

# Algèbre 1 pour les Mathématiques

Résultats principaux du Cours Magistral

Licence 1ère Année – Lyon 1 Université Claude Bernard

Laurent Bétermin\*

## Table des matières

|          |                                                                                 |           |
|----------|---------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Calculs algébriques dans <math>\mathbb{R}</math></b>                         | <b>5</b>  |
| 1.1      | Ensembles de nombres et règles de calculs . . . . .                             | 5         |
| 1.2      | Sommes, produits et identités . . . . .                                         | 7         |
| 1.2.1    | Définitions, propriétés et formules classiques . . . . .                        | 7         |
| 1.2.2    | Sommes télescopiques . . . . .                                                  | 7         |
| 1.2.3    | Identités remarquables . . . . .                                                | 8         |
| <b>2</b> | <b>Logique et raisonnements</b>                                                 | <b>9</b>  |
| 2.1      | Éléments de logique binaire . . . . .                                           | 9         |
| 2.2      | Méthodes de raisonnement . . . . .                                              | 12        |
| <b>3</b> | <b>Ensembles et applications</b>                                                | <b>13</b> |
| 3.1      | Bases de la théorie des ensembles . . . . .                                     | 13        |
| 3.2      | Applications entre ensembles . . . . .                                          | 15        |
| 3.3      | Relation binaire, relation d'équivalence . . . . .                              | 16        |
| <b>4</b> | <b>Arithmétique</b>                                                             | <b>17</b> |
| 4.1      | Divisibilité et nombres premiers . . . . .                                      | 17        |
| 4.2      | PGCD et PPCM et algorithme d'Euclide . . . . .                                  | 17        |
| 4.3      | Coefficients de Bézout et équations diophantiennes . . . . .                    | 18        |
| 4.4      | Congruences . . . . .                                                           | 19        |
| 4.5      | Bases de numération . . . . .                                                   | 19        |
| <b>5</b> | <b>Nombres complexes</b>                                                        | <b>20</b> |
| 5.1      | Définitions et premières propriétés . . . . .                                   | 20        |
| 5.2      | Interprétation géométrique, module, argument et forme trigonométrique . . . . . | 20        |
| 5.3      | Applications en trigonométrie . . . . .                                         | 21        |
| 5.4      | Racines n-ièmes, racines carrées et équation de degré 2 . . . . .               | 22        |
| 5.5      | Ensembles de points et transformations du plan . . . . .                        | 22        |
| <b>6</b> | <b>Polynômes et fractions rationnelles</b>                                      | <b>24</b> |
| 6.1      | Définitions et opérations . . . . .                                             | 24        |
| 6.2      | Arithmétique sur les polynômes . . . . .                                        | 25        |
| 6.3      | Fonction polynomiale et dérivation des polynômes . . . . .                      | 25        |
| 6.4      | Racines d'un polynôme . . . . .                                                 | 26        |
| 6.5      | Polynômes irréductibles et factorisation . . . . .                              | 27        |
| 6.6      | Fractions rationnelles . . . . .                                                | 27        |

---

\*betermin@math.univ-lyon1.fr, Bâtiment Braconnier, Bureau 201.



# Préambule

Ce cours d'Algèbre de premier semestre de L1 va vous permettre à la fois de revoir et/ou d'approfondir des concepts parfois déjà vus dans vos études antérieures.

Prendre au sérieux ce cours, c'est :

- s'améliorer techniquement, au niveau de la maîtrise des calculs (réels, complexes, polynômes) ;
- acquérir les bases, indispensables pour continuer vos études, de logique et de raisonnements (récur-  
rence, implication, équivalence, etc.) ;
- apprendre à rédiger correctement un texte mathématique, et ainsi bien comprendre ce qui est attendu  
en terme de rigueur et de justification ;
- connaître le plus parfaitement possible tous les objets mathématiques et tous les résultats enseignés  
dans cette UE, afin de pouvoir les utiliser durant toutes vos études.

**Les résumés de cours qui suivent ne constituent pas le cours en entier**, mais simplement les résultats vus en CM, sans les très importants exemples et preuves qui seront données exclusivement en CM.

Ainsi, **la présence au CM est obligatoire pour pleinement comprendre les concepts à étudier**. Croire qu'il suffit d'aller uniquement en TD est une erreur trop souvent commise par les étudiant.es.

Vous trouverez sur la **page de l'UE** de nombreux autres documents complémentaires :

- des fiches méthodologiques pour comprendre ce qui est attendu de vous en L1,
- un document expliquant ce qu'il faut savoir-faire après chaque TD,
- la liste des questions de cours qui peuvent vous être demandées en évaluations,
- des exercices supplémentaires corrigés pour vous entraîner,
- les sujets des années précédentes, là aussi pour vous entraîner,
- d'autres documents illustrant les concepts vus en CM, etc.

**Quelques références que vous pouvez trouver à la Bibliothèque Universitaire :**

1. Aassila, *400 exercices d'algèbre avec rappels de cours. Prépas sup.*  
Cf. chapitres 1. à 4.
2. Cottet-Émard, *Toutes les maths pour bien commencer sa licence en 36 fiches.*  
Cf. les fiches 1. à 12. (sauf la 9.)
3. Lehman, *Mathématiques pour l'étudiant de première année. Algèbre et géométrie.*  
Cf. chapitres 1, 2, 4, 7, 8 et 9.
4. Monier, *Algèbre et géométrie. 1ère année MPSI.*  
Cf. chapitres 1, 3, 4, 5. Exercices parfois difficiles.
5. Nguyen, *Algèbre et géométrie L1*  
Cf. chapitres 1, 2, 3, 6, 8.
6. Poineau, *Mathématiques. Exercices incontournables MPSI-PCSI-PTSI*  
Les exercices sont ici plus difficiles.
7. Teyssier, Heu et Collinet, *Fluorescence. Mathématiques.*  
Vous y trouverez des applications et exercices parfois plus « concrets ».

**Attention :** les corrections ne correspondent pas toujours au degré de rigueur attendu dans ce cours!



# 1 Calculs algébriques dans $\mathbb{R}$

## 1.1 Ensembles de nombres et règles de calculs

Dans tout ce chapitre, le terme "ensemble" signifiera "ensemble de nombres réels". Une introduction à la théorie des ensembles sera donnée au chapitre 3.

**Définition 1.1 (Généralités).** On dira qu'un ensemble  $E$  est vide, noté  $E = \emptyset$ , s'il ne contient aucun élément. Si  $E$  et  $F$  sont deux ensembles non-vides, on dit que :

1. **(appartenance)**  $x$  appartient à  $E$ , noté  $x \in E$ , si  $x$  est un des éléments de  $E$ .
2. **(inclusion)**  $E$  est inclus dans  $F$ , noté  $E \subset F$ , si tous les éléments de  $E$  appartiennent à  $F$ . On dit aussi que  $E$  est un sous-ensemble, ou une partie, de  $F$ .  
De plus, dans ce cas,  $F \setminus E$  désigne l'ensemble des éléments de  $F$  qui n'appartiennent pas à  $E$  (on reverra cette notion dans le chapitre 3).
3. **(famille, suite)** Soit  $I \subset \mathbb{N}$  et  $E$  un ensemble. On note  $(a_k)_{k \in I} \subset E$  une famille d'éléments de  $E$  indexée par l'ensemble  $I$ , c'est-à-dire que  $a_k \in E$  pour tout  $k \in I$ . Quand  $I$  est infini, on dit que c'est une suite d'éléments de  $E$ .
4. **(opération)** Si  $*$  est une opération (par exemple l'addition ou la multiplication),
  - on dit que  $E$  est stable par  $*$  si, pour tout  $x \in E$  et  $y \in E$ ,  $x * y \in E$ .
  - on dit que  $*$  est commutative si  $E$  est stable pour cette opération et que, pour tout  $x, y \in E$ ,  $x * y = y * x$ .
  - on appelle élément neutre  $e$  de  $E$  pour  $*$  un nombre  $e \in E$  tel que, pour tout  $x \in E$ ,  $x * e = e * x = x$ .
  - si  $*$  est commutative d'élément neutre  $e$ ,  $\tilde{x} \in E$  est l'inverse de  $x \in E$  si  $x * \tilde{x} = \tilde{x} * x = e$ .
5. **(distributivité)** Soient  $*$  et  $\circ$  deux opérations sur un ensemble  $E$ , alors on dit que  $*$  est distributive par rapport à  $\circ$  si, pour tout  $x, y, z \in E$ ,  $x * (y \circ z) = (x * y) \circ (x * z)$ .

En terme de notation, si  $E$  est un ensemble de nombres et  $P$  une propriété, on écrira  $\{x \in E : P(x)\}$  l'ensemble des éléments de  $E$  qui vérifient la propriété  $P$ .

| Notation                          | Nom              | Définition                                                                  | Opposé (général)   | Inverse (général)                                          |
|-----------------------------------|------------------|-----------------------------------------------------------------------------|--------------------|------------------------------------------------------------|
| $\mathbb{N}$                      | entiers naturels | $\{0, 1, 2, \dots\}$                                                        | Non                | Non                                                        |
| $\mathbb{Z}$                      | entiers relatifs | $\{\dots, -1, 0, 1, 2, \dots\}$                                             | $-n$               | Non                                                        |
| $\mathbb{D}$                      | décimaux         | $\{n \cdot 10^{-k} : n \in \mathbb{Z}, k \in \mathbb{N}\}$                  | $-n \cdot 10^{-k}$ | Non                                                        |
| $\mathbb{Q}$                      | rationnels       | $\left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\right\}$ | $-\frac{a}{b}$     | $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \ (a \neq 0)$ |
| $\mathbb{R}$                      | réels            | "toutes les quantités"                                                      | $-x$               | $x^{-1} = \frac{1}{x} \ (x \neq 0)$                        |
| $\mathbb{R} \setminus \mathbb{Q}$ | irrationnels     | les réels non-rationnels                                                    | $-x$               | $x^{-1} = \frac{1}{x}$                                     |

**Proposition 1.2 (Inclusion et stabilité des ensembles de nombres).** On a  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}$  et tous ces ensembles sont stables par l'addition  $+$  et la multiplication  $\times$ . De plus, l'ensemble des irrationnels  $\mathbb{R} \setminus \mathbb{Q}$  n'est stable ni par  $+$ , ni par  $\times$ .

**Définition 1.3.** Si  $E$  est un des ensembles de nombres ci-dessus, on notera alors :

1.  $E_- = \{x \in E : x \leq 0\}$ , par exemple  $\mathbb{Z}_- = \{\dots, -2, -1, 0\}$  et  $E_+ = \{x \in E : x \geq 0\}$ , par exemple  $\mathbb{Z}_+ = \{0, 1, 2, \dots\} = \mathbb{N}$ .
2.  $E^* = \{x \in E : x \neq 0\}$ , par exemple  $\mathbb{Q}^*$  est l'ensemble des rationnels non-nuls.
3.  $E_-^* = \{x \in E : x < 0\}$  et  $E_+^* = \{x \in E : x > 0\}$ , par exemple  $\mathbb{R}_-^* = ]-\infty, 0[$  et  $\mathbb{R}_+^* = ]0, +\infty[$ .
4.  $aE + b = \{ax + b : x \in E\}$ , où  $a$  et  $b$  sont des réels, par exemple  $2\mathbb{Z}$  est l'ensemble des nombres pairs et  $2\mathbb{Z} + 1$  celui des nombres impairs.

**Proposition 1.4 (Puissances, racines).** On rappelle que :

1. La quantité  $a^b$  existe si :
  - $a \in \mathbb{R}$  et  $b \in \mathbb{N}$  et on a  $a^b = a \times \dots \times a$ , où  $a$  apparaît  $b$  fois, avec pour convention que  $a^0 = 1$ ,
  - $a \in \mathbb{R}^*$  et  $b \in \mathbb{Z}_-$  et on a  $a^b = a^{-1} \times \dots \times a^{-1}$ , où  $a^{-1}$  apparaît  $b$  fois,
  - $a \in \mathbb{R}_+^*$  et  $b \in \mathbb{R}$  et s'écrit  $a^b = e^{b \ln a}$ .
2. Soit  $n \in \mathbb{N}^*$ , la racine  $n$ -ième d'un nombre réel  $x \geq 0$  se note  $\sqrt[n]{x} = x^{\frac{1}{n}}$  de telle sorte que  $\sqrt[n]{x}^n = x$  (c'est la solution  $y \in \mathbb{R}$  de l'équation  $y^n = x$ ). On rappelle la convention définissant la racine carrée :  $\sqrt{x} := \sqrt[2]{x}$ . Si  $x < 0$  et  $n$  est impair, alors on peut définir la racine  $n$ -ième de  $x$  par  $\sqrt[n]{x} = -\sqrt[n]{-x}$ .

**Remarque 1.5.** On a :

- pour tout  $x \in \mathbb{R}$ ,  $\sqrt{x^2} = |x|$ ;
- pour tout  $x \geq 0$ ,  $(\sqrt{x})^2 = x$ .

On rappelle maintenant les règles élémentaires des opérations sur les réels, avec  $a, b, c, d, \alpha, \beta, n, p, x, y$  réels tels que les quantités suivantes aient un sens :

|                 | Fractions                                                                         | Puissances                                                                                                       | Racines $n$ -ièmes                                                                |
|-----------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Somme</b>    | $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$                                  | $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$ (cf. après)                                                  | $\sqrt[n]{x + y} \leq \sqrt[n]{x} + \sqrt[n]{y}$                                  |
| <b>Produit</b>  | $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$                                   | $x^\alpha x^\beta = x^{\alpha+\beta}$ , $(xy)^\alpha = x^\alpha y^\alpha$ , $(x^\alpha)^\beta = x^{\alpha\beta}$ | $\sqrt[n]{xy} = \sqrt[n]{x} \sqrt[n]{y}$ , $\sqrt[n]{\sqrt[p]{x}} = \sqrt[np]{x}$ |
| <b>Quotient</b> | $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$ | $\frac{x^\alpha}{x^\beta} = x^{\alpha-\beta}$ , $\left(\frac{x}{y}\right)^\alpha = \frac{x^\alpha}{y^\alpha}$    | $\sqrt[n]{\frac{x}{y}} = \frac{\sqrt[n]{x}}{\sqrt[n]{y}}$                         |

## 1.2 Sommes, produits et identités

### 1.2.1 Définitions, propriétés et formules classiques

**Définition 1.6 (Sommes et produits).** Soit  $I \subset \mathbb{N}$  un ensemble fini et  $(a_k)_{k \in I} \subset \mathbb{R}$  une famille de réels, alors on note

$$\sum_{k \in I} a_k \quad \text{et} \quad \prod_{k \in I} a_k$$

la somme et le produit de tous les réels  $(a_k)_{k \in I}$ , avec pour convention que  $\sum_{k \in \emptyset} a_k = 0$  et  $\prod_{k \in \emptyset} a_k = 1$ .

De plus, si  $p, n \in \mathbb{Z}$ ,  $p \leq n$ , on note

$$\sum_{k=p}^n a_k = a_p + a_{p+1} + \dots + a_{n-1} + a_n \quad \text{et} \quad \prod_{k=p}^n a_k = a_p a_{p+1} \dots a_n.$$

Notons que cette somme et ce produit ont  $n - p + 1$  termes.

**Proposition 1.7.** Soit  $I$  un ensemble fini,  $(a_k)_{k \in I}$  et  $(b_k)_{k \in I}$  deux familles de réels,  $p \leq n$  deux entiers naturels,  $\lambda, q \in \mathbb{R}$ , alors :

1. Linéarité :  $\sum_{k \in I} (a_k + \lambda b_k) = \sum_{k \in I} a_k + \lambda \sum_{k \in I} b_k$ .
2. Homogénéité :  $\prod_{k=p}^n (\lambda a_k) = \lambda^{n-p+1} \prod_{k=p}^n a_k$ .
3. Sommation d'une constante :  $\sum_{k=p}^n 1 = n - p + 1$  (c'est le nombre de termes de la somme).
4. Somme arithmétique :  $\sum_{k=p}^n k = \frac{(n-p+1)(n+p)}{2}$ . En particulier  $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ .
5. Somme géométrique :  $\sum_{k=p}^n q^k = q^p \frac{1 - q^{n-p+1}}{1 - q} \left( = \frac{q^p - q^{n+1}}{1 - q} \right)$ .

**Proposition 1.8.** Soient  $I$  et  $J$  deux ensembles finis et  $(a_{i,j})_{i \in I, j \in J}$  une famille de réels indexées à la fois par  $i$  et par  $j$ , alors

$$\sum_{i \in I} \sum_{j \in J} a_{i,j} = \sum_{j \in J} \sum_{i \in I} a_{i,j}, \quad \text{notée} \quad \sum_{i \in I, j \in J} a_{i,j}.$$

De plus, si  $a_{i,j} = \alpha_i \beta_j$  avec  $(\alpha_i)_{i \in I}$  et  $(\beta_j)_{j \in J}$  des suites réelles, alors

$$\left( \sum_{i \in I} \alpha_i \right) \left( \sum_{j \in J} \beta_j \right) = \sum_{i \in I, j \in J} \alpha_i \beta_j.$$

### 1.2.2 Sommes télescopiques

**Lemme 1.9 (Changements d'indice).** Soit  $n$  et  $p$  deux entiers naturels,  $(a_k)_{k \in \mathbb{N}}$  une suite de réels et  $k \in \mathbb{Z}$ . Alors, en posant  $j = i + k$ , on effectue un **changement d'indice par translation** :

$$\sum_{i=p}^n a_{i+k} = \sum_{j=p+k}^{n+k} a_j.$$

De plus, en posant  $j = k - i$ , on effectue un **changement d'indice par retournement** :

$$\sum_{i=p}^n a_{k-i} = \sum_{j=k-n}^{k-p} a_j.$$

**Proposition 1.10 (Télescopage).** Soit  $(a_k)_{k \in \mathbb{N}}$  une suite de réels. Pour tous entiers naturels  $n$  et  $p$  tels que  $p \leq n$ ,

$$\sum_{k=p}^n (a_{k+1} - a_k) = a_{n+1} - a_p.$$

### 1.2.3 Identités remarquables

**Proposition 1.11 (Différence de puissances).** Pour tout  $(a, b) \in \mathbb{R}^2$  et tout  $n \in \mathbb{N}^*$ ,

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

**Proposition 1.12 (Carré d'une somme).** Pour toute famille  $(a_i)_{i \in I}$  de réels, avec  $I$  un ensemble fini, on a

$$\left( \sum_{i \in I} a_i \right)^2 = \sum_{i \in I} a_i^2 + \sum_{i, j \in I} a_i a_j = \sum_{i \in I} a_i^2 + 2 \sum_{\substack{i < j \\ i, j \in I}} a_i a_j$$

**Définition 1.13 (Factorielle, coefficient binomial).** On définit les quantités suivantes :

- Pour tout  $n \in \mathbb{N}^*$ , on note  $n! = \prod_{i=1}^n i = 1 \times 2 \times \dots \times n$  et on prend pour convention que  $0! = 1$ . Le nombre  $n!$  avec  $n \in \mathbb{N}$  est appelé **factorielle  $n$** .
- Pour tout entiers naturels  $n$  et  $k$  tels que  $k \leq n$ , le **coefficient binomial** est défini par

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Pour les autres valeurs de  $n$  et  $k$ , on pose  $\binom{n}{k} = 0$ .

**Lemme 1.14 (Formule de Pascal et symétrie).** Pour tous entiers naturels  $n$  et  $k$ , non simultanément nuls, on a

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

De plus, pour tous entiers naturels  $n$  et  $k$  tels que  $n \geq k$ ,  $\binom{n}{k} = \binom{n}{n-k}$ .

**Proposition 1.15 (Formule du binôme de Newton).** Pour tout  $(a, b) \in \mathbb{R}^2$  et tout  $n \in \mathbb{N}$ ,

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

## 2 Logique et raisonnements

### 2.1 Éléments de logique binaire

La logique mathématique est la science du raisonnement. Elle permet d'élaborer des raisonnements par enchaînements d'affirmations selon un langage et des règles précises. Une affirmation mathématique :

- peut être appelée proposition, assertion, énoncé, etc. (cf. ci-dessous ou fiche méthodologique)
- dépendant d'une ou plusieurs variables est appelée formule mathématique ou prédicat.

**Définition :** explication sur la signification mathématique d'un mot/concept.

**Théorème :** un énoncé vrai très important et central.

**Proposition :** un énoncé vrai, moins important/central, mais néanmoins très intéressant.

**Lemme :** un énoncé vrai utilisé pour démontrer d'autres énoncés vrais (une sorte d'outil).

**Corollaire :** un énoncé vrai qui est une simple déduction d'un théorème ou d'une proposition.

**Démonstration/Preuve :** établissement de la vérité d'un énoncé.

**Conjecture :** un énoncé que l'on pense être vrai, mais dont on n'a pas la démonstration.

**Axiome :** une supposition de base pour une situation mathématique.

#### Principes de la logique binaire :

1. une proposition mathématique doit prendre une valeur de vérité;
2. **(Principe du tiers exclu)** une proposition mathématique ne peut prendre que deux valeurs de vérité : la valeur vraie (V) ou la valeur fausse (F). Il n'y a donc pas de tierce possibilité.
3. **(Principe de non-contradiction)** une proposition mathématique ne peut pas être simultanément vraie et fausse.

**Définition 2.1 (Négation, conjonction et disjonction).** On définit les propositions suivantes.

- **Négation :** Soit  $P$  une proposition, alors la négation de  $P$ , notée  $\text{non}(P)$  (ou  $\neg P$ ), est la proposition dont les valeurs sont les contraires de celles de  $P$ .

| $P$ | $\text{non}(P)$ |
|-----|-----------------|
| V   | F               |
| F   | V               |

- **Conjonction :** Soient  $P$  et  $Q$  deux propositions. La conjonction de  $P$  et  $Q$ , notée " $P$  et  $Q$ " (ou bien  $P \wedge Q$ ), est la proposition qui n'est vraie que lorsque  $P$  et  $Q$  sont simultanément vraies.

| $P$ | $Q$ | $P \text{ et } Q$ |
|-----|-----|-------------------|
| V   | V   | V                 |
| V   | F   | F                 |
| F   | V   | F                 |
| F   | F   | F                 |

- **Disjonction :** Soient  $P$  et  $Q$  deux propositions. La disjonction de  $P$  et  $Q$ , notée " $P$  ou  $Q$ " (ou bien  $P \vee Q$ ), est la proposition qui est vraie lorsqu'au moins l'une des deux propositions est vraie.

| $P$ | $Q$ | $P \text{ ou } Q$ |
|-----|-----|-------------------|
| V   | V   | V                 |
| V   | F   | V                 |
| F   | V   | V                 |
| F   | F   | F                 |

**Proposition 2.2 (Règles élémentaires).** On a :

1. **(Tautologie)** La disjonction " $P$  ou  $\text{non}(P)$ " est toujours vraie, c'est ce qu'on appelle une tautologie.
2. **(Contradiction)** La conjonction " $P$  et  $\text{non}(P)$ " est toujours fausse, c'est une contradiction.
3. **(Loi de De Morgan)** Soient  $P$  et  $Q$  deux propositions, alors :
  - a) " $\text{non}(P \text{ ou } Q)$ " et " $\text{non}(P)$  et  $\text{non}(Q)$ " ont les mêmes valeurs de vérité;
  - b) " $\text{non}(P \text{ et } Q)$ " et " $\text{non}(P)$  ou  $\text{non}(Q)$ " ont les mêmes valeurs de vérité.
4. **(Distributivité)** Soient  $P, Q$  et  $R$  trois propositions, alors :
  - a) " $(P \text{ ou } Q) \text{ et } R$ " et " $(P \text{ et } R) \text{ ou } (Q \text{ et } R)$ " ont les mêmes valeurs de vérité;
  - b) " $(P \text{ et } Q) \text{ ou } R$ " et " $(P \text{ ou } R) \text{ et } (Q \text{ ou } R)$ " ont les mêmes valeurs de vérité.

**Définition 2.3 (Implication).** Soient  $P$  et  $Q$  deux propositions. L'implication de  $P$  à  $Q$ , notée " $P \Rightarrow Q$ " (se lit " $P$  implique  $Q$ "), est la proposition qui n'est fausse que lorsque  $P$  est vraie et  $Q$  est fausse. On appelle **réciproque** de  $P \Rightarrow Q$  l'implication  $Q \Rightarrow P$ .

| $P$ | $Q$ | $P \Rightarrow Q$ |
|-----|-----|-------------------|
| V   | V   | V                 |
| V   | F   | F                 |
| F   | V   | V                 |
| F   | F   | V                 |

Si  $P \Rightarrow Q$  est vraie, alors on dit que

- $P$  est une condition suffisante pour avoir  $Q$ ;
- $Q$  est une condition nécessaire pour avoir  $P$ .

**Proposition 2.4 (Propriétés de l'implication, contraposée).** Soient  $P, Q$  et  $R$  trois propositions.

1. **(Implication comme disjonction)** " $P \Rightarrow Q$ " et " $\text{non}(P)$  ou  $Q$ " ont les mêmes valeurs de vérité.
2. **(Négation de l'implication)** La négation d'une implication  $P \Rightarrow Q$  est la conjonction " $P$  et  $\text{non}(Q)$ ".
3. **(Contraposée)** " $P \Rightarrow Q$ " et " $\text{non}(Q) \Rightarrow \text{non}(P)$ " ont les mêmes valeurs de vérité. La proposition " $\text{non}(Q) \Rightarrow \text{non}(P)$ " est appelée **contraposée** de " $P \Rightarrow Q$ ".
4. **(Transitivité)** Si  $P \Rightarrow Q$  et  $Q \Rightarrow R$  sont vraies, alors  $P \Rightarrow R$  l'est aussi.

**Définition 2.5 (Equivalence).** Soient  $P$  et  $Q$  deux propositions. L'équivalence de  $P$  et  $Q$ , notée " $P \iff Q$ " (se lit " $P$  équivalent à  $Q$ ") est la proposition qui n'est vraie que lorsque  $P$  et  $Q$  ont même valeur de vérité (soit simultanément vraies, soit simultanément fausses). Ainsi, " $P \iff Q$ " est équivalente à la double implication " $P \Rightarrow Q$  et  $Q \Rightarrow P$ ".

| $P$ | $Q$ | $P \iff Q$ |
|-----|-----|------------|
| V   | V   | V          |
| V   | F   | F          |
| F   | V   | F          |
| F   | F   | V          |

Si  $P \iff Q$  est vraie, on dit que  $P$  est une condition nécessaire et suffisante de  $Q$  : il faut et il suffit que  $P$  soit vraie pour que  $Q$  soit vraie. On dit aussi que  $P$  est vraie **si et seulement si**  $Q$  est vraie.

**Définition 2.6 (Quantificateurs universel/existentiel).** On définit les notations suivantes :

1. L'expression " $\forall x \in A$ " se lit "quelque soit  $x$  élément de  $A$ " ou bien "pour tout  $x$  appartenant à  $A$ ".
2. L'expression " $\exists x \in A$ " se lit "il existe (au moins) un élément  $x$  de  $A$ ".
3. L'expression " $\exists! x \in A$ " se lit "il existe un unique élément  $x$  de  $A$ ".

On a de plus, étant donnée  $P(x)$  une propriété qui dépend d'une variable  $x$ ,

- La négation de " $\forall x \in A, P(x)$ " est " $\exists x \in A, \text{non}(P(x))$ ".
- La négation de " $\exists x \in A, P(x)$ " est " $\forall x \in A, \text{non}(P(x))$ ".

On écrira aussi " $\nexists x \in A, P(x)$ " pour "il n'existe pas d'élément  $x$  dans  $A$  vérifiant  $P(x)$ ".

En mathématiques, on utilise souvent des lettres des alphabets latins ( $a, b, c$ , etc.) et grecs ( $\alpha, \beta$ , etc.). Pour ne pas être trop perdu et savoir comment ces lettres grecques se prononcent à l'oral, voici l'**alphabet grec** :

| Ecriture latine de la lettre | Majuscule  | Minuscule  |
|------------------------------|------------|------------|
| alpha                        | A          | $\alpha$   |
| beta                         | B          | $\beta$    |
| gamma                        | $\Gamma$   | $\gamma$   |
| delta                        | $\Delta$   | $\delta$   |
| epsilon                      | E          | $\epsilon$ |
| zeta                         | Z          | $\zeta$    |
| eta                          | H          | $\eta$     |
| theta                        | $\Theta$   | $\theta$   |
| iota                         | I          | $\iota$    |
| kappa                        | K          | $\kappa$   |
| lambda                       | $\Lambda$  | $\lambda$  |
| mu                           | M          | $\mu$      |
| nu                           | N          | $\nu$      |
| xi                           | $\Xi$      | $\xi$      |
| omicron                      | O          | $\omicron$ |
| pi                           | $\Pi$      | $\pi$      |
| rho                          | R          | $\rho$     |
| sigma                        | $\Sigma$   | $\sigma$   |
| tau                          | T          | $\tau$     |
| upsilon                      | $\Upsilon$ | $\upsilon$ |
| phi                          | $\Phi$     | $\phi$     |
| chi                          | X          | $\chi$     |
| psi                          | $\Psi$     | $\psi$     |
| omega                        | $\Omega$   | $\omega$   |

## 2.2 Méthodes de raisonnement

À partir de postulats et d'axiomes (propriétés supposées intrinsèquement vraies, que l'on ne peut pas démontrer), on enrichit par une démarche hypothético-déductive la théorie de nouveaux résultats hiérarchisés selon des théorèmes, des propositions, des corollaires et des lemmes.

On dresse ci-après toute une liste de méthodes de raisonnement fondées sur la logique mathématique.

1. **Raisonnement direct (ou par déduction)** : si  $H$  est vraie et si l'implication  $H \Rightarrow C$  est vraie, alors  $C$  est vraie, où  $H$  est l'hypothèse et  $C$  la conclusion.
2. **Raisonnement par disjonction de cas** : c'est un raisonnement direct dans lequel l'hypothèse  $H$  peut se décomposer en plusieurs autres hypothèses, par exemple quand on a l'équivalence  $H \iff "H_1 \text{ ou } H_2"$ . Si  $H_1 \Rightarrow C$  et  $H_2 \Rightarrow C$  sont vraies, alors  $H \Rightarrow C$  est vraie.
3. **Raisonnement par contraposition** : pour montrer que  $H \Rightarrow C$ , on montre (puisque les propositions sont équivalentes) que  $\text{non}(C) \Rightarrow \text{non}(H)$ .
4. **Raisonnement par l'absurde** : pour démontrer qu'une proposition  $P$  est vraie, on suppose sa négation vraie et l'on montre que cela vient contredire une proposition  $Q$  qui est vraie. Cela vient du fait, puisque  $Q$  et  $\text{non}(Q)$  ne peuvent être vraies simultanément, que

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

5. **Raisonnement par contre-exemple** : pour montrer que la propriété " $\forall x \in A, P(x)$ " est fausse, il suffit de trouver un  $x_0 \in A$  pour lequel  $P(x_0)$  est fausse. On dit que ce  $x_0$  est un contre-exemple.
6. **Raisonnement par récurrence simple** : Pour montrer qu'une propriété  $P(n)$  est vraie pour tout entier  $n \geq n_0$  avec  $n_0 \in \mathbb{N}$  fixé, il suffit d'établir les deux propriétés suivantes :
  - *Initialisation* : la propriété  $P(n_0)$  est vraie;
  - *Hérédité* :  $\forall n \geq n_0$  fixé tel que  $P(n)$  soit vraie, alors  $P(n+1)$  est vraie.

On parlera de **récurrence double** quand la propriété est initialisée pour  $P(n_0)$  et  $P(n_0+1)$ , et que, pour tout entier  $n \geq n_0$  fixé, " $P(n)$  et  $P(n+1)$ " vraie implique que  $P(n+2)$  est vraie.

7. **Raisonnement par récurrence forte** : Pour montrer qu'une propriété  $P(n)$  est vraie pour tout entier  $n \geq n_0$  avec  $n_0 \in \mathbb{N}$  fixé, il suffit d'établir les deux propriétés suivantes :
  - *Initialisation* : la propriété  $P(n_0)$  est vraie;
  - *Hérédité* : soit  $n \geq n_0$  fixé tel que  $P(k)$  soit vraie pour tout  $n_0 \leq k \leq n$ , alors  $P(n+1)$  est vraie.

**Attention à la rédaction de la récurrence (simple, double, forte)!** (cf. fiche méthode)

8. **Raisonnement par analyse-synthèse** : Il se déroule en deux étapes :
  - i) **l'analyse** : on raisonne sur une hypothétique solution au problème considéré et l'on accumule des déductions de propriétés qu'elle doit vérifier, du seul fait qu'elle est solution;
  - ii) **la synthèse** : on examine tous les objets vérifiant les conditions nécessaires précédemment accumulées (ce sont les seuls candidats pouvant être des solutions) et l'on détermine, parmi eux, lesquels sont réellement des solutions au problème initial.

## 3 Ensembles et applications

### 3.1 Bases de la théorie des ensembles

On part ici d'une définition intuitive et peu formelle de la notion d'ensemble : c'est une collection d'objets mathématiques (nombres, fonctions, triangles, points, etc.). Traditionnellement, on essaie de noter les ensembles par des lettres majuscules et leurs éléments avec des lettres minuscules.

**Définition 3.1 (Appartenance).** Si un objet  $x$  est dans un ensemble  $E$ , on note  $x \in E$  et on dit que " $x$  appartient à  $E$ ". Sa négation " $x$  n'appartient pas à  $E$ " s'écrit  $x \notin E$ .

**Définition 3.2 (Extentionnalité).** Deux ensembles  $E$  et  $F$  sont égaux si et seulement s'ils ont les mêmes éléments :

$$E = F \iff \forall x, (x \in E \iff x \in F).$$

**Définition 3.3 (Ensemble vide).** On note  $\emptyset$  l'ensemble vide, c'est l'ensemble qui ne contient aucun élément.

**Définition 3.4 (Définition d'un ensemble en extension).** Soit  $n \in \mathbb{N}^*$ . Etant donnés des objets mathématiques  $x_1, \dots, x_n$ , on note  $\{x_1, \dots, x_n\}$  l'ensemble non-ordonné contenant exactement ces objets. De plus, si  $x$  est un objet mathématique,  $\{x\}$  est appelé un singleton.

**Définition 3.5 (Définition d'un ensemble en compréhension).** Pour tout ensemble  $E$  et toute proposition  $P$ , on note  $\{x \in E : P(x)\}$  l'ensemble dont les éléments sont exactement les éléments de  $E$  qui vérifient  $P$ . Pour tout ensemble  $E$  et toute expression  $e[x]$  contenant une variable  $x$ , on note  $\{e[x] : x \in E\}$  l'ensemble des objets mathématiques qui s'écrivent sous la forme  $e[x]$  avec  $x \in E$ .

**Définition 3.6 (Ensemble fini, infini et cardinal).** Lorsqu'un ensemble  $E$  admet un nombre fini d'éléments, ce nombre d'éléments est appelé le cardinal de  $E$ , noté  $\text{Card}(E)$ ,  $|E|$  ou  $\#E$ . Lorsque  $E$  est infini, on pose  $\text{Card}(E) = +\infty$ .

**Définition 3.7 (Inclusion et parties d'un ensemble).** Soient  $E$  et  $F$  deux ensembles. On dit que  $E$  est inclus dans  $F$ , et on note  $E \subset F$ , si tout élément de  $E$  est aussi un élément de  $F$ , c'est-à-dire

$$(\forall x \in E, x \in F) \text{ que l'on écrit aussi } (\forall x, x \in E \Rightarrow x \in F).$$

Si  $E \subset F$ , on dit que  $E$  est une partie (ou un sous-ensemble) de  $F$ . L'ensemble des parties d'un ensemble  $F$  est noté  $\mathcal{P}(F)$ . Ainsi, pour tout ensemble  $E$ , on a  $E \in \mathcal{P}(F) \iff E \subset F$ .

**Proposition 3.8 (Transitivité de l'inclusion et égalité d'ensembles).** Soient  $E, F$  et  $G$  trois ensembles.

Si  $E \subset F$  et  $F \subset G$ , alors  $E \subset G$ .

De plus, on a  $E = F \iff E \subset F$  et  $F \subset E$ .

**Définition 3.9 (Union et intersection d'ensembles).** Soit  $E$  un ensemble et  $A, B$  des parties de  $E$ .

1. On appelle **réunion** de  $A$  et  $B$ , notée  $A \cup B$ , l'ensemble dont les éléments sont exactement ceux qui sont dans  $A$  ou dans  $B$ , autrement dit,

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

2. On appelle **intersection** de  $A$  et  $B$ , notée  $A \cap B$ , l'ensemble dont les éléments sont exactement ceux qui sont à la fois dans  $A$  et dans  $B$ , autrement dit,

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

**Proposition 3.10 (Propriétés de bases de l'union et de l'intersection).** Soient  $A, B$  et  $C$  trois parties d'un ensemble  $E$ .

1.  $A \cup \emptyset = A$ ,  $A \cap \emptyset = \emptyset$ ,  $A \cup E = E$  et  $A \cap E = A$ .
2.  $\cup$  et  $\cap$  sont associatives :  $A \cup (B \cup C) = (A \cup B) \cup C =: A \cup B \cup C$  et  $A \cap (B \cap C) = (A \cap B) \cap C =: A \cap B \cap C$ .
3.  $\cup$  et  $\cap$  sont commutatives :  $A \cup B = B \cup A$  et  $A \cap B = B \cap A$ .
4. On a toujours  $A \cap B \subset A \subset A \cup B$  et  $A \cap B \subset B \subset A \cup B$ .

**Définition 3.11 (Ensembles disjoints).** On dit que deux ensembles  $A$  et  $B$  sont disjoints si  $A \cap B = \emptyset$ .

**Définition 3.12 (Différence d'ensembles et complémentaire).** Soit  $E$  un ensemble et  $A, B$  deux parties de  $E$ . On appelle différence de  $B$  et  $A$  (ou  $B$  privé de  $A$ , ou  $B$  moins  $A$ ) l'ensemble noté  $B \setminus A$  (ou  $B - A$ ) tel que, pour tout  $x \in E$ ,  $x \in B$  et  $x \notin A$ .

On appelle complémentaire de  $A$  dans  $E$  l'ensemble  $A^c = E \setminus A$ .

**Définition 3.13 (Famille d'ensembles).** Soit  $I$  un ensemble et, pour tout  $i \in I$ ,  $A_i$  un ensemble. Alors  $(A_i)_{i \in I}$  est appelée famille d'ensembles indexée par  $I$ . Quand  $I$  est un ensemble fini (resp. infini), on dit que la famille est finie (resp. infinie).

**Définition 3.14 (Généralisation à des familles d'ensembles).** Soit  $I$  un ensemble,  $(A_i)_{i \in I}$  une famille de parties d'un ensemble  $E$ , alors on note respectivement  $\bigcup_{i \in I} A_i$  et  $\bigcap_{i \in I} A_i$  la réunion et l'intersection de ces ensembles et on a

$$\begin{aligned} \forall x \in E, \quad x \in \bigcup_{i \in I} A_i &\iff \exists i \in I, x \in A_i; \\ \forall x \in E, \quad x \in \bigcap_{i \in I} A_i &\iff \forall i \in I, x \in A_i. \end{aligned}$$

**Proposition 3.15 (Distributivité).** Soit  $I$  un ensemble,  $(A_i)_{i \in I}$  une famille d'ensembles et  $B$  un ensemble, alors

$$\left( \bigcap_{i \in I} A_i \right) \cup B = \bigcap_{i \in I} (A_i \cup B) \quad \text{et} \quad \left( \bigcup_{i \in I} A_i \right) \cap B = \bigcup_{i \in I} (A_i \cap B).$$

**Proposition 3.16 (Lois de De Morgan).** Soit  $E$  et  $I$  des ensembles et  $(A_i)_{i \in I}$  une famille de parties de  $E$ . Alors

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

**Définition 3.17 (Recouvrement, partition).** Soit  $E$ ,  $A$  et  $I$  des ensembles et  $(A_i)_{i \in I}$  une famille de parties de  $E$ . Alors on dit que

1.  $(A_i)_{i \in I}$  est un recouvrement de  $A$  si  $A \subset \bigcup_{i \in I} A_i$ ;
2.  $(A_i)_{i \in I}$  est une partition de  $A$  si  $\forall i \in I, A_i \neq \emptyset$ ,  $A = \bigcup_{i \in I} A_i$  et  $\forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset$ .

**Définition 3.18 (Produit cartésien).** Soient  $E$  et  $F$  deux ensembles. On admet que l'on peut construire un ensemble noté  $E \times F$ , appelé produit cartésien de  $E$  et  $F$ , dont les éléments sont les couples  $(x_1, x_2)$  avec  $x_1 \in E$  et  $x_2 \in F$  et tels que,

$$\forall (x_1, x_2), (y_1, y_2) \in E \times F, \quad (x_1, x_2) = (y_1, y_2) \iff x_1 = y_1 \quad \text{et} \quad x_2 = y_2.$$

Soit  $n \geq 3$  un entier, on définit de même le produit cartésien de  $n$  ensembles  $E_1, \dots, E_n$ , noté  $E_1 \times \dots \times E_n$  formé des  $n$ -uplets  $(x_1, \dots, x_n)$  avec  $x_i \in E_i$  pour tout  $1 \leq i \leq n$ . Si ces  $n$  ensembles sont égaux à  $E$ , on note ce produit  $E^n$ .

**Proposition 3.19.** Soient  $A$  et  $B$  deux ensembles finis, alors  $\text{Card}(A \times B) = \text{Card}(A)\text{Card}(B)$ .

## 3.2 Applications entre ensembles

**Définition 3.20 (Application).** Une application  $f : E \rightarrow F$ ,  $x \mapsto f(x)$ , est la donnée :

- d'un ensemble de départ  $E$ ,
- d'un ensemble d'arrivée  $F$ ,
- d'une définition ou d'une formule associant à chaque élément  $x \in E$  un unique élément  $y = f(x) \in F$ .

De plus, on notera  $F^E$  l'ensemble des applications de  $E$  dans  $F$ .

**Définition 3.21 (Images, antécédents).** Soit  $f : E \rightarrow F$  une application, alors :

- pour tout  $x \in E$ , on appelle image de  $x$  par  $f$  l'élément  $y = f(x) \in F$ .
- Si  $A \subset E$ , on note  $f(A) = \{f(x) : x \in A\}$  l'image de  $A$  par  $f$ , c'est-à-dire l'ensemble des images des éléments de  $A$  par  $f$ . Si  $A = E$ ,  $f(E)$  s'appelle l'image de  $f$ .
- Si  $y \in F$  est donné, alors on dit que  $x \in E$  est un antécédent de  $y$  par  $f$  si  $f(x) = y$ .
- Si  $B \subset F$ , alors on note  $f^{-1}(B) = \{x \in E : f(x) \in B\}$  l'image réciproque de  $B$  par  $f$ . Il s'agit de l'ensemble des antécédents (éventuellement vide) des éléments de  $B$  par  $f$ .

**Définition 3.22 (Restriction, prolongement).** Soit  $f : E \rightarrow F$  une application et  $A \subset E$ . On appelle restriction de  $f$  à  $A$  l'application  $f|_A : A \rightarrow F$  définie par  $f|_A(x) = f(x)$  pour tout  $x \in A$ .

On suppose  $f : A \rightarrow F$  et  $A \subset E$  donnés. On appelle prolongement de  $f$  à  $E$  une application  $g : E \rightarrow F$  telle que  $g|_A = f$  c'est-à-dire coïncidant sur  $A$  avec  $f$ .

**Remarque 3.23 (Application ou fonction?).** En Analyse, on parlera surtout de fonctions, et peu d'applications. La distinction est la suivante :  $f : E \rightarrow F$  est

- une fonction si chaque élément de  $E$  admet une ou aucune image par  $f$  ;
- une application si chaque élément de  $E$  admet une image par  $f$ .

Il faut donc restreindre  $f$  à son ensemble de définition  $D_f \subset E$  pour que  $f : D_f \rightarrow F$  soit une application.

**Proposition 3.24 (Images directes/réciproques et opérations).** Soit  $f : E \rightarrow F$ ,  $A, B \in \mathcal{P}(E)$  et  $C, D \in \mathcal{P}(F)$ , alors :

- |                                                  |                                                            |
|--------------------------------------------------|------------------------------------------------------------|
| 1. $A \subset B \Rightarrow f(A) \subset f(B)$ ; | 4. $C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$ ; |
| 2. $f(A \cap B) \subset f(A) \cap f(B)$ ;        | 5. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$ ;         |
| 3. $f(A \cup B) = f(A) \cup f(B)$ ;              | 6. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ .         |

**Définition 3.25 (Injectivité).** On dit que l'application  $f : E \rightarrow F$  est injective si tout élément de  $F$  admet au plus un antécédent par  $f$ , c'est-à-dire si

$$\forall (x, x') \in E^2, \quad f(x) = f(x') \Rightarrow x = x'.$$

**Remarque 3.26 (Application non-injective).** On dit que  $f : E \rightarrow F$  n'est pas injective si

$$\exists (x, x') \in E^2, \quad f(x) = f(x') \text{ et } x \neq x',$$

autrement dit si deux éléments distincts de  $E$  ont même image par  $f$ .

**Définition 3.27 (Surjectivité).** On dit que l'application  $f : E \rightarrow F$  est surjective si tout élément de  $F$  admet au moins un antécédent par  $f$ , c'est-à-dire si

$$\forall y \in F, \quad \exists x \in E, \quad y = f(x).$$

**Remarque 3.28 (Application non-surjective).** On dit que  $f : E \rightarrow F$  n'est pas surjective si

$$\exists y \in F, \quad \forall x \in E, \quad y \neq f(x),$$

c'est-à-dire si au moins un élément de  $F$  n'admet pas d'antécédent par  $f$ .

**Définition 3.29 (Bijectivité).** On dit que l'application  $f : E \rightarrow F$  est bijective si tout élément de  $F$  admet un unique antécédent par  $f$ , c'est-à-dire si

$$\forall y \in F, \quad \exists! x \in E, \quad y = f(x),$$

c'est-à-dire si  $f$  est à la fois injective et surjective. Dans ce cas,  $f$  admet une application réciproque  $f^{-1} : F \rightarrow E$ ,  $x \mapsto f^{-1}(y)$  et on dit que  $E$  et  $F$  son equipotents.

**Définition 3.30 (Composition).** Soient  $f : E \rightarrow F$  et  $g : G \rightarrow H$  deux applications telles que  $f(E) \subset G$ . La composée de  $f$  par  $g$  est l'application notée  $g \circ f : E \rightarrow H$  et définie pour tout  $x \in E$  par  $(g \circ f)(x) = g(f(x))$ .

**Proposition 3.31 (Associativité de la composition).** Soient  $f : E \rightarrow E'$ ,  $g : F \rightarrow F'$  et  $h : G \rightarrow G'$  des applications telles que  $f(E) \subset F$  et  $g(F) \subset G$ . Alors on a  $h \circ (g \circ f) = (h \circ g) \circ f$  donnée par  $x \mapsto h(g(f(x)))$  et notée  $h \circ g \circ f$ .

**Définition 3.32 (Identité sur un ensemble).** Soit  $E$  un ensemble, on note  $\text{Id}_E : E \rightarrow E$ ,  $x \mapsto x$  l'application identité de  $E$ .

**Proposition 3.33 (Lien entre application, réciproque et identité).** Si  $f : E \rightarrow F$  est une bijection, alors l'application réciproque  $f^{-1} : F \rightarrow E$  satisfait :

$$f^{-1} \circ f = \text{Id}_E \quad \text{et} \quad f \circ f^{-1} = \text{Id}_F.$$

**Proposition 3.34 (Inverse d'une composée de bijections).** Si  $f : E \rightarrow F$  et  $g : F \rightarrow G$  sont des bijections, alors  $g \circ f$  est bijective et  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

### 3.3 Relation binaire, relation d'équivalence

**Définition 3.35 (Relation binaire, relation d'équivalence).** Soit  $E$  un ensemble et  $G \subset E \times E$ , alors la proposition  $\mathcal{R}$  définie par

$$\mathcal{R}(x, y) \iff (x, y) \in G$$

est appelée **relation binaire** sur  $E$ , et on notera, pour tout  $(x, y) \in G$ ,  $x\mathcal{R}y$  au lieu de  $\mathcal{R}(x, y)$ .

Une relation binaire sur un ensemble  $E$  est une **relation d'équivalence** sur  $E$  si elle est :

1. réflexive :  $\forall x \in E, x\mathcal{R}x$ ,
2. symétrique :  $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$ ,
3. transitive :  $\forall (x, y, z) \in E^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$ .

**Définition 3.36 (Classe d'équivalence).** Soit  $E$  un ensemble et  $\mathcal{R}$  une relation d'équivalence sur  $E$ . Alors l'ensemble  $\bar{x} := \{y \in E : x\mathcal{R}y\}$  est appelé classe d'équivalence de  $x$  pour la relation  $\mathcal{R}$ .

**Proposition 3.37 (Relations et classes).** Soit  $E$  un ensemble,  $\mathcal{R}$  une relation d'équivalence sur  $E$  et  $(x, y) \in E^2$ . Alors les propriétés suivantes sont équivalentes :

$$(i) \ x\mathcal{R}y \qquad (ii) \ y \in \bar{x} \qquad (iii) \ \bar{x} = \bar{y}$$

**Définition 3.38 (Représentant).** Soit  $E$  un ensemble et  $\mathcal{R}$  une relation d'équivalence sur  $E$ . Si  $A$  est une classe d'équivalence pour  $\mathcal{R}$ , on appelle représentant de la classe tout élément  $x \in A$  et on a ainsi  $\bar{x} = A$ .

**Proposition 3.39.** Soit  $E$  un ensemble. L'ensemble des classes d'équivalence pour une relation d'équivalence  $\mathcal{R}$  sur  $E$ , appelé ensemble quotient de  $E$  par  $\mathcal{R}$ , noté  $E/\mathcal{R}$ , forment une partition de  $E$ .

## 4 Arithmétique

### 4.1 Divisibilité et nombres premiers

**Définition 4.1 (Divisibilité).** Soient  $a \in \mathbb{Z}^*$  et  $b \in \mathbb{Z}$ . On dit que  $a$  divise  $b$ , et note  $a|b$  s'il existe  $k \in \mathbb{Z}$  tel que  $b = ka$ . On dit alors aussi que  $b$  est un multiple de  $a$ .

Pour tout  $b \in \mathbb{N}$ , on notera  $\text{div}(b) = \{a \in \mathbb{N} : a|b\}$  l'ensemble des diviseurs positifs de  $b$ .

Pour tout  $a, b \in \mathbb{N}$ , on notera  $\text{div}(a, b) = \text{div}(a) \cap \text{div}(b)$  l'ensemble des diviseurs communs positifs à  $a$  et  $b$ .

**Définition 4.2.** On dit que  $p \in \mathbb{N}$  est un nombre premier si  $p \geq 2$  et  $\text{div}(p) = \{1, p\}$ .

**Lemme 4.3 (Existence d'un facteur premier).** Soit  $n \in \mathbb{N}$ ,  $n \geq 2$ . Soit  $p$  le plus petit diviseur de  $n$  supérieur ou égal à 2. Alors  $p$  est premier.

**Théorème 4.4 (Théorème d'Euclide).** Il existe une infinité de nombres premiers.

**Théorème 4.5 (Théorème fondamental de l'arithmétique).** Soit  $n \geq 2$  un entier, alors il existe une unique écriture de  $n$  sous la forme

$$n = \prod_{i=1}^k p_i^{\alpha_i}$$

où, pour tout  $i \in \{1, \dots, k\}$ ,  $p_i$  est un nombre premier,  $\alpha_i \in \mathbb{N}^*$  est appelée la  $p_i$ -valuation de  $n$  et  $p_1 < p_2 < \dots < p_k$ .

**Proposition 4.6 (Division euclidienne).** Soient  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  d'entiers tels que

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

L'entier  $q$  est le quotient et  $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

### 4.2 PGCD et PPCM et algorithme d'Euclide

**Définition 4.7 (Plus Grand Commun Diviseur (PGCD)).** Soit  $(a, b) \in \mathbb{Z}^2$  tels que  $(a, b) \neq (0, 0)$ , alors l'ensemble  $\text{div}(a, b)$  des diviseurs positifs communs à  $a$  et  $b$  est fini et non-vide (car il contient  $n = 1$ ). Il admet donc un plus grand élément noté  $\text{PGCD}(a, b)$ .

**Proposition 4.8 (PGCD et décomposition en facteurs premiers).** Supposons qu'il existe  $k$  nombres premiers distincts  $\{p_1, \dots, p_k\}$  et  $2k$  nombres entiers (éventuellement nuls)  $\{\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k\}$  tels que

$$a = \prod_{i=1}^k p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^k p_i^{\beta_i},$$

alors on a  $\text{PGCD}(a, b) = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}$ .

**Proposition 4.9 (Homogénéité du PGCD).** Soient  $(a, b) \in \mathbb{Z}^2$  deux entiers non-nuls. Alors,

$$\forall k \in \mathbb{N}^*, \quad \text{PGCD}(ka, kb) = k \times \text{PGCD}(a, b).$$

**Algorithme d'Euclide pour calculer le PGCD.**

Remarques préliminaires :  $\text{PGCD}(a, b) = \text{PGCD}(b, a - b)$ ,  $\text{PGCD}(a, b) = \text{PGCD}(b, a)$  et  $\text{PGCD}(a, 0) = a$ .

Principe de l'algorithme d'Euclide : quitte à échanger  $a$  et  $b$ , on peut supposer que  $a \geq b$ .

- si  $b = 0$ , alors on a  $\text{PGCD}(a, b) = \text{PGCD}(a, 0) = a$ .
- si  $b \neq 0$ , alors on effectue la division euclidienne de  $a$  par  $b$ ,  $a = bq + r$  et on utilise la remarque préliminaire ( $q$  fois) pour dire que  $\text{PGCD}(a, b) = \text{PGCD}(b, a - qb) = \text{PGCD}(b, r)$ .

On réitère ce principe jusqu'à obtenir  $\text{PGCD}(d, 0)$  où  $d$  sera donc  $d = \text{PGCD}(a, b)$ .

**Définition 4.10 (Plus Petit Commun Multiple (PPCM)).** Soient  $(a, b) \in \mathbb{Z}^2$  tels que  $(a, b) \neq (0, 0)$ , alors l'ensemble des multiples communs à  $a$  et  $b$

$$\{n \in \mathbb{N}^* : a|n \text{ et } b|n\}$$

est non-vide (car il contient  $ab$ ). Il admet donc un plus petit élément noté  $\text{PPCM}(a, b)$ .

**Proposition 4.11 (PPCM et décomposition en facteurs premiers).** Supposons qu'il existe  $k$  nombres premiers distincts  $\{p_1, \dots, p_k\}$  et  $2k$  nombres entiers (éventuellement nuls)  $\{\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k\}$  tels que

$$a = \prod_{i=1}^k p_i^{\alpha_i}, \quad \text{et} \quad b = \prod_{i=1}^k p_i^{\beta_i},$$

alors on a  $\text{PPCM}(a, b) = \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)}.$

**Proposition 4.12 (Lien entre le PGCD et le PPCM).** Pour tout  $(a, b) \in \mathbb{Z}^2$  tels que  $(a, b) \neq (0, 0)$ ,

$$\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab.$$

**Définition 4.13 (Nombres premiers entre eux).** Soient  $(a, b) \in \mathbb{Z}^2$ . On dit que  $a$  et  $b$  sont premiers entre eux si  $\text{PGCD}(a, b) = 1$ , c'est-à-dire si le seul diviseur commun positif de  $a$  et  $b$  est 1.

**Proposition 4.14.** Soient  $(a, b) \in \mathbb{N}^2$  deux entiers non-nuls. Soit  $d$  un diviseur commun à  $a$  et  $b$  et posons  $a = da'$  ainsi que  $b = db'$  avec  $(a', b') \in \mathbb{N}$ . On a

$$\text{PGCD}(a, b) = d \iff a' \text{ et } b' \text{ sont premiers entre eux.}$$

### 4.3 Coefficients de Bézout et équations diophantiennes

**Théorème 4.15 (Identité de Bézout).** Soient  $a$  et  $b$  deux entiers naturels non nuls, alors il existe deux entiers  $(u, v) \in \mathbb{Z}^2$ , appelés coefficients de Bézout, tels que

$$au + bv = \text{PGCD}(a, b).$$

En particulier,

$$a \text{ et } b \text{ sont premiers entre eux} \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1.$$

**Théorème 4.16 (Lemme de Gauss).** Soient  $a, b, c \in \mathbb{Z}^*$  tels que  $a$  et  $b$  soient premiers entre eux. Si  $a|bc$  alors  $a|c$ .

**Définition 4.17 (Equation diophantienne).** On appelle équation diophantienne toute équation de la forme  $ax + by = c$  avec  $(a, b, c) \in \mathbb{Z}^3$  et d'inconnues  $(x, y) \in \mathbb{Z}^2$ .

**Théorème 4.18 (Solutions d'une équation diophantienne).** Soient  $a, b, c \in \mathbb{Z}$ , alors :

1. L'équation  $ax + by = c$  admet une solution  $(x, y) \in \mathbb{Z}^2$  si et seulement si  $\text{PGCD}(a, b)|c$ .
2. Si  $a$  et  $b$  sont premiers entre eux et  $(x_0, y_0)$  est une solution particulière de l'équation  $ax + by = c$ , alors l'ensemble des solutions de cette équation est  $S = \{(x_0 + kb, y_0 - ka) \in \mathbb{Z}^2 : k \in \mathbb{Z}\}.$

## 4.4 Congruences

**Définition 4.19 (Congruences).** Soit  $n \in \mathbb{N}^*$ . On dit que  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}$  sont congrus modulo  $n$  si  $n|a - b$ , c'est-à-dire si  $\exists k \in \mathbb{Z}, a = b + kn$ . On écrit  $a \equiv b [n]$ .

C'est aussi équivalent à dire que les divisions euclidiennes de  $a$  par  $n$  et de  $b$  par  $n$  donnent le même reste.

**Proposition 4.20 (Congruences et relation d'équivalence).** Soit  $n \in \mathbb{N}^*$ . La relation de congruence modulo  $n$  est une relation d'équivalence sur  $\mathbb{Z}$ , et on a, pour tout  $x \in \mathbb{Z}$ ,

$$\bar{x} = \{x + nk : k \in \mathbb{Z}\}.$$

Cette relation possède exactement  $n$  classes d'équivalence différentes dont l'ensemble noté  $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$  forme une partition de  $\mathbb{Z}$ .

**Proposition 4.21 (Opérations sur les congruences).** Soit  $n \in \mathbb{N}^*$  et  $(a, b, c, d) \in \mathbb{Z}^4$ .

1. Si  $a \equiv b [n]$  et  $c \equiv d [n]$  alors  $a + c \equiv b + d [n]$ .
2. Si  $a \equiv b [n]$  et  $c \equiv d [n]$  alors  $ac \equiv bd [n]$ .
3. Si  $a \equiv b [n]$ , alors  $\forall k \in \mathbb{N}^*, a^k \equiv b^k [n]$ .

**Théorème 4.22 (Petit théorème de Fermat).** Soit  $p$  un nombre premier et  $a \in \mathbb{N}$  tel que  $p \nmid a$ , alors  $a^{p-1} \equiv 1 [p]$ .

**Théorème 4.23 (Théorème des restes chinois).** Soient  $a, b$  deux entiers naturels non-nuls premiers entre eux et soient  $y, z \in \mathbb{Z}$ . Alors le système d'inconnue  $x \in \mathbb{Z}$

$$\begin{cases} x \equiv y [a] \\ x \equiv z [b] \end{cases}$$

admet une unique solution  $x_0$  dans  $\{0, 1, \dots, ab - 1\}$  et l'ensemble des solutions dans  $\mathbb{Z}$  de ce système est

$$S = \{x_0 + kab : k \in \mathbb{Z}\}.$$

## 4.5 Bases de numération

**Théorème 4.24 (Base de numération).** Soit  $b \geq 2$ . Tout entier  $x \in \mathbb{N}$  peut s'écrire d'une manière unique sous la forme

$$x = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0,$$

où  $n \in \mathbb{N}$  et  $\forall i \in \{0, \dots, n\}, a_i \in \{0, \dots, b-1\}$ . On dit alors que  $x = \overline{a_n a_{n-1} \dots a_0}^b$  (aussi noté  $x = (a_n a_{n-1} \dots a_0)_b$ ) est l'écriture de  $x$  en base  $b$ .

## 5 Nombres complexes

### 5.1 Définitions et premières propriétés

**Définition 5.1 (Nombres complexes).** On définit l'ensemble des nombres complexes par  $\mathbb{C} := \{a + ib : (a, b) \in \mathbb{R}^2\}$  avec  $i^2 = -1$ . Si  $z = a + ib \in \mathbb{C}$  avec  $a \in \mathbb{R}$  et  $b \in \mathbb{R}$ , alors

- $a$  est appelée la partie réelle de  $z$ , notée  $\operatorname{Re}(z) = a \in \mathbb{R}$ ,
- $b$  est appelée la partie imaginaire de  $z$ , notée  $\operatorname{Im}(z) = b \in \mathbb{R}$ .

Si  $a = 0$  et  $b \in \mathbb{R}^*$ , on dit que  $z = ib$  est imaginaire pur et on note  $i\mathbb{R}$  l'ensemble de ces nombres.

**Définition 5.2 (Opérations).** On a les opérations suivantes, pour  $z = a + ib$  et  $z' = a' + ib'$ , avec  $(a, b, a', b') \in \mathbb{R}^4$  :

- $z + z' = a + a' + i(b + b')$  ;
- $zz' = aa' - bb' + i(ab' + a'b)$  ;
- si  $z \neq 0$ , alors  $\frac{1}{z} = \frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}$

**Définition 5.3 (Conjugué).** Le conjugué d'un nombre complexe  $z = a + ib$ ,  $(a, b) \in \mathbb{R}^2$ , est  $\bar{z} = a - ib$ .

**Proposition 5.4 (Propriétés de la conjugaison).** On a :

1.  $\forall z, z' \in \mathbb{C}, \overline{z + z'} = \bar{z} + \bar{z}', \overline{zz'} = \bar{z}\bar{z}'$ .
2.  $\forall z \in \mathbb{C}, \operatorname{Re}(z) = \frac{z + \bar{z}}{2}$  et  $\operatorname{Im}(z) = \frac{z - \bar{z}}{2i}$ .
3.  $\forall z \in \mathbb{C}, z = \bar{z} \iff z \in \mathbb{R}$ .
4.  $\forall z \in \mathbb{C}, z = -\bar{z} \iff z \in i\mathbb{R}$ .
5.  $\forall z, z' \in \mathbb{C}^*, \overline{\left(\frac{z'}{z}\right)} = \frac{\bar{z}'}{\bar{z}}$ .

### 5.2 Interprétation géométrique, module, argument et forme trigonométrique

**Définition 5.5 (Repère d'Argand, affixe, coordonnées polaires et cartésiennes, module et argument).** On munit  $\mathbb{R}^2$  du repère orthonormé direct  $(O; \vec{u}, \vec{v})$ . Alors tout nombre complexe  $z = a + ib$ ,  $(a, b) \in \mathbb{R}^2$ , peut être représenté par le point  $M(a, b)$  où les réels  $a$  et  $b$  sont appelés coordonnées cartésiennes de  $M$ . Quand on veut rester dans le vocabulaire des nombres complexes, on dit que  $M$  est le point d'affixe  $z$  et on le note  $M(z)$ . Cela définit le plan complexe, aussi appelé plan d'Argand (ou Argand-Cauchy/Gauss). Les axes  $(O; \vec{u})$  et  $(O; \vec{v})$  sont appelés respectivement axes des réels et des imaginaires.

Le point  $M$  peut être également repéré par la donnée de la distance  $r = OM$  et une mesure  $\theta \in [0, 2\pi[$  de l'angle orienté dans le sens direct  $\left(\vec{u}, \overrightarrow{OM}\right)$ . Ce sont les coordonnées polaires de  $M$ , notées  $M(r, \theta)$ . Dans le langage des nombres complexes, on définit :

- le module de  $z = a + ib \in \mathbb{C}$  le nombre  $|z| = r = OM = \sqrt{a^2 + b^2}$ . Si  $z = a \in \mathbb{R}$ , alors  $|z| = |a|$  correspond à la valeur absolue de  $a$ .
- un argument  $\theta$  de  $z = a + ib \in \mathbb{C}^*$ , noté  $\arg(z)$ , en remarquant que pour tout  $k \in \mathbb{Z}$ ,  $\theta + 2k\pi$  est aussi un argument de  $z$ .

**Proposition 5.6 (Symétries).** Pour tout  $z \in \mathbb{C}$  :

- $M(z)$  et  $M'(\bar{z})$  sont symétriques par rapport à l'axe des réels.
- $M(z)$  et  $M''(-z)$  sont symétriques par rapport à l'origine  $O$  du repère.

**Proposition 5.7 (Propriétés du module).** On a les propriétés suivantes :

1.  $\forall z \in \mathbb{C}, |z| \in \mathbb{R}_+$  ;
2.  $\forall z \in \mathbb{C}, |z| = 0 \iff z = 0$  ;
3.  $\forall z, z' \in \mathbb{C}, |zz'| = |z||z'|$  ;
4.  $\forall z \in \mathbb{C}^*$  et  $z' \in \mathbb{C}, \left|\frac{z'}{z}\right| = \frac{|z'|}{|z|}$  ;
5.  $\forall z \in \mathbb{C}, |\bar{z}| = |z|$  ;
6.  $\forall z, z' \in \mathbb{C}, |z + z'| \leq |z| + |z'|$ , avec égalité si et seulement si  $\exists \lambda \in \mathbb{R}_+, z' = \lambda z$ .

**Proposition 5.8 (Lien entre module et arguments).** Soit  $z = a + ib \in \mathbb{C}$ ,  $(a, b) \in \mathbb{R}^2$ ,  $r = |z|$  son module et  $\theta = \arg(z)$  un argument de  $z$ , alors

$$a = r \cos \theta, \quad b = r \sin \theta.$$

**Définition 5.9 (Formes trigonométrique et exponentielles).** Pour tout  $z = a + ib \in \mathbb{C}$ ,  $(a, b) \in \mathbb{R}^2$ , l'écriture  $z = r \cos \theta + i r \sin \theta$ , avec  $r = |z|$  et  $\theta = \arg(z)$  un argument de  $z$ , s'appelle la forme trigonométrique de  $z$ . On note  $e^{i\theta} := \cos \theta + i \sin \theta$  l'exponentielle complexe de  $\theta$  et l'écriture  $z = r e^{i\theta}$  est appelée forme exponentielle de  $z$ .

**Proposition 5.10 (Propriétés de l'exponentielle complexe et de l'argument).** On a :

1.  $\forall \theta \in \mathbb{R}, |e^{i\theta}| = 1$  ;
2.  $\forall \theta, \theta' \in \mathbb{R}, e^{i\theta} = e^{i\theta'} \iff \exists k \in \mathbb{Z}, \theta = \theta' + 2k\pi$  ;
3.  $\forall \theta \in \mathbb{R}, e^{i(\theta+2\pi)} = e^{i\theta}, e^{i(\theta+\pi)} = -e^{i\theta}, e^{-i\theta} = \overline{e^{i\theta}} = \frac{1}{e^{i\theta}}$  ;
4.  $\forall \theta, \theta' \in \mathbb{R}, e^{i(\theta+\theta')} = e^{i\theta} e^{i\theta'}, e^{i(\theta-\theta')} = \frac{e^{i\theta}}{e^{i\theta'}}$  ;
5.  $\forall z, z' \in \mathbb{C}, \arg(zz') = \arg(z) + \arg(z')$ , et si  $z' \neq 0$ ,  $\arg\left(\frac{z}{z'}\right) = \arg(z) - \arg(z')$  ;
6. (**Formules d'Euler**)  $\forall \theta \in \mathbb{R}, \cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$  et  $\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$  ;
7. (**Formule de Moivre**)  $\forall n \in \mathbb{Z}, \forall \theta \in \mathbb{R}, (\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta)$ , c'est-à-dire  $(e^{i\theta})^n = e^{in\theta}$ .

### 5.3 Applications en trigonométrie

On peut appliquer les formules d'Euler et Moivre aux deux procédés suivants :

1. **La linéarisation** : on transforme des produits du type  $f(\cos x, \sin x)$  en sommes de  $\cos kx$  et  $\sin \ell x$ . Par exemple,  $\forall x \in \mathbb{R}$ ,

$$\sin x \cos^2 x = \left( \frac{e^{ix} - e^{-ix}}{2i} \right) \left( \frac{e^{ix} + e^{-ix}}{2} \right)^2 = \frac{e^{3ix} - e^{-3ix} + e^{ix} - e^{-ix}}{8i} = \frac{2i \sin(3x) + 2i \sin x}{8i} = \frac{\sin(3x) + \sin(x)}{4}.$$

On utilise donc la formule d'Euler (dans les deux sens) et celle du binôme de Newton.

2. **La polynomialisation** : on transforme des expressions du type  $g(\cos k_1 x, \dots, \cos k_n x, \sin \ell_1 x, \dots, \sin \ell_m x)$  en polynômes à base de  $\cos x$  et  $\sin x$ . Par exemple,  $\forall x \in \mathbb{R}$ ,

$$\begin{aligned} \cos(4x) &= \operatorname{Re} \left( e^{i4x} \right) = \operatorname{Re} \left( (\cos x + i \sin x)^4 \right) = \operatorname{Re} \left( 8 \cos^4 x - 8 \cos^2 x + 8i \sin x \cos^3 x - 4i \sin x \cos x + 1 \right) \\ &= 8 \cos^4 x - 8 \cos^2 x + 1. \end{aligned}$$

On utilise donc la formule de Moivre et celle du binôme de Newton.

## 5.4 Racines n-ièmes, racines carrées et équation de degré 2

**Proposition 5.11 (Racines n-ièmes d'un complexe).** Soit  $n \geq 2$  un entier et  $w \in \mathbb{C}$  un nombre complexe. Alors  $w$  admet exactement  $n$  racines n-ièmes, solutions  $\{z_0, \dots, z_{n-1}\}$  de l'équation  $z^n = w$ , et données par la formule

$$\forall k \in \{0, \dots, n-1\}, \quad z_k = |w|^{\frac{1}{n}} e^{i \left( \frac{\arg(w) + 2k\pi}{n} \right)}$$

On parle de racine n-ième de l'unité pour les  $n$  solutions de l'équation  $z^n = 1$  (où  $|w| = 1$  et  $\arg(w) = 0$ ).

**Proposition 5.12 (Equation du 2nd degré à coefficients complexes).** Soient  $a, b$  et  $c$  trois nombres complexes tels que  $a \neq 0$  et  $\Delta = b^2 - 4ac$ . On note  $\delta$  et  $-\delta$  les deux racines carrées de  $\Delta$ . Alors l'équation  $az^2 + bz + c = 0$  admet dans  $\mathbb{C}$  :

- une racine double  $z_0 = -\frac{b}{2a}$  si  $\Delta = 0$ , et on peut écrire  $az^2 + bz + c = a(z - z_0)^2$ ;
- deux racines distinctes  $z_1 = \frac{-b + \delta}{2a}$  et  $z_2 = \frac{-b - \delta}{2a}$  si  $\Delta \neq 0$ , et on peut écrire  $az^2 + bz + c = a(z - z_1)(z - z_2)$ .

De plus, si  $a, b$  et  $c$  sont réelles, l'équation  $az^2 + bz + c = 0$  admet :

- dans  $\mathbb{C}$ , deux racines (une double ou deux distinctes), données par les formules précédentes, en remarquant que si  $\Delta < 0$ , alors  $\delta = i\sqrt{|\Delta|}$ ;
- dans  $\mathbb{R}$ , une racine double  $z_0 = -\frac{b}{2a}$  si  $\Delta = 0$ , aucune racine si  $\Delta < 0$  et deux racines distinctes  $z_1, z_2$  données par les formules précédentes avec  $\delta = \sqrt{\Delta}$  si  $\Delta > 0$ .

**Théorème 5.13 (Théorème de d'Alembert-Gauss).** Soit  $n \geq 1$  un entier,  $\{a_0, \dots, a_n\}$  des nombres complexes avec  $a_n \neq 0$ . Toute équation polynomiale d'inconnue  $z$  de la forme

$$a_n z^n + \dots + a_2 z^2 + a_1 z + a_0 = 0$$

admet exactement  $n$  solutions dans  $\mathbb{C}$  comptées avec leur multiplicité (simple, double, etc., cf. chapitre sur les polynômes). Il existe ainsi  $n$  nombres complexes  $z_1, \dots, z_n$  (dont certains sont éventuellement confondus) tels que

$$a_n z^n + \dots + a_1 z + a_0 = a_n \prod_{k=1}^n (z - z_k).$$

## 5.5 Ensembles de points et transformations du plan

**Définition 5.14 (Affixe et longueur d'un vecteur).** Soient  $z_A, z_B \in \mathbb{C}$ ,  $A(z_A)$  et  $B(z_B)$ , alors l'affixe du vecteur  $\overrightarrow{AB}$  est  $z_B - z_A$ , et on note  $\overrightarrow{AB}(z_B - z_A)$ . De plus, la longueur du vecteur  $\overrightarrow{AB}$  est  $AB = |z_B - z_A|$  et le milieu du segment  $[AB]$  a pour affixe  $\frac{z_A + z_B}{2}$ .

**Proposition 5.15 (Linéarité et droite).** Soient  $z_u, z_v \in \mathbb{C}$ ,  $\vec{u}(z_u)$  et  $\vec{v}(z_v)$  deux vecteurs, alors  $\overrightarrow{u+v}(z_u + z_v)$  et, pour tout  $\lambda \in \mathbb{R}$ ,  $\lambda \vec{u}(\lambda z_u)$ .

Soit  $A(z_A)$  avec  $z_A \in \mathbb{C}$ . La droite passant par  $A$  et de vecteur directeur  $u$  est donnée par les affixes  $\{z_A + \lambda z_u : \lambda \in \mathbb{R}\}$ . En particulier, si  $B(z_B)$  avec  $z_B \in \mathbb{C}$ , l'ensemble des affixes des points de la droite  $(AB)$  est  $\{z_A + \lambda(z_B - z_A) : \lambda \in \mathbb{R}\}$ . Soit  $(x_0, y_0) \in \mathbb{R}^2$ . La droite horizontale (resp. verticale) d'ordonnée  $y_0$  (resp. d'abscisse  $x_0$ ) est donnée par l'ensemble des nombres complexes  $\{z \in \mathbb{C} : \text{Im}(z) = y_0\}$  (resp.  $\{z \in \mathbb{C} : \text{Re}(z) = x_0\}$ ). Ces droites partagent le plan en demi-plans.

**Proposition 5.16 (Translation).** Soit  $\vec{u}(z_u)$ , alors la translation  $t_{\vec{u}} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ,  $M \mapsto t_{\vec{u}}(M) = M'$  telle que  $\overrightarrow{MM'} = \vec{u}$  est donnée par l'application complexe  $T : \mathbb{C} \rightarrow \mathbb{C}$ ,  $z \mapsto T(z) = z + z_u$ .

**Proposition 5.17 (Homothétie et symétrie centrale).** Soit  $k \in \mathbb{R}^*$  et  $\Omega(z_\Omega)$ ,  $z_\Omega \in \mathbb{C}$ , alors l'homothétie de centre  $\Omega$  et de rapport  $k$   $h_{\Omega,k} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ,  $M \mapsto h_{\Omega,k}(M) = M'$  telle que  $\overrightarrow{\Omega M'} = k \overrightarrow{\Omega M}$  est donnée par l'application complexe  $H : \mathbb{C} \rightarrow \mathbb{C}$ ,  $z \mapsto H(z) = k(z - z_\Omega) + z_\Omega$ . Son unique point fixe, c'est-à-dire vérifiant  $H(z) = z$ , est  $z = z_\Omega$ . Si  $k = -1$ , il s'agit d'une symétrie de centre  $\Omega$ .

**Proposition 5.18 (Cercle et disque).** Soit  $R > 0$  et  $\Omega(z_\Omega)$ ,  $z_\Omega \in \mathbb{C}$ , alors :

1.  $\{z \in \mathbb{C} : |z - z_\Omega| \leq R\}$  est l'ensemble des affixes des points du disque fermé centré en  $\Omega$  et de rayon  $R$ .
2.  $\{z \in \mathbb{C} : |z - z_\Omega| = R\}$  est l'ensemble des affixes des points du cercle centré en  $\Omega$  et de rayon  $R$ .
3.  $\{z \in \mathbb{C} : |z - z_\Omega| < R\}$  est l'ensemble des affixes des points du disque ouvert centré en  $\Omega$  et de rayon  $R$ .
4.  $\{z \in \mathbb{C} : |z - z_\Omega| > R\}$  est l'ensemble des affixes des points de l'extérieur du disque fermé centré en  $\Omega$  et de rayon  $R$ .
5.  $\{z \in \mathbb{C} : |z - z_\Omega| \geq R\}$  est l'ensemble des affixes des points de l'extérieur du disque ouvert centré en  $\Omega$  et de rayon  $R$ .

**Proposition 5.19 (Rotation et multiplication par l'exponentielle complexe).** Soit  $\Omega(z_\Omega)$ ,  $z_\Omega \in \mathbb{C}$ , et  $\alpha \in \mathbb{R}$ . Alors la rotation de centre  $\Omega$  et d'angle  $\alpha$ , donnée par  $r_{\Omega,\alpha} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ,  $M \mapsto r_{\Omega,\alpha}(M) = M'$  telle que  $\overrightarrow{\Omega M} = \overrightarrow{\Omega M'}$  et  $(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}) = \alpha$  est donnée par l'application  $R : \mathbb{C} \rightarrow \mathbb{C}$ ,  $z \mapsto R(z) = e^{i\alpha}(z - z_\Omega) + z_\Omega$ . Son unique point fixe, c'est-à-dire vérifiant  $R(z) = z$ , est  $z_\Omega$ .  
En particulier, multiplier un nombre complexe  $z$ , affixe d'un point  $M$ , par  $e^{i\alpha}$ , c'est obtenir l'image de  $M$  par la rotation centrée en 0 et d'angle  $\alpha$ .

**Méthode :** Pour déterminer la nature et les éléments caractéristiques (vecteur, centre, angle, rapport) d'une transformation  $f : \mathbb{C} \rightarrow \mathbb{C}$  dont on sait qu'elle est une translation, une homothétie, une rotation ou une symétrie centrale :

1. on cherche le(s) point(s) fixe(s) en résolvant l'équation  $f(z) = z$ ,  $z \in \mathbb{C}$ ;
2. s'il n'y a pas de point fixe, alors  $f$  est une translation de vecteur  $\vec{u}(z_u)$  avec  $z_u = f(z) - z$  pour tout  $z \in \mathbb{C}$ ,

$$f(z) = z + z_u.$$

3. si on a trouvé un point fixe  $z_\Omega$ , alors on calcule, pour tout  $z \in \mathbb{C} \setminus \{z_\Omega\}$ ,  $\frac{f(z) - z_\Omega}{z - z_\Omega} = z_0$  qui donne :

- a) un nombre réel  $z_0 = k \neq -1$ , et  $f$  est donc l'homothétie de centre  $\Omega$  et de rapport  $k$ ,

$$f(z) = k(z - z_\Omega) + z_\Omega.$$

- b) le nombre réel  $z_0 = k = -1$ , et  $f$  est donc la symétrie centrale de centre  $\Omega$ ,

$$f(z) = -(z - z_\Omega) + z_\Omega = -z + 2z_\Omega.$$

- c) un nombre complexe de module 1 que l'on écrit  $z_0 = e^{i\alpha}$  avec  $\alpha \in \mathbb{R}$ , et  $f$  est la rotation de centre  $\Omega$  et d'angle  $\alpha$ ,

$$f(z) = e^{i\alpha}(z - z_\Omega) + z_\Omega.$$

## 6 Polynômes et fractions rationnelles

Dans toute la suite,  $n \in \mathbb{N}$  et l'ensemble  $\mathbb{K}$  désignera  $\mathbb{R}$  ou  $\mathbb{C}$ .

### 6.1 Définitions et opérations

**Définition 6.1 (Polynôme).** Un polynôme d'**indéterminée**  $X$  (qui est un symbole formel pouvant être remplacé par un élément qui n'est pas dans  $\mathbb{K}$ ), à coefficients dans  $\mathbb{K}$  est une expression pouvant s'écrire sous la forme

$$P(X) = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + \dots + a_n X^n$$

(avec la convention  $X^0 = 1$ ) où,  $\forall k \in \{0, \dots, n\}$ ,  $a_k \in \mathbb{K}$ .  $P$  est alors la somme des **monômes**  $\{a_k X^k\}_{k \in [0, n]}$ .

Les nombres  $\{a_0, \dots, a_n\}$  s'appellent les **coefficients** du polynôme  $P$  et on note  $\mathbb{K}[X]$  l'ensemble des polynômes d'indéterminée  $X$  à coefficients dans  $\mathbb{K}$ .

En particulier :

- si  $\forall k \in \{0, \dots, n\}$ ,  $a_k = 0$ ,  $P$  est le polynôme nul noté  $P(X) = 0$ ;
- si  $\forall k \in \{1, \dots, n\}$ ,  $a_k = 0$ ,  $P$  est un polynôme constant,  $P(X) = a_0$ ;
- $\forall (n, p) \in \mathbb{N}^2$ ,  $\forall \{a_k\}_{k \in [0, n]} \subset \mathbb{K}$ ,  $\forall \{b_k\}_{k \in [0, p]} \subset \mathbb{K}$ ,  $\sum_{k=0}^n a_k X^k = \sum_{k=0}^p b_k X^k \iff n = p \text{ et } \forall k \in [0, n], a_k = b_k$ .

**Définition 6.2 (Opérations).** Soient  $m, n \in \mathbb{N}$ ,  $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$  et  $Q(X) = \sum_{k=0}^m b_k X^k \in \mathbb{K}[X]$ , alors :

1. (Somme) Si  $n \geq m$ ,  $(P + Q)(X) = \sum_{k=0}^m (a_k + b_k) X^k + \sum_{k=m+1}^n a_k X^k$ .
2. (Produit)  $(PQ)(X) = \sum_{k=0}^{m+n} (a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0) X^k = \sum_{k=0}^{m+n} \left( \sum_{i=0}^k a_i b_{k-i} \right) X^k$ .
3. (Composition)  $(P \circ Q)(X) = \sum_{k=0}^n a_k (Q(X))^k$ .

**Définition 6.3 (Degré, coefficient dominant, polynôme unitaire).** Soit  $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$  tel que  $a_n \neq 0$ .

Alors :

- l'entier  $n$  est appelé **degré** du polynôme  $P$ , noté  $\deg(P) = n$ , et on note  $\mathbb{K}_n[X]$  l'ensemble des polynômes de  $\mathbb{K}[X]$  de degré inférieur ou égal à  $n$ ;
- le coefficient  $a_n$  est appelé **coefficient dominant** de  $P$ , et si  $a_n = 1$  on dit que  $P$  est un polynôme **unitaire**.

Par convention,  $\deg(0) = -\infty$  (pour que la règle du degré du produit ci-dessous reste vraie quand  $P = 0$ ).

**Proposition 6.4 (Degré de la somme et du produit).** Soient  $P, Q \in \mathbb{K}[X]$ , alors

1.  $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$  avec égalité en particulier si  $\deg(P) \neq \deg(Q)$ .
2.  $\deg(PQ) = \deg(P) + \deg(Q)$  et en particulier,  $\forall \alpha \in \mathbb{K}^*$ ,  $\deg(\alpha P) = \deg(P)$ .

**Proposition 6.5 (Produit nul).** Soient  $P, Q \in \mathbb{K}[X]$ , alors  $(PQ)(X) = 0 \iff P(X) = 0 \text{ ou } Q(X) = 0$ .

## 6.2 Arithmétique sur les polynômes

**Définition 6.6 (Multiple et diviseur).** Soient  $A, B \in \mathbb{K}[X]$  avec  $B \neq 0$ . On dit que  $B$  est un diviseur de  $A$ , ou que  $A$  est un multiple de  $B$ , lorsqu'il existe  $Q \in \mathbb{K}[X]$  tel que  $A(X) = B(X)Q(X)$ .

**Proposition 6.7 (Division euclidienne).** Soient  $A, B \in \mathbb{K}[X]$  avec  $B \neq 0$ . Alors il existe un unique couple de polynômes  $(Q, R) \in (\mathbb{K}[X])^2$  qui vérifient  $A(X) = B(X)Q(X) + R(X)$  avec  $\deg(R) < \deg(B)$ . On appelle  $Q$  le quotient et  $R$  le reste de la division euclidienne de  $A$  par  $B$ .

**Proposition 6.8 (PGCD et PPCM).** Soient  $A, B \in \mathbb{K}[X]$  avec  $A \neq 0$  et  $B \neq 0$ . Il existe un unique polynôme **unitaire** de plus grand degré qui divise à la fois  $A$  et  $B$ .

Cet unique polynôme unitaire est appelé le plus grand commun diviseur de  $A$  et  $B$ , noté  $\text{PGCD}(A, B)$ .

Il existe aussi un unique polynôme **unitaire**  $M$  de plus petit degré tel que  $A|M$  et  $B|M$ , appelé le plus petit commun multiple de  $A$  et  $B$ , noté  $\text{PPCM}(A, B)$ .

**Remarque 6.9 (Propriétés du PGCD).** Pour tout  $A, B \in \mathbb{K}[X]$  avec  $A \neq 0$  et  $B \neq 0$ , on a :

1. si  $A|B$ , alors  $\text{PGCD}(A, B) = \frac{1}{\lambda}A$  où  $\lambda \neq 0$  est le coefficient dominant de  $A$ ;
2. pour tout  $\lambda \in \mathbb{K}^*$ ,  $\text{PGCD}(\lambda A, B) = \text{PGCD}(A, B)$ ;
3. comme pour les entiers, si  $R$  est le reste dans la division euclidienne de  $A$  par  $B$ , alors on a, comme en Arithmétique (dans  $\mathbb{Z}$ ),  $\text{PGCD}(A, B) = \text{PGCD}(B, R)$ , ce qui justifie l'algorithme d'Euclide.

**Définition 6.10.** Soient  $A, B \in \mathbb{K}[X]$ . On dit que  $A$  et  $B$  sont premiers entre eux si  $\text{PGCD}(A, B) = 1$ .

**Théorème 6.11 (Théorème de Bézout).** Soient  $A, B \in \mathbb{K}[X]$  avec  $A \neq 0$  et  $B \neq 0$ . Alors il existe deux polynômes  $U, V \in \mathbb{K}[X]$  tels que  $AU + BV = \text{PGCD}(A, B)$ .

**Corollaire 6.12.** Soient  $A, B \in \mathbb{K}[X]$ .  $A$  et  $B$  sont premiers entre eux si et seulement s'il existe  $U, V \in \mathbb{K}[X]$  tels que  $AU + BV = 1$ .

**Corollaire 6.13.** Soient  $A, B, C \in \mathbb{K}[X]$  avec  $A \neq 0$  et  $B \neq 0$ . Si  $C|A$  et  $C|B$ , alors  $C|\text{PGCD}(A, B)$ . Si  $A|C$  et  $B|C$ , alors  $\text{PPCM}(A, B)|C$ .

**Corollaire 6.14 (Lemme de Gauss).** Soient  $A, B, C \in \mathbb{K}[X]$ . Si  $A|BC$  et  $\text{PGCD}(A, B) = 1$ , alors  $A|C$ .

## 6.3 Fonction polynomiale et dérivation des polynômes

**Définition 6.15 (Fonction polynomiale).** Soit  $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ . On appelle fonction polynomiale associée à  $P$  la fonction  $p : \mathbb{K} \rightarrow \mathbb{K}$  définie par :  $\forall x \in \mathbb{K}, p(x) = \sum_{k=0}^n a_k x^k$ .

Quand on calcule  $p(x)$  avec  $x \in \mathbb{K}$ , on dit que l'on évalue le polynôme  $P(X)$  en  $x$ , et on note cette valeur  $P(x)$ .

**Définition 6.16 (Polynôme dérivé).** Soit  $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ . On appelle polynôme dérivé de  $P$  le polynôme  $P'(X) = \sum_{k=1}^n k a_k X^{k-1}$ .

Soit  $j \in \mathbb{N}^*$ , on notera  $P^{(j)} = (P^{(j-1)})'$  la  $j$ -ième dérivée du polynôme  $P$ , avec pour convention  $P^{(0)} = P$ .

**Proposition 6.17 (Opérations sur les polynômes dérivés).** Soient  $(P, Q) \in \mathbb{K}[X]^2$  et  $\lambda \in \mathbb{K}$ , alors

- $(\lambda P + Q)' = \lambda P' + Q'$
- $(PQ)' = P'Q + PQ'$ .

**Proposition 6.18 (Degré du polynôme dérivé).** Soit  $P \in \mathbb{K}[X]$ . Si  $\deg(P) \geq 1$ , alors  $\deg(P') = \deg(P) - 1$ , sinon  $P'(X) = 0$  et donc  $\deg(P') = -\infty$ .

**Proposition 6.19 (Expression des polynômes dérivés successifs et formule de Taylor).**

Soit  $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$  de degré  $n$ . Alors :

1.  $\forall j \in \{0, \dots, n\}, \deg(P^{(j)}) = n - j$  et  $P^{(j)}(X) = \sum_{k=j}^n \frac{k!}{(k-j)!} a_k X^{k-j}$  et  $\forall j \geq n+1, P^{(j)}(X) = 0$ .

2. **Formule de Taylor :**  $\forall x_0 \in \mathbb{K}, P(X) = \sum_{k=0}^n \frac{P^{(k)}(x_0)}{k!} (X - x_0)^k$ .

## 6.4 Racines d'un polynôme

**Définition 6.20 (Racine d'un polynôme).** Soit  $P \in \mathbb{K}[X]$  et  $x_0 \in \mathbb{K}$ . On dit que  $x_0$  est une racine (ou un zéro) du polynôme  $P$  si  $P(x_0) = 0$ .

**Proposition 6.21 (Racines et divisibilité).** Soit  $P \in \mathbb{K}[X]$  et  $x_0 \in \mathbb{K}$ . Alors :

$$x_0 \text{ est racine de } P \iff X - x_0 \text{ divise } P.$$

Plus généralement, si  $m \in \mathbb{N}^*$  et  $x_1, \dots, x_m \in \mathbb{K}$  sont deux-à-deux distincts, on a

$$x_1, \dots, x_m \text{ racines de } P \iff (X - x_1)(X - x_2) \dots (X - x_m) \text{ divise } P.$$

**Définition 6.22 (Ordre de multiplicité).** Soit  $P \in \mathbb{K}[X]$ ,  $m \in \mathbb{N}^*$  et  $x_0 \in \mathbb{K}$ . On dit que  $x_0$  est une racine d'ordre de multiplicité (ou simplement "d'ordre", ou simplement "de multiplicité")  $m$  du polynôme  $P$  lorsque

- $(X - x_0)^m$  divise  $P$  ;
- $(X - x_0)^{m+1}$  ne divise pas  $P$ ,

c'est-à-dire s'il existe  $Q \in \mathbb{K}[X]$  tel que  $P(X) = (X - x_0)^m Q(X)$  et  $Q(x_0) \neq 0$ .

**Proposition 6.23 (Multiplicité et dérivées successives).** Soit  $P \in \mathbb{K}[X]$  non-nul,  $x_0 \in \mathbb{K}$  et  $m \in \mathbb{N}^*$ . Le nombre  $x_0$  est une racine de multiplicité  $m$  du polynôme  $P$  si et seulement si  $\forall k \in \{0, \dots, m-1\}, P^{(k)}(x_0) = 0$  et  $P^{(m)}(x_0) \neq 0$ .

**Définition 6.24 (Polynôme scindé).** On dit que  $P \in \mathbb{K}[X]$  est scindé sur  $\mathbb{K}$  s'il n'est pas constant et peut s'écrire comme produit de polynômes de degré 1, c'est-à-dire s'il existe  $(x_1, \dots, x_n) \in \mathbb{K}^n$  tels que

$$P(X) = a_n \prod_{k=1}^n (X - x_k),$$

ou  $a_n$  est le coefficient dominant de  $P$ .

**Proposition 6.25 (Somme et produit des racines d'un polynôme scindé unitaire).** Soit  $n \in \mathbb{N}^*$  et soit  $P \in \mathbb{K}[X]$  défini par  $P(X) = \prod_{k=1}^n (X - x_k)$  un polynôme de degré  $n$ , scindé et unitaire, alors :

- le coefficient de  $X^{n-1}$  de  $P(X)$  vaut  $-s$  où  $s = x_1 + \dots + x_n$  ;
- le coefficient constant de  $P(X)$  vaut  $(-1)^n p$  où  $p = x_1 \dots x_n$ .

Autrement dit,

$$P(X) = X^n - sX^{n-1} + \dots + (-1)^n p.$$

## 6.5 Polynômes irréductibles et factorisation

**Théorème 6.26 (Théorème de d'Alembert-Gauss).** *Tout polynôme de  $\mathbb{C}[X]$  de degré  $n \geq 1$  admet exactement  $n$  racines dans  $\mathbb{C}$ , comptées avec leurs multiplicités.*

*En notant  $a_n$  le coefficient dominant de  $P \in \mathbb{C}[X]$ , on peut écrire*

$$P(X) = a_n \prod_{k=1}^{\ell} (X - x_k)^{m_k}$$

*avec  $\ell \in \mathbb{N}^*$ ,  $(x_k)_{k \in [1, \ell]} \subset \mathbb{C}$  des racines distinctes de  $P$ ,  $m_k \in \mathbb{N}^*$  leurs ordres de multiplicité et  $\sum_{k=1}^{\ell} m_k = n$ .*

*Autrement dit, tout polynôme non-constant de  $\mathbb{C}[X]$  est scindé.*

**Proposition 6.27 (Racines conjuguées).** *Soit  $z \in \mathbb{C}$  et  $P \in \mathbb{R}[X]$ . Si  $z$  est racine de  $P$ , alors  $\bar{z}$  est également racine de  $P$ , avec le même ordre de multiplicité.*

**Définition 6.28 (Polynômes irréductibles).** *On dit que  $P \in \mathbb{K}[X]$  est irréductible dans  $\mathbb{K}[X]$  s'il est non-constant et que ses seuls diviseurs sont les constantes non-nulles et les polynômes  $\lambda P$  avec  $\lambda \in \mathbb{K}^*$ .*

**Proposition 6.29 (Décomposition en facteurs de degrés 1 et 2 dans  $\mathbb{R}$ ).** *Tout polynôme de  $\mathbb{R}[X]$  peut s'écrire comme produit d'un réel, de polynômes à coefficients réels de degré 1 et de polynômes à coefficients réels de degré 2 avec discriminants strictement négatifs.*

**Corollaire 6.30 (Polynômes irréductibles dans  $\mathbb{R}[X]$  et  $\mathbb{C}[X]$ ).** *On a :*

1. *Les polynômes irréductibles de  $\mathbb{C}[X]$  sont les polynômes de degré 1.*
2. *Les polynômes irréductibles de  $\mathbb{R}[X]$  sont les polynômes de degré 1 et les polynômes de degré 2 ayant un discriminant strictement négatif.*

## 6.6 Fractions rationnelles

**Définition 6.31 (Fraction rationnelle).** *On appelle fraction rationnelle sur  $\mathbb{K}$  tout quotient de type  $F = \frac{N}{D}$  avec  $(N, D) \in \mathbb{K}[X]$  et  $D \neq 0$ . On note  $\mathbb{K}(X)$  l'ensemble de ces fractions rationnelles. On dit que  $\frac{N}{D}$  est un représentant irréductible de  $F$  si  $\text{PGCD}(N, D) = 1$ .*

**Théorème 6.32 (Décomposition en éléments simples).** *Soit  $F \in \mathbb{K}(X)$ ,  $F \neq 0$ . Soit  $\frac{N}{D}$  un représentant irréductible de  $F$  et soit  $D = D_1^{p_1} \dots D_m^{p_m}$  la décomposition de  $D$  en facteurs irréductibles de  $\mathbb{K}[X]$ . Alors on peut écrire de manière unique*

$$F(X) = \frac{N(X)}{D(X)} = E(X) + \sum_{i=1}^m \left( \sum_{j=1}^{p_i} \frac{A_{i,j}(X)}{D_i^j(X)} \right)$$

*où  $E$  et les  $(A_{i,j})_{i,j}$  sont des polynômes de  $\mathbb{K}[X]$  avec  $\deg(A_{i,j}) < \deg(D_i)$ .  $E$  s'appelle la partie entière de  $F$  et les quotients  $\frac{A_{i,j}}{D_i^j}$  des éléments simples.*