 1, \dots, n$ .

Reste à prouver que  $\mu$  satisfait la partie (b) de la définition du pgcd. Pour cela, considérons  $k$  un diviseur commun à tous les  $a_i$ . Il est clair alors que  $k$  divise tous les éléments de  $\mathcal{I}$ . Comme  $\mu$  appartient à  $\mathcal{I}$ ,  $k$  divise donc  $\mu$ . ■

Le lemme que nous venons de montrer montre aussi le corollaire suivant, qui sera très important pour prouver le théorème de Bezout :

**Corollaire 7.4.4** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . Il existe alors des entiers relatifs  $\alpha_1, \dots, \alpha_n$  tels que

$$\text{pgcd}(a_1, \dots, a_n) = \alpha_1 a_1 + \dots + \alpha_n a_n.$$

Voici maintenant quelques propriétés du pgcd qui seront utiles plus tard :

**Proposition 7.4.5**

i) Soient  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$  et  $\alpha$  un entier relatif non nul. Alors

$$\text{pgcd}\{\alpha a_1, \dots, \alpha a_n\} = |\alpha| \text{pgcd}\{a_1, \dots, a_n\}.$$

ii) Si  $a$  et  $b$  sont deux entiers relatifs non nuls tels que  $a|b$ , alors

$$\text{pgcd}(a, b) = |a|.$$

**Preuve :** i) Posons  $\mu = \text{pgcd}\{a_1, \dots, a_n\}$  et  $\mu' = \text{pgcd}\{\alpha a_1, \dots, \alpha a_n\}$ . Il faut montrer que  $|\alpha|\mu = \mu'$ .

On remarque d'abord que  $|\alpha|\mu$  est un diviseur commun à  $\alpha a_1, \dots, \alpha a_n$ , car  $\mu$  est un diviseur commun à  $a_1, \dots, a_n$ . Donc  $|\alpha|\mu$  divise  $\mu'$ . Il existe donc  $k \in \mathbb{N}^*$  avec  $\mu' = |\alpha|\mu k$ .

Comme  $\mu'$  est le pgcd de  $\{\alpha a_1, \dots, \alpha a_n\}$ ,  $\mu' = |\alpha|\mu k$  est un diviseur commun à  $\alpha a_1, \dots, \alpha a_n$ , ce qui implique que  $\mu k$  est un diviseur commun à  $a_1, \dots, a_n$ . Or  $\mu$  étant le pgcd à  $\{a_1, \dots, a_n\}$ , cela entraîne que  $\mu k$  divise  $\mu$ . Or  $\mu > 0$  et  $\mu k > 0$ , donc  $k = 1$ . On a donc prouvé que  $\mu' = |\alpha|\mu$ .

ii) Posons  $\mu = \text{pgcd}\{a, b\}$ . Comme  $|a|$  divise à la fois  $a$  et  $b$ ,  $|a|$  divise  $\mu$ . De plus,  $\mu$  divise  $a$ , donc divise  $|a|$ . Ceci prouve que  $\mu = |a|$ .

■

La proposition suivante affirme que l'on peut toujours ramener le calcul du pgcd de  $n$  entiers à  $n$  calculs du pgcd de 2 entiers.

**Proposition 7.4.6** Soient  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ , avec  $n \geq 3$ . Alors

$$\text{pgcd}\{a_1, \dots, a_n\} = \text{pgcd}\{a_1, \text{pgcd}\{a_2, \dots, a_n\}\} .$$

**Preuve :** Posons  $\mu = \text{pgcd}\{a_1, \dots, a_n\}$ ,  $\mu' = \text{pgcd}\{a_2, \dots, a_n\}$  et  $\mu'' = \text{pgcd}\{a_1, \mu'\}$ . On veut montrer que  $\mu = \mu''$ .

Montrons d'abord que  $\mu$  divise  $\mu''$ . Comme  $\mu$  est un diviseur commun à  $a_2, \dots, a_n$ ,  $\mu$  divise  $\mu'$ . Comme de plus,  $\mu$  divise  $a_1$ ,  $\mu$  divise le pgcd de  $a_1$  et de  $\mu'$ , i.e., divise  $\mu''$ .

Réciproquement,  $\mu''$  divise à la fois  $a_1$  et  $\mu'$ . Or  $\mu'$  étant un diviseur commun à  $a_2, \dots, a_n$ ,  $\mu''$  est également un diviseur commun à  $a_2, \dots, a_n$ . Donc  $\mu''$  divise tous les  $a_i$ , avec  $i = 1, \dots, n$ , donc  $\mu''$  divise le pgcd de  $\{a_1, \dots, a_n\}$ , c'est-à-dire  $\mu$ .

En conclusion, les entiers naturels  $\mu$  et  $\mu''$  se divisent l'un l'autre, et sont donc égaux.

■

Voici maintenant le résultat principal de cette partie, qui justifie l'algorithme d'Euclide de calcul du pgcd, que nous introduisons après.

**Théorème 7.4.7** Soient  $a_1$  et  $a_2$  deux entiers naturels non nuls. Si  $a_2$  ne divise pas  $a_1$ , alors

$$\text{pgcd}\{a_1, a_2\} = \text{pgcd}\{a_2, r\}$$

où  $r$  est le reste de la division euclidienne de  $a_1$  par  $a_2$ .

**Preuve :** Soient  $q$  et  $r$  respectivement le quotient et le reste de la division euclidienne de  $a_1$  par  $a_2$  :  $a_1 = qa_2 + r$  et  $0 < r < a_2$ . Notons  $\mu = \text{pgcd}\{a_2, r\}$  et  $\mu' = \text{pgcd}\{a_1, a_2\}$ . Montrons que  $\mu = \mu'$ .

(a) Par définition,  $\mu|a_2$ . Comme  $\mu|r$  et  $\mu|a_2$ , on a aussi  $\mu|qa_2 + r = a_1$ . Donc  $\mu$  est un diviseur commun de  $a_2$  et de  $a_1$ . Donc  $\mu$  divise  $\mu'$  qui est le pgcd de  $a_1$  et  $a_2$ .

(b) Réciproquement,  $\mu'$  divise  $a_1$  et  $a_2$ , donc  $\mu'$  divise aussi  $a_1 - qa_2 = r$ . Par conséquent,  $\mu'$  divise le pgcd de  $a_2$  et de  $r$ , i.e., divise  $\mu$ .

En conclusion, les entiers naturels  $\mu$  et  $\mu'$  se divisent l'un l'autre, et sont donc égaux.

■

Décrivons maintenant l'**algorithme d'Euclide**. L'objet de l'algorithme est de calculer le pgcd de deux entiers naturels non nuls  $a_1$  et  $a_2$ .

— **Initialisation :** Posons  $r_1 = a_1$  et  $r_2 = a_2$

— tant que  $r_i > 0$ , on définit  $r_{i+1}$  comme étant le reste de la division euclidienne de  $r_{i-1}$  par  $r_i$ .

**Proposition 7.4.8** Soit  $(r_i)$  la suite définie par l'algorithme d'Euclide. Alors il existe un indice  $i_0 \leq a_2 + 2$  tel que  $r_{i_0} = 0$  et

$$\text{pgcd}\{a_1, a_2\} = r_{i_0-1} .$$

**Exemple :** Si  $a_1 = 48$  et  $a_2 = 30$ , alors  $r_1 = a_1 = 48$ ,  $r_2 = a_2 = 30$ , puis de  $48 = 30 \times 1 + 18$  on déduit  $r_3 = 48 - 1.30 = 18$ , ensuite  $r_4 = 30 - 1.18 = 12$ ,  $r_5 = 18 - 1.12 = 6$ ,  $r_6 = 12 - 2.6 = 0$ . Donc  $i_0 = 6$  et  $\text{pgcd}\{48, 30\} = \text{pgcd}\{30, 18\} = \text{pgcd}\{18, 12\} = \text{pgcd}\{12, 6\} = r_5 = 6$ .

**Preuve de la proposition 7.4.8 :** Par définition du reste de la division euclidienne, la suite  $(r_i)$  est strictement décroissante à partir du rang  $i = 2$ . On montre donc facilement par récurrence que  $r_i \leq a_2 - i + 2$  pour  $i \geq 2$ . Or  $r_i$  est positif pour tout  $i$ . L'algorithme s'arrête donc au plus tard en temps  $i_0 \leq r_2 + 2$ .

On démontre également par récurrence, en utilisant le théorème 7.4.7, que, pour tout  $i < i_0 - 1$ ,

$$(7.1) \quad \text{pgcd}\{a_1, a_2\} = \text{pgcd}\{r_{i-1}, r_i\} .$$

Or, par définition de  $i_0$ , l'entier  $r_{i_0-1}$  divise  $r_{i_0-2}$ . La proposition 7.4.5 affirme alors que

$$(7.2) \quad \text{pgcd}\{r_{i_0-2}, r_{i_0-1}\} = r_{i_0-1} .$$

En mettant ensembles les égalités (7.1) et (7.2), on obtient le résultat désiré :  $\text{pgcd}\{a_1, a_2\} = r_{i_0-1}$ . ■

## 7.5 Nombres premiers entre eux

**Définition 7.5.1** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . On dit que les nombres  $a_1, \dots, a_n$  sont premiers entre eux si leur pgcd est 1.

**Exemple :** Les nombres 30, 35 et 14 sont premiers entre eux. En effet, on a d'une part :  $\text{pgcd}\{35, 14\} = \text{pgcd}\{14, 7\} = 7$  d'après l'algorithme d'Euclide. D'autre part, on a

$$\text{pgcd}\{30, 35, 14\} = \text{pgcd}\{30, \text{pgcd}\{35, 14\}\} = \text{pgcd}\{30, 7\},$$

où  $\text{pgcd}\{30, 7\} = \text{pgcd}\{7, 2\} = \text{pgcd}\{2, 1\} = 1$  d'après l'algorithme d'Euclide. Donc on a montré que  $\text{pgcd}\{30, 35, 14\} = 1$ .

*Le théorème le plus important de cette partie, et un des plus importants de ce cours, est le théorème de Bezout :*

**Théorème 7.5.2 (Bezout)** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . Alors les nombres  $a_1, \dots, a_n$  sont premiers entre eux si et seulement si il existe  $n$  entiers relatifs  $\alpha_1, \dots, \alpha_n$  tels que

$$(7.3) \quad \alpha_1 a_1 + \dots + \alpha_n a_n = 1 .$$

On appelle **relation de Bezout** une relation du type (7.3).

**Preuve :** Supposons d'abord que  $a_1, \dots, a_n$  sont premiers entre eux. Comme le pgcd de  $a_1, \dots, a_n$  est 1, le corollaire 7.4.4 affirme qu'il existe  $n$  entiers relatifs  $\alpha_1, \dots, \alpha_n$  tels que  $\alpha_1 a_1 + \dots + \alpha_n a_n = 1$ .

Réciproquement, supposons qu'il existe  $n$  entiers relatifs  $\alpha_1, \dots, \alpha_n$  tels que  $\alpha_1 a_1 + \dots + \alpha_n a_n = 1$ . Soit  $\mu$  le pgcd de  $a_1, \dots, a_n$ . Comme  $\mu$  est un diviseur commun de  $a_1, \dots, a_n$ ,  $\mu$  divise également  $\alpha_1 a_1 + \dots + \alpha_n a_n$ , i.e.,  $\mu$  divise 1. Comme  $\mu > 0$ ,  $\mu$  ne peut être égal qu'à 1. En conclusion,  $a_1, \dots, a_n$  sont premiers entre eux. ■

### Comment trouver une relation de Bezout ?

En pratique, pour trouver une relation de Bezout, on utilise l'algorithme d'Euclide, en écrivant à chaque étape le quotient et le reste de la division euclidienne de  $r_{i+1}$  par  $r_i$  (cf les notations de l'algorithme).

Par exemple, pour les entiers  $n_1 = 48$  et  $n_2 = 29$ , cela donne :

- $n_1 = r_1 = 48$ ,  $n_2 = r_2 = 29$ ,  $r_1 = 1.r_2 + 19$ , d'où  $r_3 = 19 = n_1 - n_2$ .
- $r_2 = 1.r_3 + 10$ , d'où  $r_4 = 10 = r_2 - r_3 = n_2 - (n_1 - n_2) = 2n_2 - n_1$ .
- $r_3 = 1.r_4 + 9$  d'où  $r_5 = 9 = r_3 - r_4 = (n_1 - n_2) - (2n_2 - n_1) = 2n_1 - 3n_2$ .
- $r_4 = r_5 + 1$  d'où  $r_6 = 1 = 2n_2 - n_1 - (2n_1 - 3n_2) = -3n_1 + 5n_2$ .
- On en conclut que  $\text{pgcd}\{n_1, n_2\} = r_6 = 1$ . Les entiers  $n_1$  et  $n_2$  sont premiers entre eux. Une relation de Bezout est donc :  $-3n_1 + 5n_2 = 1$ .

**Théorème 7.5.3 (Gauss)** Soient  $a, b$  et  $c$  trois entiers naturels non nuls. Si  $a$  divise  $bc$  et est premier avec  $b$ , alors  $a$  divise  $c$ .

**Preuves :** Nous donnons deux démonstrations de ce résultat :

- *Première démonstration :* Comme  $a$  et  $b$  sont premiers entre eux, le théorème de Bezout affirme qu'il existe  $\alpha_1$  et  $\alpha_2$  tels que

$$\alpha_1 a + \alpha_2 b = 1. \quad \text{D'où } \alpha_1 a c + \alpha_2 b c = c.$$

Comme  $a$  divise à la fois  $ac$  et  $bc$ ,  $a$  divise  $\alpha_1 ac + \alpha_2 bc$ , c'est-à-dire,  $a$  divise  $c$ .

- *Seconde démonstration :* D'après la première partie de la proposition 7.4.5, on a :

$$\text{pgcd}\{ac, bc\} = c \text{pgcd}\{a, b\} = c.1 = c.$$

Comme  $a$  est un diviseur commun de  $ac$  et de  $bc$ , et que  $c$  est le pgcd de  $ac$  et  $bc$ , on en déduit que  $a$  divise  $c$ .

■

Une conséquence cruciale du théorème de Gauss est le corollaire suivant :

**Corollaire 7.5.4** Soient  $a, b, c$  trois entiers naturels, avec  $a$  et  $b$  non nuls et premiers entre eux. Si  $a|c$  et  $b|c$  alors  $ab|c$ .

**Preuve :** Comme  $a|c$ , il existe un entier  $c'$  tel que  $c = ac'$ . Or  $b|c$ , donc  $b|(ac')$ . Comme  $a$  et  $b$  sont premiers entre eux, le théorème de Gauss affirme que  $b|c'$ . Donc  $ab|c$ .

■

Une autre application du théorème de Bezout est la suivante :

**Proposition 7.5.5** Soit  $\{a_1, \dots, a_n\}$  un sous-ensemble de  $\mathbb{Z}^*$ . Alors un entier naturel  $\mu$  est le pgcd de  $a_1, \dots, a_n$  si et seulement si  $\mu$  est un diviseur commun de  $a_1, \dots, a_n$  et les entiers  $\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}$  sont premiers entre eux.

**Preuve :** Supposons d'abord que  $\mu$  est le pgcd de  $a_1, \dots, a_n$ . Alors on sait que  $\mu$  est un diviseur commun de  $a_1, \dots, a_n$ . De plus, le corollaire 7.4.4 affirme qu'il existe des entiers  $\alpha_1, \dots, \alpha_n$  tels que  $\alpha_1 a_1 + \dots + \alpha_n a_n = \mu$ . En divisant cette égalité par  $\mu$ , on obtient :

$$\alpha_1 \frac{a_1}{\mu} + \dots + \alpha_n \frac{a_n}{\mu} = 1 .$$

Le théorème de Bezout affirme alors que  $\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}$  sont premiers entre eux.

Réciproquement, supposons que  $\mu$  est un diviseur commun de  $a_1, \dots, a_n$  et les entiers  $\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}$  sont premiers entre eux. Notons  $d$  le pgcd de  $a_1, \dots, a_n$ . Comme  $\mu$  est un diviseur commun de  $a_1, \dots, a_n$ ,  $\mu$  divise  $d$  par définition du pgcd. De plus, comme  $\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}$  sont premiers entre eux, le théorème de Bezout affirme qu'il existe des entiers  $\alpha_1, \dots, \alpha_n$  tels que  $\alpha_1 \frac{a_1}{\mu} + \dots + \alpha_n \frac{a_n}{\mu} = 1$ , ce qui implique que  $\alpha_1 a_1 + \dots + \alpha_n a_n = \mu$ . Comme  $d$  est un diviseur commun de  $a_1, \dots, a_n$ ,  $d$  divise  $\alpha_1 a_1 + \dots + \alpha_n a_n$ , et donc divise  $\mu$ . Nous avons prouvé que les entiers naturels  $d$  et  $\mu$  se divisent l'un l'autre. Ils sont donc égaux. ■

Nous expliquons maintenant comment calculer le ppcm de deux nombres à partir de leur pgcd : pour cela, commençons par un résultat intermédiaire.

**Proposition 7.5.6** Soient  $a$  et  $b$  deux entiers naturels non nuls premiers entre eux. Alors le ppcm de  $a$  et  $b$  est égal à  $ab$ .

**Preuve :** Posons  $\mu = \text{ppcm}\{a, b\}$ . Comme  $ab$  est un multiple commun de  $a$  et de  $b$ ,  $\mu$  divise  $ab$  (condition (b) de la définition du ppcm).

Comme  $a$  divise  $\mu$ , il existe un entier  $k$  tel que  $\mu = ak$ . Or  $b$  divise également  $\mu$ , donc divise  $ak$ . Or  $a$  et  $b$  sont premiers entre eux. Le théorème de Gauss affirme alors que  $b$  divise  $k$ . Donc il existe un entier  $k' \in \mathbb{N}^*$  tel que  $k = bk'$ . D'où  $\mu = abk'$ . On en déduit que  $ab$  divise  $\mu$ .

Les entiers naturels  $\mu$  et  $ab$  se divisent l'un l'autre, donc sont égaux. ■

Voici maintenant la relation entre ppcm et pgcd dans le cas général :

**Théorème 7.5.7** Soient  $a$  et  $b$  deux entiers naturels non nuls. Alors

$$\text{pgcd}\{a, b\} \text{ppcm}\{a, b\} = ab .$$

**Preuve :** Posons  $d = \text{pgcd}\{a, b\}$ . La proposition 7.5.5 affirme que  $d$  divise  $a$  et  $b$  et que  $\frac{a}{d}$  et  $\frac{b}{d}$  sont premiers entre eux. D'après la proposition 7.5.6, le ppcm de  $\frac{a}{d}$  et  $\frac{b}{d}$  est égal à  $\frac{ab}{d^2}$ .

Donc

$$\text{ppcm}\{a, b\} = \text{ppcm}\left\{d \frac{a}{d}, d \frac{b}{d}\right\} = d \text{ppcm}\left\{\frac{a}{d}, \frac{b}{d}\right\} = d \frac{ab}{d^2} = \frac{ab}{d} .$$

On en déduit l'égalité désirée. ■

On conclut cette partie par la mise sous forme irréductible d'un nombre rationnel. Rappelons qu'un nombre rationnel est un nombre réel  $r$  pour lequel il existe  $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$  avec  $r = p/q$ .

**Théorème 7.5.8 (Forme irréductible d'un nombre rationnel)** *Soit  $r$  un nombre rationnel non nul. Il existe un unique couple  $(a, b) \in \mathbb{Z}^* \times \mathbb{N}^*$  tel que*

$$r = \frac{a}{b} \quad \text{et} \quad a \text{ et } b \text{ premiers entre eux .}$$

**Preuve :**

— *Existence* : On suppose que  $r$  est positif (sinon, faire le même travail avec  $-r$ ). Comme  $r$  est rationnel, il existe  $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$  avec  $r = p/q$ . On peut choisir  $p$  et  $q$  strictement positifs car  $r$  l'est. Posons  $d = \text{pgcd}\{p, q\}$ ,  $a = p/d$  et  $b = q/d$ . Alors la proposition 7.5.5 affirme que  $a$  et  $b$  sont premiers entre eux. De plus, on a bien  $r = a/b$  car

$$r = \frac{p}{q} = \frac{ad}{bd} = \frac{a}{b} .$$

— *Unicité* : Supposons qu'il existe deux couples  $(a_1, b_1) \in \mathbb{Z}^* \times \mathbb{N}^*$  et  $(a_2, b_2) \in \mathbb{Z}^* \times \mathbb{N}^*$  tels que, pour  $j = 1, 2$ ,  $r = \frac{a_j}{b_j}$  et  $a_j$  et  $b_j$  sont premiers entre eux. Alors

$$r = \frac{a_1}{b_1} = \frac{a_2}{b_2}$$

D'où  $a_1 b_2 = a_2 b_1$ . Alors  $b_2$  divise  $a_2 b_1$ . Comme  $b_2$  et  $a_2$  sont premiers entre eux, le théorème de Gauss affirme que  $b_2$  divise  $b_1$ . On obtient de même que  $b_1$  divise  $b_2$ . Les entiers naturels  $b_1$  et  $b_2$  se divisant l'un l'autre, ils sont égaux. L'égalité  $a_1 b_2 = a_2 b_1$  et le fait que  $b_1 = b_2 \neq 0$  impliquent alors que  $a_1 = a_2$ . D'où l'unicité de la mise sous forme irréductible. ■

## 7.6 Nombres premiers

**Définition 7.6.1** *On appelle nombre premier tout nombre entier naturel  $p$ , tel que  $p \geq 2$  et dont les seuls diviseurs dans  $\mathbb{N}^*$  sont 1 et  $p$ , i.e., :*

$$\text{si } q \in \mathbb{N}^* \text{ avec } q|p, \text{ alors } q = 1 \text{ ou } q = p .$$

Le théorème suivant affirme que tout entier naturel possède des diviseurs premiers :

**Théorème 7.6.2** *Soit  $n$  un entier naturel, avec  $n \geq 2$ . Il existe un nombre premier qui divise  $n$ .*

**Preuve :** Soit  $A$  le sous-ensemble des entiers naturels supérieurs à 2 et diviseurs de  $n$  :

$$A = \{q \in \mathbb{N}^* \mid q \geq 2 \text{ et } q|n\} .$$

Alors  $A$  est une partie non vide de  $\mathbb{N}$  (car  $n \in A$ ) et donc possède un plus petit élément  $p$ .

Montrons que  $p$  est premier. Soit  $k$  un nombre entier naturel qui divise  $p$ . Alors  $k$  divise aussi  $n$ , car  $p$  divise  $n$ . Il y a alors deux possibilités :

- soit  $k < 2$ , c'est-à-dire  $k = 1$ ,

- soit  $k \geq 2$ , et donc  $k$  appartient à  $A$ . Or  $p$  est le plus petit élément de  $A$ . Donc  $k \geq p$ . Mais  $k$  divise  $p$ , donc  $k = p$ .

On a prouvé que, si  $k$  divise  $p$ , alors soit  $k = 1$ , soit  $k = p$ . Donc  $p$  est un diviseur premier de  $n$ .

■

Le théorème d'Euclide affirme qu'il existe une infinité de nombres premiers :

**Théorème 7.6.3 (Euclide)** *Pour tout entier naturel  $n$ , il existe un nombre premier  $p$  supérieur à  $n$ .*

**Preuve :** Fixons un entier  $n \geq 2$ , et considérons le nombre  $q = n! + 1 = (1.2.3 \dots n) + 1$ . D'après le théorème 7.6.2, il existe un nombre premier  $p$  qui divise  $q$ .

Montrons que  $p$  est supérieur à  $n$ . En effet, si, raisonnant par l'absurde, on suppose que  $p < n$ , alors  $p$  divise  $n!$ . Donc  $p$  divise 1 ce qui est impossible car  $p \geq 2$ . On a donc trouvé une contradiction. Par conséquent,  $p$  est supérieur à  $n$ .

■

## 7.7 Décomposition d'un entier en facteurs premiers

**Théorème 7.7.1** *Tout entier naturel  $a \geq 2$  peut s'écrire d'une manière unique sous la forme :*

$$a = (p_1)^{k_1} \dots (p_m)^{k_m}$$

où  $p_1, \dots, p_m$  sont des nombres premiers distincts et  $k_1, \dots, k_m$  sont des entiers strictement positifs.

**Remarque 7.7.2** *L'unicité signifie ici que si on a deux expressions de cette forme :*

$$a = (p_1)^{k_1} \dots (p_m)^{k_m} = (q_1)^{r_1} \dots (q_n)^{r_n}$$

avec  $p_1, \dots, p_m$  (respectivement  $q_1, \dots, q_n$ ) des nombres premiers distincts et  $k_1, \dots, k_m$  (respectivement  $r_1, \dots, r_n$ ) des entiers strictement positifs, alors  $m = n$  et, pour tout  $i \in \{1, \dots, n\}$ , il existe un indice  $j \in \{1, \dots, n\}$  tel que  $p_i = q_j$  et  $k_i = r_j$ .

**Preuve :** Nous ne démontrons que l'existence, la preuve de l'unicité étant un peu plus délicate. On raisonne par récurrence généralisée sur le nombre  $a$ . Si  $a = 2$ , le résultat est évident.

Supposons le résultat vrai jusqu'au nombre  $a \geq 2$ . Montrons qu'il est encore vrai pour  $a+1$ . D'après le théorème 7.6.2, le nombre  $a+1$  possède un diviseur premier, noté  $p$ . Posons  $b = \frac{a+1}{p}$ .

Il y a alors 2 cas : soit  $b = 1$ , et alors le résultat est démontré. Soit  $b > 1$ , et on a alors  $2 \leq b \leq a$ . Par hypothèse de récurrence, il existe alors des nombres premiers distincts  $p_1, \dots, p_m$  et des entiers strictement positifs  $k_1, \dots, k_m$  tels que

$$b = (p_1)^{k_1} \dots (p_m)^{k_m} .$$

Donc

$$a + 1 = p(p_1)^{k_1} \dots (p_m)^{k_m}$$

et  $a+1$  possède une décomposition en facteurs premiers.

Par récurrence, on en déduit l'existence de la décomposition pour tout entier  $a$ .

■

**Proposition 7.7.3 Application au calcul du pgcd et du ppcm :** Soient  $a$  et  $b$  deux entiers naturels non nuls supérieurs à 2. On suppose que

$$a = (p_1)^{k_1} \dots (p_m)^{k_m} \text{ et } b = (p_1)^{r_1} \dots (p_m)^{r_m}$$

avec  $p_1, \dots, p_m$  des nombres premiers distincts et  $k_1, \dots, k_m$  (respectivement  $r_1, \dots, r_m$ ) des entiers positifs ou nuls (de façon à avoir une écriture commune pour  $a$  et  $b$ ). Alors

$$\text{pgcd}\{a, b\} = (p_1)^{\min\{k_1, r_1\}} \dots (p_m)^{\min\{k_m, r_m\}} \text{ et } \text{ppcm}\{a, b\} = (p_1)^{\max\{k_1, r_1\}} \dots (p_m)^{\max\{k_m, r_m\}}$$



# Chapitre 8

## Les polynômes

**Avertissement :** L'ensemble des polynômes partage de nombreuses propriétés communes avec l'ensemble des entiers (division euclidienne, existence d'un ppcm, d'un pgcd, notion de nombres ou de polynômes premiers, etc...) C'est pourquoi plusieurs parties de ce chapitre sont redondantes par rapport au chapitre précédent. C'est en particulier le cas des parties 8.3 à 8.7 qui ne figurent ici que par commodité du lecteur.

### 8.1 Définitions et vocabulaire

**Définition 8.1.1**

Un polynôme  $P$  est une expression de la forme

$$P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n,$$

où  $a_0, a_1, \dots, a_n$  sont les **coefficients** du polynôme.

Si  $a_0, a_1, \dots, a_n$  sont des nombres réels (resp. complexes), le polynôme est **réel** (resp. **complexes**).

L'ensemble des polynômes réels est noté  $\mathbb{R}[X]$ , tandis que l'ensemble des polynômes complexes est noté  $\mathbb{C}[X]$ .

Si  $P$  est un polynôme non nul, avec  $P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ , le **degré** du polynôme  $P$ , noté  $\deg(P)$ , est le plus grand entier  $k \in \{0, \dots, n\}$  tel que  $a_k \neq 0$ .

Si ce coefficient directeur est égal à 1, on dit que le polynôme  $P$  est **normalisé**.

Par convention, le degré du polynôme nul est  $-\infty$ .

**Proposition 8.1.2** Deux polynômes  $P_1$  et  $P_2$  sont égaux si  $P_1$  et  $P_2$  ont même degré et si les coefficients de  $P_1$  et  $P_2$  sont égaux.

**Définition 8.1.3 Somme de deux polynômes :** Soient  $P_1(X) = a_0 + a_1X + \dots + a_nX^n$  et  $P_2(X) = b_0 + b_1X + \dots + b_mX^m$ . Le polynôme  $P_1 + P_2$  est le polynôme  $(P_1 + P_2)(X) = c_0 + c_1X + \dots + c_kX^k$ , avec

- l'entier  $k$  est défini par  $k = \max\{n, m\}$ ,
- les coefficients  $c_i$  sont définis par :

$$\forall i \in \{1, \dots, k\}, c_i = \begin{cases} a_i + b_i & \text{si } i \leq \min\{n, m\} \\ a_i & \text{si } m + 1 < i \leq n \\ b_i & \text{si } n + 1 < i \leq m \end{cases}$$

**Définition 8.1.4 Produit de deux polynômes :** Soient  $P_1(X) = a_0 + a_1X + \dots + a_nX^n$  et  $P_2(X) = b_0 + b_1X + \dots + b_mX^m$ . Le polynôme  $P_1P_2$  est le polynôme  $(P_1P_2)(X) = c_0 + c_1X + \dots + c_kX^k$ , avec

- l'entier  $k$  est défini par  $k = n + m$ ,
- les coefficients  $c_i$  sont définis par :

$$\forall i \in \{1, \dots, k\}, c_i = \sum_{j+l=i} a_j b_l.$$

**Remarque 8.1.5** Cette formule correspond au développement formel du produit

$$(a_0 + a_1X + \dots + a_nX^n)(b_0 + b_1X + \dots + b_mX^m).$$

Il est facile de montrer que la somme et le produit de polynômes possèdent les propriétés habituelles (associativité, commutativité, le polynôme nul est un élément neutre pour l'addition, existence d'un opposé, distributivité).

Sauf mention contraire, dans toute la suite nous travaillerons indifféremment dans  $\mathbb{R}[X]$  ou dans  $\mathbb{C}[X]$ . Un **scalaire** sera alors, dans le premier cas, un élément de  $\mathbb{R}$ , et dans le second, un élément de  $\mathbb{C}$ .

**Théorème 8.1.6** Soient  $P_1$  et  $P_2$  deux polynômes. Alors

$$\deg(P_1 + P_2) \leq \max\{\deg(P_1), \deg(P_2)\}.$$

De plus, il y a inégalité stricte si et seulement si  $\deg(P_1) = \deg(P_2)$  et le coefficient dominant de  $P_1$  est l'opposé de celui de  $P_2$ .

$$\deg(P_1P_2) = \deg(P_1) + \deg(P_2).$$

De plus, si  $P_1$  et  $P_2$  sont non nuls, le coefficient dominant de  $P_1P_2$  est le produit du coefficient dominant de  $P_1$  et de celui de  $P_2$ .

**Remarque 8.1.7** Si  $P_1$  ou  $P_2$  est le polynôme nul, le résultat est encore valable à condition d'utiliser la convention  $-\infty + k = -\infty$  pour tout entier  $k$ .

**Preuve du théorème :** C'est une conséquence directe des définitions de la somme et du produit. ■

**Corollaire 8.1.8** *L'ensemble des polynômes est intègre c'est-à-dire : Si  $P_1$  et  $P_2$  sont deux polynômes, et si  $P_1P_2 = 0$  alors soit  $P_1 = 0$ , soit  $P_2 = 0$ .*

**Preuve :** En effet,  $\deg(P_1P_2) = \deg(P_1) + \deg(P_2) = -\infty$  car  $P_1P_2 = 0$ . Donc  $\deg(P_1) = -\infty$  ou  $\deg(P_2) = -\infty$ , c'est-à-dire que  $P_1 = 0$  ou  $P_2 = 0$ . ■

## 8.2 Division euclidienne

**Définition 8.2.1** *Soient  $A$  et  $B$  deux polynômes. On dit que  $A$  divise  $B$  noté  $A|B$  si*

- a)  $A$  n'est pas nul,
- b) il existe un polynôme  $Q$  tel que  $B = QA$ .

**Proposition 8.2.2** *Soient  $A$ ,  $B$  et  $C$  trois polynômes.*

1. si  $C \neq 0$ , alors  $A|B$  si et seulement si  $AC|BC$ ,
2. si  $A|B$ , alors  $(-A)|B$  et  $A|(-B)$ ,
3. si  $A|B$  et  $A|C$ , alors  $A|(B + C)$ .
4. si  $A|B$  et  $B|A$ , alors il existe un scalaire non nul  $\alpha$  tel que  $B = \alpha A$ .
5. si  $AB|C$  alors  $A|C$  et  $B|C$ .
6. si  $A \neq 0$  et  $A|B$ , alors, soit  $B = 0$ , soit  $\deg(A) \leq \deg(B)$ .

**Preuve :** Cette proposition est une conséquence immédiate de la définition de la division. Nous la laissons en exercice. ■

**Théorème 8.2.3** *Soient  $A$  et  $B$  deux polynômes avec  $B \neq 0$ . Il existe alors un unique couple  $(Q, R)$  de polynômes, avec*

$$A = QB + R \text{ et } \deg(R) < \deg(B) .$$

*Le polynôme  $Q$  s'appelle le quotient de la division euclidienne de  $A$  par  $B$ , tandis que le polynôme  $R$  s'appelle le reste.*

**Preuve :**

— **Preuve de l'unicité :** Supposons que  $(Q_1, R_1)$  et  $(Q_2, R_2)$  soient deux couples de polynômes tels que

$$A = Q_1B + R_1 = Q_2B + R_2 \text{ avec } \deg(R_1) < \deg(B) \text{ et } \deg(R_2) < \deg(B) .$$

Alors, comme  $(Q_1 - Q_2)B = R_2 - R_1$ , le polynôme  $B$  divise le polynôme  $R_2 - R_1$  qui est de degré strictement inférieur à celui de  $B$ . Donc  $R_1 = R_2$ , ce qui implique, puisque  $B \neq 0$ , que  $Q_1 = Q_2$ .

Nous avons donc prouvé qu'il existe au plus un couple  $(Q, R)$  de polynômes vérifiant la relation désirée.

— **Preuve de l'existence :** On suppose que  $B$  ne divise pas  $A$ , car sinon le résultat est évident. Notons

$$E = \{n \in \mathbb{N} \mid \exists \text{ un polynôme } C \text{ avec } \deg(A - BC) = n\}.$$

L'ensemble  $E$  n'est pas vide car il contient par exemple  $\deg(A)$  (prendre  $C = 0$ ). Donc  $E$  contient un plus petit élément  $r$ . Comme  $r \in E$ , il existe un polynôme  $Q$  tel que le polynôme  $R = (A - BQ)$  a pour degré  $r$ . Montrons que  $r < \deg(B)$ .

Pour cela, on raisonne par l'absurde en supposant au contraire que  $r = \deg(R) \geq \deg(B)$ . Posons  $n = \deg(B)$  et appelons  $b_n$  et  $c_r$  respectivement le coefficient dominant de  $B$  et de  $R$ . Alors on affirme que le polynôme  $Q_1 = Q + \frac{c_r}{b_n} X^{r-n}$  (avec la convention  $X^0 = 1$ ) vérifie :  $\deg(A - BQ_1) < r$ . En effet,

$$A - BQ_1 = A - B\left(Q + \frac{c_r}{b_n} X^{r-n}\right) = R - \frac{c_r}{b_n} X^{r-n} B.$$

Les polynômes  $R$  et  $\frac{c_r}{b_n} X^{r-n} B$  sont de même degré  $r$  et ont même coefficient dominant  $c_r$ . Donc  $A - BQ_1$  a un degré strictement inférieur à  $r$ . Comme  $\deg(A - BQ_1)$  appartient à  $E$  par définition de  $E$  (notons que  $A - BQ_1 \neq 0$  car  $B$  ne divise pas  $A$ ), on a trouvé une contradiction car  $r$  est le plus petit élément de  $E$  et  $\deg(A - BQ_1) < r$ . Par conséquent, on a prouvé que  $r = \deg(R) < \deg(B)$ . Ceci achève la démonstration de l'existence du couple  $(Q, R)$  tel que  $A = QB + R$  et  $\deg(R) < \deg(B)$ . ■

### 8.3 Le ppcm d'une famille de polynômes

**Définition 8.3.1 (PPCM)** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. On appelle plus petit commun multiplicateur (ppcm) de  $\{A_1, \dots, A_n\}$  l'unique polynôme non nul et normalisé  $P$  noté  $\text{ppcm}\{A_1, \dots, A_n\}$  tel que

- a)  $\forall i = 1, \dots, n, A_i \mid P$ ,  
 b) Pour tout polynôme non nul  $Q$ , si  $\{\forall i = 1, \dots, n, A_i \mid Q\}$ , alors  $P \mid Q$ .

Montrons l'existence du  $\text{ppcm}\{A_1, \dots, A_n\}$ .

**Théorème 8.3.2** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. Le ppcm de  $\{A_1, \dots, A_n\}$  existe et est unique. C'est le polynôme de plus petit degré parmi les polynômes non nuls et normalisés qui sont multiples communs de  $A_1, \dots, A_n$ .

**Preuve :** Soit  $E$  l'ensemble des entiers naturels non nuls défini par

$$E = \{k \in \mathbb{N}^* \mid \exists \text{ un polynôme } Q \text{ tel que } \forall i = 1, \dots, n, A_i \mid Q \text{ et } k = \deg(Q)\}.$$

L'ensemble  $E$  est non vide car il contient l'entier  $k = \deg(A_1 \dots A_n)$ . En effet,  $A_1 \dots A_n$  est un multiple commun de  $A_1, \dots, A_n$ . Donc  $E$  possède un plus petit élément noté  $p$ . Comme  $p$  appartient à  $E$ , il existe un polynôme  $P$  (que l'on peut choisir normalisé) qui est multiple commun à tous les  $A_i$  et tel que  $\deg(P) = p$ . Montrons que  $P$  est le ppcm de  $\{A_1, \dots, A_n\}$ .

Par construction,  $P$  est non nul et vérifie la condition (a) de la définition. Pour montrer que  $P$  vérifie aussi (b), il suffit de montrer que  $P$  divise  $A$  pour tout  $A$  multiple commun à  $A_1, \dots, A_n$ .

On raisonne par l'absurde en supposant qu'il existe  $A$  multiple commun à  $A_1, \dots, A_n$  qui n'est pas divisible par  $P$ . Soient  $Q$  et  $R$  respectivement le quotient et le reste de la division euclidienne de  $A$  par  $P$ . On a  $A = QP + R$  et  $0 \leq \deg(R) < \deg(P)$ . Comme, pour tout  $i = 1, \dots, n$ ,  $A_i$  divise  $A$  et  $P$ ,  $A_i$  divise  $R$ . Donc  $R$  est un multiple commun à tous les  $A_i$  et  $\deg(R)$  appartient à  $E$ . Ceci contredit le fait

que  $p = \deg(P)$  est le plus petit élément de  $E$ . Donc  $P$  divise  $A$  pour tout  $A$  multiple commun à tous les  $A_i$ . On a montré l'existence du ppcm de  $\{A_1, \dots, A_n\}$ .

Montrons l'unicité du ppcm. Si  $P_1$  et  $P_2$  sont deux ppcm de  $\{A_1, \dots, A_n\}$ , alors  $P_1$  divise  $P_2$  et  $P_2$  divise  $P_1$ . Comme  $P_1$  et  $P_2$  sont normalisés, cela implique que  $P_1 = P_2$ . Le ppcm est donc unique. ■

Voici quelques propriétés du ppcm :

**Proposition 8.3.3**

i) Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls et  $B$  un polynôme non nul et de coefficient dominant  $b$ . Alors

$$\text{ppcm}\{BA_1, \dots, BA_n\} = \frac{1}{b}B \text{ppcm}\{A_1, \dots, A_n\}.$$

ii) Si  $A$  et  $B$  sont deux polynômes non nuls, avec  $A|B$ , et si  $b$  est le coefficient dominant de  $B$ , alors

$$\text{ppcm}\{A, B\} = \frac{1}{b}B.$$

**Preuve :** i) Quitte à remplacer  $B$  par  $\frac{1}{b}B$ , on peut supposer que  $B$  est normalisé. Appelons  $P$  le ppcm de  $\{A_1, \dots, A_n\}$ . Il faut montrer que  $BP$  (qui est alors normalisé) est le ppcm de  $\{BA_1, \dots, BA_n\}$ .

Comme, pour tout  $i = 1, \dots, n$ ,  $A_i$  divise  $P$ , on a que  $BA_i$  divise  $BP$ . Donc  $BP$  vérifie le (a) de la définition du ppcm.

Soit  $Q$  un polynôme non nul tel que, pour tout  $i = 1, \dots, n$ ,  $BA_i$  divise  $Q$ . Alors  $B$  divise  $Q$  et on note  $Q_1 = \frac{Q}{B}$ . Remarquons que  $Q_1 \neq 0$  car  $Q \neq 0$ .

Comme, pour tout  $i = 1, \dots, n$ ,  $BA_i$  divise  $Q = BQ_1$ , on en déduit que  $A_i$  divise  $Q_1$ . De plus,  $P$  étant le ppcm de  $\{A_1, \dots, A_n\}$ , la propriété (b) de la définition du ppcm implique que  $P$  divise  $Q_1$ . Donc  $BP$  divise  $Q = BQ_1$ . Par conséquent,  $BP$  vérifie la condition (b) de la définition du ppcm.

ii) On suppose encore que  $B$  est normalisé. Comme  $A$  et  $B$  divisent clairement  $B$ ,  $B$  vérifie (a) de la définition du ppcm.

Le polynôme  $B$  vérifie le (b) de la définition du ppcm de façon évidente. Donc  $B = \text{ppcm}\{A, B\}$ . ■

## 8.4 Le pgcd d'une famille de polynômes

**Définition 8.4.1 (PGCD)** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. On appelle plus grand commun diviseur (pgcd) de  $\{A_1, \dots, A_n\}$  l'unique polynôme non nul et normalisé  $P$ , noté  $\text{pgcd}\{A_1, \dots, A_n\}$ , tel que

a)  $\forall i = 1, \dots, n, P|A_i$ ,

b) pour tout polynôme non nul  $Q$ , si  $\{\forall i = 1, \dots, n, Q|A_i\}$ , alors  $Q|P$ .

**Théorème 8.4.2** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. Le pgcd de  $\{A_1, \dots, A_n\}$  existe et est unique.

**Preuve de l'unicité :** L'unicité du pgcd est claire puisque, si  $P_1$  et  $P_2$  sont deux pgcd de  $\{A_1, \dots, A_n\}$ , alors  $P_1$  et  $P_2$  se divisent l'un l'autre, et, étant normalisés, sont donc égaux.

■

Le lemme suivant montre l'existence du pgcd :

**Lemme 8.4.3** Soient  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls et  $\mathcal{I}$  l'ensemble des polynômes défini par :

$$\mathcal{I} = \{A \neq 0 \mid \exists Z_1, \dots, Z_n \text{ des polynômes tels que } A = Z_1 A_1 + \dots + Z_n A_n\}.$$

Alors cet ensemble est non vide et possède un polynôme normalisé  $P$  de plus petit degré dans  $\mathcal{I}$ . Ce polynôme est le pgcd de  $\{A_1, \dots, A_n\}$ .

**Preuve :** L'ensemble  $\mathcal{I}$  est non vide car, par exemple  $A_1^2$  appartient à  $\mathcal{I}$  (prendre  $Z_1 = A_1$ ,  $Z_2 = \dots = Z_n = 0$ ). Soit

$$E = \{n \in \mathbb{N} \mid \exists A \in \mathcal{I} \text{ avec } \deg(A) = n\}.$$

Comme  $E$  est une partie non vide de  $\mathbb{N}$ ,  $E$  possède un plus petit élément noté  $p$ . Comme  $p$  appartient à  $E$ , il existe un polynôme  $P$ , que l'on peut choisir normalisé, tel que  $\deg(P) = p$ . Montrons que  $P$  est le pgcd de  $A_1, \dots, A_n$ .

Comme  $P \in \mathcal{I}$ , il existe des polynômes  $Z_1, \dots, Z_n$  tels que  $P = Z_1 A_1 + \dots + Z_n A_n$ . Vérifions que  $P$  satisfait (a) de la définition du pgcd. Pour cela, on raisonne par l'absurde en supposant qu'il existe  $i \in \{1, \dots, n\}$  tel que  $P$  ne divise pas  $A_i$ . Soit  $Q$  et  $R$  respectivement le quotient et le reste de la division euclidienne de  $A_i$  par  $P$  :  $A_i = QP + R$  et  $0 \leq \deg(R) < \deg(P)$ . Alors  $R$  appartient à  $\mathcal{I}$  car  $R \neq 0$  par hypothèse et

$$R = A_i - QP = (-Z_1 Q)A_1 + \dots + (-Z_{i-1} Q)A_{i-1} + (1 - Z_i Q)A_i \\ + (-Z_{i+1} Q)A_{i+1} + \dots + (-Z_n Q)A_n.$$

Donc  $\deg(R)$  appartient à  $E$ . Mais d'autre part  $\deg(R) < p$  et  $p$  est le plus petit élément de  $E$ . On a donc trouvé une contradiction. Par conséquent  $P$  divise tous les  $A_i$ ,  $i = 1, \dots, n$ .

Reste à prouver que  $P$  satisfait la partie (b) de la définition du pgcd. Pour cela, considérons  $Q$  un diviseur commun à tous les  $A_i$ . Il est clair alors que  $Q$  divise tous les éléments de  $\mathcal{I}$ . Comme  $P$  appartient à  $\mathcal{I}$ ,  $Q$  divise donc  $P$ .

■

On déduit de la démonstration le corollaire suivant :

**Corollaire 8.4.4** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. Il existe alors des polynômes  $Z_1, \dots, Z_n$  tels que

$$\text{pgcd}(A_1, \dots, A_n) = Z_1 A_1 + \dots + Z_n A_n.$$

Voici maintenant quelques propriétés du pgcd qui seront utiles plus tard :

**Proposition 8.4.5**

i) Soient  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls et  $B$  un polynôme non nul de coefficient dominant  $b$ . Alors

$$\text{pgcd}\{BA_1, \dots, BA_n\} = \frac{B}{b} \text{pgcd}\{A_1, \dots, A_n\}.$$

ii) Si  $A$  et  $B$  sont deux polynômes non nuls tels que  $A|B$ , et si  $a$  est le coefficient dominant de  $A$ , alors

$$\text{pgcd}(A, B) = \frac{A}{a}.$$

**Preuve :** i) On suppose pour simplifier les notations que  $B$  est normalisé. Posons  $P_1 = \text{pgcd}\{A_1, \dots, A_n\}$  et  $P_2 = \text{pgcd}\{BA_1, \dots, BA_n\}$ . Il faut montrer que  $BP_1 = P_2$ .

On remarque d'abord que  $BP_1$  est un diviseur commun à  $BA_1, \dots, BA_n$ , car  $P_1$  est un diviseur commun à  $A_1, \dots, A_n$ . Donc  $BP_1$  divise  $P_2$ . Il existe donc un polynôme  $Q$  non nul avec  $P_2 = QBP_1$ .

Comme  $P_2$  est le pgcd de  $\{BA_1, \dots, BA_n\}$ ,  $P_2 = QBP_1$  est un diviseur commun à  $BA_1, \dots, BA_n$ , ce qui implique que  $QP_1$  est un diviseur commun à  $A_1, \dots, A_n$ . Or  $P_1$  étant le pgcd de  $\{A_1, \dots, A_n\}$ , cela entraîne que  $QP_1$  divise  $P_1$ . Or  $P_1 \neq 0$  et  $Q \neq 0$ , donc  $Q$  est un scalaire non nul. On a donc prouvé que  $P_2 = QBP_1$ , avec  $Q$  scalaire non nul. Comme  $P_1, B$  et  $P_2$  sont normalisés, on en déduit que  $Q = 1$  et que  $P_2 = BP_1$ .

ii) On suppose que  $A$  est normalisé. Posons  $P = \text{pgcd}\{A, B\}$ . Comme  $A$  divise à la fois  $A$  et  $B$ ,  $A$  divise  $P$ . De plus,  $P$  divise  $A$  par définition du pgcd. Comme  $A$  et  $P$  sont normalisés et se divisent l'un l'autre, on a  $P = A$ .

■

La proposition suivante affirme que l'on peut toujours ramener le calcul du pgcd de  $n$  polynômes à  $n$  calculs du pgcd de 2 polynômes.

**Proposition 8.4.6** Soient  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls, avec  $n \geq 3$ . Alors

$$\text{pgcd}\{A_1, \dots, A_n\} = \text{pgcd}\{A_1, \text{pgcd}\{A_2, \dots, A_n\}\}.$$

**Preuve :** Posons  $P_1 = \text{pgcd}\{A_1, \dots, A_n\}$ ,  $P_2 = \text{pgcd}\{A_2, \dots, A_n\}$  et  $P_3 = \text{pgcd}\{A_1, P_2\}$ . On veut montrer que  $P_1 = P_3$ .

Montrons d'abord que  $P_1$  divise  $P_3$ . Comme  $P_1$  est un diviseur commun à  $A_2, \dots, A_n$ ,  $P_1$  divise  $P_2$ . Comme de plus,  $P_1$  divise  $A_1$ ,  $P_1$  divise le pgcd de  $A_1$  et de  $P_2$ , i.e., divise  $P_3$ .

Réciproquement,  $P_3$  divise à la fois  $A_1$  et  $P_2$ . Or  $P_2$  étant un diviseur commun à  $A_2, \dots, A_n$ ,  $P_3$ , divisant  $P_2$ , est également un diviseur commun à  $A_2, \dots, A_n$ . Donc  $P_3$  divise tous les  $A_i$ , avec  $i = 1, \dots, n$ , ce qui implique que  $P_3$  divise le pgcd de  $\{A_1, \dots, A_n\}$ , c'est-à-dire  $P_1$ .

En conclusion, les polynômes normalisés  $P_1$  et  $P_3$  se divisent l'un l'autre, et sont donc égaux.

■

Voici maintenant le résultat principal de cette partie, qui justifie l'algorithme d'Euclide de calcul du pgcd, que nous introduisons après.

**Théorème 8.4.7** Soient  $A_1$  et  $A_2$  deux polynômes non nuls. Si  $A_2$  ne divise pas  $A_1$ , alors

$$\text{pgcd}\{A_1, A_2\} = \text{pgcd}\{A_2, R\}$$

où  $R$  est le reste de la division euclidienne de  $A_1$  par  $A_2$ .

**Preuve :** Soient  $Q$  et  $R$  respectivement le quotient et le reste de la division euclidienne de  $A_1$  par  $A_2$  :  $A_1 = QA_2 + R$  et  $0 \leq \text{deg}(R) < \text{deg}(A_2)$ . Posons  $P_1 = \text{pgcd}\{A_2, R\}$  et  $P_2 = \text{pgcd}\{A_1, A_2\}$ . Montrons que  $P_1 = P_2$ .

(a) Par définition,  $P_1|A_2$ . Comme  $P_1|R$  et  $P_1|A_2$ , on a aussi  $P_1|QA_2 + R = A_1$ . Donc  $P_1$  est un diviseur commun de  $A_2$  et de  $A_1$ . Donc  $P_1$  divise  $P_2$  qui est le pgcd de  $A_1$  et  $A_2$ .

(b) Réciproquement,  $P_2$  divise  $A_1$  et  $A_2$ . Donc  $P_2$  divise aussi  $R = A_1 - QA_2$ . Par conséquent,  $P_2$  divise le pgcd de  $A_2$  et de  $R$ , i.e., divise  $P_1$ .

En conclusion, les polynômes normalisés  $P_1$  et  $P_2$  se divisent l'un l'autre, et sont donc égaux.

■

Décrivons maintenant l'**algorithme d'Euclide**. Comme dans  $\mathbb{Z}$ , l'objet de l'algorithme est de calculer le pgcd de polynômes non nuls  $A_1$  et  $A_2$ .

- **Initialisation** : Posons  $R_1 = A_1$  et  $R_2 = A_2$
- tant que  $R_i \neq 0$ , on définit  $R_{i+1}$  comme étant le reste de la division euclidienne de  $R_{i-1}$  par  $R_i$ .

**Proposition 8.4.8** Soit  $(R_i)$  la suite de polynômes définie par l'algorithme d'Euclide. Alors il existe un indice  $i_0 \leq \deg(A_2) + 2$  tel que  $R_{i_0} = 0$  et

$$\text{pgcd}\{A_1, A_2\} = \frac{1}{r_{i_0-1}} R_{i_0-1},$$

où  $r_{i_0-1}$  est le coefficient dominant de  $R_{i_0-1}$ .

**Exemple 8.4.9** Si  $A_1 = X^3 + X + 2$  et  $A_2 = X^2 - 1$ , on a

- $R_1 = A_1 = X^3 + X + 2$  et  $R_2 = A_2 = X^2 - 1$ ,
- $R_3 = 2X + 2$  car  $R_1 = XR_2 + 2X + 2$
- $R_4 = 0$  car  $R_3$  divise  $R_2$ .
- Conclusion :  $\text{pgcd}(A_1, A_2) = \frac{1}{2}R_3 = X + 1$

**Preuve de la proposition 8.4.8** : Par définition du reste de la division euclidienne, la suite  $(\deg(R_i))$  est strictement décroissante à partir du rang  $i = 2$ . On montre donc facilement par récurrence que  $\deg(R_i) \leq \deg(R_2) - i + 2$  pour  $i \geq 2$ . Or  $\deg(R_i) \geq 0$  est positif pour tout  $i < i_0$ . L'algorithme s'arrête donc au plus tard en temps  $i_0 \leq \deg(R_2) + 2$ .

On démontre également par récurrence, en utilisant le théorème 8.4.7, que, pour tout  $i < i_0 - 1$ ,

$$(8.1) \quad \text{pgcd}\{A_1, A_2\} = \text{pgcd}\{R_{i-1}, R_i\}.$$

Or, par définition de  $i_0$ , le polynôme  $R_{i_0-1}$  divise  $R_{i_0-2}$ . La proposition 8.4.5 affirme alors que

$$(8.2) \quad \text{pgcd}\{R_{i_0-2}, R_{i_0-1}\} = \frac{1}{r_{i_0-1}} R_{i_0-1}.$$

En mettant ensemble les égalités (8.1) et (8.2), on obtient le résultat désiré :  $\text{pgcd}\{A_1, A_2\} = \frac{1}{r_{i_0-1}} R_{i_0-1}$ . ■

## 8.5 Polynômes premiers entre eux

**Définition 8.5.1** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. On dit que les polynômes  $A_1, \dots, A_n$  sont premiers entre eux si leur pgcd est 1.

**Exemple 8.5.2** Par exemple, les polynômes  $A_1(X) = X^4 + X^2 + 1$  et  $A_2(X) = X^2 + 1$  sont premiers entre eux car  $\text{pgcd}(A_1, A_2) = \text{pgcd}(A_2, 1) = 1$  car 1 est le reste de la division euclidienne de  $A_1$  par  $A_2$ .

**Théorème 8.5.3 (Bezout)** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. Alors les polynômes  $A_1, \dots, A_n$  sont premiers entre eux si et seulement si il existe  $n$  polynômes  $Z_1, \dots, Z_n$  tels que

$$(8.3) \quad Z_1 A_1 + \dots + Z_n A_n = 1.$$

On appelle **relation de Bezout** une relation du type (8.3).

**Preuve :** Supposons d'abord que  $A_1, \dots, A_n$  sont premiers entre eux. Comme le pgcd de  $A_1, \dots, A_n$  est 1, le corollaire 8.4.4 affirme qu'il existe  $n$  polynômes  $Z_1, \dots, Z_n$  tels que  $Z_1A_1 + \dots + Z_nA_n = 1$ .

Réciproquement, supposons qu'il existe  $n$  polynômes  $Z_1, \dots, Z_n$  tels que  $Z_1A_1 + \dots + Z_nA_n = 1$ . Soit  $P$  le pgcd de  $A_1, \dots, A_n$ . Comme  $P$  est un diviseur commun de  $A_1, \dots, A_n$ ,  $P$  divise également  $Z_1A_1 + \dots + Z_nA_n$ , i.e.,  $P$  divise 1. Comme  $P$  est normalisé,  $P$  ne peut être égal qu'à 1. En conclusion,  $A_1, \dots, A_n$  sont premiers entre eux. ■

### Comment trouver une relation de Bezout ?

Comme dans  $\mathbb{Z}$ , pour trouver une relation de Bezout, on utilise l'algorithme d'Euclide, en écrivant à chaque étape le quotient et le reste de la division euclidienne de  $R_{i+1}$  par  $R_i$  (cf les notations de l'algorithme).

Par exemple, soit  $A_1 = X^4 + 1$  et  $A_2 = X^3 + 1$ .

— Posons  $R_1 = A_1$  et  $R_2 = A_2$ .

— Effectuons la division euclidienne de  $R_1$  par  $R_2$ . Alors  $R_1 = XR_2 + (-X + 1)$ , donc  $R_3 = (-X + 1) = A_1 - XA_2$ .

— Effectuons maintenant la division euclidienne de  $R_2$  par  $R_3$ . Alors  $R_2 = R_3(-X^2 - X - 1) + 2$  et on pose  $R_4 = 2$ .

— D'où

$$\begin{aligned} 1 &= \frac{1}{2}A_2 + \frac{1}{2}(X^2 + X + 1)(-X + 1) = \frac{1}{2}A_2 + \frac{1}{2}(X^2 + X + 1)(A_1 - XA_2) \\ &= \frac{1}{2}(X^2 + X + 1)A_1 - \frac{1}{2}(X^3 + X^2 + X - 1)A_2. \end{aligned}$$

On a donc trouvé la relation de Bezout suivante :

$$\frac{1}{2}(X^2 + X + 1)A_1 - \frac{1}{2}(X^3 + X^2 + X - 1)A_2 = 1.$$

**Théorème 8.5.4 (Gauss)** Soient  $A, B$  et  $C$  trois polynômes non nuls. Si  $A$  divise  $BC$  et est premier avec  $B$ , alors  $A$  divise  $C$ .

**Preuve :** Comme  $A$  et  $B$  sont premiers entre eux, le théorème de Bezout affirme qu'il existe  $Z_1$  et  $Z_2$  tels que

$$Z_1A + Z_2B = 1. \quad \text{D'où } Z_1AC + Z_2BC = C.$$

Comme  $A$  divise à la fois  $AC$  et  $BC$ ,  $A$  divise  $Z_1AC + Z_2BC$ , c'est-à-dire que  $A$  divise  $C$ . ■

Une conséquence cruciale du théorème de Gauss est le corollaire suivant :

**Corollaire 8.5.5** Soient  $A, B$  et  $C$  trois polynômes, avec  $A$  et  $B$  non nuls et premiers entre eux. Si  $A|C$  et  $B|C$  alors  $(AB)|C$ .

**Preuve :** Comme  $A|C$ , il existe un polynôme  $D$  tel que  $C = AD$ . Or  $B|C$ , donc  $B|(AD)$ . Comme  $A$  et  $B$  sont premiers entre eux, le théorème de Gauss affirme que  $B|D$ . Donc  $(AB)|C$ . ■

Une autre application du théorème de Bezout est la suivante :

**Proposition 8.5.6** Soit  $\{A_1, \dots, A_n\}$  une famille de polynômes non nuls. Alors un polynôme non nul et normalisé  $P$  est le pgcd de  $A_1, \dots, A_n$  si et seulement si  $P$  est un diviseur commun de  $A_1, \dots, A_n$  et les polynômes  $\frac{A_1}{P}, \dots, \frac{A_n}{P}$  sont premiers entre eux.

**Preuve :** Supposons d'abord que  $P$  est le pgcd de  $A_1, \dots, A_n$ . Alors on sait que  $P$  est un diviseur commun de  $A_1, \dots, A_n$ . De plus, le corollaire 8.4.4 affirme qu'il existe des polynômes  $Z_1, \dots, Z_n$  tels que  $Z_1 A_1 + \dots + Z_n A_n = P$ . En divisant cette égalité par  $P$ , on obtient :

$$Z_1 \frac{A_1}{P} + \dots + Z_n \frac{A_n}{P} = 1 .$$

Le théorème de Bezout affirme alors que les polynômes  $\frac{A_1}{P}, \dots, \frac{A_n}{P}$  sont premiers entre eux.

Réciproquement, supposons que  $P$  est un diviseur commun de  $A_1, \dots, A_n$  et les polynômes  $\frac{A_1}{P}, \dots, \frac{A_n}{P}$  sont premiers entre eux. Notons  $D$  le pgcd de  $A_1, \dots, A_n$ . Comme  $P$  est un diviseur commun de  $A_1, \dots, A_n$ ,  $P$  divise  $D$  par définition du pgcd. De plus, comme  $\frac{A_1}{P}, \dots, \frac{A_n}{P}$  sont premiers entre eux, le théorème de Bezout affirme qu'il existe des polynômes  $Z_1, \dots, Z_n$  tels que  $Z_1 \frac{A_1}{P} + \dots + Z_n \frac{A_n}{P} = 1$ , ce qui implique que  $Z_1 A_1 + \dots + Z_n A_n = P$ . Comme  $D$  est un diviseur commun de  $A_1, \dots, A_n$ ,  $D$  divise  $Z_1 A_1 + \dots + Z_n A_n$ , et donc divise  $P$ . Nous avons prouvé que les polynômes normalisés  $D$  et  $P$  se divisent l'un l'autre. Ils sont donc égaux. ■

Nous expliquons maintenant comment calculer le ppcm de deux polynômes à partir de leur pgcd : pour cela, commençons par un résultat intermédiaire.

**Proposition 8.5.7** Soient  $A$  et  $B$  deux polynômes non nuls premiers entre eux, de coefficients dominant respectif  $a$  et  $b$ . Alors le ppcm de  $A$  et  $B$  est égal à  $\frac{1}{ab} AB$ .

**Preuve :** On suppose pour simplifier, que  $A$  et  $B$  sont normalisés. Posons  $P = \text{ppcm}\{A, B\}$ . Comme  $AB$  est un multiple commun de  $A$  et de  $B$ ,  $P$  divise  $AB$  (condition (b) de la définition du ppcm).

Comme  $A$  divise  $P$ , il existe un polynôme  $K$  tel que  $P = AK$ . Or  $B$  divise également  $P$ , donc divise  $AK$ . Or  $A$  et  $B$  sont premiers entre eux. Le théorème de Gauss affirme alors que  $B$  divise  $K$ . Donc il existe un polynôme  $R$  tel que  $K = BR$ . D'où  $P = ABR$ . On en déduit que  $AB$  divise  $P$ .

Les polynômes normalisés  $P$  et  $AB$  se divisent l'un l'autre, donc sont égaux. ■

Voici maintenant la relation entre ppcm et pgcd dans le cas général :

**Théorème 8.5.8** Soient  $A$  et  $B$  deux polynômes non nuls de coefficient dominant respectivement  $a$  et  $b$ . Alors

$$ab \text{pgcd}\{A, B\} \text{ppcm}\{A, B\} = AB .$$

**Preuve :** On suppose pour simplifier que  $A$  et  $B$  sont normalisés. Posons  $D = \text{pgcd}\{A, B\}$ . La proposition 8.5.6 affirme que  $D$  divise  $A$  et  $B$  et que les polynômes  $\frac{A}{D}$  et  $\frac{B}{D}$  sont premiers entre eux. D'après la proposition 8.5.7, le ppcm de  $\frac{A}{D}$  et  $\frac{B}{D}$  est égal à  $\frac{AB}{D^2}$ .

Donc

$$\text{ppcm}\{A, B\} = \text{ppcm}\left\{D \frac{A}{D}, D \frac{B}{D}\right\} = D \text{ppcm}\left\{\frac{A}{D}, \frac{B}{D}\right\} = D \frac{AB}{D^2} = \frac{AB}{D} .$$

On en déduit l'égalité désirée. ■

## 8.6 Polynômes premiers

**Définition 8.6.1** On appelle polynôme premier tout polynôme  $P$  non nul, de degré supérieur ou égal à 1, qui n'est divisible que par les polynômes constants ou par les polynômes de la forme  $\lambda P$  où  $\lambda$  est un scalaire non nul.

Voici un exemple fondamental :

**Proposition 8.6.2** Soit  $P$  un polynôme de degré 1. Alors  $P$  est premier.

**Preuve :** Si  $Q$  est un diviseur de  $P$ , comme  $P \neq 0$ ,  $\deg(Q) = 0$  ou  $\deg(Q) = 1$ . Dans le premier cas,  $Q$  est un polynôme constant. Dans le second,  $Q$  est un polynôme de degré 1, et le quotient de  $P$  par  $Q$  est un polynôme constant. Donc  $Q$  est de la forme  $\lambda P$  avec  $\lambda \neq 0$ . Par conséquent,  $P$  est un polynôme premier. ■

Le théorème suivant affirme que tout polynôme possède des diviseurs premiers :

**Théorème 8.6.3** Soit  $A$  un polynôme, avec  $\deg(A) \geq 1$ . Il existe un polynôme premier qui divise  $A$ .

**Preuve :** Notons  $\mathcal{I}$  l'ensemble des polynômes de degré supérieur ou égal à 1 qui divisent  $A$ . Notons que  $\mathcal{I}$  est non vide car  $A$  appartient à  $\mathcal{I}$ . Soit maintenant

$$E = \{n \in \mathbb{N}^* \mid \exists B \in \mathcal{I} \text{ avec } n = \deg(B)\} .$$

Comme  $A$  appartient à  $\mathcal{I}$ ,  $n = \deg(A)$  appartient à  $E$ . Donc  $E$  est une partie non vide de  $\mathbb{N}$  et possède un plus petit élément, noté  $p$ . Par définition de  $E$ , il existe un polynôme  $P \in \mathcal{I}$  de degré  $p$ . Comme  $P \in \mathcal{I}$ ,  $p = \deg(P) \geq 1$ .

Montrons que  $P$  est premier. Soit  $Q$  un polynôme qui divise  $P$ . Alors  $Q$  divise aussi  $A$ , car, comme  $P \in \mathcal{I}$ ,  $P$  divise  $A$ . Il y a alors deux possibilités :

- soit  $\deg(Q) = 0$ , c'est-à-dire que  $Q$  est constant,
- soit  $\deg(Q) \geq 1$ , et donc  $\deg(Q)$  appartient à  $E$ . Or  $p = \deg(P)$  est le plus petit élément de  $E$ .

Donc  $\deg(Q) \geq \deg(P)$ . Comme  $Q$  divise  $P$ , il existe un scalaire non nul  $\lambda$  tel que  $Q = \lambda P$ .

On a prouvé que, si  $Q$  divise  $P$ , alors soit  $Q$  est constant, soit  $Q$  est de la forme  $\lambda P$  avec  $\lambda \neq 0$ . Donc  $P$  est un diviseur premier de  $A$ . ■

## 8.7 Décomposition d'un polynôme en facteurs premiers

**Théorème 8.7.1** Tout polynôme non nul  $A$  peut s'écrire d'une manière unique sous la forme :

$$A = \lambda (P_1)^{k_1} \dots (P_m)^{k_m}$$

où  $\lambda$  est un scalaire non nul,  $P_1, \dots, P_m$  sont des polynômes premiers et normalisés distincts et  $k_1, \dots, k_m$  sont des entiers strictement positifs.

**Remarque 8.7.2** *L'unicité signifie ici que si on a deux expressions de cette forme :*

$$A = \lambda_1(P_1)^{k_1} \dots (P_m)^{k_m} = \lambda_2(Q_1)^{r_1} \dots (Q_n)^{r_n}$$

avec  $\lambda_1$  et  $\lambda_2$  des scalaires non nuls,  $P_1, \dots, P_m$  (respectivement  $Q_1, \dots, Q_n$ ) des polynômes premiers et normalisés distincts et  $k_1, \dots, k_m$  (respectivement  $r_1, \dots, r_n$ ) des entiers strictement positifs, alors  $m = n$ ,  $\lambda_1 = \lambda_2$  et, pour tout  $i \in \{1, \dots, n\}$ , il existe un indice  $j \in \{1, \dots, n\}$  tel que  $P_i = Q_j$  et  $k_i = r_j$ .

**Preuve :** On ne démontre que l'existence. On raisonne par récurrence généralisée sur le degré de  $A$ . Si  $\deg(A) = 1$ , le résultat est évident car  $A$  est premier.

Supposons le résultat vrai pour tous les polynômes de degré inférieur ou égal à  $n$ ,  $n \geq 1$ . Montrons qu'il est encore vrai pour les polynômes de degré  $n + 1$ . Soit  $A$  un polynôme de degré  $n + 1$ . D'après le théorème 8.6.3, le polynôme  $A$  possède un diviseur premier, noté  $P$ . Posons  $B = \frac{A}{P}$ .

Il y a alors 2 cas : soit  $B$  est constant, et alors le résultat est démontré. Soit  $\deg(B) \geq 1$ , et on a alors  $1 \leq \deg(B) < \deg(A) = n + 1$ . Par hypothèse de récurrence, il existe alors un scalaire  $\lambda \neq 0$ , des polynômes premiers et normalisés distincts  $P_1, \dots, P_m$  et des entiers strictement positifs  $k_1, \dots, k_m$  tels que

$$B = \lambda(P_1)^{k_1} \dots (P_m)^{k_m} .$$

Donc

$$A = \lambda P (P_1)^{k_1} \dots (P_m)^{k_m}$$

et  $A$  possède une décomposition en facteurs premiers.

Par récurrence, on en déduit l'existence de la décomposition pour tout polynôme  $A$ . ■

**Proposition 8.7.3 Application au calcul du pgcd et du ppcm :** *Soient  $A$  et  $B$  deux polynômes non nuls de degré supérieurs à 1. On suppose que*

$$A = \lambda_1(P_1)^{k_1} \dots (P_m)^{k_m} \text{ et } B = \lambda_2(P_1)^{r_1} \dots (P_m)^{r_m}$$

avec  $\lambda_1$  et  $\lambda_2$  des scalaires non nuls,  $P_1, \dots, P_m$  des polynômes premiers et normalisés distincts et  $k_1, \dots, k_m$  (respectivement  $r_1, \dots, r_m$ ) des entiers positifs ou nuls (de façon à avoir une écriture commune pour  $A$  et  $B$ ). Alors

$$\text{pgcd}\{A, B\} = (P_1)^{\min\{k_1, r_1\}} \dots (P_m)^{\min\{k_m, r_m\}} \text{ et } \text{ppcm}\{A, B\} = (P_1)^{\max\{k_1, r_1\}} \dots (P_m)^{\max\{k_m, r_m\}} .$$

## 8.8 Racine d'un polynôme

A partir de maintenant, nous sommes obligés de faire une nette distinction entre le cas réel et le cas complexe. Afin de ne pas trop alourdir les énoncés, on introduit la notation  $\mathbf{k}$  qui signifie indifféremment  $\mathbb{R}$  ou  $\mathbb{C}$ , et  $\mathbf{k}[X]$  qui signifie  $\mathbb{R}[X]$  ou  $\mathbb{C}[X]$ . La notation  $\mathbf{k}$  signifie toujours la même chose à l'intérieur d'un même énoncé.

**Définition 8.8.1 (Racine)** *Soit  $P$  un polynôme de  $\mathbf{k}[X]$  et  $\alpha \in \mathbf{k}$  un scalaire. On dit que  $\alpha$  est une racine de  $P$  si  $P(\alpha) = 0$ .*

**Exemple 8.8.2** *Le polynôme  $P(X) = X^2 + 1$  n'a pas de racine réelle, mais a pour racines complexes  $i$  et  $-i$ .*

**Lemme 8.8.3** Soit  $P(X) = aX + b$  un polynôme de  $\mathbf{k}[X]$  avec  $a \neq 0$ . Alors  $P$  possède une, et une seule, racine dans  $\mathbf{k}$ .

**Preuve :** Il est clair que la seule racine de  $P$  est  $-b/a$ . ■

**Lemme 8.8.4** Si  $P|Q$  et  $\alpha$  est une racine de  $P$ , alors  $\alpha$  est une racine de  $Q$ .

**Preuve :** En effet, comme  $P$  divise  $Q$ , il existe un polynôme  $A$  tel que  $Q = AP$ . Alors  $Q(\alpha) = A(\alpha)P(\alpha) = 0$  car  $P(\alpha) = 0$ . ■

La caractérisation suivante des racines joue un rôle essentiel dans toute la suite :

**Théorème 8.8.5** Soit  $P \in \mathbf{k}[X]$  et  $\alpha \in \mathbf{k}$ . Alors  $\alpha$  est une racine de  $P$  si et seulement si  $(X - \alpha)$  divise  $P$  dans  $\mathbf{k}[X]$ .

**Preuve :** On suppose d'abord que  $\alpha$  est une racine de  $P$ . Pour montrer que  $(X - \alpha)$  divise  $P$ , notons  $Q$  et  $R$  le quotient et le reste de la division euclidienne de  $P$  par  $(X - \alpha)$  :

$$P(X) = Q(X)(X - \alpha) + R(X) \text{ et } \deg(R) < \deg(X - \alpha) = 1.$$

Comme  $\deg(X - \alpha) = 1$ ,  $R$  est un polynôme constant. Or

$$0 = P(\alpha) = Q(\alpha) \cdot 0 + R(\alpha) = R(\alpha)$$

car  $\alpha$  est une racine de  $P$ . Donc le polynôme constant  $R$  est nul, ce qui prouve que  $(X - \alpha)$  divise  $P$ .

Réciproquement, si  $(X - \alpha)$  divise  $P$ , alors comme  $\alpha$  est une racine de  $(X - \alpha)$ ,  $\alpha$  est aussi une racine de  $P$ . ■

**Corollaire 8.8.6** Soient  $n$  un entier naturel et  $P$  un polynôme de degré inférieur ou égal à  $n$ . Si  $P$  a au moins  $n + 1$  racines distinctes, alors  $P$  est égal au polynôme nul.

**Preuve :** On fait la preuve par récurrence sur  $n$ . Pour  $n = 0$ , c'est vrai car un polynôme constant qui s'annule en au moins un point est identiquement nul.

On suppose que le résultat est vrai pour  $n$ . Montrons-le pour  $n + 1$ . Soit  $P$  un polynôme de degré au plus  $(n + 1)$ , qui possède au moins  $(n + 2)$  racines distinctes  $\alpha_1, \dots, \alpha_{n+2}$ . On sait alors que  $P$  est divisible par  $(X - \alpha_{n+2})$ . Soit  $Q$  tel que  $P(X) = Q(X)(X - \alpha_{n+2})$ . Comme le degré de  $P$  est au plus  $n + 1$ , le degré de  $Q$  est au plus  $n$ . Montrons que  $\alpha_1, \dots, \alpha_{n+1}$  sont des racines de  $Q$ . En effet

$$\forall i \in \{1, \dots, n + 1\}, P(\alpha_i) = 0 = (\alpha_i - \alpha_{n+2})Q(\alpha_i).$$

Comme  $\alpha_i \neq \alpha_{n+2}$  si  $i \in \{1, \dots, n + 1\}$ , cette dernière égalité montre que  $Q(\alpha_i) = 0$ . Donc, pour tout  $i \in \{1, \dots, n + 1\}$ ,  $\alpha_i$  est une racine de  $Q$ . Nous avons montré que le polynôme  $Q$ , de degré au plus  $n$ , possède au moins  $n + 1$  racines distinctes. L'hypothèse de récurrence affirme alors que  $Q$  est nul. Donc  $P = (X - \alpha_{n+2})Q$  l'est aussi. ■

Le théorème suivant est souvent appelé **théorème fondamental de l'algèbre** :

**Théorème 8.8.7 (dit de d'Alembert)** Soit  $P \in \mathcal{C}[X]$  un polynôme non constant. Alors  $P$  possède au moins une racine complexe.

On dit aussi que  $\mathcal{C}$  est algébriquement clos. La démonstration de ce résultat est difficile et hors programme.

**Corollaire 8.8.8** Les polynômes premiers de  $\mathcal{C}[X]$  sont les polynômes de degré 1.

**Preuve :** Soit  $P$  un polynôme de degré 1. Alors nous avons déjà montré que  $P$  est premier.

Réciproquement, soit  $P$  un polynôme premier de  $\mathcal{C}[X]$ . Comme  $\deg(P) \geq 1$ ,  $P$  n'est pas constant. Donc le théorème de d'Alembert affirme que  $P$  possède au moins une racine  $\alpha \in \mathcal{C}$ . Donc  $(X - \alpha)$  divise  $P$ . Comme  $P$  est premier, cela implique qu'il existe une constante  $\beta \in \mathcal{C}^*$  telle que  $P(X) = \beta(X - \alpha)$  et prouve que  $P$  est un polynôme de degré 1. ■

On en déduit la factorisation en facteurs premiers d'un polynôme de  $\mathcal{C}[X]$ .

**Théorème 8.8.9** Soit  $P$  un polynôme de  $\mathcal{C}[X]$ ,  $\alpha_1, \dots, \alpha_n$  les racines distinctes de  $P$  dans  $\mathcal{C}$ . Il existe alors une constante  $\beta \in \mathcal{C}^*$ , et des entiers strictement positifs  $k_1, \dots, k_n$  tels que

$$P(X) = \beta(X - \alpha_1)^{k_1} \dots (X - \alpha_n)^{k_n} .$$

De plus, le degré de  $P$  est  $k_1 + k_2 + \dots + k_n$ .

**Preuve :** C'est une conséquence immédiate du théorème de factorisation en facteurs premiers d'un polynôme et de la caractérisation des polynômes premiers de  $\mathcal{C}[X]$ . ■

Nous cherchons maintenant à caractériser les polynômes premiers de  $\mathbb{R}[X]$ . Pour cela, nous avons besoin de deux résultats préliminaires :

**Lemme 8.8.10** Soit  $P$  un polynôme de  $\mathbb{R}[X]$  et  $\alpha \in \mathcal{C}$  une racine de  $P$  dans  $\mathcal{C}[X]$ .

Alors le conjugué de  $\alpha$ , noté  $\bar{\alpha}$ , est aussi une racine de  $P$ .

**Preuve :** En effet, si  $P(X) = a_0 + a_1X + \dots + a_nX^n$ ,  $\alpha$  est une racine de  $P$  signifie que  $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ . Prenons le conjugué de cette expression :

$$0 = \overline{a_0 + a_1\alpha + \dots + a_n\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \dots + \overline{a_n\alpha^n} = a_0 + a_1\bar{\alpha} + \dots + a_n\bar{\alpha}^n = P(\bar{\alpha})$$

car les coefficients  $a_i$  sont réels. Ceci prouve que  $\bar{\alpha}$  est une racine de  $P$ . ■

**Lemme 8.8.11** Soient  $P$  et  $Q$  deux polynômes de  $\mathbb{R}[X]$ . On suppose que  $Q$  divise  $P$  dans  $\mathcal{C}[X]$ . Alors  $Q$  divise  $P$  dans  $\mathbb{R}[X]$ .

**Preuve :** Par hypothèse, il existe un polynôme  $R \in \mathcal{C}[X]$  tel que  $P = QR$ . Montrons que les coefficients de  $R$  sont en fait réels. En effet, comme  $P$  et  $Q$  sont des polynômes réels,

$$\bar{P} = P = \overline{QR} = \bar{Q}\bar{R} = Q\bar{R} .$$

Donc  $\bar{R}$  est également le quotient de  $P$  par  $Q$ . Ce quotient étant unique, cela prouve que  $\bar{R} = R$ , c'est-à-dire que  $R$  est à coefficients réels.

Nous décrivons maintenant les polynômes premiers de  $\mathbb{R}[X]$ .

**Théorème 8.8.12** *Soit  $P$  un polynôme de  $\mathbb{R}[X]$ . Alors  $P$  est premier si et seulement si, soit  $\deg(P) = 1$ , soit  $\deg(P) = 2$  et  $P$  n'a pas de racine réelle.*

**Preuve :** Montrons d'abord que,  $\deg(P) = 1$ , ou si  $\deg(P) = 2$  et  $P$  n'a pas de racine réelle, alors  $P$  est premier. Si  $\deg(P) = 1$ , nous avons vu que c'est bien le cas. Supposons maintenant que  $\deg(P) = 2$  et que  $P$  n'a pas de racine réelle. Si  $Q \in \mathbb{R}[X]$  est un diviseur de  $P$ , alors, comme  $P \neq 0$ , on a  $\deg(Q) = 0, 1$  ou  $2$ . Supposons un instant que  $\deg(Q) = 1$ . Alors  $Q$  possède une racine réelle  $\alpha \in \mathbb{R}$ . Or  $Q$  divise  $P$ , donc  $\alpha$  est aussi une racine de  $P$ . C'est impossible car  $P$  n'a pas de racine réelle par hypothèse. Donc soit  $\deg(Q) = 0$ , et  $Q$  est alors constant, soit  $\deg(Q) = 2 = \deg(P)$ , et, comme  $Q$  divise  $P$ , il existe un réel non nul  $\lambda$  tel que  $Q = \lambda P$ . Ceci prouve que  $P$  est premier.

Réciproquement, supposons que  $P$  soit un polynôme premier. Comme  $\deg(P) \geq 1$ ,  $P$  possède au moins une racine  $\alpha$ , réelle ou complexe (cf théorème de d'Alembert). Si  $\alpha$  est réel, alors le polynôme réel  $(X - \alpha)$  divise  $P$ . Comme  $P$  est premier, il existe  $\beta \in \mathbb{R}^*$  tel que  $P(X) = \beta(X - \alpha)$ . Donc  $P$  est de degré 1. Supposons maintenant que  $\alpha \notin \mathbb{R}$ . Alors le conjugué de  $\alpha$ , noté  $\bar{\alpha}$ , est différent de  $\alpha$  et est aussi une racine de  $P$ . Les polynômes  $(X - \alpha)$  et  $(X - \bar{\alpha})$  divisent  $P$  dans  $\mathbb{C}[X]$ . Ces polynômes sont premiers (car de degré 1), et distincts, car  $\alpha \neq \bar{\alpha}$ . Donc ces polynômes sont premiers entre eux. Comme chacun d'eux divise  $P$  dans  $\mathbb{C}[X]$ , leur produit  $(X - \alpha)(X - \bar{\alpha})$  divise aussi  $P$  dans  $\mathbb{C}[X]$ . Or

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$$

est un polynôme réel. Donc  $X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$  divise  $P$  dans  $\mathbb{R}[X]$ . Comme  $P$  est premier, il existe une constante  $\beta \in \mathbb{R}^*$  telle que  $P(X) = \beta(X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2)$ , et  $P$  est un polynôme de degré 2 sans racine réelle.

## 8.9 Dérivée d'un polynôme et formule de Taylor

**Définition 8.9.1 (Dérivée)** *Soit  $P$  un polynôme de  $\mathbf{k}[X]$ ,  $P(X) = a_0 + a_1X + \dots + a_nX^n = \sum_{k=0}^n a_kX^k$ . Le polynôme dérivé de  $P$ , noté  $P'$ , est le polynôme*

$$P'(X) = a_1 + 2a_2X + 3a_3X^2 + \dots + na_nX^{n-1} = \sum_{k=1}^n ka_kX^{k-1}.$$

Notons en particulier que :

**Proposition 8.9.2** *Si  $P \in \mathbf{k}[X]$  et si  $\deg(P) \geq 1$ , alors  $\deg(P') = \deg(P) - 1$ .*

**Proposition 8.9.3** *Si  $P_1$  et  $P_2$  sont deux polynômes de  $\mathbf{k}[X]$ , et si  $\lambda \in \mathbf{k}$ , alors*

1. **Dérivée d'une somme :**  $(P_1 + P_2)' = P_1' + P_2'$ ,
2. **Dérivée du produit par un scalaire :**  $(\lambda P)' = \lambda P'$ ,
3. **Dérivée d'un produit de polynômes :**  $(P_1 P_2)' = P_1' P_2 + P_1 P_2'$ .

**Preuve :** Seule la dernière assertion pose vraiment une difficulté de démonstration, c'est donc elle seule que nous démontrons. Remarquons d'abord que le résultat est vrai si  $P_1(X) = X^m$  et  $P_2(X) = X^n$ . En effet,

$$(P_1P_2)'(X) = (X^{m+n})' = (m+n)X^{n+m-1}$$

tandis que

$$P_1'(X)P_2(X) + P_1(X)P_2'(X) = mX^{m-1}X^n + X^m(nX^{n-1}) = mX^{m+n-1} + nX^{m+n-1} = (m+n)X^{n+m-1}.$$

Démontrons maintenant le résultat dans le cas général. Soient  $P_1(X) = \sum_{k=0}^n a_k X^k$  et  $P_2(X) = \sum_{i=0}^n b_i X^i$ . Alors

$$\begin{aligned} (P_1P_2)'(X) &= \left( \sum_{k=0}^n \sum_{i=0}^n a_k b_i X^{k+i} \right)' \\ &= \sum_{k=0}^n \sum_{i=0}^n a_k b_i (X^{k+i})' \\ &= \sum_{k=0}^n \sum_{i=0}^n a_k b_i ((X^k)'X^i + X^k(X^i)') \\ &= \left( \sum_{k=0}^n \sum_{i=0}^n a_k b_i (X^k)'X^i \right) + \left( \sum_{k=0}^n \sum_{i=0}^n a_k b_i X^k(X^i)' \right) \\ &= \left( \sum_{k=0}^n a_k (X^k)' \right) \left( \sum_{i=0}^n b_i X^i \right) + \left( \sum_{k=0}^n a_k X^k \right) \left( \sum_{i=0}^n b_i (X^i)' \right) \\ &= P_1'(X)P_2(X) + P_1(X)P_2'(X) \end{aligned}$$

■

**Définition 8.9.4 (Dérivées nièmes)** Pour  $n \in \mathbb{N}^*$ , on définit par récurrence la dérivée nième d'un polynôme, notée  $P^{(n)}$  :

$P^{(1)}(X) = P'(X)$  et, si  $P^{(n)}$  a été défini, alors  $P^{(n+1)} = (P^{(n)})'$ .

**Par convention,** on notera  $P^{(0)} = P$ .

**Proposition 8.9.5 Exemple fondamental**

Si  $P(X) = X^m$  (avec  $m \geq 1$ ), alors

$$\forall k \in \{0, \dots, m\}, P^{(k)}(X) = \frac{m!}{(m-k)!} X^{m-k},$$

et

$$\forall k \geq m+1, P^{(k)}(X) = 0.$$

**Preuve :** On fait la preuve par récurrence sur  $k$ . Pour  $k = 0$  et  $k = 1$ , c'est évident.

On suppose le résultat vrai pour  $k \geq 1$ , et on le montre pour  $k+1$ . L'hypothèse de récurrence affirme que, si  $k \leq m$ , alors  $P^{(k)}(X) = \frac{m!}{(m-k)!} X^{m-k}$ , et si  $k > m$ , alors  $P^{(k)}(X) = 0$ .

Supposons d'abord  $k+1 \leq m$ . On dérive l'égalité  $P^{(k)}(X) = \frac{m!}{(m-k)!} X^{m-k}$  :

$$P^{(k+1)}(X) = \frac{m!}{(m-k)!} (m-k) X^{m-k-1} = \frac{m!}{(m-k-1)!} X^{m-k-1},$$

ce qui est le résultat désiré. Si  $k = m$ , alors  $P^{(k)}(X)$  est un polynôme constant. Donc sa dérivée est nulle :  $P^{(k+1)}(X) = 0$ . Finalement, si  $k > m$ , alors  $P^{(k)}(X)$  est nul, donc  $P^{(k+1)}(X) = 0$ . Nous avons montré le résultat au rang  $k+1$ .

Par récurrence, on en déduit le résultat pour tout  $k$ .

■

**Théorème 8.9.6 (Formules de Taylor)** Soient  $n$  un entier naturel et  $P$  un polynôme de  $\mathbf{k}[X]$  de degré au plus  $n$ . Alors, pour tout  $\alpha \in \mathbf{k}$ , on a

$$P(X) = \sum_{k=0}^n \frac{(X-\alpha)^k}{k!} P^{(k)}(\alpha).$$

**Preuve :** Démontrons d'abord la formule pour les polynômes  $P_i(X) = X^i$  ( $i \in \{0, \dots, n\}$ ) :

$$\sum_{k=0}^n \frac{(X-\alpha)^k}{k!} P_i^{(k)}(\alpha) = \sum_{k=0}^i \frac{(X-\alpha)^k}{k!} \frac{i!}{(i-k)!} \alpha^{(i-k)} = \sum_{k=0}^i \frac{i!}{k!(i-k)!} (X-\alpha)^k \alpha^{(i-k)}$$

Appliquons la formule du binôme de Newton à cette égalité :

$$\sum_{k=0}^i \frac{i!}{k!(i-k)!} (X-\alpha)^k \alpha^{(i-k)} = (X-\alpha+\alpha)^i = X^i = P_i(X).$$

Donc la formule est démontrée pour les polynômes  $P_i(X) = X^i$ .

Montrons-la maintenant pour un polynôme  $P$  quelconque de degré inférieur ou égal à  $n$  :  $P(X) = \sum_{i=0}^n a_i X^i = \sum_{i=0}^n a_i P_i(X)$ .

$$\sum_{k=0}^n \frac{(X-\alpha)^k}{k!} P^{(k)}(\alpha) = \sum_{k=0}^n \frac{(X-\alpha)^k}{k!} \left( \sum_{i=0}^n a_i P_i^{(k)}(\alpha) \right) = \sum_{i=0}^n a_i \left( \sum_{k=0}^n \frac{(X-\alpha)^k}{k!} P_i^{(k)}(\alpha) \right)$$

Or nous avons déjà montré la formule de Taylor pour les polynômes  $P_i$ . Donc

$$\sum_{k=0}^n \frac{(X-\alpha)^k}{k!} P^{(k)}(\alpha) = \sum_{i=0}^n a_i P_i(X) = P(X).$$

■

## 8.10 Multiplicité d'une racine

**Théorème 8.10.1 (Multiplicité d'une racine)** Soit  $P$  un polynôme non nul de  $\mathbf{k}[X]$  et  $\alpha \in \mathbf{k}$  une racine de  $P$ .

Il existe un unique entier  $k \in \mathbb{N}^*$  tel que

- a)  $(X-\alpha)^k$  divise  $P$ ,
- b)  $(X-\alpha)^{k+1}$  ne divise pas  $P$ .

On dit que la racine  $\alpha$  est de multiplicité  $k$ .

Une racine de multiplicité 1 est également appelée **racine simple**, une racine de multiplicité 2, **racine double**, etc...

**Preuve :** Montrons d'abord qu'il existe un entier  $k \geq 1$  tel que  $(X-\alpha)^k$  divise  $P$  et  $(X-\alpha)^{k+1}$  ne divise pas  $P$ . Soit  $A$  l'ensemble des entiers naturels  $n$  tels que  $(X-\alpha)^n$  divise pas  $P$ . Alors  $A$  est non vide car, comme  $P$  est non nul,  $n = \deg(P)$  appartient à  $A$ . Soit  $k$  le plus petit élément de  $A$ . Alors  $k \geq 1$  car  $(X-\alpha)$  divise  $P$ , et donc  $0 \notin A$ . De plus, comme  $k$  appartient à  $A$ ,  $(X-\alpha)^{k+1}$  ne divise pas  $P$ . Enfin, comme  $k$  est le plus petit élément de  $A$ , l'entier naturel  $k-1$  n'appartient pas à  $A$ , et donc  $(X-\alpha)^k$  divise  $P$ . Donc nous avons prouvé l'existence d'un entier  $k$  possédant les propriétés désirées.

Montrons maintenant que cet entier est unique. Soit  $n \geq 1$  un autre entier tel que  $(X - \alpha)^n$  divise  $P$  et  $(X - \alpha)^{n+1}$  ne divise pas  $P$ . Notons que  $n$  appartient à l'ensemble  $A$  défini plus haut. De plus, pour tout entier  $m < n$ , le polynôme  $(X - \alpha)^{m+1}$  divise  $(X - \alpha)^n$ , et donc divise  $P$ . On a donc montré que, pour tout entier  $m < n$ ,  $m$  n'appartient pas à  $A$ . Donc  $n$  est le plus petit élément de  $A$ , et  $n = k$ .

■

**Théorème 8.10.2** Soient  $P$  un polynôme non nul de  $\mathbf{k}[X]$ ,  $\alpha \in \mathbf{k}$  une racine de  $P$  et  $k$  un entier naturel non nul.

Alors  $\alpha$  est de multiplicité  $k$  si et seulement si

$$\forall n \in \{0, \dots, k-1\}, P^{(n)}(\alpha) = 0 \text{ et } P^{(k)}(\alpha) \neq 0.$$

**Preuve :** Soit  $r \geq 1$  le plus grand entier tel que  $\forall n \in \{0, \dots, r-1\}, P^{(n)}(\alpha) = 0$ . Un tel entier existe car, si  $P$  est de degré  $d$ , alors  $P^{(d)}$  est un polynôme constant et non nul. Donc  $P^{(d)}(\alpha) \neq 0$ . Notre objectif est de montrer que  $r$  est la multiplicité de la racine  $\alpha$ .

Notons d'abord que  $P^{(r)}(\alpha) \neq 0$ . Ecrivons la formule de Taylor en  $\alpha$  : si  $\deg(P) = m$  (avec  $m \geq r$ ), alors

$$P(X) = \sum_{n=0}^m \frac{(X - \alpha)^n}{n!} P^{(n)}(\alpha) = \sum_{n=r}^m \frac{(X - \alpha)^n}{n!} P^{(n)}(\alpha) = (X - \alpha)^r \left( \sum_{n=r}^m \frac{(X - \alpha)^{n-r}}{n!} P^{(n)}(\alpha) \right).$$

Notons  $Q(X)$  le polynôme  $\sum_{n=r}^m \frac{(X - \alpha)^{n-r}}{n!} P^{(n)}(\alpha)$ . On peut remarquer que  $Q(\alpha) = \frac{P^{(r)}(\alpha)}{r!}$  est non nul.

Donc  $(X - \alpha)^r$  divise  $P$  mais  $(X - \alpha)^{r+1}$  ne divise pas  $P$  car sinon,  $(X - \alpha)$  diviserait  $Q$ , ce qui est en contradiction avec le fait que  $Q(\alpha) \neq 0$ .

On a donc prouvé que  $r$  est la multiplicité de  $\alpha$ .

■

## 8.11 Applications aux fractions rationnelles

**Définition 8.11.1** On appelle fraction rationnelle toute expression de la forme  $\frac{P}{Q}$  où  $P \in \mathbf{k}[X]$ ,  $Q \in \mathbf{k}[X]$  et  $Q \neq 0$ .

**Notation :** L'ensemble des fractions rationnelles sur  $\mathbf{k}$  (avec  $\mathbf{k} = \mathbb{R}$  ou  $\mathbf{k} = \mathbb{C}$ ) est noté  $\mathbf{k}(X)$ .

**Proposition 8.11.2 (Forme irréductible d'une fraction rationnelle)** Soit  $R \in \mathbf{k}(X)$  une fraction rationnelle non nulle. Il existe alors un unique couple de polynômes  $(P, Q) \in \mathbf{k}[X] \times \mathbf{k}[X]$  tels que

- i)  $Q \neq 0$  est normalisé,
- ii)  $R = \frac{P}{Q}$ ,
- iii)  $P$  et  $Q$  sont premiers entre eux.

**Terminologie :** Lorsque l'on écrit la fraction rationnelle  $R$  sous la forme  $\frac{P}{Q}$  avec  $P$  et  $Q$  comme ci-dessus, on dit que la fraction rationnelle  $R$  est mise **sous forme irréductible**.

La preuve du théorème étant identique à celle du théorème correspondant dans  $\mathbb{Q}$ , nous l'omettons.



# Chapitre 9

## Matrices

Dans ce chapitre, nous apprenons les rudiments du calcul matriciel : comment (et quand) additionner deux matrices, les multiplier, les inverser.

### 9.1 Définitions et terminologie

#### 9.1.1 Définitions et notations

**Définition 9.1.1 (Matrices)**

Soient  $n$  et  $p$  deux entiers non nuls. On appelle matrice à coefficients réels (resp. complexes) la donnée de  $n \times p$  nombres réels (resp. complexes) notés

$$\{a_{ij}\}_{i \in \{1, \dots, n\}, j \in \{1, \dots, p\}}$$

On représente la matrice sous forme d'un tableau  $A$  à  $n$  lignes et  $p$  colonnes :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1p} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{ip} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{np} \end{pmatrix}$$

On dit que  $a_{ij}$  est le terme général de la matrice  $A$  : le premier indice (ici  $i$ ) désigne toujours l'indice de ligne et le second indice (ici  $j$ ) l'indice de colonne. On écrit aussi sous forme condensée :  $A = (a_{ij})_{n,p}$  ou encore  $A = (a_{ij})$  s'il n'y a aucune ambiguïté.

Le couple  $(n, p)$  s'appelle le format de la matrice.

On désigne par  $M_{n,p}(\mathbb{R})$  (resp.  $M_{n,p}(\mathbb{C})$ ) l'ensemble des matrices à coefficients réels (resp. complexes) à  $n$  lignes et  $p$  colonnes. Si  $n = p$ , on dit que la matrice est une matrice carrée d'ordre  $n$ . Les termes  $a_{ii}$  pour  $1 \leq i \leq n$  forment la diagonale principale de la matrice de la matrice  $A$ . On note  $M_n(\mathbb{R})$  l'ensemble des matrices carrées d'ordre  $n$ .

#### 9.1.2 Matrices particulières

Soit  $A$  une matrice de  $M_{n,p}$ , c'est une

— **matrice-ligne** si  $n = 1$  et dans ce cas  $A = (x_1, \dots, x_p) \in M_{1,p}$ .

- **matrice-colonne** si  $p = 1$  et dans ce cas  $A = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ .
- **matrice triangulaire supérieure** si  $n = p$  et
 
$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, n\}, i > j \implies a_{ij} = 0.$$
- **matrice triangulaire inférieure** si  $n = p$  et
 
$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, n\}, i < j \implies a_{ij} = 0.$$
- **matrice nulle** de  $M_{n,p}(\mathbb{R})$  notée  $O$  (le contexte donnera les valeurs de  $n$  et  $p$ ) si tous ses coefficients sont nuls.
- **matrice élémentaire**  $E_{kl}$  où  $k \in \{1, \dots, n\}$  et  $l \in \{1, \dots, p\}$ ,
 
$$E_{kl} = (e_{ij})_{n,p} \text{ où } e_{kl} = 1 \text{ et tous les autres coefficients sont nuls.}$$

**Exemple 9.1.2 :**

$$A_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, A_2 = (1 \ 0 \ 4 \ 2 \ 5), A_3 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 4 & 5 \\ -1 & 5 & 9 \end{pmatrix}$$

$A_1$  est une matrice colonne, élément de  $M_{3,1}(\mathbb{R})$ ,  $A_2$  est une matrice ligne, élément de  $M_{1,5}(\mathbb{R})$ ,  $A_3$  est une matrice carrée d'ordre 3, élément de  $M_3(\mathbb{R})$ .

$$E_{21} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ est une matrice élémentaire de } M_{3,4}(\mathbb{R}).$$

$$B = \begin{pmatrix} 4 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{pmatrix} \text{ et } C = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 0 & 5 \\ 0 & 0 & 2 \end{pmatrix} \text{ sont des matrices triangulaires supérieures.}$$

et

$$D = \begin{pmatrix} 4 & 0 & 0 \\ 5 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix} \text{ est une matrice triangulaire inférieure.}$$

**Notations** On considère la matrice  $A$  par la matrice de format  $n \times p$  dont le terme courant est  $a_{ij}$ .

On note  $C_j$  la  $j$ ème colonne de  $A$  donc  $C_j$  est une matrice colonne. On notera

$$A = [C_1, \dots, C_i, \dots, C_p].$$

**Exemple 9.1.3** La matrice  $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$  de  $M_{4,3}(\mathbb{R})$  peut s'écrire

$$A = [C_1, C_2, C_3]$$

où

$$C_1 = \begin{pmatrix} 1 \\ 0 \\ 4 \\ 0 \end{pmatrix}, C_2 = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, C_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 3 \end{pmatrix}.$$

Dans la suite du chapitre, pour simplifier l'exposé, on étudie les matrices à coefficients réels, mais les définitions et les propriétés restent vraies pour les matrices à coefficients complexes. On écrira donc simplement  $M_{n,p}$  au lieu de  $M_{n,p}(\mathbb{R})$  ou  $M_{n,p}(\mathbb{C})$ .

## 9.2 Opérations sur les matrices

### 9.2.1 Egalité de deux matrices

**Définition 9.2.1 (Egalité de deux matrices)**

Deux matrices  $A = (a_{ij})_{n,p}$  et  $B = (b_{ij})_{m,q}$  sont égales si et seulement si :

-  $A$  et  $B$  ont même format :  $n = m$  et  $p = q$

et

-  $\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, p\}, a_{ij} = b_{ij}$ .

### 9.2.2 Somme de deux matrices de $M_{n,p}$

**Définition 9.2.2** Soient  $A = (a_{ij})$  et  $B = (b_{ij})$  deux éléments de  $M_{n,p}$ . On appelle somme de  $A$  et  $B$  la matrice  $C = (c_{ij})$  de format  $(n,p)$  dont le terme général est :

$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, p\}, c_{ij} = a_{ij} + b_{ij}$$

On note  $C = A + B$ .

**Proposition 9.2.3 (Propriétés de l'addition)**

1. elle est commutative :

$$\forall A \in M_{n,p}, \forall B \in M_{n,p}, \quad A + B = B + A.$$

2. elle est associative :

$$\forall A \in M_{n,p}, \forall B \in M_{n,p}, \forall C \in M_{n,p}, \quad A + (B + C) = (A + B) + C.$$

3. elle admet un élément neutre, qui est la matrice nulle :

$$\forall A \in M_{n,p}, \quad A + O = O + A = A.$$

4. toute matrice  $A$  a un unique symétrique pour l'addition, noté  $-A$  :

$$\forall A \in M_{n,p}, \quad A + (-A) = (-A) + A = O, \quad \text{avec } -A = (-a_{ij}) \text{ si } A = (a_{ij})$$

**Preuve :**

- Si  $A = (a_{ij})$  et  $B = (b_{ij})$ , le terme général de la matrice  $A + B$  est  $(a_{ij} + b_{ij})$ , tandis que le terme général de la matrice  $B + A$  est  $(b_{ij} + a_{ij})$ . Comme  $(a_{ij} + b_{ij}) = (b_{ij} + a_{ij})$ , on en déduit que les deux matrices  $A + B$  et  $B + A$ , qui ont même format  $(n,p)$  et même terme général, sont égales.

2. Si  $A = (a_{ij})$ ,  $B = (b_{ij})$  et  $C = (c_{ij})$ , la matrice  $B + C$  a pour terme général  $(b_{ij} + c_{ij})$  et la matrice  $A + (B + C)$  a pour terme général  $a_{ij} + (b_{ij} + c_{ij})$ . De même, la matrice  $(A + B) + C$  a pour terme général  $(a_{ij} + b_{ij}) + c_{ij}$ . Comme  $a_{ij} + (b_{ij} + c_{ij}) = (a_{ij} + b_{ij}) + c_{ij}$ , les matrices  $A + (B + C)$  et  $(A + B) + C$ , qui ont même format  $(n, p)$  et même terme général sont égales.
3. Si  $A = (a_{ij})$ , comme la matrice  $O$  a pour terme général  $0$ , la matrice  $A + O$  a pour terme général  $a_{ij} + 0 = a_{ij}$ . Donc les matrices  $A$  et  $A + O$ , qui ont même format  $(n, p)$  et même terme général, sont égales. On vérifie de même l'égalité  $O + A = A$ .
4. Si  $A = (a_{ij})$ , alors la somme  $A + (-A)$  a pour terme général  $(a_{ij} + (-a_{ij})) = 0$ . Comme les matrices  $A + (-A)$  et  $O$  ont même format  $(n, p)$  et même terme général, elles sont égales. Réciproquement, si  $B = (b_{ij})$  est un symétrique de  $A$ , alors on doit avoir  $A + B = O$ , c'est-à-dire  $a_{ij} + b_{ij} = 0$  pour tout  $i \in 1, \dots, n$  et tout  $j \in 1, \dots, p$ . Donc on a  $b_{ij} = -a_{ij}$  pour tout  $i \in 1, \dots, n$  et tout  $j \in 1, \dots, p$ . Par conséquent, toute matrice a un unique symétrique. ■

### 9.2.3 Multiplication d'une matrice de $M_{n,p}$ par un scalaire

**Définition 9.2.4** Soit  $A = (a_{ij})$  une matrice de  $M_{n,p}$ , et soit  $\lambda$  un scalaire (réel ou complexe suivant le cas). On appelle multiplication de la matrice  $A$  par le scalaire  $\lambda$  la matrice  $B = (b_{ij})$  de format  $(n, p)$  dont le terme général est

$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, p\}, \quad b_{ij} = \lambda a_{ij}.$$

On note  $B = \lambda A$ .

#### Proposition 9.2.5 (Propriétés de la multiplication par un scalaire)

$\forall A \in M_{n,p}, \forall B \in M_{n,p}, \forall (\lambda, \mu) \in \mathbb{R} \times \mathbb{R}$ ,

1.  $\lambda(A + B) = \lambda A + \lambda B$
2.  $(\lambda + \mu)A = \lambda A + \mu A$
3.  $\lambda(\mu A) = (\lambda\mu)A = \mu(\lambda A)$
4.  $1.A = A$

**Preuve :** On pose  $A = (a_{ij})$  et  $B = (b_{ij})$ .

1. La matrice  $(A + B)$  a pour terme général  $(a_{ij} + b_{ij})$ , et la matrice  $\lambda(A + B)$  a pour terme général  $(\lambda(a_{ij} + b_{ij}))$ . D'autre part, les matrices  $\lambda A$  et  $\lambda B$  ont pour terme général respectivement  $(\lambda a_{ij})$  et  $(\lambda b_{ij})$ . Donc la matrice  $\lambda A + \lambda B$  a pour terme général  $(\lambda a_{ij}) + (\lambda b_{ij})$ . Comme  $\lambda(a_{ij} + b_{ij}) = (\lambda a_{ij}) + (\lambda b_{ij})$ , on en déduit que les matrices  $\lambda(A + B)$  et  $\lambda A + \lambda B$ , qui ont même format  $(n, p)$  et même terme général, sont égales.
2. La matrice  $(\lambda + \mu)A$  a pour terme général  $((\lambda + \mu)a_{ij})$ . D'autre part, les matrices  $\lambda A$  et  $\mu A$  ont pour terme général respectivement  $(\lambda a_{ij})$  et  $(\mu a_{ij})$ . Donc la matrice  $\lambda A + \mu A$  a pour terme général  $(\lambda a_{ij}) + (\mu a_{ij})$ . Comme  $(\lambda + \mu)a_{ij} = (\lambda a_{ij}) + (\mu a_{ij})$ , on en déduit que les matrices  $(\lambda + \mu)A$  et  $\lambda A + \mu A$ , qui ont même format  $(n, p)$  et même terme général, sont égales.
3. La matrice  $\mu A$  a pour terme général  $(\mu a_{ij})$ , et la matrice  $\lambda(\mu A)$  a alors pour terme général  $(\lambda(\mu a_{ij}))$ . D'autre part, la matrice  $(\lambda\mu)A$  a pour terme général  $(\lambda\mu a_{ij})$ . Comme  $(\lambda(\mu a_{ij})) = (\lambda\mu a_{ij})$ , on en déduit que les matrices  $\lambda(\mu A)$  et  $(\lambda\mu)A$ , qui ont même format  $(n, p)$  et même terme général, sont égales.

L'égalité  $(\lambda\mu)A = \mu(\lambda A)$  s'obtient de la même façon.

4. La matrice  $1.A$  a pour terme général  $1a_{ij} = a_{ij}$ . Donc les matrices  $1.A$  et  $A$ , qui ont même format  $(n, p)$  et même terme général, sont égales. ■

### 9.2.4 Produit de deux matrices

**Définition 9.2.6 Produit  $LC$  (ligne par colonne).** Soient une matrice ligne  $L = (a_1, \dots, a_n)$  de  $M_{1,n}$  et une matrice colonne  $C = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$  de  $M_{n,1}$ . La matrice produit  $LC$  est la matrice carrée de  $M_1$  définie par :

$$LC = (a_1, \dots, a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{k=1}^n a_k b_k.$$

Cette matrice n'a qu'un seul terme, elle est identifiée à un réel.

**Exemple 9.2.7** Si  $L = (x \ y \ z)$  et  $C = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$  alors  $LC = x + 2y + 3z$ .

**Remarque 9.2.8** Si  $L$  est une matrice-ligne de  $M_{1,p}$  et  $C$  une matrice colonne de  $M_{q,1}$ , le produit matriciel  $LC$  n'est possible que si  $p = q$  c'est-à-dire, si le nombre de colonnes de  $L$  est égal au nombre de lignes de  $C$ .

**Définition 9.2.9** Soient  $A = (a_{ij})_{n,p}$  un élément de  $M_{n,p}$  et  $B = (b_{ij})_{p,q}$  un élément de  $M_{p,q}$ . On appelle produit de  $A$  par  $B$  la matrice  $C$  de format  $(n, q)$  dont le terme général  $c_{ij}$  est défini par :

$$\forall i \in \{1, \dots, n\}, \forall j \in \{1, \dots, q\}, \quad c_{ij} = \sum_{k=1}^p a_{ik} b_{kj}$$

On note  $C = AB$ .

**Remarque 9.2.10** Le produit de deux matrices n'est pas toujours défini. Le produit  $AB$  n'a de sens que si le nombre de colonnes de  $A$  est égal au nombre de lignes de  $B$ .

Pour éviter les erreurs, il est conseillé d'adopter la présentation suivante des calculs, proposée ici sur un exemple :

$$B = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix} \quad AB = \begin{pmatrix} 5 & 3 & 3 & 10 \\ 2 & 1 & 2 & 5 \end{pmatrix}$$

Cette disposition permet de vérifier que la matrice  $AB$  obtenue a le même nombre de lignes que  $A$  et le même nombre de colonnes que  $B$ ; elle a de plus l'avantage de bien se prêter aux calculs itérés.

**Proposition 9.2.11 (Propriétés du produit matriciel)**

Avec les hypothèses convenables pour que les produits existent :

1. le produit matriciel est associatif :

$$A(BC) = (AB)C$$

2. il est distributif par rapport à l'addition :

$$A(B+C) = AB + AC \quad \text{et} \quad (A+B)C = AC + BC$$

3.  $\forall \lambda \in \mathbb{R}$ ,

$$A(\lambda B) = (\lambda A)B = \lambda(AB)$$

**Remarque 9.2.12 Le produit matriciel n'est pas commutatif :**

- le produit  $AB$  peut avoir un sens alors que  $BA$  n'en a pas : c'est le cas lorsque  $A$  est une matrice  $(n, p)$  et  $B$  une matrice  $(p, q)$  avec  $n \neq q$ .
- même si les produits  $AB$  et  $BA$  ont un sens, les matrices  $AB$  et  $BA$  ne sont en général pas du même format, donc certainement pas égales ; par exemple  $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ ,  $B =$

$$\begin{pmatrix} 1 & 0 \\ -1 & -1 \\ 0 & 1 \end{pmatrix} \text{ alors :}$$

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad BA = \begin{pmatrix} 1 & 1 & 1 \\ -2 & -2 & -2 \\ 1 & 1 & 1 \end{pmatrix}$$

- enfin même dans le cas a priori le plus favorable, c'est-à-dire si  $A$  et  $B$  sont des matrices carrées de même ordre  $n$ , les deux matrices  $AB$  et  $BA$  sont aussi des matrices carrées de même ordre  $n$ , mais en général elles ne sont pas égales. Par exemple  $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$  alors :

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad BA = \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix}$$

On peut donc avoir  $AB = O$  sans que  $A = O$  ou  $B = O$ .

**Remarque 9.2.13**  $AB = AC$  n'implique pas forcément  $B = C$ . Par exemple  $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$ ,  $C = \begin{pmatrix} 2 & 2 \\ -2 & -3 \end{pmatrix}$  on a :  $AB = AC = \begin{pmatrix} 0 & -1 \\ 0 & -1 \end{pmatrix}$  et pourtant  $B \neq C$ .

**Preuve de la proposition 9.2.11 :**

1. Si  $A = (a_{ij})_{n,p}$ ,  $B = (b_{ij})_{p,q}$ ,  $C = (c_{ij})_{q,r}$ , alors :

La matrice  $D = BC$  a pour terme général  $D = (d_{ij})_{pr}$  où

$$d_{ij} = \sum_{k=1}^q b_{ik}c_{kj}$$

et la matrice  $E = A(BC) = AD$  a alors pour terme général  $E = (e_{ij})_{n,r}$  où

$$e_{ij} = \sum_{l=1}^p a_{il} d_{lj} = \sum_{l=1}^p \sum_{k=1}^q a_{il} b_{lk} c_{kj}$$

D'autre part, la matrice  $F = (AB)$  a pour terme général  $F = (f_{ik})_{n,q}$  où

$$f_{ik} = \sum_{l=1}^p a_{il} b_{lk}$$

et la matrice  $G = (AB)C = FC$  a pour terme général  $G = (g_{ij})_{n,r}$  où

$$g_{ij} = \sum_{k=1}^q f_{ik} c_{kj} = \sum_{k=1}^q \sum_{l=1}^p a_{il} b_{lk} c_{kj}$$

Comme on peut permuter deux sommes finies, on en déduit que les matrices  $E = A(BC)$  et  $G = (AB)C$ , qui ont même format  $(n, r)$  et même terme général, sont égales.

2. Montrons l'égalité  $A(B+C) = AB + AC$ . Si  $A = (a_{ij})_{n,p}$ ,  $B = (b_{ij})_{p,q}$ ,  $C = (c_{ij})_{p,q}$ , alors la matrice  $(B+C)$  a pour terme général  $(b_{ij} + c_{ij})$  et pour format  $(p, q)$ . Le produit  $D = A(B+C)$  a alors pour format  $(n, q)$  et pour terme général

$$d_{ij} = \sum_{k=1}^p a_{ik} (b_{kj} + c_{kj}) .$$

D'autre part, les matrices  $AB$  et  $AC$  ont même format  $(n, q)$  et pour terme général respectif  $(\sum_{k=1}^p a_{ik} b_{kj})$  et  $(\sum_{k=1}^p a_{ik} c_{kj})$ . Donc la matrice  $E = AB + AC$  a pour format  $(n, q)$  et pour terme général

$$e_{ij} = \sum_{k=1}^p a_{ik} b_{kj} + \sum_{k=1}^p a_{ik} c_{kj} = d_{ij}$$

Comme les matrices  $D$  et  $E$  ont même format  $(n, q)$  et même terme général  $d_{ij} = e_{ij}$ , on en déduit que  $D = E$ .

L'égalité  $(A+B)C = AC + BC$  se montre de même (attention au format des matrices!).

3. Montrons l'égalité  $A(\lambda B) = \lambda(AB)$ . Si  $A = (a_{ij})_{n,p}$ ,  $B = (b_{ij})_{p,q}$  et  $\lambda \in \mathbb{R}$ , alors la matrice  $\lambda B$  a pour format  $(p, q)$  et terme général  $(\lambda b_{ij})$ . Donc la matrice  $C = A(\lambda B)$  a pour format  $(n, q)$  et terme général

$$c_{ij} = \sum_{k=1}^p a_{ik} (\lambda b_{kj}) .$$

D'autre part, la matrice  $AB$  a pour format  $(n, q)$  et terme général  $(\sum_{k=1}^p a_{ik} b_{kj})$ . Donc la matrice  $D = \lambda(AB)$  a pour format  $(n, q)$  et terme général

$$d_{ij} = \lambda \left( \sum_{k=1}^p a_{ik} b_{kj} \right) = c_{ij} .$$

Comme les matrices  $C = A(\lambda B)$  et  $D = \lambda(AB)$  ont même format  $(n, q)$  et même terme général  $c_{ij} = d_{ij}$ , on en déduit l'égalité  $A(\lambda B) = \lambda(AB)$ .

L'égalité  $(\lambda A)B = \lambda(AB)$  se montre de même. ■

**Proposition 9.2.14** Soient  $A \in M_{p,n}$  et  $B \in M_{n,q}$ . Notons  $b_1, \dots, b_q$  les matrices colonnes de la matrice  $B$ .

La matrice produit  $AB$  est la matrice de  $M_{p,q}$ , dont les colonnes sont les vecteurs  $Ab_1, \dots, Ab_q$ . Autrement dit :

$$AB = A[b_1, \dots, b_q] = [Ab_1, \dots, Ab_q].$$

**preuve** Il suffit de reprendre la règle ligne colonne. ■

**Exemple 9.2.15**

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (a \quad b \quad c)$$

avec

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \\ 8 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$$

donc

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 2 \\ 5 & 0 & 3 \\ 8 & 0 & 1 \end{pmatrix}$$

Cette règle présente un intérêt lorsque une matrice comporte une ou des colonnes de 0.

**Proposition 9.2.16** Soient  $A \in M_{p,n}$  et  $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  une matrice colonne. Notons

$A_1, \dots, A_n$  les colonnes de la matrice  $A$ .

Le produit de  $A$  par  $\mathbf{x}$  noté  $A\mathbf{x}$  est la combinaison linéaire des colonnes de  $A$  c'est-à-dire

$$A\mathbf{x} = [A_1, \dots, A_n] \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 A_1 + \dots + x_n A_n = \sum_{k=1}^n x_k A_k.$$

**preuve** On note  $a_{ij}$  le terme courant de la matrice  $A$ . Le produit  $Y = A\mathbf{x}$  est une matrice colonne de format  $p$  lignes et une colonne. On note  $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}$  et pour tout  $1 \leq i \leq p$ , on a

$$y_i = \sum_{k=1}^n a_{ik} x_k$$

donc

$$Y = \sum_{k=1}^n x_k \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix} = \sum_{k=1}^n x_k A_k.$$

■

**Exemple 9.2.17**

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + 3 \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}.$$

**Exemple 9.2.18**  $C = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$  et  $L = (4 \ 5 \ 6 \ 7)$ , alors  $CL = [4C, 5C, 6C, 7C] = \begin{pmatrix} 4 & 5 & 6 & 7 \\ 8 & 10 & 12 & 14 \\ 12 & 15 & 18 & 21 \end{pmatrix}$

### 9.2.5 Transposée d'une matrice

**Définition 9.2.19** Soit  $A = (a_{ij})_{n,p}$  une matrice de  $M_{n,p}$ . On appelle transposée de  $A$  la matrice  $A' = (a'_{ij})_{p,n}$  de format  $(p, n)$  dont le terme général est

$$\forall i \in \{1, \dots, p\}, \forall j \in \{1, \dots, n\}, \quad a'_{ij} = a_{ji}.$$

On la note  $A' = A^T$ .

**Proposition 9.2.20**

1.  $\forall A \in M_{n,p}, \forall B \in M_{n,p}, \forall \lambda \in \mathbb{R}, \quad (A+B)^T = A^T + B^T$  et  $(\lambda A)^T = \lambda A^T$ .
2.  $\forall A \in M_{n,p}, \quad (A^T)^T = A$ .
3.  $\forall A \in M_{n,p}, \forall B \in M_{p,q}, \quad (AB)^T = B^T A^T$ .

**Preuve :**

1. Si  $A = (a_{ij})_{n,p}$  et  $B = (b_{ij})_{n,p}$ , alors la matrice  $A+B$  a pour terme général  $(a_{ij} + b_{ij})$  et pour format  $(n, p)$ , et donc la matrice  $(A+B)^T$  a pour terme général  $(a_{ji} + b_{ji})$  et pour format  $(p, n)$ . D'autre part, les matrices  $A^T$  et  $B^T$  ont pour terme général respectivement  $(a_{ji})$  et  $(b_{ji})$ , donc la matrice  $A^T + B^T$  a pour terme général  $(a_{ji} + b_{ji})$  et pour format  $(p, n)$ . Les matrices  $(A+B)^T$  et  $A^T + B^T$  ont même format  $(p, n)$  et même terme général. Elles sont donc égales. On montre de même l'égalité  $(\lambda A)^T = \lambda A^T$ .
2. Si  $A = (a_{ij})_{n,p}$ , la matrice  $A^T$  a pour terme général  $(a_{ji})$  et pour format  $(p, n)$ . Donc la matrice  $(A^T)^T$  a pour terme général  $(a_{ij})$  et pour format  $(n, p)$ . On en déduit l'égalité  $(A^T)^T = A$ .
3. Si  $A = (a_{ij})_{n,p}$  et  $B = (b_{ij})_{p,q}$ , alors  $AB$  a pour format  $(n, q)$  et pour terme général  $(\sum_{k=1}^p a_{ik} b_{kj})$ . Par conséquent, la matrice  $C = (AB)^T$  a pour format  $(q, n)$  et pour terme général

$$c_{ij} = \sum_{k=1}^p a_{jk} b_{ki}.$$

D'autre part, les matrices  $A^T$  et  $B^T$  ont pour format respectif  $(p, n)$  et  $(q, p)$  et pour terme général  $(a_{ji})$  et  $(b_{ji})$ . Le produit  $D = B^T A^T$  existe donc, a pour format  $(q, n)$  et pour terme général

$$d_{ij} = \sum_{k=1}^p b_{ki} a_{jk} = c_{ij}$$

Les matrices  $C$  et  $D$  ont même format  $(q, n)$  et même terme général  $c_{ij} = d_{ij}$ . Elles sont donc égales.

■

**Définition 9.2.21 (Adjointe d'une matrice)**

Soit  $A = (a_{ij})$  une matrice de  $M_{n,p}(\mathbb{C})$  (à coefficients complexes). On appelle adjointe de  $A$  la matrice  $A' = (a'_{ij})$  de format  $(p, n)$  dont le terme général est

$$\forall i \in \{1, \dots, p\}, \forall j \in \{1, \dots, n\}, \quad a'_{ij} = \overline{a_{ji}}.$$

(ici  $\bar{z}$  désigne le conjugué du complexe  $z$ ). On note  $A' = A^*$ .

### 9.3 Les matrices carrées

Nous allons étudier dans ce paragraphe les matrices carrées de format (ou d'ordre)  $n$ . Toutes les propriétés vues dans le cas général restent bien entendu valables, mais nous allons voir que ces matrices possèdent en plus des propriétés particulières. L'ensemble des matrices carrées d'ordre  $n$  à coefficients réels (resp. complexes) se note  $M_n(\mathbb{R})$  (resp.  $M_n(\mathbb{C})$ ) et plus simplement  $M_n$ . Comme ci-dessus nous faisons l'exposé dans le cas réel.

#### 9.3.1 Quelques matrices carrées particulières

- si  $A = (a_{ij})_n$  est une matrice carrée d'ordre  $n$ , les termes  $a_{ii}$  constituent la **diagonale principale** de  $A$ .
- une matrice  $A = (a_{ij})_n$  est **diagonale** si tous ses termes sont nuls, sauf peut-être ceux de la diagonale principale :

$$\forall (i, j) \in \{1, \dots, n\}^2, \quad i \neq j \Rightarrow a_{ij} = 0.$$

- la **matrice identité** d'ordre  $n$ , notée  $I_n$  est la matrice diagonale dont tous les termes diagonaux sont égaux à 1. Dans le cas où il n'y a pas de risque d'ambiguïté sur l'ordre de la matrice, on la note plus simplement  $I$  :

Exemple : si  $n = 3$  
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- une matrice  $A$  est **scalaire** si c'est une matrice diagonale dont tous les termes diagonaux sont égaux :

$$A \text{ scalaire} \Leftrightarrow \exists \lambda \in \mathbb{R}, \quad A = \lambda I_n$$

- une matrice  $A$  est **symétrique** si elle est égale à sa transposée :  $A = A^T$ .
- une matrice  $A$  **antisymétrique** si elle est égale à l'opposée de sa transposée :  $A = -A^T$ .
- dans le cas complexe, une matrice  $A$  est **auto-adjointe** si elle est égale à son adjointe :  $A = A^*$ .

### 9.3.2 Opérations dans $M_n$

**Proposition 9.3.1**

Si  $I_n$  est la matrice identité définie ci-dessus, on a :

$$\forall A \in M_n, \quad AI_n = I_n A = A.$$

On dit que  $I_n$  est élément neutre pour la multiplication. De manière plus générale pour toute matrice  $A$  de format  $(n, p)$ , on a

$$I_n A = A I_p = A.$$

**Preuve de la proposition :** Montrons l'égalité  $AI_n = A$ . Si  $A = (a_{ij})_n$  et  $I_n = (b_{ij})_n$ , alors le produit  $AI_n$  a pour format  $(n, n)$  et terme général  $(\sum_{k=1}^n a_{ik}b_{kj})$ . D'après la définition de  $I_n$ , on a

$$\forall (i, j) \in \{1, \dots, n\}^2, \quad b_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

Donc le terme général de la matrice  $AI_n$  est  $(\sum_{k=1}^n a_{ik}b_{kj} = a_{ij})$ , ce qui prouve l'égalité  $AI_n = A$ . On montre de même que  $I_n A = A$  et les dernières égalités. ■

### 9.3.3 Puissances d'une matrice carrée

**Définition 9.3.2** Soit  $A$  une matrice de  $\mathcal{M}_n(\mathbb{R})$ . Les puissances de  $A$  sont définies par récurrence :

$$A^0 = I_n, \quad A^1 = A \text{ et } \forall p \in \mathbb{N}, \quad A^{p+1} = A^p A = A A^p.$$

Les preuves des propositions suivantes sont laissées en exercice.

**Proposition 9.3.3 Puissance nième d'une matrice diagonale** Pour tout entier naturel  $p$ , on a

$$\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix}^p = \begin{pmatrix} a_1^p & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n^p \end{pmatrix}.$$

**Proposition 9.3.4** On a

1. Si  $I_n$  est la matrice unité de  $\mathcal{M}_n(\mathbb{R})$  alors pour tout entier  $p$ ,  $I_n^p = I_n$
2. Pour tous entiers positifs  $p$  et  $q$ , pour toute matrice  $A$  de  $\mathcal{M}_n(\mathbb{R})$

$$A^p A^q = A^{p+q} = A^q A^p \text{ et } (A^p)^q = A^{pq} = (A^q)^p.$$

3. Pour tout entier  $p$  positif et pour tout réel  $\lambda$  :  $(\lambda A)^p = \lambda^p A^p$ .
4. Pour tout entier positif  $p$  et pour toute matrice  $A$  de  $\mathcal{M}_n(\mathbb{R})$ ,  ${}^t(A^p) = ({}^t A)^p$ .

**Définition 9.3.5** Une matrice  $A$  de  $\mathcal{M}_n(\mathbb{R})$  est dite nilpotente s'il existe un entier positif  $m$  tel que :  $A^m = O$ . Remarquons qu'alors, pour tout  $p \geq m$ ,  $A^p = O$ .

**Exemple 9.3.6** Soit  $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ , on a  $A^2 = O$ .

**Proposition 9.3.7 Formule du binôme** Soient  $A$  et  $B$  deux matrices de  $\mathcal{M}_n(\mathbb{R})$ . Si  $A$  et  $B$  commutent ( $AB = BA$ ), on peut appliquer la formule du binôme de Newton :

$$\forall p \in \mathbb{N}, (A + B)^p = \sum_{k=0}^p \binom{p}{k} A^k B^{p-k}.$$

On rappelle que

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Cas particulier : si  $B = I$ ,  $(A + I)^p = \sum_{k=0}^p \binom{p}{k} A^k$ .

**Exemple 9.3.8** Soit  $A = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ , on peut écrire

$$A = I_3 + B, \text{ où } B = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

On vérifie que  $B^2 = \begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$  et  $B^3 = 0$  donc pour tout entier  $k \geq 3$ ,  $B^k = 0$ . On applique la formule du binôme de Newton puisque  $B$  et  $I_3$  commutent donc pour tout entier  $n$

$$\begin{aligned} A^n &= (B + I)^n \\ &= \sum_{k=0}^n \binom{n}{k} B^k \\ &= I_3 + nB + \frac{n(n-1)}{2} B^2 \\ &= \begin{pmatrix} 1 & 2n & 2n + 3n(n-1) \\ 0 & 1 & 3n \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

### 9.3.4 Matrices inversibles

**Définition 9.3.9 (Matrices inversibles)**

Soit  $A$  une matrice de  $M_n$ . On dit que  $A$  est inversible ou régulière s'il existe une matrice  $B$  de  $M_n$  telle que :

$$AB = BA = I_n .$$

Dans ce cas, la matrice  $B$  est unique et s'appelle l'inverse de  $A$ . On note  $B = A^{-1}$ .

**Preuve de l'unicité :** Supposons qu'il existe deux matrices  $B_1$  et  $B_2$  telles que

$$AB_1 = B_1A = I_n = AB_2 = B_2A .$$

Comme  $AB_1 = I_n$ , on a, en multipliant cette égalité à gauche par  $B_2$  :

$$B_2(AB_1) = B_2I_n .$$

Or

$$B_2(AB_1) = (B_2A)B_1 = I_n B_1 = B_1 \quad \text{et} \quad B_2I_n = B_2 .$$

On en déduit que  $B_1 = B_2$ . ■

**Théorème 9.3.10 (admis)** Soit  $A$  et  $B$  deux matrices de  $M_n$ . Si  $AB = I_n$ , alors  $A$  et  $B$  sont inversibles et  $B = A^{-1}$ .

**Proposition 9.3.11 (Produit de deux matrices inversibles)**

Soient  $A$  et  $B$  deux matrices inversibles de  $M_n$  : alors le produit  $AB$  est inversible et

$$(AB)^{-1} = B^{-1}A^{-1} .$$

**Preuve :** Calculons le produit  $(B^{-1}A^{-1})(AB)$  :

$$\begin{aligned} (B^{-1}A^{-1})(AB) &= B^{-1}(A^{-1}A)B && \text{par associativité} \\ &= B^{-1}I_n B && \text{par définition de } B^{-1} \\ &= B^{-1}B \\ &= I_n \end{aligned}$$

On montre de même que

$$(AB)(B^{-1}A^{-1}) = I_n$$

et on en déduit que  $AB$  est inversible et d'inverse  $(B^{-1}A^{-1})$ . ■

**Proposition 9.3.12 (Transposée d'une matrice inversible)**

Si  $A$  est une matrice carrée inversible, alors  $A^T$  est inversible et

$$(A^T)^{-1} = (A^{-1})^T .$$

De même dans le cas complexe,  $A^*$  est inversible et  $(A^*)^{-1} = (A^{-1})^*$ .

**Preuve :** En transposant l'égalité  $AA^{-1} = I_n$ , on obtient

$$(A^{-1})^T A^T = (I_n)^T = I_n.$$

De même, en transposant l'égalité  $A^{-1}A = I_n$ , on obtient

$$A^T (A^{-1})^T = I_n$$

On en déduit que  $A^T$  est inversible et que son inverse est  $(A^{-1})^T$ .

La démonstration pour l'adjointe est identique. ■

**Proposition 9.3.13**

*Si  $A$  est inversible, et si  $AB = AC$  (respectivement  $BA = CA$ ) alors  $B = C$ .*

**Preuve :** On multiplie l'égalité  $AB = AC$ , à gauche, par  $A^{-1}$  pour obtenir

$$A^{-1}(AB) = A^{-1}(AC)$$

Par associativité, on obtient :

$$A^{-1}(AB) = (A^{-1}A)B = I_n B = B$$

De même,  $A^{-1}(AC) = C$ . Donc  $B = C$ .

L'autre égalité s'obtient de la même façon, en multipliant à droite l'égalité  $BA = CA$  par  $A^{-1}$ . ■

# Chapitre 10

## systèmes linéaires

### 10.1 Définitions et écriture matricielle

**Définition 10.1.1** On appelle *équation linéaire à  $p$  inconnues*  $(x_1, x_2, \dots, x_p)$  une équation de la forme :  $a_1x_1 + a_2x_2 + \dots + a_px_p = b$  où  $a_1, a_2, \dots, a_p$  et  $b$  sont des réels.

On appelle *système linéaire de  $n$  équations à  $p$  inconnues*  $(x_1, x_2, \dots, x_p)$  tout système  $(S)$  de la forme :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1p}x_p & = & b_1 \\ \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{np}x_p & = & b_n \end{cases}$$

où pour tout  $1 \leq i \leq n$  et  $1 \leq j \leq p$ ,  $a_{ij} \in \mathbb{R}$  et  $b_i \in \mathbb{R}$ .

Les inconnues de  $(S)$  sont  $x_1, \dots, x_i, \dots, x_p$ .

Les coefficients de  $(S)$  sont les réels  $a_{ij}$ , ils sont affectés d'un double indice, le premier,  $i$ , est l'indice de l'équation, le second,  $j$ , l'indice de l'inconnue :  $a_{ij}$  est le coefficient de la  $j$ ème inconnue dans la  $i$ ème équation.

Le second membre de  $(S)$  est la matrice  $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ .

$(S)$  est dit homogène lorsque le second membre est nul.

Le système homogène associé à  $(S)$  est le système  $(S')$  obtenu à partir de  $(S)$  en remplaçant le second membre par le vecteur nul de  $\mathbb{R}^n$ .

Une solution de  $(S)$  est une matrice  $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$  qui vérifie les  $n$  équations.

Résoudre  $(S)$  c'est déterminer toutes les solutions de  $(S)$ . Il n'y a que trois situations

- $(S)$  est dit impossible s'il n'admet aucune solution.
- $(S)$  est dit indéterminé s'il admet plusieurs solutions.
- $(S)$  admet une solution unique.

De plus on dit que  $(S)$  est un système de Cramer si  $n = p$  et s'il admet une solution unique.

Deux systèmes  $(S)$  et  $(S')$  sont dits équivalents s'ils ont le même ensemble de solutions.

**Définition 10.1.2** *Écriture matricielle* On appelle  $A$  la matrice des coefficients du système  $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$ , La  $i$ ème ligne de la matrice  $A$  contient les coefficients de la  $i$ ème équation. La  $j$ ème colonne de la matrice  $A$  contient les coefficients de la  $j$ ème inconnue. Le système s'écrit

$$A\mathbf{x} = \mathbf{b}.$$

**Exemple 10.1.3** Soit le système

$$\begin{cases} 2x + y + z = 2 \\ y + 2z = -1 \\ 5z = 5 \end{cases}$$

La matrice du système est

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

et

$$\mathbf{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 2 \\ -1 \\ 5 \end{pmatrix}.$$

## 10.2 Systèmes faciles à résoudre

### 10.2.1 Systèmes triangulaires

**Définition 10.2.1** Un système  $(S)$  est dit triangulaire si la matrice du système est triangulaire sans valeurs nulles sur la diagonale.

On admet le résultat suivant :

**Proposition 10.2.2** Tout système linéaire triangulaire de  $n$  équations à  $n$  inconnues admet une solution unique, c'est un système de Cramer.

En particulier l'unique solution d'un système linéaire triangulaire homogène est le vecteur nul.

**Exemple 10.2.3** Soit le système

$$\begin{cases} 2x + y + z = 2 \\ y + 2z = -1 \\ 5z = 5 \end{cases}$$

C'est un système triangulaire car la matrice  $A = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \end{pmatrix}$  est triangulaire sans valeurs nulles sur la diagonale.

Ce système se résout "de proche en proche" (en commençant par la dernière équation) par la méthode dite de "substitutions remontantes". La dernière équation donne  $z = 1$ . En reportant dans la deuxième on trouve  $y + 2 = -1$  ce qui donne  $y = -3$ . En reportant les valeurs trouvées pour  $z$  et  $y$  dans la première équation on obtient :  $2x - 3 + 1 = 2$  soit  $2x = 4$  c'est-à-dire  $x = 2$ . le système admet une solution unique  $x = 2$ ,  $y = -3$ ,  $z = 1$ .

### 10.2.2 Systèmes échelonnés

#### Exemple 10.2.4

$$\begin{cases} x_1 + x_2 + 2x_3 + x_4 = 5 \\ 2x_3 - 4x_4 = 0 \end{cases}$$

Ce système se ramène à un système triangulaire en l'écrivant sous la forme :

$$\begin{cases} x_1 + 2x_3 = 5 - x_2 - x_4 \\ x_3 = 2x_4 \end{cases} \iff \begin{cases} x_1 = 5 - x_2 - 5x_4 \\ x_3 = 2x_4 \end{cases}$$

Le dernier système admet une infinité de solutions. Il est indéterminé. Une solution s'obtient en choisissant arbitrairement des valeurs pour  $x_2$  et  $x_4$  et en calculant les valeurs correspondantes de  $x_1$  et  $x_3$ . On dit que  $x_2$  et  $x_4$  sont des paramètres.

On peut écrire l'ensemble des solutions sous la forme suivante, dite représentation paramétrique du système :

$$\left\{ \begin{pmatrix} 5 - x_2 - 5x_4 \\ x_2 \\ 2x_4 \\ x_4 \end{pmatrix}, x_2 \in \mathbb{R}, x_4 \in \mathbb{R} \right\}$$

La matrice du système s'écrit :  $A = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & -4 \end{pmatrix}$ . Elle n'est pas triangulaire mais vérifie la définition suivante.

**Définition 10.2.5** Une matrice échelonnée en ligne est une matrice telle que

- chaque ligne commence par plus de zéros que la ligne précédente, le premier élément non nul de chaque ligne s'appelle **pivot**.
- Si une ligne est nulle, alors toutes les lignes suivantes sont nulle.

**Exemple 10.2.6** Les deux matrices des systèmes précédents sont échelonnées en ligne. La première a 3 pivots. La deuxième a 2 pivots.

$$\text{Les matrices } B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } D = \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

sont échelonnées en ligne.  $B$  a 3 pivots.  $C$  a 2 pivots.  $D$  a 3 pivots.

$$\text{Les matrices } E = \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} F = \begin{pmatrix} 0 & 2 & 0 & 4 \\ 5 & 0 & 1 & 2 \end{pmatrix}, G = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 0 & 4 & 0 & 5 \\ 6 & 0 & 0 & 1 \end{pmatrix} \text{ ne sont pas}$$

échelonnées en ligne.

Les pivots d'une matrice échelonnée en ligne forment un échelon (une marche) d'un escalier qui descend du haut à gauche vers le bas à droite. La matrice  $E$  n'est pas échelonnée en lignes car on saute brutalement deux marches !

Les matrices triangulaires supérieures n'ayant aucun zéro sur la diagonale principale sont échelonnées en ligne.

Par contre pour les matrices triangulaires supérieures qui ont des zéros sur la diagonale principale. Il faut raisonner au cas par cas. La matrice  $D$  est échelonnée en ligne. La matrice  $E$  n'est pas échelonnée en ligne.

**Proposition 10.2.7** *Pour une matrice échelonnée en ligne comportant  $n$  lignes et  $p$  colonnes, on a*

$$\text{nombre de pivots} \leq \min(n, p).$$

**preuve** Pour une matrice échelonnée en ligne, le nombre de pivots est égal au nombre de lignes non nulles. Donc le nombre de pivots est inférieur au nombre de lignes.

Par ailleurs, tous les éléments d'une colonne situés sous un pivot sont nuls car un pivot est le premier élément non nul d'une ligne. Les lignes suivantes doivent avoir au moins un zéro de plus en tête. Donc le nombre de pivots est inférieur au nombre de colonnes. ■

**Définition 10.2.8** *Un système  $(S)$  est dit échelonné si sa matrice est échelonnée en ligne. Un système triangulaire est échelonné.*

La méthode de Gauss, appelée aussi méthode du pivot, est une méthode systématique qui consiste, en un nombre fini d'étapes, à transformer un système  $(S)$  quelconque en un système échelonné  $(T)$  équivalent à  $(S)$ .

A chaque étape de cette méthode, nous utiliserons les opérations sur les lignes, dites opérations élémentaires, et définies dans le paragraphe suivant.

## 10.3 Opérations élémentaires sur les lignes

### 10.3.1 Définition et propriété

Soit  $(S)$  un système de  $n$  équations à  $p$  inconnues. Pour tout entier  $1 \leq i \leq n$ , on note  $L_i$  la  $i$ ème équation de  $(S)$ , appelée aussi la  $i$ ème ligne de  $(S)$ .

**Définition 10.3.1** *On appelle opération élémentaire sur les lignes l'une des trois transformations suivantes :*

- *cadrage* : on multiplie la  $i$ ème ligne par  $a$  ( $a \neq 0$ ), cette opération est codée  $L_i \leftarrow aL_i$ .
- *échange* : on échange les lignes  $i$  et  $j$  de  $(S)$ , ( $i \neq j$ ), opération codée par :  $L_i \leftrightarrow L_j$ .
- *remplacement* : on ajoute à la ligne  $i$ , la ligne  $j$  ( $i \neq j$ ) multipliée par  $a$ , opération codée  $L_i \leftarrow L_i + aL_j$ .

On admet le résultat suivant :

**Proposition 10.3.2** *On obtient un système équivalent à  $(S)$  en conservant une équation  $L_i$  et en ajoutant à toutes les autres (sauf à  $L_i$ ) un multiple de  $L_i$ .*

$$L_i \leftarrow L_i \text{ et pour } j \neq i, \quad L_j \leftarrow aL_j + bL_i \text{ avec } a \neq 0, \quad b \in \mathbb{R}.$$

En effectuant une succession d'étapes, on obtient à chaque fois un système qui a le même ensemble de solutions que le système précédent, donc que le système initial.

**Exemple 10.3.3** : Soit à résoudre le système  $S$

$$\begin{cases} x_1 + 8x_2 - 2x_3 & = & -4 \\ 3x_1 + 15x_2 + 7x_3 & = & 30 \\ x_1 + 4x_2 + 2x_3 & = & 8 \end{cases}$$

On transforme ce système  $S$  en un système triangulaire équivalent.

$$\begin{aligned} (S) &\iff \begin{cases} x_1 + 8x_2 - 2x_3 & = & -4 & L_1 \leftarrow L_1 \\ -9x_2 + 13x_3 & = & 42 & L_2 \leftarrow L_2 - 3L_1 \\ -4x_2 + 4x_3 & = & 12 & L_3 \leftarrow L_3 - L_1 \end{cases} \\ &\iff \begin{cases} x_1 + 8x_2 - 2x_3 & = & -4 & L_1 \leftarrow L_1 \\ x_2 - x_3 & = & -3 & L_2 \leftarrow \frac{-1}{4}L_3 \\ -9x_2 + 13x_3 & = & 42 & L_3 \leftarrow L_2 \end{cases} \\ &\iff \begin{cases} x_1 + 8x_2 - 2x_3 & = & -4 & L_1 \leftarrow L_1 \\ x_2 - x_3 & = & -3 & L_2 \leftarrow L_2 \\ 4x_3 & = & 15 & L_3 \leftarrow L_3 + 9L_2 \end{cases} \end{aligned}$$

On a donc un système triangulaire dont la résolution donne

$$\begin{cases} x_1 & = & -5/2 \\ x_2 & = & 3/4 \\ x_3 & = & 15/4 \end{cases}$$

**Exemple 10.3.4** On considère le système  $S$

$$\begin{cases} x + y & = & 2 \\ x - y & = & 3 \end{cases}$$

et le système obtenu par des opérations sur les lignes

$$\begin{cases} 2x & = & 5 & L_1 \leftarrow L_1 + L_2 \\ 2x & = & 5 & L_2 \leftarrow L_2 + L_1 \end{cases}$$

Il est clair que ces deux systèmes ne sont pas équivalents. En effet on modifie les lignes simultanément, on n'applique pas la proposition précédente.

### 10.3.2 Disposition pratique des calculs

Nous pouvons au cours de cette résolution faire abstraction des inconnues  $x_1, x_2, x_3$  pour ne travailler que sur les coefficients, ce qui donne au départ le tableau :

$$\begin{array}{cccc|c} 1 & 8 & -2 & -4 & L_1 \\ 3 & 15 & 7 & 30 & L_2 \\ 1 & 4 & 2 & 8 & L_3 \end{array}$$

Cette écriture met en évidence la matrice du système et son second membre. La matrice ainsi obtenue est appelée matrice augmentée du système. C'est la juxtaposition de la matrice  $A$  du système et de la matrice colonne  $b$ , du second membre. On notera  $A'$ , cette matrice augmentée  $A' = [A, b]$ .

On opère alors sur les lignes de la matrice augmentée (qui sont les lignes du système). On réécrit le système après la dernière étape pour la résolution finale.

$$\begin{array}{cccc|l}
1 & 8 & -2 & -4 & L_1 \\
3 & 15 & 7 & 30 & L_2 \\
1 & 4 & 2 & 8 & L_3 \\
\hline
1 & 8 & -2 & -4 & L_1 \\
0 & -9 & 13 & 42 & L_2 \leftarrow L_2 - 3L_1 \\
0 & -4 & 4 & 12 & L_3 \leftarrow L_3 - L_1 \\
\hline
1 & 8 & -2 & -4 & L_1 \\
0 & 1 & -1 & -3 & L_2 \leftarrow -L_3/4 \\
0 & -9 & 13 & 42 & L_3 \leftarrow L_2 \\
\hline
1 & 8 & -2 & -4 & L_1 \\
0 & 1 & -1 & -3 & L_2 \\
0 & 0 & 4 & 15 & L_3 \leftarrow L_3 + 9L_2
\end{array}$$

donc le système que l'on résout directement

$$\begin{cases} x_1 + 8x_2 - 2x_3 = -4 \\ x_2 - x_3 = -3 \\ 4x_3 = 15 \end{cases}$$

Dans la suite, nous traiterons tous les calculs de cette façon.

## 10.4 Méthode de Gauss

### 10.4.1 Exposé de la méthode

Soit le système  $(S)$  de  $n$  équations et  $p$  inconnues.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}x_p = b_n \end{cases}$$

On note  $A$  la matrice du système et  $A'$  la matrice augmentée. On suppose que l'un au moins des coefficients de la première colonne est non nul, sinon l'inconnue  $x_1$  disparaît.

A l'aide des opérations élémentaires sur les lignes de la matrice augmentée, on transforme le système  $(S)$  en un système échelonné équivalent.

#### — étape 1 : choix du pivot

Par hypothèse l'un au moins des coefficients de la première colonne est non nul. On choisit l'un d'entre eux :  $a_{i_0 1}$ . (si possible un coefficient égal à 1).  $a_{i_0 1}$  est alors le premier pivot. Si  $i_0 \neq 1$ , on échange les lignes  $L_1$  et  $L_{i_0}$ .

Le premier pivot est donc l'élément  $a_{11}$  de la matrice obtenue après l'opération d'échange.

#### — étape 2 : élimination

La (première) ligne contenant le pivot ne sera plus modifiée. On se sert du pivot pour faire apparaître, avec des opérations de remplacement, des zéros sous le pivot de la première colonne ce qui revient à éliminer la première inconnue des lignes  $L_2$  à  $L_n$ .

#### — étape 3 : boucle

A l'issue des deux étapes précédentes on a obtenu une matrice dont la première ligne et la première colonne sont bien celles d'une matrice échelonnée. Cette ligne et cette colonne ne seront plus modifiées. On va appliquer les étapes précédentes (1 et 2) à la sous-matrice obtenue en enlevant la première ligne et la première colonne. On distingue deux cas.

- cas 1 : la première colonne de la sous-matrice est non nulle. On applique les étapes 1 et 2 à la sous-matrice .
- cas 2 : la première colonne de la matrice est nulle. On recherche alors dans la sous-matrice la colonne non nulle la plus à gauche. Supposons que ce soit la  $j$ ème. On applique les étapes 1 et 2 à la nouvelle sous-matrice dont la première colonne est non nulle.
- Au terme de cette deuxième itération on recommence l'étape 3 avec la nouvelle sous-matrice obtenue jusqu'à ce qu'il n'y ait plus de lignes ou plus de lignes non nulles dans la matrice augmentée. La dernière matrice augmentée obtenue est donc échelonnée en ligne.  
Comme chaque itération de la boucle travaille sur une matrice qui a au moins une colonne de moins que la précédente, il est clair qu'au bout d'au plus  $p$  itérations on aura construit une matrice échelonnée.

### 10.4.2 Réduite de Gauss d'une matrice A

La méthode précédente qui permet d'obtenir une matrice échelonnée peut s'appliquer à n'importe quelle matrice. D'où la définition suivante :

**Définition 10.4.1** *Toute matrice échelonnée en ligne obtenue par application de la méthode de Gauss aux lignes d'une matrice A, est appelée réduite de Gauss de A. Une réduite de Gauss n'est pas unique, elle dépend des opérations élémentaires effectuées.*

On admet le résultat suivant

**Proposition 10.4.2** *Si R et R' sont deux réduites de Gauss d'une même matrice A, alors R et R' ont le même nombre de pivots.*

**Proposition 10.4.3** *Soit R une réduite de Gauss de A, alors on a deux systèmes équivalents*

$$Ax = b \iff Rx = b'.$$

### 10.4.3 Exemples

**Exemple 10.4.4** : Soit à résoudre le système

$$\begin{cases} x + y + z & = & 3 \\ 2x + y + 3z & = & 1 \\ x - y + 3z & = & 5 \end{cases}$$

La matrice du système est  $A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 1 & -1 & 3 \end{pmatrix}$  et  $\vec{b} = \begin{pmatrix} 3 \\ 1 \\ 5 \end{pmatrix}$ . La méthode donne

$$\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 2 & 1 & 3 & 1 \\ 1 & -1 & 3 & 5 \end{array} \quad \begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array}$$

$$\begin{array}{cccc|l} 1 & 1 & 1 & 3 & L_1 \\ 0 & -1 & 1 & -5 & L_2 \leftarrow L_2 - 2L_1 \\ 0 & -2 & 2 & 2 & L_3 \leftarrow L_3 - L_1 \\ \hline 1 & 1 & 1 & 3 & L_1 \\ 0 & -1 & 1 & -5 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & 12 & L_3 \leftarrow L_3 - 2L_2 \end{array}$$

Une réduite de  $A$  est  $R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$  qui possède deux pivots. Pour terminer la résolution, on revient au système

$$\begin{cases} x + y + z = 3 \\ -y + z = -5 \\ 0 = 12 \end{cases}$$

La dernière équation se lit  $0 = 12$ , le système est donc impossible.

**Exemple 10.4.5** : Soit à résoudre le système

$$\begin{cases} x + y + z + t = 4 \\ x + y + 6z + 4t = 3 \\ 2x + 2y + 3z = 5 \end{cases}$$

$$\begin{array}{cccc|l} 1 & 1 & 1 & 1 & 4 & L_1 \\ 1 & 1 & 6 & 4 & 3 & L_2 \\ 2 & 2 & 3 & 0 & 5 & L_3 \\ \hline 1 & 1 & 1 & 1 & 4 & L_1 \\ 0 & 0 & 5 & 3 & -1 & L_2 \leftarrow L_2 - L_1 \\ 0 & 0 & 1 & -2 & -3 & L_3 \leftarrow L_3 - 2L_1 \\ \hline 1 & 1 & 1 & 1 & 4 & L_1 \\ 0 & 0 & 5 & 3 & -1 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & -13 & -14 & L_3 \leftarrow 5L_3 - L_2 \end{array}$$

On en déduit qu'une réduite de  $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 6 & 4 \\ 2 & 2 & 3 & 0 \end{pmatrix}$  est  $R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 5 & 3 \\ 0 & 0 & 0 & -13 \end{pmatrix}$  qui possède trois pivots.

Le système initial est équivalent à

$$\begin{cases} x + y + z + t = 4 \\ 5z + 3t = -1 \\ -13t = -14 \end{cases}$$

En considérant  $y$  comme un paramètre, le système est triangulaire.

Le système admet une infinité de solutions :  $x = -y + \frac{49}{13}$ ,  $z = -\frac{11}{13}$  et  $t = \frac{14}{13}$ .

On dit que le système est indéterminé et l'ensemble des solutions s'écrit sous forme paramétrique :

$$\left\{ \left( -y + \frac{49}{13}, y, -\frac{11}{13}, \frac{14}{13} \right), y \in \mathbb{R} \right\}$$

**Exemple 10.4.6** : Soit à résoudre le système

$$\begin{cases} x + y + z + t = 4 \\ x + y + 6z + 4t = 3 \\ 2x + 2y + 3z = 5 \\ x + y + 3t = 7 \end{cases}$$

$$\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 & L_1 \\ 1 & 1 & 6 & 4 & 3 & L_2 \\ 2 & 2 & 3 & 0 & 5 & L_3 \\ 1 & 1 & 0 & 3 & 7 & L_4 \\ \hline 1 & 1 & 1 & 1 & 4 & L_1 \\ 0 & 0 & 5 & 3 & -1 & L_2 \leftarrow L_2 - L_1 \\ 0 & 0 & 1 & -2 & -3 & L_3 \leftarrow L_3 - 2L_1 \\ 0 & 0 & -1 & 2 & 3 & L_4 \leftarrow L_4 - L_1 \\ \hline 1 & 1 & 1 & 1 & 4 & L_1 \\ 0 & 0 & 5 & 3 & -1 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & -13 & -14 & L_3 \leftarrow 5L_3 - L_2 \\ 0 & 0 & 0 & 13 & 14 & L_4 \leftarrow 5L_4 + L_2 \\ \hline 1 & 1 & 1 & 1 & 4 & L_1 \\ 0 & 0 & 5 & 3 & -1 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & 13 & 14 & L_3 \leftarrow -L_3 \\ 0 & 0 & 0 & 0 & 0 & L_4 \leftarrow L_4 + L_3 \end{array}$$

Le système est équivalent à

$$\begin{cases} x + y + z + t = 4 \\ 5z + 3t = -1 \\ 13t = 14 \\ 0 = 0 \end{cases}$$

La quatrième équation est redondante. Le système est équivalent à

$$\begin{cases} x + y + z + t = 4 \\ 5z + 3t = -1 \\ 13t = 14 \end{cases} \iff \begin{cases} x = -y + 49/13 \\ z = -11/13 \\ t = 14/13 \end{cases}$$

Le système admet une infinité de solutions, il est indéterminé et l'ensemble des solutions s'écrit sous forme paramétrique :

$$\left\{ \left( -y + \frac{49}{13}, y, -\frac{11}{13}, \frac{14}{13} \right), y \in \mathbb{R} \right\}.$$

C'est le même ensemble de solutions que dans l'exemple 3.4.5, les deux systèmes sont donc équivalents.

#### 10.4.4 Choix des pivots

On choisit le pivot le plus simple (égal à 1 si possible) et le cas échéant indépendant des paramètres pour éviter de commencer une discussion trop rapidement.

**Exemple 10.4.7** : système avec paramètre.

Soit le système

$$\begin{cases} ax - z + t = a \\ x - y + at = a \\ -x + y + az = -a \\ ay + z - t = a \end{cases}$$

où  $a$  est un paramètre réel. Il s'agit de déterminer le nombre de solutions en fonction de  $a$ . On échange  $L_1$  et  $L_2$  de façon à avoir un pivot constant non nul.

$$\begin{array}{ccccc|l} a & 0 & -1 & 1 & a & L_1 \\ 1 & -1 & 0 & a & a & L_2 \\ -1 & 1 & a & 0 & -a & L_3 \\ 0 & a & 1 & -1 & a & L_4 \\ \hline 1 & -1 & 0 & a & a & L_1 \leftrightarrow L_2 \\ a & 0 & -1 & 1 & a & L_2 \leftrightarrow L_1 \\ -1 & 1 & a & 0 & -a & L_3 \leftarrow L_3 \\ 0 & a & 1 & -1 & a & L_4 \leftarrow L_4 \\ \hline 1 & -1 & 0 & a & a & L_1 \\ 0 & a & -1 & 1 - a^2 & a - a^2 & L_2 \leftarrow L_2 - aL_1 \\ 0 & 0 & a & a & 0 & L_3 \leftarrow L_3 + L_1 \\ 0 & a & 1 & -1 & a & L_4 \leftarrow L_4 \end{array}$$

On commence la discussion :

1. Si  $a \neq 0$ ,  $a$  est un pivot donc

$$\begin{array}{ccccc|l} 1 & -1 & 0 & a & a & L_1 \\ 0 & a & -1 & 1 - a^2 & a - a^2 & L_2 \leftarrow L_2 \\ 0 & 0 & 1 & 1 & 0 & L_3 \leftarrow \frac{1}{a}L_3 \\ 0 & 0 & 2 & -2 + a^2 & a^2 & L_4 \leftarrow L_4 - L_2 \\ \hline 1 & -1 & 0 & a & a & L_1 \\ 0 & a & -1 & 1 - a^2 & a - a^2 & L_2 \leftarrow L_2 \\ 0 & 0 & 1 & 1 & 0 & L_3 \leftarrow L_3 \\ 0 & 0 & 0 & -4 + a^2 & a^2 & L_4 \leftarrow L_4 - 2L_3 \end{array}$$

(a) Si  $a^2 - 4 \neq 0$ , alors on a une réduite de Gauss de  $A$  avec 4 pivots. Il admet une solution unique que l'on calcule par le principe de remontée. Le système est de Cramer.

(b) Si  $a^2 - 4 = 0$ , alors en revenant au système, la dernière équation s'écrit  $0 = 4$  donc le système est impossible.

2. Si  $a = 0$ , on a

$$\begin{array}{ccccc|l} 1 & -1 & 0 & 0 & 0 & L_1 \\ 0 & 0 & -1 & 1 & 0 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & 0 & 0 & L_3 \leftarrow L_3 \\ 0 & 0 & 1 & -1 & 0 & L_4 \leftarrow L_4 \\ \hline 1 & -1 & 0 & 0 & 0 & L_1 \\ 0 & 0 & -1 & 1 & 0 & L_2 \leftarrow L_2 \\ 0 & 0 & 0 & 0 & 0 & L_3 \leftarrow L_3 \\ 0 & 0 & 0 & 0 & 0 & L_4 \leftarrow L_4 + L_2 \end{array}$$

On revient au système

$$\begin{cases} x - y & = & 0 \\ -z + t & = & 0 \end{cases}$$

Le système est alors indéterminé et l'ensemble des solutions s'écrit sous forme paramétrique :

$$\{(y, y, z, z), y \in \mathbb{R} z \in \mathbb{R}\}$$

### 10.4.5 Cas général : résolution du système

Le système  $Ax = b$  est équivalent au système  $Rx = b'$  où  $R$  est une réduite de Gauss de  $A$ . On note  $r$  le nombre de pivots notés  $a_1, \dots, a_r$  réels non nuls. On distingue plusieurs cas

— Si  $r = n$ , alors la matrice  $R$  s'écrit

$$R = \begin{pmatrix} a_1 & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & a_2 & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & \cdots \\ 0 & 0 & 0 & a_r & \cdots \end{pmatrix}$$

et le système

$$\begin{cases} a_1 x_1 & & & + & a'_{1,r+1} x_{r+1} & \cdots & + & a'_{1,p} x_p & = & b'_1 \\ & a_2 x_2 & & + & a'_{2,r+1} x_{r+1} & \cdots & + & a'_{2,p} x_p & = & b'_2 \\ & & \ddots & + & \vdots & & + & \vdots & = & \vdots \\ & & & a_r x_r & + & a'_{r,r+1} x_{r+1} & \cdots & + & a'_{r,p} x_p & = & b'_r \end{cases}$$

On en déduit que

- si  $r = p$ , le système est de Cramer, il y a une unique solution,
- si  $r < p$ , le système est indéterminé, il y a une infinité de solutions.
- Si  $r < n$ , alors les  $n - r$  dernières lignes de la matrice  $R$  sont nulles et  $R$  s'écrit

$$R = \begin{pmatrix} a_1 & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & a_2 & \cdots & \cdots \\ 0 & 0 & 0 & a_r & \cdots \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

et le système est

$$\begin{cases} a_1 x_1 & & & + & a'_{1,r+1} x_{r+1} & \cdots & + & a'_{1,p} x_p & = & b'_1 \\ & a_2 x_2 & & + & a'_{2,r+1} x_{r+1} & \cdots & + & a'_{2,p} x_p & = & b'_2 \\ & & \ddots & + & \vdots & & + & \vdots & = & \vdots \\ & & & a_r x_r & + & a'_{r,r+1} x_{r+1} & \cdots & + & a'_{r,p} x_p & = & b'_r \\ & & & & & & & 0 & = & b'_{r+1} \\ & & & & & & & 0 & = & b'_{r+2} \\ & & & & & & & \vdots & = & \vdots \\ & & & & & & & 0 & = & b'_n \end{cases}$$

on en déduit que

- si  $\exists i \in [r+1, n]$  tel que  $b'_i \neq 0$ , alors le système est impossible,
- si  $\forall i \in [r+1, n]$ ,  $b'_i = 0$ , alors le système est indéterminé si  $r < p$  et admet une unique solution si  $r = p$ .

On en déduit le résultat suivant pour le cas particulier d'un système homogène.

**Proposition 10.4.8 système homogène** *On considère un système homogène  $A\mathbf{x} = 0$ , où  $A$  est une matrice de format  $n \times p$ . Soit  $r$  le nombre de pivots d'une réduite de  $A$ . Alors*

- *Le système admet une solution unique si et seulement si  $r = p$ .*
- *Le système est indéterminé si et seulement si  $r < p$ .*
- *Le système n'est jamais impossible.*

### 10.4.6 Solutions d'un système linéaire quelconque

On a vu qu'un système homogène avait toujours au moins la solution  $(0, 0, \dots, 0)$ . En revanche, un système non homogène n'a pas forcément de solutions. On dit alors qu'il est incompatible.

Soit  $(S)$  un système linéaire :  $A\mathbf{x} = b$ . Soit  $(S_0)$  le système homogène associé :  $A\mathbf{x} = 0$ . Soit  $S$  et  $S_0$  l'ensemble des solutions de  $(S)$  et de  $(S_0)$ , respectivement. Pour tout  $\mathbf{x} = (x_1, \dots, x_p) \in \mathbb{R}^p$ , on note

$$\mathbf{x} + S_0 = \{\mathbf{x} + \mathbf{y}, \mathbf{y} \in S_0\} = \{\mathbf{x}' \in \mathbb{R}^p, \exists \mathbf{y} \in S_0, \mathbf{x}' = \mathbf{x} + \mathbf{y}\}$$

l'ensemble des p-uplet de réels de la forme  $\mathbf{x} + \mathbf{y}$  avec  $\mathbf{y} \in S_0$ .

**Proposition 10.4.9** *Si le système linéaire  $(S)$  admet la solution  $\mathbf{x}$ , alors*

$$S = \mathbf{x} + S_0$$

**Preuve :** Soit  $\mathbf{x}$  une solution de  $(S)$ . Montrons  $S = \mathbf{x} + S_0$  par double inclusion. Montrons tout d'abord  $S \subset \mathbf{x} + S_0$ . Soit  $\mathbf{x}' = (x'_1, x'_2, \dots, x'_p) \in S$ . Soit  $\mathbf{y} = \mathbf{x}' - \mathbf{x}$ . On a :

$$A\mathbf{y} = A\mathbf{x}' - A\mathbf{x} = b - b = 0$$

donc  $\mathbf{y}$  est solution de  $(S_0)$ . Or  $\mathbf{x}' = \mathbf{x} + \mathbf{y}$ . Donc  $\mathbf{x}' \in \mathbf{x} + S_0$ , donc  $S \subset \mathbf{x} + S_0$ .

Montrons maintenant  $\mathbf{x} + S_0 \subset S$ . Soit  $\mathbf{y} \in S_0$  et  $\mathbf{x}' = \mathbf{x} + \mathbf{y}$ . Alors

$$A\mathbf{x}' = A\mathbf{x} + A\mathbf{y} = b + 0 = b$$

Donc  $\mathbf{x}' \in S$ . Donc  $\mathbf{x} + S_0 \subset S$ , et par double inclusion,  $S = \mathbf{x} + S_0$ . ■

La proposition précédente se retient de la manière suivante : *la solution générale d'un système linéaire est donnée par la somme d'une solution particulière de ce système et de la solution générale du système homogène associé.*

**Proposition 10.4.10** *Un système linéaire n'a soit aucune solution, soit exactement une solution, soit une infinité de solutions.*

**Preuve :** Si un système linéaire est compatible, alors, d'après la proposition précédente 10.4.9, l'ensemble  $S$  de ses solutions est en bijection avec l'ensemble des solutions du système homogène associé. Donc  $S$  a donc soit un seul élément, soit une infinité. ■

Géométriquement, l'égalité  $S = \mathbf{x} + S_0$  de la proposition 10.4.9 s'interprète de la manière suivante : si  $\mathbf{x}$  est solution de  $(\mathcal{S})$ , alors l'ensemble des solutions de  $(\mathcal{S})$  est l'image par la translation de vecteur  $\mathbf{x}$  de l'ensemble des solutions du système homogène associé. Si l'ensemble des solutions de  $(\mathcal{S})$  est non vide, il a donc la même "forme" que l'ensemble des solutions du système homogène associé. C'est donc soit un point (si  $r = p$ ), soit une droite (si  $r = p - 1$ ), soit un plan (si  $r = p - 2$ ), soit un espace à trois dimensions (si  $r = p - 3$ ), soit un espace "du même type" mais de plus grande dimension.

## 10.5 Matrices et systèmes linéaires

### 10.5.1 Interprétation matricielle des opérations élémentaires

Considérons un système linéaire sous forme matricielle  $AX = B$ , où  $A \in M_{n,p}$ .

**Proposition 10.5.1** Soit  $P \in M_n$  une matrice inversible. Soit  $X \in M_{p,1}$ . On a :

$$PAX = PB \Leftrightarrow AX = B$$

**Preuve :** Si  $AX = B$ , alors  $(PA)X = P(AX) = PB$ . Réciproquement, si  $(PA)X = PB$  alors, puisque  $P$  est inversible,  $P^{-1}(PA)X = P^{-1}(PB)$  donc  $I_n AX = I_n B$  donc  $AX = B$ .

■

Ainsi, si on multiplie l'égalité  $AX = B$  par une matrice inversible, on transforme le système initial en un système équivalent. On va voir dans cette section que les opérations élémentaires sur un système correspondent à multiplier l'égalité  $AX = B$  par des matrices inversibles particulières.

Considérons un système linéaire  $AX = B$  où  $A \in M_{n,p}$ ,  $X \in M_{p,1}$  et  $B \in M_{n,1}$ . Soit  $\lambda \in \mathbb{R}$ . Soient  $i$  et  $j$  des éléments de  $\{1, 2, \dots, n\}$ . On définit les matrices  $P(i, \lambda)$ ,  $Q(i, j)$  et  $R(i, j, \lambda)$  de la manière suivante :

- $P(i, \lambda)$  est la matrice  $n \times n$  obtenue à partir de la matrice identité en multipliant la  $i$ ème ligne par  $\lambda$ , c'est à dire la matrice diagonale dont tous les coefficients diagonaux sont égaux à 1 sauf le  $i$ ème qui vaut  $\lambda$ .
- $Q(i, j)$  est la matrice qu'on obtient à partir de la matrice identité en échangeant la ligne  $i$  avec la ligne  $j$ .
- $R(i, j, \lambda)$  est la matrice qu'on obtient à partir de la matrice identité en rajoutant  $\lambda$  fois la ligne  $j$  à la ligne  $i$ . On a donc  $R(i, j, \lambda) = I_n + \lambda E_{ij}$  où  $I_n$  est la matrice identité d'ordre  $n$  et  $E_{ij}$  la matrice  $n \times n$  dont tous les coefficients sont nuls, sauf celui situé sur la ligne  $i$  et la colonne  $j$  qui vaut 1.

**Exemple 10.5.2** Pour  $n = 6$ ,  $i = 2$  et  $j = 5$ , on a :

$$I_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad P(2, \lambda) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$Q(2, 5) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad R(2, 5, \lambda) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

**Proposition 10.5.3** Considérons le système linéaire  $AX = B$ .

1. Multiplier par  $\lambda$  la ligne  $i$  revient à multiplier l'égalité  $AX = B$  par  $P(i, \lambda)$ , c'est à dire à transformer le système  $AX = B$  en le système  $PAX = PB$ , où  $P = P(i, \lambda)$ .
2. Echanger les lignes  $i$  et  $j$  du système linéaire  $AX = B$  revient à multiplier l'égalité  $AX = B$  par  $Q(i, j)$ , c'est à dire à transformer le système  $AX = B$  en le système  $QAX = QB$ , où  $Q = Q(i, j)$ .
3. Ajouter  $\lambda$  fois la ligne  $j$  à la ligne  $i$  revient à multiplier l'égalité  $AX = B$  par  $R(i, j, \lambda)$ , c'est à dire à transformer le système  $AX = B$  en le système  $RAX = RB$ , où  $R = R(i, j, \lambda)$ .

**Preuve :** On l'admet (c'est un calcul simple mais un peu long à écrire : essayez de le faire). ■

**Proposition 10.5.4** Soient  $i$  et  $j$  des entiers dans  $\{1, 2, \dots, n\}$ .

1. Si  $\lambda \neq 0$ , la matrice  $P(i, \lambda)$  est inversible, d'inverse  $P(i, 1/\lambda)$ .
2. La matrice  $Q(i, j)$  est inversible, d'inverse elle-même
3. Si  $i \neq j$ , que  $\lambda$  soit nul ou non, la matrice  $R(i, j, \lambda)$  est inversible, d'inverse  $R(i, j, -\lambda)$ .

**Preuve :** Preuve du 1. D'après la proposition précédente, la matrice  $P(i, 1/\lambda)P(i, \lambda)$  est la matrice qu'on obtient en multipliant par  $1/\lambda$  la  $i$ ème ligne de  $P(i, \lambda)$ , c'est donc la matrice  $I_n$ . Donc  $P(i, \lambda)$  est inversible d'inverse  $P(i, 1/\lambda)$ . Les autres preuves sont similaires. ■

Comme tout système linéaire peut être transformé en un système échelonné réduit par une suite d'opérations élémentaires, cette proposition s'interprète matriciellement de la manière suivante :

**Proposition 10.5.5** Soit  $A \in \mathcal{M}_{n,p}$  une matrice. Il existe un entier  $k$  et des matrices d'opération élémentaire  $P_1, P_2, \dots, P_k$  telles que la matrice  $P_k P_{k-1} \dots P_2 P_1 A$  est échelonné réduite (le système  $P_k P_{k-1} \dots P_2 P_1 A = P_k P_{k-1} \dots P_2 P_1 B$  est alors échelonné réduit et équivalent à  $AX = B$ ).

### 10.5.2 Calcul de l'inverse d'une matrice par la méthode du pivot

**Proposition 10.5.6** Soit  $A \in \mathcal{M}_n$ . Supposons qu'en faisant une suite d'opérations élémentaires sur les lignes de la matrice  $A$ , on parvienne à la transformer en la matrice identité  $I_n$ . Alors la matrice  $A$  est inversible et en faisant la même suite d'opérations élémentaires sur la matrice  $I_n$  on obtient à la fin la matrice  $A^{-1}$ .

**Preuve :** Supposons qu'en faisant une suite de  $k$  opérations élémentaires sur les lignes de la matrice  $A$ , on parvienne à la transformer en la matrice identité  $I_n$ . Cela veut dire qu'il existe un entier  $k$  et des matrices d'opération élémentaire  $P_1, P_2, \dots, P_k$  telles que  $P_k P_{k-1} \dots P_2 P_1 A = I_n$ . Soit  $B = P_k P_{k-1} \dots P_2 P_1$ . On a  $BA = I_n$ , donc  $A$  est inversible et  $A^{-1} = B$ . De plus, en faisant la même suite d'opérations élémentaires à partir de la matrice  $I_n$  on obtient la matrice  $P_k P_{k-1} \dots P_2 P_1 I_n = P_k P_{k-1} \dots P_2 P_1 = A^{-1}$ .

■

**Exemple 10.5.7** Soit

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ -2 & -2 & 1 \end{pmatrix}$$

On forme le tableau contenant  $A$  dans la partie gauche et  $I_3$  dans la partie droite :

$$\left( \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 3 & 5 & 0 & 1 & 0 \\ -2 & -2 & -1 & 0 & 0 & 1 \end{array} \right)$$

Puis on fait des opérations élémentaires sur les lignes de manière à mettre la partie gauche sous forme échelonné réduite :

$$\begin{array}{l} L_1 \\ L_2 - L_1 \\ L_3 + 2L_1 \end{array} \left( \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 4 & -1 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & 1 \end{array} \right)$$

$$\begin{array}{l} L_1 \\ \frac{1}{2}L_2 \\ L_3 \end{array} \left( \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1/2 & 1/2 & 0 \\ 0 & 0 & 1 & 2 & 0 & 1 \end{array} \right)$$

$$\begin{array}{l} L_1 - L_3 \\ L_2 - 2L_3 \\ L_3 \end{array} \left( \begin{array}{ccc|ccc} 1 & 1 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & -9/2 & 1/2 & -2 \\ 0 & 0 & 1 & 2 & 0 & 1 \end{array} \right)$$

$$\begin{array}{l} L_1 - L_2 \\ L_2 \\ L_3 \end{array} \left( \begin{array}{ccc|ccc} 1 & 0 & 0 & 7/2 & -1/2 & 1 \\ 0 & 1 & 0 & -9/2 & 1/2 & -2 \\ 0 & 0 & 1 & 2 & 0 & 1 \end{array} \right)$$

On est parvenu à transformer la partie de gauche en le tableau correspondant à  $I_3$ . La matrice  $A$  est donc inversible, d'inverse :

$$A^{-1} = \begin{pmatrix} 7/2 & -1/2 & 1 \\ -9/2 & 1/2 & -2 \\ 2 & 0 & 1 \end{pmatrix}$$

Un conseil : à ce stade, vérifiez vos calculs en multipliant  $A$  et la matrice que vous avez trouvée pour  $A^{-1}$ . Si vous ne vous êtes pas trompés, vous devez trouver  $I_n$  ( $I_3$  ici).