**Notes de Cours**

# M101 : FONDEMENTS DE L'ALGÈBRE

Clément BOULONNE
Web : http://clementboulonne.new.fr
Mail : clement.boulonne@gmail.com

**Université des Sciences et Technologies de Lille**
**U.F.R de Mathématiques Pures et Appliquées**
Licence de Mathématiques — Semestre 1

# Table des matières

# Programme du cours

Math101 : **Fondements de l'algèbre** [S1, 5 ECTS]
Prérequis : Aucun

- (14 h) Vocabulaire de théorie des ensembles.
  Notions de logique : Connecteurs logiques, modes de raisonnement (et, ou, négation, implication, équivalence, raisonnement par l'absurde, raisonnement par récurrence). Quantificateurs. [1]
  Ensembles : Définition, sous-ensemble, intersection, réunion, complémentaire, produit cartésien, ensemble des parties.
  Applications, injection, surjection, bijection, exemples.
  Dénombrement, combinaisons, arrangements, égalité de Pascal, formule du binôme.
  Relations d'équivalence : Définition, classes d'équivalence, partition d'un ensemble, ensemble quotient, exemples simples.
- (16 h) Arithmétique dans $\mathbf{Z}$.
  Divisibilité : division euclidienne, $\mathrm{PGCD}$, algorithme d'Euclide, Bezout, Gauss, équations diophantiennes, $\mathrm{PPCM}$. Nombres premiers : théorème d'Euclide, crible d'Erastosthène, théorème fondamental d'arithmétique. Congruences : propriétés, équations de congruence, « petit » théorème de Fermat, l'ensemble $\mathbf{Z}/n\mathbf{Z}$. Les nombres rationnels et irrationnels.
- (12 h) Groupes - Anneaux - corps.
  Définition d'un groupe. Exemples simples : $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{R}^*$, $\mathbf{Z}/n\mathbf{Z}$, $(\mathbf{Z}/n\mathbf{Z})^\times$, définition de la fonction $\phi$ d'Euler, un exemple de groupe non commutatif $\mathscr{S}_3$. Sous-groupes. Intersection de sous-groupes. La réunion n'est pas un sous-groupe en général. Les sous-groupes de $\mathbf{Z}$. Morphisme de groupes, noyau, image, isomorphisme. Groupes cycliques : Si $G$ est un groupe cyclique d'ordre $n$, $G$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ ; $G$ admet $\phi(n)$ générateurs.
  Définitions d'un anneau, d'un sous-anneau, d'un corps, d'un sous-corps. Exemples simples : $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z}$.

1. Le chapitre « Arithmétique dans $\mathbf{Z}$ » présente un terrain idéal pour appliquer cette partie de programme.

– (8 h) Les nombres complexes.
Définition, parties réelles et imagiaires, module. . .C est un corps. L'exponentielle complexe, Formule de Moivre. Racines de l'unité, groupe des racines de l'unité. Interprétations géométriques. Racines d'une équation de second degré.

# Chapitre 1

# Logique et théorie des ensembles

## 1.1 Notions de logique

### 1.1.1 Opérateurs logiques

#### Proposition

**Définition 1.1** (Proposition)**.** *Une* proposition $P$ *est un énoncé mathématique qui peut être vrai (on notera* $V$*, le fait que la proposition soit vraie) ou faux (on notera* $F$*, le fait que la proposition soit fausse).*

**Exemples 1.2.**

1. La proposition $2 > 1$ est vraie.
2. La proposition $\pi \leq 3$ est fausse (pour rappel, $\pi$ vaut approximativement $3,14156$).
3. La proposition $x^2 > 0$ est vraie si $x \neq 0$ et fausse sinon.

#### Connecteurs logiques

**Définition 1.3** (Table de vérité)**.** *Une* table de vérité *prend, en entrée les résultats des divers propositions et en sortie, les résultats des opérations logiques faites entre ces propositions.*

**Définition 1.4** (et)**.** *Soient* $P$ *et* $Q$ *deux propositions, on dit que* $P$ et $Q$ *est une proposition vraie si et seulement si la proposition* $P$ *est vraie et, en même temps, la proposition* $Q$ *est vraie. On notera la proposition* $P$ *et* $Q$*,* $P \wedge Q$*.*

La table 1.1 représente la table de vérité du connecteur logique « et ».

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

TABLE 1.1 – Table de vérité du connecteur logiqe « et »

**Définition 1.5** (ou)**.** *Soient $P$ et $Q$ deux propositions, on dit que $P$* ou *$Q$ est une proposition vraie si et seulement si l'une des deux propositions est vraie. On notera la proposition $P$ ou $Q$, $P \vee Q$.*

La table 1.2 représente la table de vérité du connecteur logique « ou ».

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

TABLE 1.2 – Table de vérité du connecteur logiqe « ou »

**Exemple 1.6.** Soient les propositions suivantes :

$$4^2 > 12 \qquad (P)$$

$$\sqrt{2} > 2 \qquad (Q)$$

La propostion $P$ est vraie car $4^2 = 16$ mais, par contre, la proposition $Q$ est fausse car $\sqrt{2}$ vaut approximativement $1,41$. D'où $P \wedge Q$ est faux et $P \vee Q$ est vrai.

### Négation

**Définition 1.7** (Negation)**.** *On appelle* négation *d'une proposition $P$, le contraire de $P$. On note* $\text{non}\, P$ *ou $\neg P$, la négation de $P$.*

**Exemple 1.8.** Soit la proposition suivante :

$$\sin\left(\frac{\pi}{3}\right) > \frac{1}{2}. \qquad (P)$$

Cette proposition est vraie, sa négation est :

$$\sin\left(\frac{\pi}{3}\right) \leq \frac{1}{2} \qquad (\neg P)$$

qui est, évidemment, fausse.

### Relations entre deux propositions

**Définition 1.9** (Implication, [4]). *Soient $P$ et $Q$ deux propositions, on dit que $P$* implique *$Q$ ($P \Rightarrow Q$) si la proposition « $\neg P \vee Q$ » est vraie.*

**Remarque 1.10. Attention !** Si $P$ est faux alors l'implication est vraie.

La table 1.3 nous donne la table de vérité de l'implication entre deux propositions.

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

TABLE 1.3 – Table de vérité de la relation « si . . .alors » [1]

**Définition 1.11** (Hypothèse et conclusion). *Dans la définition 1.9, on dit que $P$ est l'*hypothèse *dans l'implication et $Q$ est la* conclusion.

**Exemples 1.12.**
1. « Si $x \neq 0$ alors $x^2 > 0$ » est un énoncé vrai,
2. « Si $x > 0$ alors $x^3 > 0$ » est un énoncé vrai,
3. « $1 < 0 \Rightarrow 2 < 1$ est aussi un énoncé vrai car l'hypothèse $1 < 0$ est fausse.

**Définition 1.13** (Équivalence,[5]). *Soient $P$ et $Q$ deux propositions. On dit que $P$ et $Q$ sont* logiquement équivalent *si $P$ et $Q$ ont simultanément même valeur de vérité (c'est-à-dire « vrai » ou « faux » en même temps).*

La table 1.4 nous donne la table de vérité de la relation « si et seulement si ».

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

TABLE 1.4 – Table de vérité de la relation « si et seulement si »

**Exemple 1.14.** La proposition « $x > 0 \Leftrightarrow x^3 > 0$ est vraie.

**Règles logiques**

**Proposition 1.15** (Loi de non-contradiction)**.** *Soit $P$ une proposition. Alors $P \wedge \neg P$ est fausse.*

**Proposition 1.16** (Loi du tiers exclu)**.** *Soit $P$ une proposition. Alors $P \vee \neg P$ est vraie.*

**Proposition 1.17.** *Soient $P$ et $Q$ deux propositions. On a alors :*

$$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

**Exemple 1.18.** Pour montrer la proposition « $x > 0$ si et seulement si $x^3 > 0$ », il faut montrer que « $x > 0 \Rightarrow x^3 > 0$ » et « $x^3 > 0 \Rightarrow x > 0$ ».

**Proposition 1.19** (Transivité)**.** *Soient $P$ et $Q$ deux propositions. Si la proposition « $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ est vraie alors la proposition « $P \Rightarrow R$ » est vraie.*

**Proposition 1.20** (Règle d'inférence)**.** *Soient $P$ et $Q$ deux propositions. Si la proposition « $P \wedge (P \Rightarrow Q) \Rightarrow Q$ est vraie alors $Q$ est vraie.*

**Proposition 1.21** (Double négation)**.** *Soit $P$ une proposition. On a le resultat suivant :*

$$\neg(\neg P) \Leftrightarrow P.$$

On peut vérifier les règles logiques définies en propositions 1.15, 1.16, 1.17, 1.19, 1.20 et 1.21 à l'aide d'une table de vérité.

**Remarque 1.22.** Si on veut démontrer que $P \Rightarrow Q$ n'est pas vrai (ou $P \not\Rightarrow Q$), il suffit de donner un *contre-exemple*, c'est-à-dire un exemple où $P$ est vrai mais $Q$ est faux.

## 1.1.2 Quantificateurs

**Notion d'ensembles**

**Définition 1.23** (Ensemble)**.** *Un* ensemble *est une collection d'objets. Ces objets s'appellent les* éléments *de l'ensemble.*

**Définition 1.24** (Appartenance)**.** *Si $E$ est un ensemble et $x$ un élément de $E$ alors on dit que $x$* appatient *à $E$ et on note $x \in E$.*

**Remarque 1.25.** On note $x \notin E$ si $x$ n'apppartient pas à $E$. C'est la négation de la proposition de l'appartenance à un ensemble ($\neg(x \in E)$).

**Exemple 1.26.** On définit les ensembles de nombres suivants (leur construction sera justifiée dans [3]) :

- $\mathbf{N}$ est l'ensemble des nombres entiers naturels :

$$\mathbf{N} = \{0, 1, 2, 3, \ldots\}.$$

- $\mathbf{Z}$ est l'ensemble des nombres entiers positifs et négatifs :

$$\mathbf{Z} = \{-2, -1, 0, 1, 2, 3, \ldots\}.$$

- $\mathbf{Q}$ est l'ensemble des nombres rationnels :

$$\mathbf{Q} = \left\{0, -\frac{2}{3}, 1, \frac{9}{19}, \ldots\right\}.$$

- $\mathbf{R}$ est l'ensemble des nombres réels :

$$\mathbf{R} = \left\{0, \pi, -\sqrt{2}, 2, \ldots\right\}.$$

- $\mathbf{C}$ est l'ensemble des nombres complexes (voir le chapitre 4).

**Exemple 1.27** (Appartenance)**.** L'élément $17$ appartient à $\mathbf{N}$ ($17 \in \mathbf{N}$ car $17 \geq 0$) et donc appartient à $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$. Par contre, $-17$ n'appartient pas à $\mathbf{N}$ ($17 \notin \mathbf{N}$ car $-17 \ngeq 0$) mais il appartient à $\mathbf{Z}$ ($-17 \in \mathbf{Z}$). $\frac{3}{4}$ n'appartient pas à $\mathbf{Z}$ ($\frac{3}{4} \notin \mathbf{Z}$) mais il appartient à $\mathbf{Q}$ ($\frac{3}{4} \in \mathbf{Q}$).

### Quantificateur universel

**Définition 1.28** (Quantificateur universel)**.** *Soient $E$ un ensemble et $P$ une proposition. La proposition*

$$\forall x \in E, \quad P$$

*veut dire que* tout élément *de $E$ vérifie la proposition $P$.*

**Exemple 1.29.** La proposition « $\forall x \in \mathbf{N}$, $x \geq 0$ » est vraie (c'est même la définition de l'ensemble $\mathbf{N}$).

### Quantificateur existenciel

**Définition 1.30** (Quantificateur existenciel)**.** *Soient $E$ un ensemble et $P$ une proposition. La proposition*

$$\exists x \in E, \quad P$$

*veut dire qu'il* existe *qui vérifie $P$ (c'est-à-dire qu'il y a un élément $x$ de $E$ qui vérifie $P$).*

**Exemple 1.31.** La proposition

$$\exists x \in \mathbf{Z}, \quad x < 0$$

est vraie, sa traduction en langue française est : « il existe un $x$ qui appartient à l'ensemble $\mathbf{Z}$ tel que $x$ est strictement négatif. »

**Remarque 1.32.** Il faut faire attention dans quel on écrit les quantificateurs. La proposition

$$\forall x \in \mathbf{Z},\ \exists y \in \mathbf{Z}, \quad y > x$$

est vraie (on peut prendre $y = x + 1$) mais, par contre, la proposition

$$\exists x \in \mathbf{Z},\ \forall y \in \mathbf{Z}, \quad y > x$$

est fausse (on peut prendre $y = x$).

### Négation des quantificateurs

**Proposition 1.33** (Négation des quantificateurs)**.** *1. La négation du quantificateur universel est un quantificateur existenciel (c'est-à-dire que « $\neg\forall$ » correspond à un « $\exists$ »).*

*2. La négation du quantificateur existenciel est un quantificateur universel (c'est-à-dire que « $\neg\exists$ » correspond à un « $\forall$ »).*

**Exemples 1.34.** 1. $\neg(\forall x \in E,\ P) \Leftrightarrow \exists x \in E,\ \neg P$ ;

2. $\neg(\exists x \in E,\ P) \Leftrightarrow \forall x \in E,\ \neg P$.

## 1.1.3 Méthodes de démonstration

### Démonstration par contraposition

**Proposition 1.35** (Démonstration par contraposition)**.** *Soient $P$ et $Q$ deux propositions. Alors les deux assertions sont équivalentes :*

*(i)* $P \Rightarrow Q$ *;*

*(ii)* $\neg Q \Rightarrow \neg P$.

*On appelle* contraposée *de « $P \Rightarrow Q$ », la proposition* $(\neg Q \Rightarrow \neg P)$.

**Exemple 1.36.** Soient $n \in \mathbf{Z}$ et les propositions suivantes :

$$n^2 \text{ est impair}, \qquad (P)$$

$$n \text{ est impair}. \qquad (Q)$$

On veut démontrer que $P \Rightarrow Q$ par contraposition (c'est-à-dire on montre que si $n$ est pair [1] alors $n^2$ est pair). Comme $n$ est pair, il existe $k \in \mathbf{Z}$ tel que $n = 2k$. D'où $n^2 = 4k^2$ est pair. Par contraposée, l'énoncé de départ est vrai. On a même l'équivalence des propositions $P$ et $Q$.

### Raisonnement par l'absurde

**Proposition 1.37** (Raisonnement par l'absurde, [1])**.** *On veut démontrer la propriété $P$. On suppose donc $\neg P$ qu'on appelle* hypothèse de raisonnement par l'absurde *et on déduit une contradiction, c'est-à-dire une proposition $Q$ telle que $Q$ et $\neg Q$ soient vraie. On conclut alors que $P$ est vraie.*

**Exemple 1.38.** Soit la proposition suivante :

$$n^2 \text{ impair} \Rightarrow n \text{ impair}. \tag{1.1}$$

On montre que $P$ est vraie par l'absurde. Supposons que $P$ soit faux, c'est-à-dire que $n$ pair et $n^2$ impair. Mais, d'après l'exemple 1.36, on obtient une contradiction. Donc $\neg P$ est faux et ainsi $P$ est vrai.

**Remarque 1.39.** Dans l'exemple 1.38, la proposition $Q$ auxiliaire telle que $\neg P \Leftrightarrow Q \wedge \neg Q$ est « $n^2$ est impair ».

### Raisonnement par réccurence

**Proposition 1.40** (Raisonnement par réccurence)**.** *Soit $P_n$ une proposition qui dépend d'un même énoncé qui dépend d'un certain paramètre $n$ (où $n \in \mathbf{N}$). Soit $N \in \mathbf{N}$, si on veut démontrer que $P_n$ est vraie, pour tout $n \geq N$, il suffit de montrer*

1. *$P_N$ est vraie, c'est ce qu'on appelle l'*initialisation*,*
2. *$\forall n \geq N$, on a : $P_n \Rightarrow P_{n+1}$, c'est ce qu'on appelle la* réccurence*.*

**Exemple 1.41.** Soit la proposition suivante :

$$2^n > n. \tag{$P_n$}$$

On veut démontrer que $P_n$ est vraie, pour tout $n \geq 1$, $n \in \mathbf{N}$.

**Initialisation** La proposition $P_1$ est « $2^1 > 1 \Leftrightarrow 2 > 1$ » qui est logiquement vraie.

1. Pour une définition de « pair » et « impair », voir la définition 2.3.

**Récurrence** On suppose que $P_n$ est vraie (c'est-à-dire que « $2^n > n$ » est vraie). On veut montrer que $P_n \Rightarrow P_{n+1}$. On mutliplie par $2$, les deux membres de l'inégalité de $P_n$. Cela donne

$$2^n > n \Rightarrow 2^{n+1} > 2n. \tag{1.2}$$

Mais :

$$2n \geq n+1 \Leftrightarrow n \geq 1. \tag{1.3}$$

D'où, en combinant (1.2) et (1.3), on obtient $2^{n+1} \geq n+1$ et ainsi $P_n \Rightarrow P_{n+1}$.

Par le principe de démonstration par récurrence, on a donc $P_n$ est vraie pour tout $n \geq 1$, $n \in \mathbf{N}$.

**Remarque 1.42.** Dans l'exemple 1.41, on aurait pu démontrer que la propriété $P_n$ est vraie pour tout $n \geq 0$ car $P_0$ est vraie : $2^0 > 0$.

## 1.2 Ensembles

La définition 1.23 nous a défini ce qu'est un ensemble. Passons aux définitions d'un ensemble vide et du cardinal d'un ensemble.

### 1.2.1 Premières définitions et notations

**Définition 1.43** (Ensemble vide)**.** *Un ensemble* vide *est un ensemble qui ne contient aucun élément. On notera l'ensemble vide* $\emptyset$.

**Définition 1.44** (Cardinal d'un ensemble)**.** *Un ensemble $E$ est fini s'il contient un nombre fini d'éléments. On appelle le nombre d'éléments d'un ensemble, le* cardinal *de $E$ (qu'on note* $\mathrm{card}(E)$*).*

Il convient que le cardinal de l'ensemble vide est égale à $0$, d'où $\mathrm{card}(\emptyset) = 0$.

**Exemple 1.45.** Soit

$$E = \{n \in \mathbf{Z},\ |n| \leq 2\} = -2, -1, 0, 1, 2.$$

Alors $\mathrm{card}(E) = 5$.

**Définition 1.46** (Inclusion)**.** *Soient $E$ et $F$ deux ensembles. On dit que $E$ est inclu dans $F$ ($E \subset F$) si tous les éléments de $E$ sont dans $F$ (c'est-à-dire : « $\forall x \in E,\ x \in F$ »).*

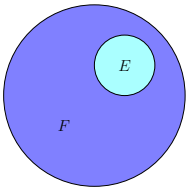


FIGURE 1.1 – $E$ est inclu dans $F$ ($E \subset F$)

**Remarque 1.47.** On dit aussi que $E$ est un sous-ensemble de $F$ (ou $E$ est une partie de $F$).

**Exemple 1.48** (Chaîne d'inclusion)**.** On a :

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

**Définition 1.49** (Ensemble des parties)**.** *Soit $E$ un ensemble. On note $\mathscr{P}(E)$, l'*ensemble des parties *de $E$.*

**Exemple 1.50.** Soit $E = \{1, 2, 3\}$. On a :

$$\mathscr{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, E\}$$

et $\mathrm{card}(\mathscr{P}(E)) = 8$.

**Remarque 1.51.** $E$ est un sous-ensemble de $E$.

### 1.2.2 Opérations sur les ensembles

**Définition 1.52** (Intersection et réunion)**.** *Soient $E$ et $F$ deux ensembles. L'*intersection *de $E$ et de $F$ (noté $E \cap F$) est l'ensemble des éléments qui appartient à $E$ et $F$, c'est-à-dire en opérations logiques :*

$$x \in E \cap F \Leftrightarrow (x \in E) \wedge (x \in F).$$

*La réunion de $E$ et $F$ (noté $E \cup F$) est l'ensemble des éléments qui appartiennent à $E$ ou à $F$, c'est-à-dire :*

$$x \in E \cup F \Leftrightarrow (x \in E) \vee (x \in F).$$

**Remarque 1.53.** On a les inclusions suivantes :

1. $E \cap F \subset E \subset E \cup F$,
2. $E \cap F \subset F \subset E \cup F$.

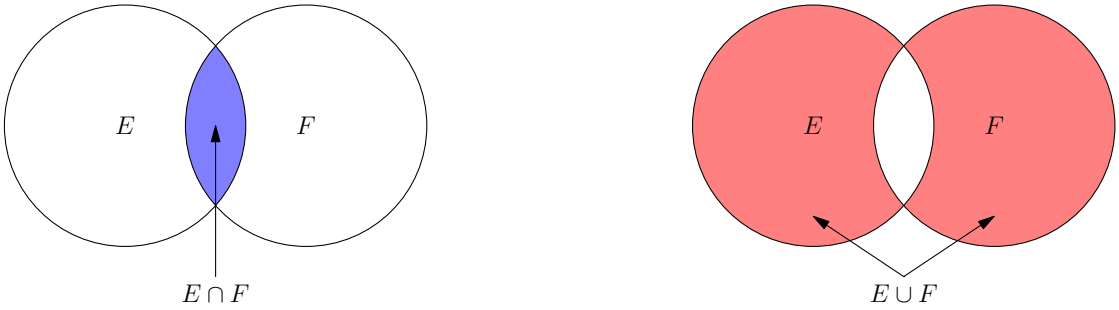


FIGURE 1.2 – Intersection et réunion de deux ensembles $E$ et $F$

**Théorème 1.54.** *Soient $E, F$ et $G$ trois ensembles. Alors, on a :*

*(i)* $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$,

*(ii)* $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$.

*Démonstration.* (i)

$$\begin{aligned} x \in E \cup (F \cap G) &\Leftrightarrow (x \in E) \vee (x \in F \cap G) \\ &\Leftrightarrow (x \in E) \vee ((x \in F) \wedge (x \in G)) \\ &\Leftrightarrow ((x \in E) \wedge (x \in F)) \vee ((x \in E) \wedge (x \in F)) \\ &\Leftrightarrow x \in (E \cup F) \cap (E \cup G). \end{aligned}$$

(ii)

$$\begin{aligned} x \in E \cap (F \cup G) &\Leftrightarrow (x \in E) \wedge (x \in F \cup G) \\ &\Leftrightarrow (x \in E) \wedge ((x \in F) \vee (x \in G)) \\ &\Leftrightarrow ((x \in E) \vee (x \in F)) \wedge ((x \in E) \vee (x \in F)) \\ &\Leftrightarrow x \in (E \cap F) \cup (E \cap G). \end{aligned}$$

□

**Définition 1.55** (Complémentaire)**.** *Soient $E$ un ensemble et $A$ un sous-ensemble de $E$. Le* complémentaire *de $A$ dans $E$ (noté $A^c$ ou $E \setminus A$ ou $\complement_A(E)$) est l'ensemble des éléments de $E$ qui n'appartient pas à $A$, c'est-à-dire :*

$$\complement_A(E) = \{x \in E,\ x \in A\}.$$

**Définition 1.56** (Différence)**.** *Soient $E$ un ensemble et $A$ et $B$ deux sous-ensembles de $E$. La* différence *des deux parties $A$ et $B$ (noté $A \setminus B$) est l'ensemble des éléments de $A$ qui n'appartient pas à $B$, c'est-à-dire :*

$$x \in A \setminus B \Leftrightarrow (x \in A) \wedge (x \notin B).$$

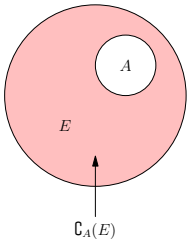


FIGURE 1.3 – Complémentaire de $A$ dans $E$

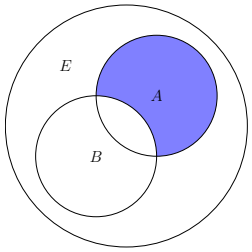


FIGURE 1.4 – Différence de $A$ et $B$ dans $E$

**Proposition 1.57.** *Soit $E$ un ensemble et $A$ et $B$ des sous-ensembles de $E$.*

*(i)* $A \cap A^c = \emptyset$,

*(ii)* $A \cup A^c = E$,

*(iii)* $\emptyset^c = E$,

*(iv)* $E^c = \emptyset$,

*(v)* $(A^c)^c = A$,

*(vi)* $A \subset B \Rightarrow B^c \subset A^c$,

*(vii)* $A \setminus B \Rightarrow A \cap B^c$,

*(viii)* $(A \cup B)^c = A^c \cap B^c$,

*(ix)* $(A \cap B)^c = A^c \cup B^c$.

*Démonstration.* Les cinq premières assertions sont évidentes.

(vi)

$$x \in A \subset B \Leftrightarrow (x \in A \Rightarrow x \in B) \Leftrightarrow (x \notin B \Rightarrow x \notin A)$$
$$\Leftrightarrow (x \in B^c \Rightarrow x \in A^c) \Leftrightarrow B^c \subset A^c.$$

(vii)

$$x \in A \setminus B \Leftrightarrow (x \in A) \wedge (x \notin B) \Leftrightarrow (x \in A) \wedge (x \in B^c) \Leftrightarrow x \in A \cap B^c.$$

(viii)

$$x \in (A \cup B)^{\mathsf{c}} \Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow (x \notin A) \vee (x \notin B)$$
$$\Leftrightarrow (x \in A^{\mathsf{c}}) \wedge (x \in B^{\mathsf{c}}) \Leftrightarrow x \in A^{\mathsf{c}} \cap B^{\mathsf{c}}.$$

(ix)

$$x \in (A \cap B)^{\mathsf{c}} \Leftrightarrow \neg(x \in A \cap B) \Leftrightarrow \neg((x \in A) \wedge (x \in B))$$
$$\Leftrightarrow (x \notin A) \vee (x \notin B) \Leftrightarrow (x \in A^{\mathsf{c}}) \vee (x \in B^{\mathsf{c}}) \Leftrightarrow x \in A^{\mathsf{c}} \cup B^{\mathsf{c}}.$$

□

**Exercice 1.58.**
1. Simplifier $[1\,,3] \cap [2\,,4]$ et $[1\,,3] \cup [2\,,4]$.
2. Pour tout $n \in \mathbf{N}$, on note $n\mathbf{Z}$ l'ensemble des entiers relatifs multiples de $n$ :
$$n\mathbf{Z} = \{np,\ p \in \mathbf{Z}\}\,.$$
Simplifier $2\mathbf{Z} \cap 3\mathbf{Z}$.

**Définition 1.59** (Produit cartésien)**.** *Le* produit cartésien de deux ensembles $E$ *et* $F$ *(noté* $E \times F$*) est l'ensemble des couples* $(x, y)$ *avec* $x \in E$ *et* $y \in F$.

$$E \times F = \{(x, y),\ x \in E \text{ et } y \in F\}\,.$$

**Exemple 1.60.** On note $\mathbf{R}^2$, l'ensemble des couples $(x, y)$ tels que $x \in \mathbf{R}$ et $y \in \mathbf{R}$, c'est-à-dire :

$$\mathbf{R}^2 = \{(x, y),\ x \in \mathbf{R} \text{ et } y \in \mathbf{R}\} = \mathbf{R} \times \mathbf{R}.$$

**Définition 1.61** (Produit cartésien de plusieurs ensembles)**.** *De la même manière que la définition 1.59, on définit le* produit cartésien des $n$ ensembles*,* $E_1, \ldots, E_n$ *:*

$$E_1 \times \cdots \times E_n = \{(x_1, \ldots, x_n),\ x_i \in E_i,\ i \in \{1, \ldots, n\}\}\,.$$

**Exemple 1.62.**

$$\mathbf{R}^n = \underbrace{\mathbf{R} \times \mathbf{R} \times \cdots \times \mathbf{R}}_{n \text{ fois}}$$

**Exemple 1.63.**

$$\mathbf{Z}^2 = \mathbf{Z} \times \mathbf{Z} = \{(x, y),\ x \in \mathbf{Z} \text{ et } y \in \mathbf{Z}\}\,,$$

et on a : $\mathbf{Z}^2 \subset \mathbf{R}^2$.

# 1.3 Applications

## 1.3.1 Définitions

**Définition 1.64** (Application)**.** *Soient $E$ et $F$ deux ensembles. Une* application *$f$ de $E$ dans $F$ est une loi qui associe tout élément $x$ de $E$ à un élément de $F$ qui est $f(x)$. On notera :*

$$\begin{array}{rccc} f & : & E & \to & F \\ & & x & \mapsto & f(x) \end{array}.$$

**Exemples 1.65.**

1. Soient $E = \{1, 2, 3\}$ et $F = \{4, 5, 6\}$, on définit la fonction $f : E \to F$ telle que
$$f(1) = 6,\ f(2) = 4 \text{ et } f(3) = 5.$$
2. Soient $E = \mathbf{Z}$ et $F = \mathbf{Z}$, on définit la fonction
$$\begin{array}{rccc} f & : & \mathbf{Z} & \to & \mathbf{Z} \\ & & x & \mapsto & f(x) = 2x + 1 \end{array}.$$

**Définition 1.66** (Image et antécédent)**.** *Soit $f : E \to F$. On appelle $E$* l'ensemble de départ *de la fonction $f$ et $F$* l'ensemble d'arrivée*. $f(x)$ est l'*image *de $x$ par la fonction $f$ et $x \in E$ est l'*antécédent *de $y$ si $f(x) = y$ (avec $y \in F$).*

**Définition 1.67** (Graphe de la fonction)**.** *Le* graphe *d'une application $f : E \to F$ est l'ensemble*

$$\mathscr{G}_f = \{(x, f(x)),\ x \in E,\ f(x) \in F\}.$$

*Le graphe de $f$ est un sous-ensemble du produit cartésien de $E \times F$.*

**Définition 1.68** (Égalité de fonctions)**.** *Soient $f : E \to F$ et $g : E' \to F'$ deux fonctions. On dit que $f = g$ si :*

1. *$E = E'$,*
2. *$F = F'$,*
3. *pour tout $x \in E$, $f(x) = g(x)$.*

**Définition 1.69** (Application identité)**.** *Si $E$ est un ensemble, on note $\mathrm{id}_E$, l'application identique daans $E$, l'application suivante :*

$$\begin{array}{rccc} \mathrm{id}_E & : & E & \to & E \\ & & x & \mapsto & x \end{array}.$$

### 1.3.2 Restriction et prolongement

**Définition 1.70** (Restriction)**.** *Soient $E$ et $F$ deux ensembles, $f : E \to F$ une application et $A \subset E$. On appelle la* restriction *de $f$ à $A$, l'application :*

$$\begin{array}{rccl} f|_A & : & A & \to & F \\ & & x & \mapsto & f|_A(x) = f(x),\ \forall x \in A \end{array}.$$

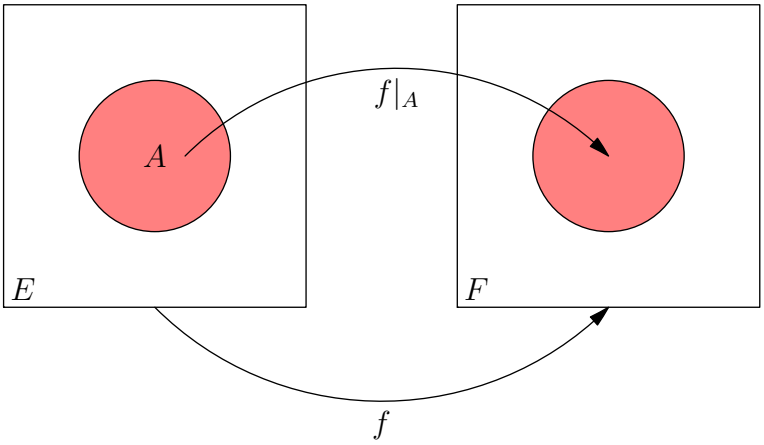


FIGURE 1.5 – Restriction d'une fonction $f$ à $A$

**Définition 1.71** (Prolongement)**.** *Soit $g : A \to F$ une application. On appelle* prolongement *de $g$ à $E$, toute application $f : E \to F$ telle que $f|_a = g$.*

**Remarque 1.72.** Le prolongement n'est pas unique.

**Exemple 1.73.** Soit la fonction

$$\begin{array}{rccl} g & : & \mathbf{N}^* & \to & \mathbf{Q} \\ & & x & \mapsto & g(x) = \frac{1}{x} \end{array}$$

avec $A = \mathbf{N}^*$, $E = \mathbf{N}$ et $F = \mathbf{Q}$. On pose :

$$\begin{array}{rccl} f_1 & : & \mathbf{N} & \to & \mathbf{Q} \\ & & x & \mapsto & f_1(x) = \begin{cases} \frac{1}{x} & \textbf{si } x \neq 0, \\ 0 & \textbf{si } x = 0. \end{cases} \end{array}$$

et

$$\begin{array}{rccl} f_2 & : & \mathbf{N} & \to & \mathbf{Q} \\ & & x & \mapsto & f_2(x) = \begin{cases} \frac{1}{x} & \textbf{si } x \neq 0, \\ 1 & \textbf{si } x = 0. \end{cases} \end{array}$$

Comme $f_1|_{\mathbf{N}^*} = g$ et $f_2|_{\mathbf{N}^*} = g$, $f_1$ et $f_2$ sont deux prolongements de $g$.

### 1.3.3 Composition

**Définition 1.74.** *Soient $E$, $F$ et $G$ trois ensembles, $f\colon E \to F$ et $g\colon F \to G$ deux applications. La* composée *de $f$ et $g$ est l'application :*

$$\begin{array}{rccl} g \circ f & : & E & \to & G \\ & & x & \mapsto & (g \circ f)(x) = g(f(x)) \end{array}.$$

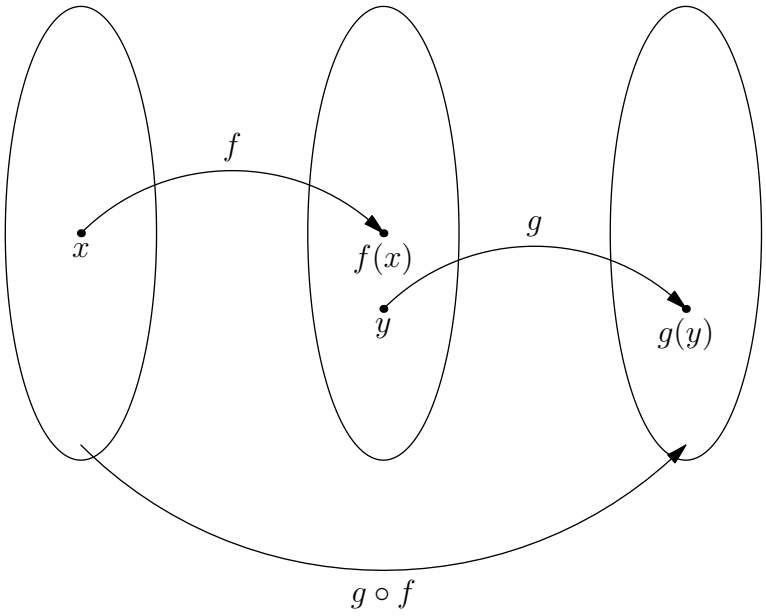


FIGURE 1.6 – Composition de deux fonctions $f$ et $g$

### 1.3.4 Image directe et réciproque

**Définition 1.75** (Image directe)**.** *Soient $E$ et $F$ deux ensembles et $f\colon E \to F$ une application. On appelle* image directe *de $A$ par $f$ (où $A \subset E$) l'ensemble :*

$$f(A) = \{f(x),\ x \in A\} \subset F.$$

**Définition 1.76** (Image réciproque)**.** *Soient $E$ et $F$ deux ensembles, $f\colon E \to F$ une application et $B$ un sous-ensemble de $F$. On appelle* image réciproque *de $B$ sur $F$, l'ensemble :*

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

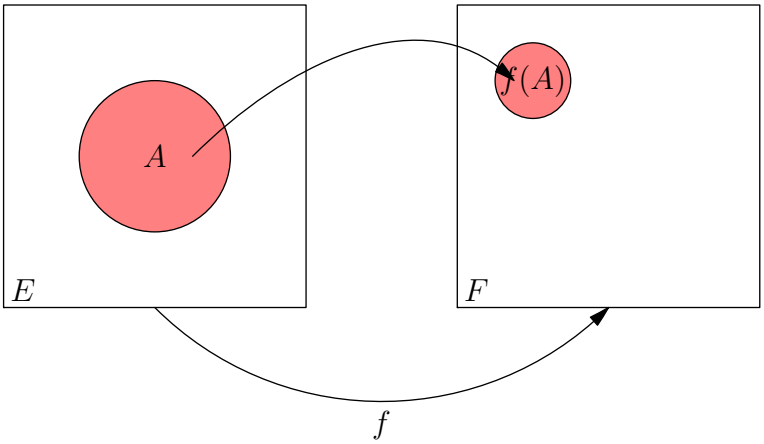


FIGURE 1.7 – Image directe de $A$ par $f$

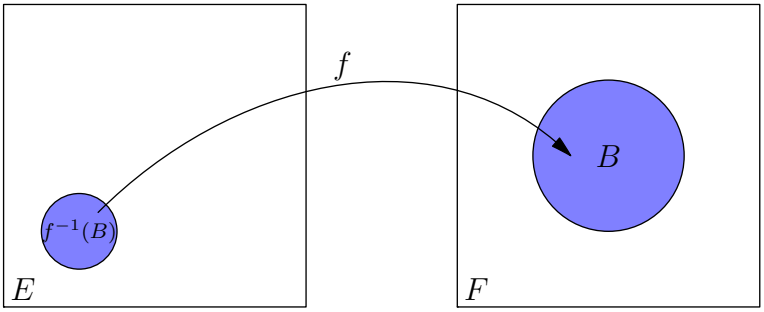


FIGURE 1.8 – Image réciproque de $B$ sur $F$ par $f$

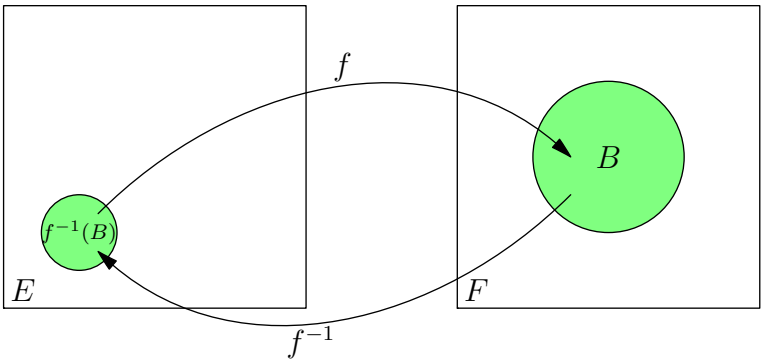


FIGURE 1.9 – Ne pas confondre « image réciproque » ($f^{-1}(B)$) et « application réciproque » (l'application $f^{-1}$ qui envoie $E$ sur $F$ si $f$ est une bijection.)

**Remarque 1.77. Attention !** Ne pas confondre l'image réciproque avec l'application réciproque. L'image réciproque par $f$ s'identifie avec l'image directe par $f^{-1}$ quand $f$ est une bijection (voir la figure 1.9).

**Exemple 1.78.** Soient l'application :

$$\begin{array}{rccc} f & : & \mathbf{R} & \to & \mathbf{R} \\ & & x & \mapsto & f(x) = x^2 \end{array}$$

et six ensembles :

$$A_1 = [0\,,+\infty[,\ A_2 = \mathbf{R},\ A_3 = [-1\,,2],\ B_1 = [1\,,4],\ B_2 = \{9\}\,,\ B_3 = \{-1\}\,.$$

On veut déterminer les images directes de $A_1$, $A_2$ et $A_3$ par $f$ et les images réciproques de $B_1$, $B_2$ et $B_3$ par $f$. On a :

$$\begin{array}{c} f(A_1) = \left\{x^2,\ x \in [0\,,+\infty[\right\} = [0\,,+\infty[,\ f(A_2) = [0\,,+\infty[,\ f(A_3) = [0\,,4] \\ f^{-1}(B_1) = [1\,,2] \cup [-1\,,-2],\ f^{-1}(B_2) = \{-3,3\}\,,\ f^{-1}(B_3) = \emptyset. \end{array}$$

### 1.3.5 Injection, surjection et bijection

**Définition 1.79** (Injection)**.** *Soient $E$ et $F$ des ensembles et $f\colon E \to F$ une application. L'application $f$ est* injectif *si tout élément de $F$ admet au plus un antécédent. Ceci est équivalent à dire que si deux éléments de $E$ ont la même image alors ils sont égaux :*

$$\forall x \in E,\ \forall y \in E, \quad f(x) = f(y) \Rightarrow x = y$$

$$\Leftrightarrow \forall x \in E,\ \forall y \in E, \quad x \neq y \Rightarrow f(x) \neq f(y).$$

**Définition 1.80** (Surjection)**.** *Soient $E$ et $F$ des ensembles et $f\colon E \to F$ une application. L'application $f$ est* surjectif *si tout élément $x \in F$ admet au moins un antécédent. C'est-à-dire $f$ est surjective si et seulement :*

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

**Définition 1.81** (Bijection)**.** *Soient $E$ et $F$ des ensembles et $f\colon E \to F$ une application. L'application $f$ est* bijective *si elle est à la fois injective et surjective. Ceci revient à dire que tout élément de $F$ possède un unique antécédent.*

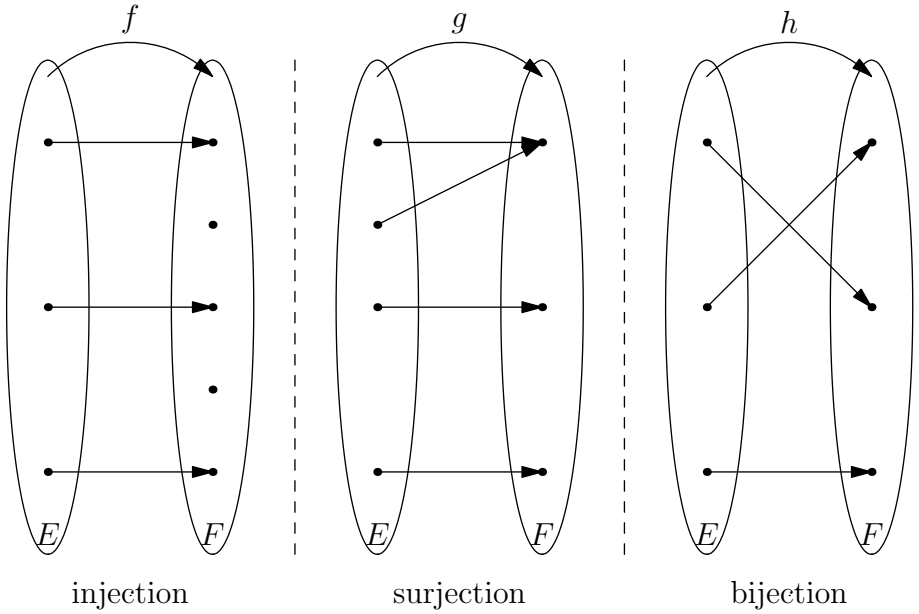


FIGURE 1.10 – Représentation des fonctions injectives, surjectives et bijectives [6]

**Définition 1.82** (Réciproque)**.** *Soient $E$ et $F$ deux ensembles. Si $f : E \to F$ est une application bijective alors il existe une réciproque :*

$$\begin{array}{rccl} f^{-1} & : & F & \to & E \\ & & y & \mapsto & f^{-1}(y) = x. \end{array}$$

*On appelle $f^{-1}$ la* réciproque *de $f$.*

**Exemple 1.83** (L'hôtel, [6])**.** Un groupe de touristes doit être logé dans un hôtel. On considère l'application qui consiste à ranger l'ensemble des touristes (qu'on nommera $T$) dans l'ensemble des chambres (qu'on nommera $C$).

- Les touristes veulent que l'application soit *injective*, c'est-à-dire que *chacun d'entre eux* ait une chambre individuelle. Ceci est possible si le nombre de chambre dépasse le nombre de touristes.
- L'hôtelier, lui, veut que l'application soit *surjective*, c'est-à-dire que chaque chambre soit occupée. Ceci est possible si le nombre de touristes dépasse le nombre de chambres.
- Ainsi, on voit clairement que pour satisfaire les deux parties, il faut que l'application soit bijective, c'est-à-dire que chaque touriste occupe une chambre et que toutes les chambres soient occupées.

**Exemple 1.84.** Soit l'application

$$\begin{array}{rccc} f & : & \mathbf{R} & \to & \mathbf{R} \\ & & x & \mapsto & f(x) = x^2 \end{array} .$$

L'application n'est ni injectif car $f(1) = f(-1) = 1$ (c'est-à-dire que $1$ possède deux antécédents), ni surjectif car $-1 \notin f(\mathbf{R})$. D'où $f$ n'est pas bijective. Mais si on prend la restriction de $f$ sur $\mathbf{R}_+$, c'est-à-dire la fonction :

$$\begin{array}{rccc} g = f|_{\mathbf{R}_+} & : & \mathbf{R}_+ & \to & \mathbf{R}_+ \\ & & x & \mapsto & g(x) = x^2 \end{array} ,$$

on peut montrer que cette fonction est bijective.

**Injectivité** Supposons que $f(x) = f(y)$ alors

$$g(x) = g(y) \Rightarrow x^2 = y^2 \Rightarrow x = y \ (x > 0,\ y > 0).$$

D'où $g$ est injective.

**Surjectivité** Soit $y \in \mathbf{R}_+$ alors $x = \sqrt{y}$ est un antécédent de $y$. On a donc : $g([0\,, +\infty[) = [0\,, +\infty[$, d'où $g$ est surjective.

Comme $g$ est injective et surjective, $g$ est donc bijective.

### 1.3.6 Injectivité, surjectivité des fonctions composées

**Proposition 1.85.** *Soient $E, F$ et $G$ trois ensembles, $f\colon E \to f$ et $g\colon F \to G$ deux applications. Alors :*

*(i) Si $g \circ f$ est injective alors $f$ est injective.*

*(ii) Si $g \circ f$ est surjective alors $g$ est surjective.*

*Démonstration.* (i) Il faut démontrer, pour tout $x, y \in E$,

$$f(x) = f(y) \Rightarrow x = y.$$

Or,

$$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow (g \circ f)(x) = (g \circ f)(y) \Rightarrow x = y$$

car $g \circ f$ est injective. D'où le résultat.

(ii) Il faut montrer que pour tout $z \in G$, il existe un $y \in F$ tel que $g(y) = z$. Or : $g \circ f$ est surjective donc il existe $x \in E$ tel que $(g \circ f)(x) = z$. On pose $y = f(x)$ et

$$g(y) = g(f(x)) = (g \circ f)(x) = z.$$

Donc $g$ est une application surjective.

□

**Proposition 1.86.** *Soient $E, F$ et $G$ trois ensembles, $f\colon E \to F$ et $g\colon F \to G$ deux applications. Alors*

*(i) Si $f$ et $g$ sont injectives alors $g \circ f$ est injective.*

*(ii) Si $f$ et $g$ sont surjectives alors $g \circ f$ est surjective.*

*Démonstration.* (i) Supposons que $(g \circ f)(x) = (g \circ f)(y)$, on a :

$$(g \circ f)(x) = (g \circ f)(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y) \Rightarrow x = y.$$

D'où le résultat.

(ii) Soit $z \in G$, on cherche $x \in E$ tel que $(g \circ f)(x) = z$. Comme $g$ est surjective, il existe un $y \in F$ tel que $g(y) = z$ et, comme $f$ est surjective, il existe un $x \in E$ tel que $f(x) = y$. Alors :

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

D'où le résultat.

□

### 1.3.7 Injection, surjection et bijection dans le cas des ensembles finis

**Proposition 1.87.** *Soient $E$ et $F$ des ensembles finis et $f\colon E \to F$ une application. Alors :*

*(i) Si $f$ est bijective alors $E$ et $F$ ont le même nombre d'éléments :* $\operatorname{card}(E) = \operatorname{card}(F)$,

*(ii) Si $f$ est injective alors* $\operatorname{card}(E) \leq \operatorname{card}(F)$,

*(iii) Si $f$ est surjective alors* $\operatorname{card}(E) \geq \operatorname{card}(F)$.

Cette proposition aurait pu être vu grâce à la figure 1.10 et l'exemple 1.83.

*Démonstration.* (i) Si $f$ est bijective alors à chaque élément de $E$ correspond à un élément de $F$, c'est-à-dire que $\operatorname{card}(E) = \operatorname{card}(F)$.

(ii) Si $f$ est injective alors à chaque élément de $F$ correspond au plus à un élément de $E$, ainsi $\operatorname{card}(E) \leq \operatorname{card}(F)$. On pose $E' = f(E) \subset F$ et $f\colon E \to F$ est injective, ainsi $f\colon E \to E'$ est une application bijective, ce qui entraîne par le (i) que $\operatorname{card}(E) = \operatorname{card}(E') \leq \operatorname{card}(F)$ car $E' \subset F$.

(iii) Comme l'image de chaque élément est unique, on a toujours l'inégalité $\operatorname{card}(E) \geq \operatorname{card}(f(E))$. On a supposé que $f$ est surjective donc $f(E) = F$ et ainsi $\operatorname{card}(E) \geq \operatorname{card}(F)$.

□

**Remarque 1.88.** La réciproque est fausse. Soient les deux ensembles $E = \{1, 2, 3\}$, $F = \{1, 2\}$ et $f : E \to F$ une application telle que :

$$f(1) = 1,\ f(2) = 1,\ f(3) = 1.$$

On a bien $\mathrm{card}(E) \geq \mathrm{card}(F)$ mais $f$ n'est pas surjective.

**Corollaire 1.89.** *Soient $E$ et $F$ deux ensembles de cardinal fini tel que $\mathrm{card}(E) = \mathrm{card}(F)$ et $f : E \to F$ une application. Alors les énoncés suivants sont équivalents :*

*(i)* *$f$ est injective,*

*(ii)* *$f$ est surjective,*

*(iii)* *$f$ est bijective.*

*Démonstration.* Pour montrer que tous les énoncés sont équivalents, il suffit de montrer que (i) implique (ii), puis que (ii) implique (iii), et enfin que (iii) implique (i).

((i) $\Rightarrow$ (ii)) On suppose que $f$ est injective, d'où $f : E \to f(E)$ est bijective. D'où $\mathrm{card}(E) = \mathrm{card}(f(E))$ mais d'après l'hypothèse qu'on a fait sur $E$ et $F$, on a $\mathrm{card}(f(E)) = \mathrm{card}(F)$, d'où $f(E) = F$ (car $f(E) \subset F$) et ainsi $f$ est surjective.

((ii) $\Rightarrow$ (iii)) Supposons qu'il existe $x, y \in E$ tel que $f(x) = f(y)$ et $x \neq y$ alors $\mathrm{card}(f(E)) < \mathrm{card}(E)$. Or $f$ est surjective, d'où $f(E) = f$ et $\mathrm{card}(f(E)) = \mathrm{card}(F)$. Par hypothèse, on a : $\mathrm{card}(E) = \mathrm{card}(F) = \mathrm{card}(f(E))$, ce qui nous amène à une contraction. Donc $f$ est aussi injective, d'où $f$ est bijective.

((iii) $\Rightarrow$ (i)) Évident car si $f$ est bijective alors $f$ est injective.

□

## 1.4 Dénombrements

**Théorème 1.90** (Arrangement)**.** *Soient $E$ et $F$ des ensembles de cardinal fini. Si $p \leq n$ avec $p = \mathrm{card}(F)$ et $n = \mathrm{card}(E)$ alors l'ensemble :*

$$\mathscr{F} = \{f : F \to E,\ f \text{ est injective}\}$$

*est un ensemble fini (qu'on appelle* ensemble des arrangements *de $E$ dans $F$) de cardinal $n(n-1)\cdots(n-p-1)$.*

*Démonstration.* Comme $F$ est de cardinal $p$, on peut noter $F = \{x_1, \ldots, x_d\}$. Soit $f : F \to E$ une application injective, cela implique que $f(x_i) \neq f(x_j)$ pour

$i \neq j$. Il y a donc $n$ possibilités pour choisir $f(x_1)$. Comme $f(x_2)$ doit être différent de $f(x_1)$, on a donc $(n-1)$ possibilités pour $f(x_2)$. Ainsi de suite pour arriver à $f(x_p)$ qui peut être choisi parmi les $n-p+1$ éléments restants dans $E$. D'où $\mathrm{card}(\mathscr{F}) = n(n-1)(n-2)\cdots(n-p+1)$. □

**Définition 1.91** (Permutation)**.** *Soit $E = \{x_1, \ldots, x_n\}$ un ensemble tel que $\mathrm{card}(E) = n$. On appelle* permutation*, toute application $\sigma$ bijective de $E$ dans $E$.*

**Exemple 1.92.** Soit $E = \{x_1, x_2\}$. Si on définit l'application $\sigma\colon E \to E$ telle que $\sigma(x_1) = x_2$ et $\sigma(x_2) = x_1$, alors $\sigma$ est une permutation de $E$.

**Corollaire 1.93.** *Soit $E$ un ensemble fini de cardinal $n$ alors l'ensemble des permutations $\mathscr{S}_E$ est un ensemble de cardinal fini et*

$$\mathrm{card}(\mathscr{S}_E) = n! = \prod_{k=0}^{n} k$$

*avec $0! = 1$. $n!$ est appelé la* factorielle *de $n$.*

*Démonstration.* On peut reprendre la démonstration du théorème 1.90 avec $F = E$ (d'où $n = p$. D'après le corollaire 1.89, $\mathrm{card}(E) = \mathrm{card}(F)$ implique que $f$ est bijective d'où $f$ est une permutation de $E$ et ainsi, toujours d'après le théorème 1.90, on a :

$$\mathrm{card}(\mathscr{S}_E) = n(n-1)\cdots(n-n+1) = n!\,.$$

□

**Théorème 1.94** (Combinaison)**.** *Soit $E$ un ensemble fini de cardinal $n$ et soit $p$ un entier tel que $1 \leq p \leq n$ alors l'ensemble des parties de $E$ ayant $p$ éléments (appelé aussi* combinaison *de $p$ éléments de $E$) est un ensemble fini de cardinal :*

$$\mathrm{C}_n^p = \frac{n(n-1)\cdots(n-p+1)}{p!}.$$

D'autres notations pour désigner le nombre de combinaisons de $p$ éléments de $E$ sont :

$$\mathrm{C}_n^p = \binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}.$$

*Démonstration.* On peut s'inspirer de la démonstration du théorème 1.90 pour en déduire que l'ensemble des combinaisons de $p$ éléments de $E$ est au nombre de $\mathrm{C}_n^p$. □

**Exemple 1.95.** Soit $E = \{1, 2, 3\}$ et $p = 2$. Alors l'ensemble des combinaisons de 2 éléments de $E$ sont

$$\mathscr{C}_E = \{\{1, 2\}, \{2, 3\}, \{1, 3\}\}.$$

D'où

$$\text{card}(\mathscr{C}_E) = \text{C}_3^2 = \frac{3!}{2!} = 3.$$

**Théorème 1.96** (Égalité de Pascal)**.** *Soient $n$ et $p$ deux entiers tels que $1 \leq p \leq n$. Alors :*

$$\text{C}_n^p = \text{C}_{n-1}^{p-1} + \text{C}_{n-1}^p.$$

**Définition 1.97** (Formule du binôme de Newton)**.** *Soient $a, b \in \mathbf{R}$ et soit $n \in \mathbf{N}$ avec $n \geq 1$, alors :*

$$(a + b)^n = \sum_{p=0}^{n} \text{C}_n^p a^{n-p} b^p.$$

**Théorème 1.98.** *Soit $E$ un ensemble fini de cardinal $n$, alors on a :*

$$\text{card}(\mathscr{P}(E)) = 2^n.$$

*Démonstration.* On a, d'après le théorème 1.94,

$$\text{card}(\{F \subset E,\ \text{card}(F) = p\} = \text{C}_n^p.$$

D'où

$$\text{card}(\mathscr{P}(E)) = \sum_{p=0}^{n} \text{C}_n^p = (1 + 1)^n = 2^n.$$

□

## 1.5 Relations d'équivalence

**Définition 1.99** (Relation)**.** *Soit $E$ un ensemble. Une* relation *$\mathscr{R}$ dans $E$ est un sous-ensemble de $E \times E$.*

**Définition 1.100** (Relation d'équivalence)**.** *Soient $E$ un ensemble et $\mathscr{R}$ une relation dans $E$. On dit que $\mathscr{R}$ est une* relation d'équivalence *si :*

1. *pour tout $x \in E$, $(x, x) \in \mathscr{R}$ (réflexivité),*
2. *pour tout $x, y \in E$, si $(x, y) \in \mathscr{R}$ alors $(y, x) \in \mathscr{R}$ (symétrie),*

3. *pour tout* $x, y, z \in E$*, si* $(x, y) \in \mathscr{R}$ *et* $(y, z) \in \mathscr{R}$ *alors* $(x, z) \in \mathscr{R}$ *(transitivité).*

*Si* $(x, y) \in \mathscr{R}$*, on note :* $x \sim y$ *ou* $x\mathscr{R}y$*.*

**Définition 1.101** (Classe)**.** *Soit* $x \in E$*. On appelle* classe *de* $x$ *relativement à* $\mathscr{R}$*, l'ensemble :*

$$\overline{x} = \{y \in E,\ x \in y\}\,.$$

**Remarque 1.102.** On trouvera parfois la notation $C|_{\mathscr{R}}(x)$ pour désigner la classe de $x$ relativament à $\mathscr{R}$.

**Définition 1.103** (Ensemble des classes)**.** *L'*ensemble des classes *est noté*

$$E/\mathscr{R} = \{\overline{x},\ x \in E\}\,.$$

**Définition 1.104** (Surjection canonique)**.** *L'application* $\pi\colon E \to E/\mathscr{R}$ *définie par* $\pi(x) = \overline{x}$ *est surjective. Cette application est appelée la* surjection canonique *de* $E$ *vers* $E/\mathscr{R}$*.*

**Exemple 1.105.** (i) Soient $E = \mathbf{Z}$ et $\mathscr{R}$ une relation dans $\mathbf{Z}$ définie par :

$$\mathscr{R} = \{(x, y) \in \mathbf{Z},\ x - y \text{ est pair}\}\,.$$

On montre que $\mathscr{R}$ est une relation d'équivalence :

1. Soit $x \in \mathbf{Z}$, on a $x - x = 0$ qui est, lui-même, un nombre pair. Donc : $(x, x) \in \mathscr{R}$.
2. Soit $x, y \in \mathbf{Z}$, on suppose que $(x, y) \in \mathscr{R}$. On a donc $x - y$ pair. Notons $n = x - y$ alors $-n$ garde la même parité que $n$. D'où $-n = -x + y = y - x$ est pair et ainsi $(y, x) \in \mathscr{R}$.
3. Soit $x, y, z \in \mathbf{Z}$. On suppose que $(x, y) \in \mathscr{R}$ et $(y, z) \in \mathscr{R}$. On a ainsi $x - y$ pair et $y - z$ pair. Maintenant,

$$x - z = x - y + y - z$$

et comme « pair + pair = pair », on obtient que $x - z$ est un nombre pair d'où $(x, z) \in \mathscr{R}$.

On détermine les classes d'équivalences de $\mathscr{R}$. Soit $x \in \mathbf{Z}$, alors :

$$\overline{x} = \{y \in \mathbf{Z},\ x - y \text{ est pair}\}\,.$$

– Si $x$ est pair alors $\overline{x} = \{y \in \mathbf{Z},\ y \text{ est pair}\}$ d'où $\overline{x} = \overline{0} = \overline{2} = \overline{4} = \cdots$.
– Si $x$ est impair alors $\overline{x} = \{y \in \mathbf{Z},\ y \text{ est pair}\}$, d'où $\overline{x} = \overline{1} = \overline{3} = \overline{5} = \cdots$.

On a, donc, $\mathbf{Z}/\mathscr{R} = \{\overline{0}, \overline{1}\}$. On note cet ensemble $\mathbf{Z}/2\mathbf{Z}$.

(ii) Soient $E = \mathbf{Z} \times \mathbf{Z}^*$ et la relation $\mathscr{R}$ sur $E$ définie par :

$$\mathscr{R} = \left\{(a,b),(a',b') \in (\mathbf{Z} \times \mathbf{Z}^*)^2,\ ab' = a'b\right\}.$$

Le lecteur est invité à vérifer que $\mathscr{R}$ est bien une relation d'équivalence. Soit $(a,b) \in \mathbf{Z} \times \mathbf{Z}^*$, on a :

$$\overline{(a,b)} = \{(a'b') \in \mathbf{Z} \times \mathbf{Z}^*,\ ab' = ba'\} = \{(a',b') \in \mathbf{Z} \times \mathbf{Z}^*\}\ \frac{a}{b} = \frac{a'}{b'}.$$

De plus, l'application

$$\begin{array}{rccc} f & : & (\mathbf{Z} \times \mathbf{Z}^*)/\mathscr{R} & \to & \mathbf{Q} \\ & & \overline{(a,b)} & \mapsto & f(\overline{(a,b)}) = \frac{a}{b} \end{array}$$

est bijective.

**Définition 1.106** (Partition)**.** *Soient $E$ un ensemble et $E_1, \ldots, E_n$ des sous-ensembles de $E$. On dit que $E_1, \ldots, E_n$ réalisent une partition de $E$ si :*

1. $E_i \cap E_j = \emptyset$ *si* $i \neq j$,
2. $\bigcup_{k=0}^{n} E_k = E$.

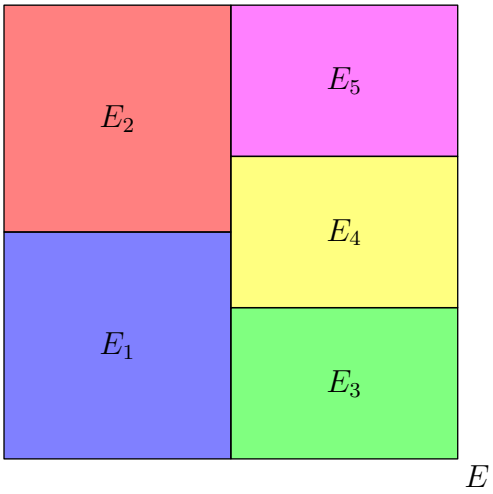


FIGURE 1.11 – $E_1$, $E_2$, $E_3$, $E_4$ et $E_5$ réalisent une partition de $E$

**Exemple 1.107.** Soient $E = \mathbf{Z}$, $A_1 = \{x \in \mathbf{Z},\ x \text{ est pair}\}$ et $A_2 = \{x \in \mathbf{Z},\ x \text{ est impair}\}$. Comme un entier est soit pair ou impair (voir la définition 2.3) et ne peut pas être à la fois pair et impair, $A_1$ et $A_2$ forment une partition de $\mathbf{Z}$.

**Proposition 1.108.** *Soit $E$ un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Alors on a :*

*(i) pour tout $x \in E$ et $y \in E$, $\overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \emptyset$.*

*(ii) $\overline{x} = \overline{y}$ si et seulement si $x \mathscr{R} y$.*

**Définition 1.109** (Ensemble de représentants)**.** *Un* ensemble de représentants *pour la relation d'équivalence $\mathscr{R}$ est un sous-ensemble $\mathscr{T} \subset E$ tel que*

1. *pour tout $x \in E$, il existe un $y \in \mathscr{T}$ tel que $\overline{x} = \overline{y}$,*
2. *pour tout $x, y \in \mathscr{T}$, si $x \neq y$ alors $\overline{x} \neq \overline{y}$.*

**Proposition 1.110.** *Soient $E$ un ensemble, $\mathscr{R}$ une relation sur $E$ et $\mathscr{T} \subset E$ un ensemble de représentants. ALors les ensembles $\overline{x}$ (avec $x \in \mathscr{T}$) réalisent une partition de $E/\mathscr{R}$.*

**Exemple 1.111.** Soient $E = \mathbf{Z}$ et $\mathscr{R}$ la relation sur $E$ définie par :

$$\mathscr{R} = \left\{(x, y) \in \mathbf{Z}^2,\ x - y \text{ est pair}\right\}.$$

On a : $\mathscr{T} = \{0, 1\}$ qui est un ensemble de représentatnts de $\mathscr{R}$ et $\mathbf{Z}/\mathscr{R} = \left\{\overline{0}, \overline{1}\right\}$.

## 1.6 Exercices

**Exercice 1.1** (Le missionaire et les cannibales)**.** Les cannibales d'une tribu se préparent à manger un missionnaire. Désirant lui prouver une dernière fois leur respect de la dignité et de la liberté humaine, les cannibales proposent au missionnaire de décider lui-même de son sort en faisant une courte déclaration : si celle-ci est vraie, le missionnaire sera rôti, et il sera bouilli dans le cas contraire. Que doit dire le missionnaire pour sauver sa vie ? (d'après Cervantès)

**Exercice 1.2** ([2])**.** Nier la proposition : « Tous les habitants de la rue du Havre qui ont les yeux bleus gagenront au loto et prendront leur retraite avant $50$ ans ».

**Exercice 1.3** ([2])**.** Compléter les pointillés par le connecteur logique qui s'impose : $\Leftrightarrow$, $\Rightarrow$, $\Leftarrow$.

1. Pour $x \in \mathbf{R}$, $x^2 = 4 \ldots\ldots\ldots x = 2$ ;
2. Pour $z \in \mathbf{C}$, $z = \overline{z} \ldots\ldots\ldots z \in \mathbf{R}$ ;
3. Pour $x \in \mathbf{R}$, $x = \pi \ldots\ldots\ldots \mathrm{e}^{2\mathrm{i}x} = 1$.

**Exercice 1.4** ([2])**.** Montrer :

1.
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \quad \forall n \in \mathbf{N}^*.$$

2.
$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \quad \forall n \in \mathbf{N}^*.$$

**Exercice 1.5.** Donner la liste des éléments de $\mathscr{P}(\mathscr{P}(\{1,2\}))$.

**Exercice 1.6.** Soit $A$ une partie d'un ensemble $E$, on appelle fonction caractéristqiue de $A$, l'application $\mathbf{1}_A$ de $E$ dans l'ensemble à deux éléments $\{0,1\}$, telle que :
$$\mathbf{1}_A(x) = \begin{cases} 0 & \text{si } x \notin A, \\ 1 & \text{si } x \in A. \end{cases}$$
Soient $A$ et $B$ deux parties de $E$, $\mathbf{1}_A$ et $\mathbf{1}_B$ leurs fonctions caractéristiques. Montrer que les fonctions suivantes sont les fonctions caractéristiques d'ensembles que l'on déterminera :

1. $1 - \mathbf{1}_A$,
2. $\mathbf{1}_A \cdot \mathbf{1}_B$,
3. $\mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \cdot \mathbf{1}_B$.

**Exercice 1.7.** Soient $E, F, G$ et $H$ quatre ensembles. Comparer les ensembles $(E \times F) \cap (G \times H)$ et $(E \cap G) \times (F \cap H)$.

**Exercice 1.8.** Soient $f\colon \mathbf{R} \to \mathbf{R}$ et $g\colon \mathbf{R} \to \mathbf{R}$ telles que $f(x) = 3x + 1$ et $g(x) = x^2 - 1$. A-t-on $f \circ g = g \circ f$ ?

**Exercice 1.9.** Les applications suivantes sont-elles injectives, surjectives, bijectives ?

1.
$$\begin{array}{rccc} f & : & \mathbf{N} & \to & \mathbf{N} \\ & & n & \mapsto & n+1 \end{array},$$

2.
$$\begin{array}{rccc} g & : & \mathbf{Z} & \to & \mathbf{Z} \\ & & n & \mapsto & n+1 \end{array},$$

3.
$$\begin{array}{rccc} h & : & \mathbf{R}^2 & \to & \mathbf{R}^2 \\ & & (x,y) & \mapsto & (x+y, x-y) \end{array},$$

4.
$$\begin{array}{rccc} k & : & \mathbf{R}\setminus\{1\} & \to & \mathbf{R} \\ & & x & \mapsto & \frac{x+1}{x-1} \end{array}.$$

**Exercice 1.10.** Soit $f\colon \mathbf{R}\to\mathbf{R}$ définie par $f(x)=\frac{2x}{1+x^2}$.

1. $f$ est-elle injective ? surjective ?
2. Montrer que $f(\mathbf{R})=[-1\,,1]$.
3. Montrer que la restriction
$$\begin{array}{rccc} g & : & [-1\,,1] & \to & [-1\,,1] \\ & & x & \mapsto & g(x)=f(x) \end{array}$$
est une bijection.
4. Retrouver ce résultat en étudiant les variations de $f$.

**Exercice 1.11** ([2])**.** Soit $E$ un ensemble et une application $f\colon E\to E$ tel que $f^0=\mathrm{id}$ pour $n\in\mathbf{N}$, $f^{n+1}=f^n\circ f$.

1. Montrer que, pour tout $n\in\mathbf{N}$, $f^{n+1}=f\circ f^n$.
2. Montrer que si $f$ est bijective alors, pour tout $n\in\mathbf{N}$, $(f^{-1})^n=(f^n)^{-1}$.

**Exercice 1.12** ([8])**.** Soit $n$ un entier supérieur à $2$. Montrer que $\sum_{p=0}^{n-1}\frac{n!}{p!}$ est un entier pair.

**Exercice 1.13** ([10])**.** En utilisant la formule du binôme, montrer :

1.
$$\sum_{k=0}^{n}(-1)^k\mathrm{C}_n^k=0,$$
2.
$$\sum_{k=0}^{n}k^2\mathrm{C}_n^k=n(n-1)2^{n-2}+n2^{n-1}.$$

**Exercice 1.14.** 1. Dans le plan, on considère trois droites $\Delta_1$, $\Delta_2$, $\Delta_3$ forment un « vrai » triangle : elles ne sont pas concourantes, et il n'y en a pas deux parallèles. Donner le nombre $R_3$ de régions (zones blanches) découpées par ces trois droites.

2. On considère quatre droites $\Delta_1,\ldots,\Delta_4$ telles qu'il n'en existe pas trois concourantes, ni deux parallèles. Donner le nombre $R_4$ de régions découpées par ces quatre droites.

3. On considère $n$ droites $\Delta_1, \ldots, \Delta_n$ telles qu'il n'en existe pas trois concourantes, ni deux parallèles. Soit $R_n$ le nombre de régions délimitées par $\Delta_1, \ldots, \Delta_n$ et $R_{n-1}$ le nombre de régions délimitées par $\Delta_1, \ldots, \Delta_{n-1}$. Montrer que $R_n = R_{n-1} + n$.
4. Calculer par récurrence le nombre de régions délimitées par $n$ droites en position générale, c'est-à-dire telles qu'il n'en existe pas trois concourantes ni deux parallèles.

**Exercice 1.15** ([9])**.** Montrer que la relation $\mathscr{R}$ définie sur R par :

$$x \mathscr{R} y \Leftrightarrow x\mathrm{e}^y = y\mathrm{e}^x$$

est une relation d'équivalence. Préciser, pour $x$ fixé dans R, le nombre d'éléments de la classe de $x$ modulo $\mathscr{R}$.

# Chapitre 2

# Arithmétique dans Z

## 2.1 Divisibilité

**Définition 2.1** (Divisibilité)**.** *Soient $a$ et $b$ deux entiers. On dit que $a$* divise *$b$ (qu'on notera $a \mid b$) s'il existe un entier $k$ tel que $b = ka$. Si $a$ ne divise pas $b$, on notera $a \nmid b$.*

**Exemple 2.2.** On a : $7 \mid 91$ mais $5 \nmid 91$.

**Définition 2.3** (Nombre pair et impair)**.** *Un nombre entier est* pair *s'il est divisible par $2$ ; il est* impair *sinon.*

**Propriétés 2.4** (Propriétés de divisibilité)**.** *Soient $a, b$ et $c$ trois entiers. Alors :*

*(i)* $a \mid a$*,*

*(ii)* *si* $a \mid b$ *et* $b \mid a$ *alors* $|a| = |b|$*,*

*(iii)* *si* $a \mid b$ *et* $b \mid c$ *alors* $a \mid c$*,*

*(iv)* *si* $a \mid b$ *et* $a \mid c$ *alors* $a \mid bx + cy$*, pour tout* $(x, y) \in \mathbf{Z}^2$*,*

*(v)* *si* $b \neq 0$ *et* $a \mid b$ *alors* $|a| \leq |b|$*.*

*Démonstration.* (i) On a bien $a = 1 \times a$, donc $a \mid a$.

(ii) On suppose que $a \mid b$ et $b \mid a$. Il existe donc $k, k' \in \mathbf{Z}$ tel que $b = ka$ et $a = k'b$. D'où

$$a = (kk')a \Rightarrow (1 - kk')a = 0.$$

Les solutions sont $a = 0$ et $kk' = 1$. Si $a = 0$ alors $b = k \times 0 = 0$, d'où $|a| = |b| = 0$. Si $kk' = 1$ alors $|k'| = 1$, d'où $a = b$ ou $-a = -b$, ce qui implique que $|a| = |b|$.

(iii) On a :

$$a \mid b \Rightarrow \exists k \in \mathbf{Z}, \quad b = ka \tag{2.1}$$
$$b \mid c \Rightarrow \exists k' \in \mathbf{Z}, \quad c = k'b. \tag{2.2}$$

En combinant (2.1) et (2.2), on obtient

$$c = k'b = k'ka = (kk')a \Rightarrow a \mid c.$$

(iv) On a supposé $a \mid b$ et $a \mid c$ donc il existe $k, k' \in \mathbf{Z}$ tel que $b = ka$ et $c = k'a$. On a donc :

$$bx + cy = kax + k'ay = a(kx + k'y),$$

ce qui implique que $a \mid bx + cy$.

(v) Si $a \mid b$ alors il existe $k \in \mathbf{Z}$ tel que $b = ka$. Comme $b \neq 0$, cela implique que $k \neq 0$, d'où $|k| \geq 1$. On a donc :

$$b = ka \Rightarrow |b| = |k| \cdot |a| \geq |a|.$$

□

## 2.2 Division euclidienne

**Proposition 2.5.** *Soient $a$ et $b$ deux entiers tel que $b \neq 0$ alors il existe un unique entier $q$ et un unique entier $r$ tel qu'on a :*

$$a = qb + r \quad \textit{avec } O \leq r \leq |b|.$$

*Démonstration.* **Existence** On suppose que $b > 0$ (la même démonstration est à faire pour $b < 0$). Soit $q$ le plus grand entier tel que $qb \leq a$ alors $q = \left[\frac{a}{b}\right]$ où $[x]$ désigne la partie entière de $x$. On a alors :

$$qb \leq a \leq (q+1)b. \tag{2.3}$$

On peut poser $r = a - qb$ et donc (2.3) implique que $0 \leq r \leq b$.

**Unicité** On suppose que $a = qb + r = q'b + r'$. On a alors :

$$(qb + r) - (q'b + r') = 0 \Rightarrow qb - q'b + r - r' \Rightarrow (q - q')b = r' - r.$$

On peut supposer que $r' \geq r$ alors $r' - r \in \{0, \ldots, b-1\}$ et si $(q - q')b = r' - r$, on a (comme $(q - q')$ est un entier) que $b \mid r' - r$. Ainsi,

$$r' - r = 0 \Rightarrow r = r'$$

et donc $(q - q')b = 0$ implique que $(q - q') = 0$. C'est ce qu'il fallait démontrer.

□

**Exemple 2.6.** 1. On cherche à faire la division euclidienne de $28$ par $6$. On a $24 = 6 \times 4$ et $30 = 5 \times 6$, d'où $28 = 6 \times 4 + 4$ (donc $q = 4$ et $r = 4$).

2. On cherche à faire la division euclidienne de $28$ par $-3$. On a : $28 = (-9) \times (-3) + 1$, d'où $q = -9$ et $r = 1$.

# 2.3 Plus grand commun diviseur

## 2.3.1 Plus grand commun diviseur

**Définition 2.7** (Plus grand commun diviseur)**.** *Soient $a$ et $b$ deux entiers tel que $a \neq 0$ et $b \neq 0$. Le* plus grand diviseur commun *de $a$ et $b$ (qu'on note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$) est l'unique entier positif $d$ qui vérifie :*

1. *$d \mid a$ et $d \mid b$,*
2. *si $c \mid a$ et $c \mid b$ alors $|c| \leq d$.*

**Remarque 2.8.** Si $a = 0$ ou $b = 0$ alors $\mathrm{PGCD}(a, b) = 0$.

**Proposition 2.9.** *(i) Si $a$ et $b$ sont des entiers non nuls alors* $\mathrm{PGCD}(a, b)$ existe *(c'est-à-dire que l'ensemble $\{c \in \mathbf{Z},\ c \mid a$ et $c \mid b\}$ est non vide et est fini).*

*(ii)* Unicité : *si $d$ et $d'$ vérifient les conditions de la définition alors $d' \leq d$ et $d \leq d'$ (c'est-à-dire $d = d'$).*

*(iii)* $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|)$ *(on a : $d \mid a$ et $d \mid b$ si et seulement si $d \mid |a|$ et $d \mid |b|$).*

*(iv) Si* $\mathrm{PGCD}(a, b) = d$ *alors $a$ et $b$ s'écrivent $a = da'$ et $b = db'$ avec* $\mathrm{PGCD}(a', b') = 1$.

*Démonstration.* Pour montrer la dernière proposition, supposons qu'il existe un entier $k > 0$ tel que $k \mid a'$ et $k \mid b'$. On a donc $dk \mid da'$ et $dk \mid db'$, ce qui implique que $dk \mid a$ et $dk \mid b$. D'où $dk = d$ et donc $k = 1$. □

## 2.3.2 Nombres premiers entre eux

**Définition 2.10** (Nombres premiers entre eux)**.** *On dit que $a$ et $b$ sont* premiers entre eux *si* $\mathrm{PGCD}(a, b) = 1$.

**Exemple 2.11.** On a $\mathrm{PGCD}(7, 4) = 1$, d'où $7$ et $4$ sont premiers entre eux.

**Définition 2.12.** *On dit que deux nombres sont premiers entre eux s'ils n'ont pas de diviseurs en commun autre que $1$ et $-1$.*

### 2.3.3 Algorithme d'Euclide pour le calcul du PGCD

**Lemme 2.13.** *Soient $a$, $b$, $q$ et $r$ des entiers tels que $a = qb+r$ alors* $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$.

*Démonstration.* Pour cela, on montre que $\mathrm{PGCD}(a,b) \leq \mathrm{PGCD}(b,r)$ et que $\mathrm{PGCD}(b,r) \leq \mathrm{PGCD}(a,b)$.

1. On pose $d = \mathrm{PGCD}(a,b)$ alors $d \mid a$ et $d \mid b$. Alors $d \mid a - qb$ ce qui implique que $d \mid r$ et comme $d \mid r$, on a bien $d \leq \mathrm{PGCD}(b,r)$.
2. On pose $d' = \mathrm{PGCD}(b,r)$ alors $d' \mid b$ et $d' \mid r$ alors $d' \mid bq + r$ et ainsi $d \mid a$. On a donc $d \mid a$ et $d \mid b$, d'où $d' \leq \mathrm{PGCD}(a,b)$.

□

**Théorème 2.14** (Algorithme d'Euclide)**.** *Soient $a$ et $b$ deuxs entiers. On a alors cinq cas :*

1. *Si $a = 0$ alors* $\mathrm{PGCD}(a,b) = |b|$.
2. *Si $b = 0$ alors* $\mathrm{PGCD}(a,b) = |a|$.
3. *Si $a \mid b$ alors* $\mathrm{PGCD}(a,b) = |a|$.
4. *Si $b \mid a$ alors* $\mathrm{PGCD}(a,b) = |b|$.
5. *Si on n'a pas ces quatre cas là, il faut effectuer des divisions euclidiennes successives pour obtenir une suite d'équations*

$$\begin{aligned}
a &= q_1 b + r_1 \quad && \text{avec } 0 < r_1 < |b|, \\
b &= q_2 r_1 + r_2 \quad && \text{avec } 0 < r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3 \quad && \text{avec } 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \quad && \text{avec } 0 < r_n < r_{n-1}, \\
r_{n-1} &= q_{n+1} r_n \quad && \text{avec } r_n = 0,
\end{aligned}$$

*alors* $\mathrm{PGCD}(a,b) = r_n$ *(c'est le dernier reste non nul).*

*Démonstration.* L'algorithme est justifié par le lemme 2.13. On a :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r_1) = \mathrm{PGCD}(r_1,r_2) = \cdots = \mathrm{PGCD}(r_n,r_{n+1}) = r_n$$

car $r_{n+1} = 0$. □

**Exemple 2.15.** On cherche $\mathrm{PGCD}(246, 54)$ par l'algorithme d'Euclide. On fait des divisions euclidiennes successives :

$$\begin{aligned} 246 &= 54 \times 4 + 30, \\ 54 &= 30 \times 1 + 24 \\ 30 &= 24 \times 1 + 6 \\ 24 &= 4 \times 6. \end{aligned}$$

On a donc : $\mathrm{PGCD}(246, 54) = 6$.

# 2.4 Théorème de Bezout

## 2.4.1 Théorème de Bezout

**Théorème 2.16** (Bezout)**.** *Soient $a$ et $b$ des entiers non nuls. Alors il existe des entiers $u$ et $v$ tels que :*

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

*Démonstration.* 1. Il existe $c \in \mathbf{Z}^*$ tel que $c = ax + by$ avec $x, y \in \mathbf{Z}$. On a :

$$\begin{aligned} a &= 1 \times a + 0 \times b, \\ b &= 0 \times a + 1 \times b, \\ -a &= -1 \times a + 0 \times b, \\ -b &= 0 \times a + -1 \times b. \end{aligned}$$

Or comme $a$ et $b$ sont supposés non nuls, il existe un $x \in \{a, -a, b, -b\}$ tel que $x > 0$.

2. Soit $d$ le plus petit entier positif qui s'écrit sous la forme $d = ax + by$ avec $x, y \in \mathbf{Z}$. On fait la division euclidienne de $a$ par $d$ et $b$ par $d$ :

$$\begin{aligned} a &= qd + r \quad \text{avec } 0 \leq r < d, \\ b &= q'd + r' \quad \text{avec } 0 \leq r < d \end{aligned}$$

On a alors

$$r = a - qd = a - q(ax + by) = a - qax - qbx = a(1 - qx) - qby,$$

c'est une combinaison linéaire de $a$ et $b$. Posons $x' = 1 - qx$ et $y' = -qy$, on a donc : $r = ax' + by'$. Or, on a en plus que $0 \leq r \leq d$, d'où $r = 0$ et $d \mid a$. On fait la même chose avec $r'$ :

$$r' = b - qd = b - q(ax + by) = b(1 - qy) - qax = by' + ax'.$$

Or les conditions $r' = ax' + by'$ et $0 \leq r' \leq d$ nous donne que $r' = 0$, d'où $d \mid b$. Ainsi, on a $d \mid a$ et $d \mid b$, donc $\mathrm{PGCD}(a, b) \geq d$.
Réciproquement, on a $\mathrm{PGCD}(a, b) \mid a$ et $\mathrm{PGCD}(a, b) \mid b$, cela implique que

$$\mathrm{PGCD}(a, b) \mid ax + by, \qquad \text{pour tout } x, y \in \mathbf{Z}.$$

Comme $d = ax + by$, on a bien $\mathrm{PGCD}(a, b) \mid d$ et donc $d \geq \mathrm{PGCD}(a, b)$. D'où : $\mathrm{PGCD}(a, b) = d = ax + by$.

□

**Remarques 2.17.**

1. $u$ et $v$ ne sont pas uniques. Par exemple, si on prend $a = 15$ et $b = 6$, on a : $\mathrm{PGCD}(a, b) = 3$. Or,

$$\mathrm{PGCD}(a, b) = 15 - 2 \times 6 = 3 \times 15 - 7 \times 6.$$

2. Il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$. On peut avoir $d \neq \mathrm{PGCD}(a, b)$ et dans ce cas, $\mathrm{PGCD}(a, b) \mid d$. Par exemple, soit $a = 15$ et $b = 6$, on a : $2 \times 15 + 1 \times 6 = 36$ mais $36 \neq \mathrm{PGCD}(15, 6)$.
3. Pour trouver les entiers $u$ et $v$ tels que $\mathrm{PGCD}(a, b) = au + bv$, on utilise l'algorithme d'Euclide. On peut, par exemple, reprendre l'algorithme d'Euclide pour trouver le $\mathrm{PGCD}(246, 54)$ (vu en exemple 2.15).

$$246 = 4 \times 54 + 30, \tag{2.4}$$
$$54 = 1 \times 30 + 24, \tag{2.5}$$
$$30 = 1 \times 24 + 4, \tag{2.6}$$
$$24 = 4 \times 6$$

On trouve donc $\mathrm{PGCD}(a, b) = 6$ et

(2.4) $\Rightarrow 30 = 246 - 4 \times 54$,
(2.5) $\Rightarrow 24 = 54 - 30 = 54 - (246 - 4 \times 54) = -246 + 5 \times 54$,
(2.6) $\Rightarrow 6 = 30 - 24 = (246 - 4 \times 54) - (-246 + 5 \times 54) = 2 \times 246 - 9 \times 54$.

Donc : $u = 2$ et $v = -9$.

### 2.4.2 Corollaires du théorème de Bezout

**Corollaire 2.18.** *Soient $a$ et $b$ des entiers non nuls. Si $c \mid a$ et $c \mid b$ alors $c \mid \mathrm{PGCD}(a, b)$.*

*Démonstration.* Soit $d = \mathrm{PGCD}(a, b)$. On a, par le théorème de Bezout, qu'il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$. Comme $c \mid a$ et $c \mid b$, cela implique que $c \mid au + bv$ et donc que $c = d$. □

**Corollaire 2.19.** *Soient $a$ et $b$ deux entiers non nuls. Si $\mathrm{PGCD}(a,b)=1$ alors il existe $u,v\in\mathbf{Z}$ tels que $au+bv=1$.*

*Démonstration.* ($\Rightarrow$) On utilise le théorème de Bezout.
($\Leftarrow$) Soit $c\in\mathbf{N}^*$ tel que $c\mid a$ et $c\mid b$. Alors, on a : $c\mid au+bv$, ce qui implique que $c\mid 1$ et donc que $c=1$. On obtient donc $\mathrm{PGCD}(a,b)=1$.

□

**Corollaire 2.20** (Lemme de Gauss)**.** *Soient $a$, $b$ et $c$ des entiers tels que $a\mid bc$ et $\mathrm{PGCD}(a,b)=1$, alors $a\mid c$.*

*Démonstration.* L'hypothèse « $\mathrm{PGCD}(a,b)=1$ » implique qu'il existe $u,v\in\mathbf{Z}$ tels que $au+bv=1$. En multipliant par $c$ dans chaque membre de l'égalité, on obtient

$$auc+bvc=c.$$

Or, comme $a\mid a$ et $a\mid b$, on a :

$$a\mid acu+bcv\Rightarrow a\mid c.$$

□

**Remarque 2.21.** L'énoncé est faux sans l'hypothèse $\mathrm{PGCD}(a,b)=1$.

**Corollaire 2.22.** *Soient $a,b$ et $c$ trois entiers tels que $a\mid c$, $b\mid c$ et $\mathrm{PGCD}(a,b)=1$ alors $ab\mid c$.*

*Démonstration.* Comme $\mathrm{PGCD}(a,b)=1$, il existe $u,v\in\mathbf{Z}$ tels que $au+bv=1$. On multiplie, dans chaque membre de l'équation, par $c$ : $acu+bcv=c$. On utilise ensuite les hypothèse de divisibilité de $a$ et $b$. $a\mid c$ implique qu'il existe $k\in\mathbf{Z}$ tel que $c=ka$ et $b\mid c$ implique qu'il existe $k'\in\mathbf{Z}$ tel que $c=k'b$. On a donc :

$$acu+bcv=c\Rightarrow ak'bu+bkav=c\Rightarrow ab(k'u+kv)=c\Rightarrow ab\mid c.$$

□

**Remarque 2.23.** Encore une fois, l'énoncé est faux sans l'hypothèse $\mathrm{PGCD}(a,b)=1$.

## 2.5 Équations diophantiennes linéaires

**Définition 2.24** (Équation diophantienne)**.** *Une* équation diophantienne *linéaire en deux variables est une équation du type $ax+by=c$ où $a,b$ et $c$ sont des entiers et les inconnus $x$ et $y$ sont des entiers.*

**Théorème 2.25.** *Soient $a, b$ et $c$ des entiers. On considère l'équation diophantienne suivante :*

$$ax + by = c \quad \text{avec } x, y \in \mathbf{Z}. \tag{$E$}$$

*On pose $d = \mathrm{PGCD}(a, b)$. Alors :*

*(i) ($E$) admet une solution $(x, y) \in \mathbf{Z}^2$ si et seulement si $d \mid c$,*

*(ii) si $d \mid c$ et si $(x_0, y_0) \in \mathbf{Z}^2$ est une solution particulière de ($E$) alors les solutions générales sont du type :*

$$\begin{cases} x = x_0 + k \cdot \frac{b}{d} \\ y = y_0 - k \cdot \frac{a}{d} \end{cases} \quad \text{avec } k \in \mathbf{Z}.$$

*Démonstration.* (i) Dans le sens direct, on a $d \mid a$ et $d \mid b$ qui implique qu'il existe $x$ et $y$ tels que $d \mid ax$ et $d \mid by$. En faisant l'addition des deux, on obtient : $d \mid ax + by$ et comme $ax + by = c$, $d \mid c$.
Dans le sens contraire, on utilise le théorème de Bézout. Il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$. On suppose que $d \mid c$, donc il existe $k \in \mathbf{Z}$ tel que $c = kd$. On obtient alors :

$$au + bv = d \Rightarrow kau + kav = kd \Rightarrow kau + kbv = c \Rightarrow (x, y) = (ku, kv).$$

(ii) Soit l'équation ($E$) : $ax + by = c$ avec $d \mid a$ et $d \mid b$. On suppose aussi que $d \mid c$, on a alors :

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}. \tag{2.7}$$

On pose donc $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $c' = \frac{c}{d}$. (2.7) devient donc $a'x + b'y = c'$ avec $\mathrm{PGCD}(a', b') = 1$. Soit $(x_0, y_0)$ une solution particulière de ($E$), on a donc : $a'x_0 + b'y_0 = c'$. Soient

$$a'x + b'y = c' \tag{2.8}$$
$$a'x_0 + b'y_0 = c' \tag{2.9}$$

On fait (2.8) $-$ (2.9), ce qui donne :

$$a'(x - x_0) + b'(y - y_0) = 0 \Rightarrow b' \mid a'(x - x_0),$$

comme $\mathrm{PGCD}(b', a') = 1$, on a donc :

$$b' \mid (x - x_0) \Rightarrow x - x_0 = kb' \quad \text{avec } k \in \mathbf{Z}.$$

On a donc :

$$x = x_0 + kb' \Rightarrow x = x_0 + k \cdot \frac{b}{d}.$$

On peut faire la même chose pour $y$, on obtient

$$y = y_0 - k \cdot \frac{a}{d}.$$

Vérifions maintenant qu'on a une solution de l'équation ($E$) :

$$ax + by = c \Leftrightarrow a \cdot \left(x_0 + k \cdot \frac{b}{d}\right) + b \cdot \left(y_0 + k \cdot \frac{a}{d}\right) = ax_0 + bx_0 = c.$$

□

**Exemple 2.26.** Soit à résoudre l'équation

$$40x + 18x = 4, \quad \text{avec } x, y \in \mathbf{Z}. \tag{2.10}$$

On utilise l'algorithme d'Euclide pour trouver le $\mathrm{PGCD}(40, 18)$ :

$$\begin{aligned} 40 &= 18 \times 2 + 4 \\ 18 &= 4 \times 4 + 2 \\ 4 &= 2 \times 2. \end{aligned}$$

D'où $\mathrm{PGCD}(40, 18) = 2$. On divise l'équation (2.10) par $\mathrm{PGCD}(40, 18)$, on obtient une nouvelle équation :

$$20x + 9y = 2 \tag{2.11}$$

qui a les mêmes solutions que (2.10). 0n a :

$$\begin{aligned} &4 = 40 - 2 \times 18, \\ &2 = 18 - 4(40 - 2 \times 18) = -4 \times 40 + 9 \times 18 = -8 \times 20 + 18 \times 9. \end{aligned}$$

D'où $(x_0, y_0) = (-8, 18)$ est une solution particulière de (2.10). Les solutions générales sont donc, par le théorème 2.25,

$$\begin{cases} x = -8 + 9k \\ y = 18 - 20k \end{cases} \quad \text{avec } k \in \mathbf{Z}.$$

Avant de terminer ce paragraphe sur les équations diophantiennes, on peut donner une interprétation géométrique. La droite d'équation $ax + by = c$ (avec $x, y \in \mathbf{R}$) contient des points dont les coordonnées sont des nombres entiers si et seulement si $d \mid c$. Si $(x_0, y_0)$ est un point de coordonnées entières sur la droite alors $(x_0 + k \cdot b, y_0 - k \cdot a)$ se trouve sur la droite (avec $k \in \mathbf{N}$).

## 2.6 Plus petit commun multiplicateur

**Définition 2.27** (Plus petit commun multiplicateur)**.** *Soient $a$ et $b$ deux entiers non nuls. Le* plus petit commun multiple *(PPCM) de $a$ et $b$ (noté* $\mathrm{PPCM}(a,b)$ *ou $a \vee b$) est l'unique entier positif $m$ qui vérifie les deux propriétés suivantes :*

1. $a \mid m$ *et* $b \mid m$*,*
2. *si* $a \mid c$ *et* $b \mid c$ *alors* $m \leq |c|$.

**Remarque 2.28.** Si $a = 0$ ou $b = 0$ alors $\mathrm{PPCM}(a,b) = 0$.

**Proposition 2.29.** *Soient $a$ et $b$ deux entiers non nuls alors* $\mathrm{PPCM}(a,b) \cdot \mathrm{PGCD}(a,b) = |ab|$.

*Démonstration.* On a : $\mathrm{PGCD}(a,b) \geq 0 = \mathrm{PGCD}(|a|,|b|$ et $\mathrm{PPCM}(a,b) = \mathrm{PPCM}(|a|,|b|)$. On peut supposer que $a \geq 0$ et $b \geq 0$. On pose $d = \mathrm{PGCD}(a,b)$. Ainsi si $d \mid ab$ alors il existe un entier $m \in \mathbf{Z}$ tel que $ab = dm$. On veut montrer que $m = \mathrm{PPCM}(a,b)$. Or on a $d \mid a$ et $d \mid b$ donc $a = da'$ et $b = db'$ avec $a'b' \in \mathbf{Z}$ et $\mathrm{PGCD}(a',b') = 1$. On a :

$$md = ab = da'db' = d^2a'b' \Rightarrow m = da'b' = ab' = b'a \tag{2.12}$$

car $a \mid m$ et $b \mid m$. On suppose que $a \mid c$ et $b \mid c$, on a alors $c = ka$ et $c = k'b$. Ce qui implique

$$ka = k'b \Rightarrow ka' = k'b'$$

, d'où $b' \mid ka'$ et donc (comme $m = ab' \leq ak \leq c$),

$$b' \mid k \Rightarrow b' \leq k. \tag{2.13}$$

En combinant et , on a $m = \mathrm{PPCM}(a,b)$, d'où le résultat. □

## 2.7 Nombres premiers

### 2.7.1 Définition des nombres premiers

**Définition 2.30** (Entier premier)**.** *Un* entier premier *est un entier $p > 1$ tel que les seuls diviseurs de $p$ sont $-1$, $-p$, $1$ et $p$.*

**Exemple 2.31.** $17$ est un nombre premier mais par contre $87$ n'en est pas un car $\sqrt{87} \approx 9$ et $\frac{87}{7} = 29$.

**Remarque 2.32.** Soit $n$ un entier et $p$ un nombre premier. Si $p \nmid n$ alors $\mathrm{PGCD}(p,n) = 1$.

### 2.7.2 Lemme d'Euclide

**Lemme 2.33** (Euclide)**.** *Soit $p$ un entier premier et soient $a$ et $b$ deux entiers. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.*

*Démonstration.* On suppose que $p$ et $a$ sont premiers entre eux (si $p \mid a$, on a le résultat voulu). Les seuls diviseurs positiffs sont $1$ et $p$, Or $p$ divise $ab$, donc d'après le théorème de Gauss, $p$ divise $b$. □

**Remarque 2.34.** Plus généralement, si on a : $p \mid \prod_{i=1}^{n} a_i$ alors il existe $i$ tel que $p \mid a_i$.

**Proposition 2.35.** *Soit $n$ un entier tel que $n > 1$ alors il existe un nombre premier $p$ tel que $p \mid n$.*

*Démonstration.* Supposons qu'il existe un entier $n \geq 1$ tel que aucun nombre premier $p$ divise $n$. On pose l'ensemble :

$$E = \{a \in \mathbf{Z},\ a > 1 \text{ et aucun nombre premier ne divise } a\}$$

alors $n \in E$, donc $E \neq \emptyset$. Soit $m \in E$, le plus petit élément de $E$ alors $m > 1$ et $m$ n'est pas un nombre premier. Donc, il existe $d \in \mathbf{Z}$ tel que $d \mid n$ et $1 < d < m$. Mais $d < m$ implique que $d \notin E$ donc il existe un nombre premier $p$ tel que $p \mid d$. Or $p \mid d$ et $d \mid m$, d'où $p \mid m$, ce qui nous mène à une contradiction. □

### 2.7.3 Théorème d'Euclide

**Théorème 2.36** (Euclide)**.** *Il existe une infinité de nombres premiers.*

*Démonstration.* On note $\mathscr{P}$ l'ensemble des nombres premiers. Supposons qu'il est de cardinal fini donc on peut supposer que $\mathscr{P} = \{p_1, p_2, \ldots, p_n\}$. On considère le nombre :

$$N = \prod_{i=1}^{n} p_i + 1.$$

alors $p_i \nmid N$ car s'il existe $i \in \{1, \ldots, n\}$ tel que $p_i \mid N$ alors

$$p_i \mid N - \prod_{i=1}^{n} p_i \Rightarrow p_i \mid 1.$$

On aboutit à une contradiction. D'où l'entier $N$ n'est pas divisible par un nombre premier. □

**Proposition 2.37.** *Soit $n$ un entier tel que $n > 1$. $n$ est un nombre premier si et seulement si $n$ n'admet pas de diviseurs $d$ tel que $1 < d \leq \sqrt{n}$.*

*Démonstration.* ($\Longrightarrow$) C'est évident !

($\Longleftarrow$) Par contraposition, on montrer que si $n$ n'est pas un nombre premier alors $n$ n'admet pas de diviseurs $d$ tel que $1 < d \leq \sqrt{n}$. Comme $n$ n'est pas premier, il existe $k \in \mathbf{Z}$ tel que $k \mid n$ avec $k > 1$. Soit $l$ le plus petit diviseur de $n$ tel que $l > 1$, alors $l$ s'écrit $n = lm$ avec $m \geq l$. On a :

$$m \geq l \Rightarrow ml \geq l^2 \Rightarrow n \geq l^2 \Rightarrow l \leq \sqrt{n}.$$

On peut donc prendre $d = l$.

□

**Exemple 2.38.** On montre que $73$ est premier. On a $\sqrt{73} \leq \sqrt{81} \leq 9$. Ainsi on teste si $k$ divise $73$ avec $k$ nombre premier compris entre $1$ et $9$. On a :

$$2 \nmid 73,\ 3 \nmid 73,\ 5 \nmid 73,\ 7 \nmid 73.$$

D'où, $73$ est bien un nombre premier.

### 2.7.4 Crible d'Erastosthène

Le crible d'Erastosthène de taille $n$ consiste à :
- écrire une liste de tous les entiers $k$ tels que $1 \leq k \leq n$,
- rayer tous les nombres pairs (sauf $2$),
- rayer tous les multiples de $3$ (sauf $3$),
- ...
- rayer tous les multiples de $p$ (sauf $p$), pour $p$ un nombre premier compris entre $1$ et $\sqrt{n}$.

Ainsi, le crible d'Erastosthène de taille $n$ donne tous les nombres premiers qui sont compris entre $1$ et $n$. La figure 2.1 nous donne le crible d'Erastosthène de taille $100$.

**Proposition 2.39.** *Soit $p$ un nombre premier alors $\sqrt{p}$ est irrationnel (c'est-à-dire qu'il n'existe pas d'entiers $a$ et $b$ tels que $\sqrt{p} = \frac{a}{b}$).*

*Démonstration.* On suppose que $\sqrt{p} \in \mathbf{Q}$ alors il existe $a, b \in \mathbf{Z}$ tel que $b \neq 0$ et $\sqrt{p} = \frac{a}{b}$. De plus, on suppose que $\mathrm{PGCD}(a, b) = 1$ (car si $\mathrm{PGCD}(a, b) = d$, on pourra remplacer $a$ par $a' = \frac{a}{d}$ et $b$ par $b' = \frac{b}{d}$). On a :

$$\sqrt{p} = \frac{a}{b} \Rightarrow p = \frac{a^2}{b^2} \Rightarrow a^2 = pb^2.$$

D'où $p \mid a$ donc il existe $k \in \mathbf{Z}$ tel que $a = kp$. On obtient donc :

$$a^2 = k^2p^2 \Rightarrow p^2 \mid a^2 \Rightarrow p^2 \mid pb \Rightarrow p \mid b^2$$

et ainsi, $p \mid b$. On aurait donc $\mathrm{PGCD}(a, b) = p$ mais $p = 1$ et $1$ n'est pas un nombre, on aboutit donc à une contradiction. □

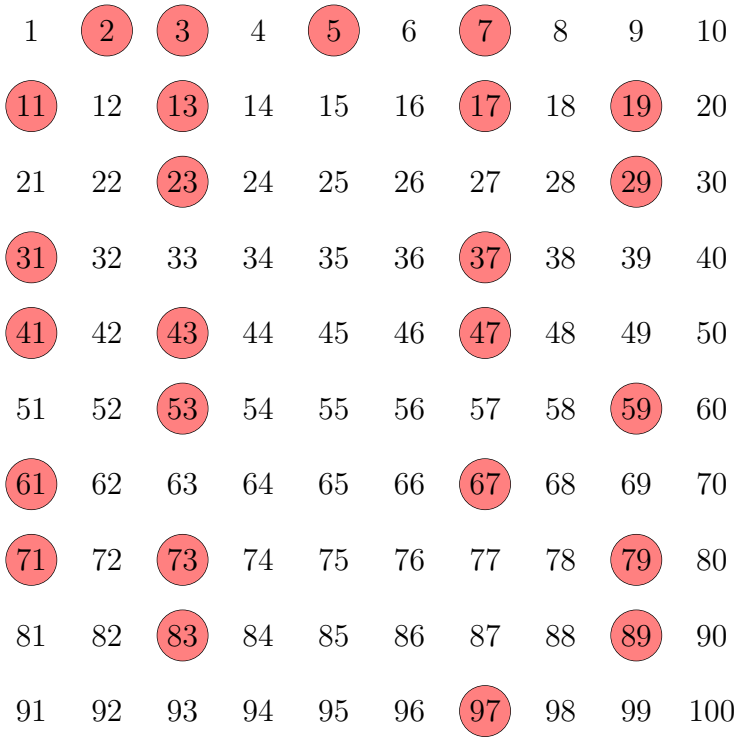


FIGURE 2.1 – Crible d'Erastosthène de taille 100 : les nombres premiers sont entourés en rouge, le reste devrait être rayé

### 2.7.5 Théorème fondamental de l'arithmétique

**Théorème 2.40** (fondamental de l'arithmétique)**.** *Tout entier $n > 1$ peut s'écrire comme un produit de nombres premiers, c'est-à-dire $n$ s'écrit :*

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

*avec $p_1, \ldots, p_k$ des nombres premiers, $a_k$ des nombres entiers supérieur à $1$ et $k \geq 1$. Cette décomposition est unique à l'ordre de facteurs près.*

*Démonstration.* On démontre le théorème par l'absurde. On suppose qu'il existe un entier $n > 1$ qui n'est pas produit de nombres premiers. Soit

$$E = \{a \in \mathbf{Z},\ a > 1 \text{ et } a \text{ n'est pas un nombre premier}\}.$$

$E$ n'est pas un ensemble vide car $n \in E$, donc $E$ possède un plus petit élément $m$. Il existe donc un nombre premier tel que $p \mid n$ et ainsi $m$ s'écrit $m = pm'$ avec $1 < m' < n$. Or $m' < m$, d'où $m' \in E$ et $m'$ est un produit de nombres premiers donc s'écrit :

$$m' = p_1^{b_1} \cdots p_l^{b_l}.$$

Comme

$$m = pm' = pp_1^{b_1} \cdots pp_l^{b_l}$$

, c'est donc bien un produit de nombres premiers.

On montre maintenant l'unicité de la décomposition. Supposons que :

$$n = p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_l^{b_l}$$

avec $p_i$, $q_j$ des nombres premiers. On a donc

$$p_i^{a_i} \mid n \Rightarrow p_i^{a_i} \mid q_1^{b_1} \cdots q_l^{b_l},$$

d'où l'existence d'un indice $1 \leq j \leq l$ tel que $p_i = q_j$ et $b_j \geq a_i$. De même :

$$q_j^{b_j} \mid n \Rightarrow q_j^{b_j} \mid p_1^{a_1} \cdots p_k^{a_k}$$

donc il existe un indice $1 \leq i \leq j$ tel que $p_i = q_j$ et $a_i \geq b_j$. La conclusion de tout cela est que $k = l$, $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_j\}$ et pour tout $i$, il existe $j$ tel que $a_i = b_j$ : c'est bien l'unicité à l'ordre des facteurs près. □

**Exemples 2.41.**

1. $24 = 2^3 \times 3 = 8 \times 4$,
2. $87 = 3 \times 29$,
3. $315 = 3^2 \times 5 \times 7$.

**Corollaire 2.42.** *Soit un entier $n \geq 1$. On peut donc écrire $n = p_1^{a_1} \cdots p_k^{a_k}$ avec $p_1, \ldots, p_k$ des nombres premiers et $a_1, \ldots, a_k$ des entiers positifs. Si $d > 0$ et $d \mid n$ alors $d \mid p_i$, pour tout $1 \leq i \leq k$ et :*

$$d = p_1^{b_1} \cdots p_k^{b_k} \quad \text{avec } 0 \leq b_i \leq a_i.$$

*Le nombre de diviseurs positifs de $n$ est donc $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$.*

*Démonstration.* Soit $p$ un nombre premier tel que $p \mid d$ alors comme $p \mid n$, il existe $1 \leq i \leq k$ tel que $p = p_i$. Donc les diviseurs premiers de $d$ appartiennent à l'ensemble $\{p_1, \ldots, p_k\}$. On écrit $d = p_1^{b_1} \cdots p_k^{b_k}$. Or $d \mid n$, donc $0 \leq b_i \leq a_i$ pour $i \in \{1, \ldots, k\}$. Comme $b_i \in \{0, \ldots, a_i\}$, il y a $a_i + 1$ possibilités pour choisir $b_i$, d'où $(a_1 + 1) \cdots (a_k + 1)$ possibilités pour choisir $d$. □

**Exemple 2.43.** Soit $12 = 2^2 + 3$, donc $p_1 = 2$, $p_2 = 3$, $a_1 = 2$ et $a_2 = 1$. Le nombre de diviseurs de $12$ est $3 \times 2 = 6$.

**Corollaire 2.44.** *Soient $a$ et $b$ des entiers tel que $a > 1$ et $b > 1$. On écrit :*

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad b = p_1^{\beta_1} \cdots p_j^{\beta_j}$$

*avec $p_i$ des nombres premiers et $a_i, b_i \geq 0$. Alors :*

$$\mathrm{PGCD}(a, b) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)},$$
$$\mathrm{PPCM}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_k^{\max(a_k, b_k)}.$$

*Démonstration.*

– Soit $c$ un entier positif. Si $c \mid a$ et $c \mid b$ alors $c$ s'écrit :

$$c = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

avec $\gamma_i \leq a_i$ et $\gamma_i \leq b_i$, d'où $\gamma_i \leq \min(b_i, a_i)$. Ainsi, on obtient que le $\mathrm{PGCD}(a, b) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}$.

– Soit $d$ un entier positif tel que $a \mid d$ et $b \mid d$ alors $d$ s'écrit :

$$d = p_1^{\sigma_1} \cdots p_k^{\sigma_k}$$

avec $\sigma_i \geq a_1$ et $\sigma_i \geq b_i$. D'où $\sigma_1 \geq \max(a_i, b_i)$ et $\mathrm{PPCM}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_k^{\max(a_k, b_k)}$.

□

**Exemple 2.45.** Soit $a = 180$ et $b = 378$. On décompose $a$ et $b$ en facteurs de nombres premiers :

$$180 = 3 \times 2 \times 5 \times 2 \times 3 = 2^2 \times 3^2 \times 5,$$
$$378 = 2 \times 3 \times 3 \times 3 \times 7 = 2 \times 3^3 \times 7.$$

D'où :

$$\mathrm{PGCD}(a, b) = 2 \times 3^2 = 18,$$
$$\mathrm{PPCM}(a, b) = 2^2 \times 3^3 \times 5 \times 7 = 3780.$$

## 2.8 Congruences

### 2.8.1 Premiers résultats

**Définition 2.46** (Congruences)**.** *Soit $n$ un entier tel que $n > 1$ et soient $a$ et $b$ des entiers. On dit que $a$ et $b$ sont* congrus modulo $n$ *(noté $a \equiv b \pmod{n}$) si $n \mid a - b$.*

**Exemples 2.47.** 1. $9 \equiv 1 \pmod{4}$,

2. $19 \equiv -1 \pmod{5}$.

**Remarque 2.48.** On a : $a \equiv 0 \pmod{n}$ si et seulement si $a$ est divisible par $n$ (en vertu de la définition).

**Proposition 2.49.** *(i) La relation « congru modulo » est une relation d'équivalence.*

*(ii) Si $a \equiv b \pmod{n}$ et si $c \equiv d \pmod{n}$ alors $a+c \equiv b+d \pmod{n}$ et $ac \equiv bd \pmod{n}$.*

*(iii) Si $a \equiv b \pmod{n}$ alors, pour tout $k \in \mathbb{N}$, on a : $a^k \equiv b^k \pmod{n}$.*

*Démonstration.* (i) On montre que la relation « congru modulo » est une relation d'équivalence.

**Réflexivité** On a : $a \equiv a \pmod{n}$ car $n \mid a - a$.

**Symétrie** Si $a \equiv b \pmod{n}$, on a alors : $n \mid a - b$, d'où $n \mid b - a$ ou encore $b \equiv a \pmod{n}$.

**Transitivité** On suppose que $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. On a alors $n \mid a - b$ et $n \mid b - c$. En faisant la somme, on obtient :

$$n \mid a - b + b - c \Rightarrow n \mid a - c,$$

d'où le résultat.

Ainsi, « congru modulo » est bien une relation d'équivalence.

(ii) Soit $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ donc on a : $n \mid a - b$ et $n \mid c - d$. D'où :

$$n \mid a - b + c - d \Rightarrow n \mid (a + c) - (b + d) \Rightarrow a + c \equiv b + d \pmod{n}.$$

De plus,

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d),$$

ce qui implique que $n \mid c(a - b) + b(c - d)$ et donc $n \mid ac - bd$.

(iii) On peut démontrer cet énoncé par réccurence sur $k$ en utilisant (ii). □

**Définition 2.50** ($\mathbf{Z}/n\mathbf{Z}$). *Soit $\mathscr{R}$ la relation d'équivalnce définie par :*

$$a\mathscr{R}b \Leftrightarrow a \equiv b \pmod{n}.$$

*La classe de $a$ associée $\mathscr{R}$ est :*

$$\overline{a} = \{x \in \mathbf{Z},\ a \equiv x \pmod{n}\} = \{x \in \mathbf{Z},\ n \mid a - x\}.$$

*On note donc*

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/\mathscr{R} = \{\overline{a},\ a \in \mathbf{Z}\}.$$

**Exemple 2.51.** Soient $n = 3$ et $a = 2$, on a donc :

$$\overline{2} = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Un système de représentant pour $n$ est l'ensemble $\{0, 1, 2, \ldots, n-1\}$. Donc :

$$\mathbf{Z}/n\mathbf{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}.$$

**Exemples 2.52.**

1. Soit $n = 2$, alors $\mathbf{Z}/2\mathbf{Z} = \left\{\overline{0}, \overline{1}\right\}$ et :

$$\begin{aligned}\overline{0} &= \{x \in \mathbf{Z},\ x \equiv 0 \pmod{2}\} = \{x \in \mathbf{Z},\ x \text{ est pair}\},\\ \overline{1} &= \{x \in \mathbf{Z},\ x \equiv 1 \pmod{2}\} = \{x \in \mathbf{Z},\ x \text{ est impair}\}.\end{aligned}$$

2. Soit $n = 2$, alors $\mathbf{Z}/3\mathbf{Z} = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ et :

$$\begin{aligned}\overline{0} &= \{x \in \mathbf{Z},\ x \equiv 0 \pmod{3}\},\\ \overline{1} &= \{x \in \mathbf{Z},\ x \equiv 1 \pmod{3}\},\\ \overline{2} &= \{x \in \mathbf{Z},\ x \equiv 2 \pmod{3}\}.\end{aligned}$$

**Remarque 2.53.** Soit $r$ le reste de la divison euclidienne de $a$ par $n$. On a donc :

$$a = qn + r, \quad \text{avec } 0 \leq r \leq n-1.$$

Alors $a \equiv r \pmod{n}$.

### 2.8.2 Équations de congruences linéaires

**Théorème 2.54.** *Soit $n$ un entier tel que $n > 1$ et soient $a$ et $b$ deux entiers. On considère l'équation :*

$$ax \equiv b \pmod{n} \tag{$E$}$$

*d'inconnue entière $x$ alors :*

*(i)* *($E$) admet une solution si et seulement si* $\mathrm{PGCD}(a, n) \mid b$.

*(ii)* *On pose $d = \mathrm{PGCD}(a, n)$. Si $d \mid b$ alors l'équation ($E$) admet exactement $d$ solutions modulo $n$.*

*Démonstration.* (i) Si $ax \equiv b \pmod{n}$ alors $n \mid ax - b$, ce qui est équivalent à l'existence d'un $y \in \mathbf{Z}$ tel que $(ax - b) = ny$. Donc ($E$) admet une solution si et seulement s'il existe $x, y \in \mathbf{Z}$ tels que $ax - ny = b$, d'où $\mathrm{PGCD}(a, n) \mid b$.

(ii) On pose $d = \mathrm{PGCD}(a, n)$. On suppose donc que $d \mid b$ et on pose alors :

$$a' = \frac{a}{d},\ b' = \frac{b}{d},\ n' = \frac{n}{d}.$$

L'équation ($E$) est donc équivalente à

$$a'x - n'y = b'. \tag{$E'$}$$

Soit $(x_0, y_0)$ une solution particulière de ($E'$). Les solutions de ($E'$) s'écrivent donc :

$$\begin{cases} x = x_0 + kn' \\ y = y_0 + ka' \end{cases}, \quad \text{avec } k \in \mathbf{Z}.$$

En posant $x_k = x_0 + kn'$, on a :

$$\begin{aligned} x_k \equiv x_k \pmod{n} &\Leftrightarrow x_0 + kn' \equiv x_0 + ln' \pmod{n} \\ &\Leftrightarrow n \mid (k - l)n' \Leftrightarrow d \mid k - l. \end{aligned}$$

Ainsi, il y a exactement $d$ solutions de ($E$) modulo $n$ : $x_0, x_1, \ldots, x_{d-1}$ avec :

$$\begin{aligned} x_1 &= x_0 + n', \\ x_2 &= x_0 + 2n', \\ &\vdots \\ x_{d-1} &= x_0 + (d - 1)n'. \end{aligned}$$

car $x_d \equiv x_0 \pmod{n}$.

□

**Exemples 2.55.** 1. Soit l'équation

$$2x \equiv 3 \pmod 5. \tag{2.14}$$

On a : $\mathrm{PGCD}(2,5) = 1$ et $1 \mid 3$, donc il y a exactement une solution modulo $5$. Résoudre 2.14 est équivalent à résoudre l'équation diophantienne suivante :

$$2x - 5y = 3. \tag{2.15}$$

La solution particulière est $(x_0, y_0) = (1, -1)$ et modulo $5$, cela donne $(x_0, y_0) = (1, 4)$ (car $-1 \equiv 4 \pmod 5$).

2. Soit l'équation

$$5x \equiv 4 \pmod 7. \tag{2.16}$$

On a : $\mathrm{PGCD}(5,7) = 1$ donc il y a une solution modulo $7$. Résoudre 2.16 est équivalent à résoudre l'équation diophantienne suivante :

$$5x - 7y = 4. \tag{2.17}$$

La solution particulière est $(x_0, y_0) = (12, 8)$ et modulo $7$, $(x_0, y_0) = (5, 1)$.

### 2.8.3 Petit théorème de Fermat

**Proposition 2.56.** *Soit $p$ un nombre premier alors, pour tout entier $k$ avec $1 \leq k \leq p-1$, on a :*

$$\mathrm{C}_p^k \equiv 0 \pmod p.$$

*Démonstration.* On a :

$$\mathrm{C}_p^k = \frac{p!}{k!(p-k)!} \Rightarrow p! = \mathrm{C}_p^k k!(p-k)!.$$

Or : $p \mid p!$, ce qui implique $p \mid \mathrm{C}_p^k k!(p-k)!$. D'après le lemme d'Euclide, $p \mid \mathrm{C}_p^k$ ou $p \mid k!$ ou $p \mid (p-k)!$. Mais : $k < p$ et $p - k < p$, donc $p \nmid k!$ et $p \nmid (p-k)!$. La seule possibilité est donc $p \mid \mathrm{C}_p^k$. □

**Théorème 2.57** (Petit théorème de Fermat)**.** *Soit $p$ un nombre premier et soit $a$ un entier alors :*

$$a^p \equiv a \pmod p.$$

*Si $p \nmid a$ alors :*

$$a^{p-1} \equiv 1 \pmod p.$$

*Démonstration.* On utilise la formule du binôme de Newton pour développer $(a+1)^p$ :

$$(a+1)^p = a^p + \mathrm{C}_p^1 a^{p-1} + \mathrm{C}_p^2 a^{p-2} + \cdots + \mathrm{C}_p^{p-1} a + 1.$$

D'après la proposition 2.56, on a $p \mid \mathrm{C}_p^k$ si $1 \leq k \leq p-1$ et ainsi :

$$(a+1)^p \equiv a^p + 1 \pmod{p}. \tag{2.18}$$

Supposons que $a > 0$ :

$$\begin{aligned}
(2.18) &\Rightarrow a^p \equiv (a-1)^p + 1 \pmod{p}, \\
&\Rightarrow a^p \equiv (a-2)^p + 2 \pmod{p}, \\
&\vdots \\
&\Rightarrow a^p \equiv 0^p + 1 \pmod{p}.
\end{aligned}$$

On a donc $\equiv a^p ap$. De façon analogue, on montre que $a^p \equiv a \pmod{p}$ pour $a < 0$. On a alors :

$$a^p \equiv a \pmod{p} \Rightarrow p \mid a^p - a \Rightarrow p \mid a(a^{p-1} - 1).$$

D'après le lemme de Gauss, on obtient $p \mid a$ ou $p \mid a^{p-1} - 1$. Or : $p \nmid a$, donc :

$$p \mid a^{p-1} - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

□

## 2.9 Exercices

**Exercice 2.1** ([11])**.** Combien $15!$ admet-il de diviseurs ?

**Exercice 2.2.** Quel est le reste de la division euclidienne de $565$ par $13$ ?

**Exercice 2.3.** Décider si :

1. $13$ et $7$ sont premiers entre eux,
2. $37$ et $20$ sont premiers entre eux,
3. $9$ et $123$ sont premiers entre eux,
4. $38$ et $20$ sont premiers entre eux.

**Exercice 2.4.** Calculer $\mathrm{PGCD}(132, 60)$, $\mathrm{PGCD}(99099, 43928)$ et $\mathrm{PGCD}(-1023, 4561)$.

**Exercice 2.5.** En utilisant l'exercice 2.4, trouver :

1. $x, y \in \mathbf{Z}$ tels que $132x + 60y = 8$,
2. $a, b \in \mathbf{Z}$ tels que $99099a + 43928b = 5$,
3. $u, v \in \mathbf{Z}$ tels que $1023u + 4561v = 1$.

**Exercice 2.6.** Trouver les solutions entières de l'équation :

$$102x - 18018y = 18.$$

Combien y a-t-il de solutions telles que $x$ et $y$ soient compris entre $0$ et $4000$ ?

**Exercice 2.7.** Résoudre dans $\mathbf{Z}$ l'équation :

$$5a + 16b + 6c = 2.$$

**Exercice 2.8.** Dire, en justifiant la réponse, si les énoncés sont vrais ou faux.

1. Si $a$ divise $mn$, $a$ divise $m$ ou $n$.
2. Si $a$ divise $n$ ou $a$ divise $n$, $a$ divise $mn$.
3. Si $a$ divise $mn$ et $a$ ne divise pas $m$, $a$ divise $n$.
4. $\mathrm{PGCD}(a, b) \cdot \mathrm{PPCM}(a, b) = ab$.
5. $\mathrm{PGCD}(a, b, c) = \mathrm{PGCD}(\mathrm{PGCD}(a, b), c)$.
6. Si $a$ divise $42n + 37$ et $7n + 4$, alors $a$ divise $13$.

**Exercice 2.9.** Calculer $\mathrm{PGCD}(n, n + 1)$ et $\mathrm{PPCM}(n, n + 1)$ pour $n \in \mathbf{Z}$.

**Exercice 2.10.** Montrer que, pour tout entier $m$, il existe un $n$ tel que l'intervalle $[m\,, n + m]$ ne contient aucun nombre premier. *Indication : considérer des nombres du type* $n! + k$.

**Exercice 2.11.** Trouver le chiffre des unités de $109^{2007}$ et $23^{23^{23}}$.

**Exercice 2.12.** Quel est le reste de la division euclidienne de $\sum_{k=1}^{k=2002} k!$ par $15$ ?

**Exercice 2.13.** Résoudre les congruences :

1. $20x \equiv 3 \pmod{10}$,
2. $123x \equiv 7 \pmod{5}$,
3. $107x \equiv 112 \pmod{11}$.

# Chapitre 3

# Groupes, anneaux et corps

## 3.1 Groupes

### 3.1.1 Définitions et exemples

**Définition 3.1** (Groupe)**.** *Soit $G$ un ensemble non vide muni d'une* opération *(ou une* loi de composition *notée « $*$ ») :*

$$\begin{array}{rccc} * & : & G \times G & \to & G \\ & & (x, y) & \mapsto & x * y \end{array}.$$

*On dit que $(G, *)$ est un* groupe *si :*

*(i) pour tout $x \in G$, pour tout $y \in G$, $x * y \in G$. On dit alors que $G$ est* stable *par la loi de composition.*

*(ii) Pour tout $x, y, z \in G$, on a :*

$$x * (y * z) = (x * y) * z.$$

*On dit que la loi de composition est* associative*.*

*(iii) Il existe $e \in G$, qu'on appelle* élément neutre *tel que pour tout $x \in E$,*

$$x * e = e * x = x.$$

*(iv) Tout élément de $G$ admet un* inverse *(on dit aussi que tout élément de $G$ est* inversible*), c'est-à-dire :*

$$\forall x \in G,\ \exists y \in G, \quad x * y = e \text{ et } y * x = e,$$

*$y$ est appelé l'*inverse *de $x$ et on note $y = x^{-1}$.*

**Remarques 3.2.** 1. Si, en plus, on a :

$$\forall x, y \in G, \quad x * y = y * x,$$

on dit que $(G, *)$ est un groupe *abélien* ou *commutatif*.

2. Soit $(G, *)$ un groupe, on peut montrer que l'élément neutre $e$ et l'élément inverse $y = x^{-1}$ sont uniques.

*Démonstration de la remarque 3.2-2.* On montre tout d'abord que l'élément neutre $e$ est unique. Supposons que $e$ et $e'$ sont deux éléments neutres de $(G, *)$ alors on a,

$$x * e = e * x = x, \tag{3.1}$$
$$x * e' = e' * x = x. \tag{3.2}$$

Si on remplace dans (3.1), $x$ par $e'$ et dans (3.2), $x$ par $e$, on obtient :

$$e * e' = e' * e,$$

c'est-à-dire $e = e'$.

On démontre finalement que l'élément inversible $y = x^{-1}$ est unique. Supposons que $y$ et $y'$ sont deux éléments inversibles de $x$ dans $(G, *)$, alors on a :

$$x * y = y * x = e, \tag{3.3}$$
$$x * y' = y' * x = e. \tag{3.4}$$

En tenant compte de (3.3) et (3.4), on obtient :

$$(y' * x) * y = y' * (x * y) \Rightarrow e * y = e * y',$$

d'où $y = y'$. □

**Exemples 3.3.** 1. $(\mathbf{Z}, +)$ est un groupe abélien avec $0$ comme élément neutre et d'inverse $x^{-1} = -x$, pour $x \in \mathbf{Z}$.

2. $(\mathbf{R}, +)$ est un groupe abélien avec $0$ comme élément neutre et d'inverse $x^{-1} = -x$, pour $x \in \mathbf{R}$.

3. $(\mathbf{Q}^*, \times)$ est un groupe abélien avec $1$ comme élément neutre et d'inverse $x^{-1} = \frac{1}{x}$, pour $x \in \mathbf{Q}$.

4. $(\mathbf{R}^*, \times)$ est un groupe abélien.

### 3.1.2 Sous-groupes

**Définition 3.4.** *Soient $(G, *)$ un groupe et $H$ un sous-ensemble de $G$. On dit que $(H, *)$ est un* sous-groupe *de $G$ si $(H, *)$ est un groupe lui-même.*

**Proposition 3.5.** *Soient $(G, *)$ un groupe, $e$ l'élément neutre de $(G, *)$ et $H$ un sous-ensemble de $G$. Alors $(H, *)$ est un sous-groupe de $(G, *)$ si :*

*(i)* $e \in H$,

*(ii) pour tout* $x, y \in H$, $x * y \in H$,

*(iii) pour tout* $x \in H$, $x^{-1} \in H$.

*Démonstration.* On vérifie les propriétés (i)-(iv) de la définition d'un groupe pour $(H, *)$ :

(i) Cette propriété est vérifié par la condition (ii) de la proposition.

(ii) L'opération $*$ est associative sur $H$ car elle est associative sur $G$.

(iii) Il existe un élément neutre dans $H$ grâce à la condition (i) de la proposition.

(iv) Chaque élément $x \in H$ admet un inverse par la condition (iii) de la proposition.

□

**Exemples 3.6.**

1. $(\mathbf{Z}, +)$ et $(\mathbf{Q}, +)$ sont des sous-groupes de $(\mathbf{R}, +)$.
2. $(\mathbf{Q}^*, \times)$ est un sous-groupe de $(\mathbf{R}^*, \times)$.
3. On montre que si $H = \{-1, 1\}$, $(H, \times)$ est un sous-groupe de $(\mathbf{R}^*, times)$. Pour cela, il suffit de vérifier les trois assertions de la proposition 3.5.
   (i) $1$ est l'élément neutre de $(\mathbf{R}^*, \times)$ et $1$ est bien dans $H$.
   (ii) Il faut vérifier que pour tout $x, y \in H$, on ait bien $x \times y \in H$. Mais :
   $$1 \times 1 = 1,\ 1 \times -1 = -1,\ -1 \times -1 = 1,\ -1 \times 1 = -1.$$
   (iii) On montre que pour tout $x \in H$, il existe $y \in H$ tel que $x \times y = y \times x = e$. Si $x = 1$, on prend $y = 1$ et si $x = -1$, on prend $y = -1$.
4. Soient $G = (\mathbf{R}^*, \times)$ et $H' = \left\{1, 2, \frac{1}{2}\right\}$. Cette fois-ci, on montre que $(H', \times)$ n'est pas un sous-groupe de $G$. On a bien l'élément neutre $(1)$ de $G$ dans $H'$ mais on a $2 \times 2 = 4$ et $4$ n'appartient pas $H'$. D'où $H'$ n'est pas un sous-groupe de $G$.

**Définition 3.7** (Puissance d'un élément d'un groupe)**.** *Soient* $(G, *)$ *un groupe,* $e$ *l'élément neutre de* $G$ *et* $x \in G$*. Soit* $n \in \mathbf{Z}$*, on note :*

$$x^n = \begin{cases} e & \textit{si } n = 0, \\ \underbrace{x * x * \cdots * x}_{n \textit{ fois}} & \textit{si } n > 0, \\ \underbrace{x^{-1} * x^{-1} * \cdots * x^{-1}}_{n \textit{ fois}} & \textit{si } n < 0. \end{cases}$$

**Exemple 3.8.** Si $x \in G$ alors $x^{-2} = x^{-1} * x^{-1}$.

**Remarque 3.9.** Si l'opération est l'addition alors $x^n = x + x + \cdots + x = nx$.

**Définition 3.10** (Sous-groupe engendré)**.** *On appelle* sous-groupe engendré *par* $x$*, le plus petit (au sens inclusion) sous-groupe de* $G$ *qui contient* $x$*. On peut noter ce sous-groupe* $\langle x \rangle$ *et on dit que* $x$ *est un* générateur *du groupe* $\langle x \rangle$*. On peut aussi noter :*

$$\langle x \rangle = \{x^n,\ n \in \mathbf{Z}\}.$$

**Exemple 3.11.** Soient $G = (\mathbf{Z}, +)$ et $a \in \mathbf{Z}$, on définit :

$$\langle a \rangle = \{na,\ n \in \mathbf{Z}\} = a\mathbf{Z}.$$

Pour $a = 2$, $\langle 2 \rangle = 2\mathbf{Z}$ correspond à l'ensemble des nombres pairs.

### 3.1.3 Étude du groupe $\mathbf{Z}/n\mathbf{Z}$

$\mathbf{Z}/n\mathbf{Z}$

On rappelle que la relation :

$$x \mathscr{R} y \Leftrightarrow a \equiv b \pmod{n}$$

est une relation d'équivalence sur $\mathbf{Z}$ et la définition 2.50 :

**Définition 3.12** ($\mathbf{Z}/n\mathbf{Z}$)**.** *Soit* $\mathscr{R}$ *la relation d'équivalnce définie par :*

$$a \mathscr{R} b \Leftrightarrow a \equiv b \pmod{n}.$$

*La classe de* $a$ *associée* $\mathscr{R}$ *est :*

$$\overline{a} = \{x \in \mathbf{Z},\ a \equiv x \pmod{n}\} = \{x \in \mathbf{Z},\ n \mid a - x\}.$$

*On note donc*

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/\mathscr{R} = \{\overline{a},\ a \in \mathbf{Z}\}.$$

On va montrer dans ce paragraphe que l'ensemble $\mathbf{Z}/n\mathbf{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$ forme un groupe avec des opérations bien précises.

### Addition dans $\mathbf{Z}/n\mathbf{Z}$

On définit l'addition dans $\mathbf{Z}/n\mathbf{Z}$ :

**Définition 3.13** (Addition dans $\mathbf{Z}/n\mathbf{Z}$)**.** *L'opération* $\oplus$ *correspond à l'*addition *dans* $\mathbf{Z}/n\mathbf{Z}$ *:*

$$\begin{array}{rccc} \oplus & : & \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} & \to & \mathbf{Z}/n\mathbf{Z} \\ & & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \oplus \overline{b} = \overline{a+b} \end{array}.$$

**Remarque 3.14.** Cette opération est bien définie, c'est-à-dire qu'elle est indépendante du choix d'un représentant :

$$\begin{aligned} \overline{a} = \overline{a'} \text{ et } \overline{b} = \overline{b'} \Rightarrow a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \\ \Rightarrow a + b \equiv a' + b' \pmod{n} \Rightarrow \overline{a+b} = \overline{a'+b'}. \end{aligned}$$

**Exemple 3.15.** On se place dans $\mathbf{Z}/4\mathbf{Z}$ :

1. $\overline{3} \oplus \overline{2} = \overline{3+2} = \overline{5} = \overline{1}$,
2. $\overline{7} \oplus \overline{3} = \overline{7+3} = \overline{10} = \overline{2}$.

**Proposition 3.16.** $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ *est un groupe abélien avec* $e = \overline{0}$ *et* $\overline{a}^{-1} = -\overline{a}$*.*

*Démonstration.* En exercice. □

### Multiplication dans $\mathbf{Z}/n\mathbf{Z}$

**Définition 3.17** (Multiplication dans $\mathbf{Z}/n\mathbf{Z}$)**.** *On définit une* multiplication *dans* $\mathbf{Z}/n\mathbf{Z}$ *:*

$$\begin{array}{rccc} \otimes & : & \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} & \to & \mathbf{Z}/n\mathbf{Z} \\ & & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \otimes \overline{b} = \overline{a \cdot b} \end{array}.$$

**Remarque 3.18.** Cette opération est bien définie car si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$ alors :

$$a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n} \Rightarrow \overline{ab}a'b'.$$

Mais $(\mathbf{Z}/n\mathbf{Z}, \otimes)$ n'est pas un groupe car il existe des éléments non inversibles. Par exemple, on se place dans $\mathbf{Z}/4\mathbf{Z}$ et on regarde la classe $\overline{2} \in \mathbf{Z}/4\mathbf{Z}$ :

$$\begin{aligned} \overline{2} \otimes \overline{0} &= \overline{2 \times 0} = \overline{0} \\ \overline{2} \otimes \overline{1} &= \overline{2 \times 1} = \overline{2} \\ \overline{2} \otimes \overline{2} &= \overline{2 \times 2} = \overline{0} \\ \overline{2} \otimes \overline{3} &= \overline{2 \times 3} = \overline{2} \end{aligned}$$

La classe de $2 \in \mathbf{Z}/4\mathbf{Z}$ n'est donc pas inversible.

Pour cela, on va réduire l'ensemble $\mathbf{Z}/n\mathbf{Z}$ en son ensemble des éléments inversibles pour l'opération $\otimes$.

**Définition 3.19** ($(\mathbf{Z}/n\mathbf{Z})^\times$)**.** *On définit l'ensemble* $(\mathbf{Z}/n\mathbf{Z})^\times$*, l'ensemble de toutes les classes* $\overline{a}$ *inversibles par la multiplication.*

**Proposition 3.20.** $((\mathbf{Z}/n\mathbf{Z})^\times, \otimes)$ *forme un groupe abélien.*

**Exemple 3.21.** On se place dans l'ensemble $\mathbf{Z}/4\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. On veut déterminer $(\mathbf{Z}/4\mathbf{Z})^\times$. On a vu que $\overline{2}$ n'est pas inversible pour $\otimes$ et, évidemment, $\overline{0}$ n'est pas inversible pour $\otimes$. On cherche donc les inverses des éléments $\overline{1}$ et $\overline{3}$, on a :

$$\overline{1}^{-1} = \overline{1}, \quad \overline{3}^{-1} = \overline{3}.$$

D'où :

$$(\mathbf{Z}/4\mathbf{Z})^\times = \{\overline{1}, \overline{3}\}$$

et c'est un groupe pour la multiplication.

**Proposition 3.22.** $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ *est inversible pour la multiplication si et seulement si* $\mathrm{PGCD}(a, n) = 1$.

*Démonstration.* ($\Rightarrow$) On suppose $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ inversible donc il existe $b \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{a} \otimes \overline{b} = \overline{1}$. On traduit cela en terme de la relation « congru modulo » :

$$ab \equiv 1 \pmod{n}$$

, il existe donc $k \in \mathbf{Z}$ tel que $ab - nk = 1$, d'où $\mathrm{PGCD}(a, n) = 1$.

($\Leftarrow$) On suppose que $\mathrm{PGCD}(a, b) = 1$, il existe donc $u, v \in \mathbf{Z}$ tel que $au + bv = 1$, c'est-à-dire :

$$\overline{au + nv} = 1 \Rightarrow \overline{au} = \overline{1}.$$

Donc $\overline{a}$ est inversible d'inverse $\overline{u}$.

□

**Définition 3.23** (Fonction indicatrice d'Euler)**.** *L'*indicatrice d'Euler $\varphi\colon \mathbf{N}^* \to \mathbf{N}^*$ *est une fonction telle que :*

$$\varphi(1) = 1, \quad \varphi(n) = \mathrm{card}\left\{k \in \{1, \ldots, n\},\ \mathrm{PGCD}(k, n) = 1\right\}, \ \textit{pour } n > 1.$$

*C'est-à-dire* $\varphi(n)$ *est le nombre d'entiers postifs et premiers à* $n$.

**Corollaire 3.24.** *L'ensemble* $(\mathbf{Z}/n\mathbf{Z})^\times$ *est l'ensemble des classes* $\overline{a}$ *tels que* $\mathrm{PGCD}(a, n) = 1$. *D'après la définition 3.23,* $(\mathbf{Z}/n\mathbf{Z})^\times$ *a pour cardinal* $\varphi(n)$.

**Proposition 3.25.** *Si* $p$ *est un nombre premier alors* $\varphi(p) = p - 1$.

**Exemple 3.26.** Pour $n = 5$, $(\mathbf{Z}/5\mathbf{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$. On a $\varphi(5) = 4$ et pour $1 \leq k \leq 5$, on obtient $\mathrm{PGCD}(k, 5) = 1$ si $k \neq 5$. Pour $n = 9$, on obtient :

$$(\mathbf{Z}/9\mathbf{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}.$$

D'où $\varphi(9) = 6$.

### 3.1.4 Homomorphismes de groupes

**Définition 3.27** (Homomorphisme de groupes)**.** *Soient $(G, *)$ et $(G', \square)$ deux groupes et $f : G \to G'$ une application. On dit que $f$ est un* homomorphisme *(ou* morphisme*) de groupe si :*

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

*Si $G = G'$, on dit que $f$ est un* endomorphisme*. Si $f$ est un homomorphisme bijective, on dit que $f$ un* isomorphisme *et, de plus, $f$ est un endomorphisme, on dit que $f$ est un* automorphisme*.*

**Proposition 3.28.** *Soient $G$ et $G'$ deux groupes, $f : G \to G'$ un homomorphisme de groupe et soient $e$ (resp. $e'$) élément neutre de $G$ (resp. élémént neutre de $G'$) alors :*

*(i)* $f(e) = e'$*,*

*(ii) pour tout* $x \in G$*,* $f(x^{-1}) = f(x)^{-1}$*.*

*Démonstration.* (i) On a :

$$f(e) \square f(e) = f(e * e) = f(e) = f(e) \square e'.$$

On peut donc simplier par $f(e)$ pour obtenir $f(e) = e'$.

(ii) Soit $x \in G$, on a :

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

De même :

$$f(x) \square f(x^{-1}) = e',$$

d'où le résultat.

□

**Définition 3.29** (Image et noyau d'un morphisme)**.** *Soient $f : G \to G'$ un morphisme de groupe et $e$ (resp. $e'$) l'élément neutre de $G$ (resp. de $G'$). Le* noyau *de $f$ (noté $\ker(f)$) est l'ensemble*

$$\ker(f) = \{x \in G,\ f(x) = e'\} = f^{-1}(\{e'\}).$$

*L'*image *de $f$ est l'ensemble :*

$$\mathrm{Im}(f) = \{f(x),\ x \in G\} = f(G).$$

**Remarque 3.30.** Comme $f(e) = e'$, on a : $e' \in \ker(f)$ et $e' \in \mathrm{Im}(f)$.

**Proposition 3.31.** *Soit $f : G \to G'$ un homomorphisme de groupe. Alors :*

*(i)* $\ker(f)$ *est un sous-groupe de* $G$.

*(ii)* $\mathrm{Im}(f)$ *est un sous-groupe de* $G'$.

*(iii)* $f$ *est injective si et seulement si* $\ker(f) = \{e\}$.

*(iv)* $f$ *est surjective si et seulement si* $\mathrm{Im}(f) = G'$.

*Démonstration.* (i) 1. $e \in \ker(f)$.

2. Si $x, y \in \ker(f)$, on a :

$$f(x) = f(y) = e' \Rightarrow f(x * y) = f(x) \square f(y) = e' \square e' = e'.$$

D'où $x * y \in \ker(f)$.

3. Soit $x \in \ker(f)$, on veut montrer que $x^{-1}$ appartient à $\ker(f)$.

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

D'où $x^{-1} \in \ker(f)$.

En conclusion, $\ker(f)$ est un sous-groupe de $G$.

(ii) 1. $e' \in \mathrm{Im}(f)$.

2. Si $x', y' \in \mathrm{Im}(f)$ alors il existe $x \in G$ tel que $f(x) = x'$ et il existe $y \in G$, $f(y) = y'$. D'où :

$$x' \square y' = f(x) \square f(y) = f(x * y)$$

et $x * y \in \mathrm{Im}(f)$.

3. Si $x' \in \mathrm{Im}(f)$ alors il existe $x \in G$ tel que $f(x) = x'$. Ainsi,

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

D'où $x'^{-1} \in \mathrm{Im}(f)$.

$\mathrm{Im}(f)$ est donc un sous-groupe de $G'$.

(iii) On veut montrer que $f$ est injective si et seulement si $\ker(f) = e$.

($\Rightarrow$) Soit $x \in \ker(f)$ alors $f(x) = e$. Comme $f$ est injective, on a : $e = f(e)$, ce qui implique que $x = e$. Donc $\ker(f) = e$.

($\Leftarrow$) On suppose que $f(x) = f(y)$ alors

$$f(x) \square f(y^{-1}) = f(x * y^{-1}) = f(x) \square f(y)^{-1} = f(x) \square f(x)^{-1} = e'.$$

D'où $x * y^{-1} \in \ker(f) = \{e\}$ donc

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

Conclusion, on a bien $x = y$ et $f$ est injective.

(iv) L'assertion est claire, c'est la définition de la surjectivité.

□

### 3.1.5 Groupes de permutations

On rappelle la définition d'une permutation.

**Définition 3.32** (Permutation)**.** *Soit $n$ un entier tel que $n \geq 1$. Une* permutation *est une application $\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$.*

**Exemple 3.33.** L'application $\sigma\colon \{1,2,3\} \to \{1,2,3\}$ telle que :

$$\sigma(1) = 3,\ \sigma(2) = 2,\ \sigma(3) = 1$$

est une permutation.

**Définition 3.34** (Ensemble des permutations)**.** *On note $\mathscr{S}_n$ l'*ensemble des permutations *de $n$ éléments. Il y a $n!$ élément dans $\mathscr{S}_n$.*

**Définition 3.35** (Composition)**.** *L'opération suivante :*

$$\begin{array}{rccc} \circ & : & \mathscr{S}_n \times \mathscr{S}_n & \to & \mathscr{S}_n \\ & & (\sigma,\tau) & \mapsto & \sigma\circ\tau \end{array}$$

*tel que pour tout $n$, $(\sigma\circ\tau)(n) = \sigma(\tau(n))$ est appelée* composition*.*

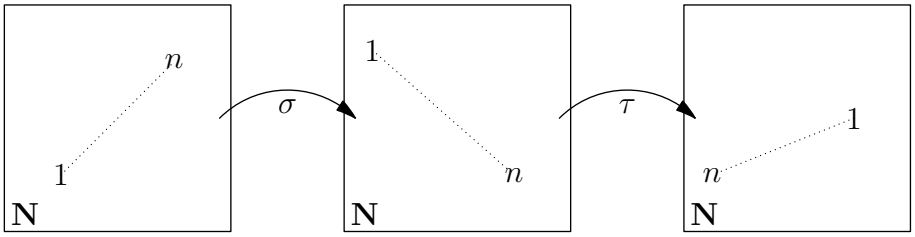


FIGURE 3.1 – Composition

**Proposition 3.36.** *$(\mathscr{S}_n, \circ)$ est un groupe d'élément neutre* $\mathrm{id}$ *(tel que* $\mathrm{id}(n) = n$ *et si $\sigma \in \mathscr{S}_n$ alors $\sigma^{-1}$ est l'inverse de $\sigma$ ($\sigma^{-1}\circ\sigma = \mathrm{id}$).*

**Remarque 3.37.** Si $n \leq 2$ alors $(\mathscr{S}_n, \circ)$ est un groupe abélien. Si $n > 2$ alors $(\mathscr{S}_n, \circ)$ n'est pas un groupe abélien.

**Exemple 3.38.** On se place dans l'ensemble $\mathscr{S}_3$. On considère $\sigma, \tau \in \mathscr{S}_3$ tels que :

$$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1,$$
$$\tau(1) = 2,\ \tau(1) = 2,\ \tau(3) = 3.$$

On a alors :

$$(\sigma\circ\tau)(1) = \sigma(\tau(1)) = \sigma(2) = 3,$$
$$(\tau\circ\sigma)(1) = \tau(\sigma(1)) = \tau(2) = 1.$$

D'où $\sigma\circ\tau \neq \tau\circ\sigma$.

## 3.2 Anneaux

### 3.2.1 Anneaux

**Définition 3.39** (Anneaux)**.** *Soit $A$ un ensemble muni de deux opérations appelés* addition *(notée $+$) et* multiplication *(notée $\cdot$). On dit que $(A, +, \cdot)$ est un* anneau *si :*

1. *$(A, +)$ est un groupe commutatif, on note $e$ l'élément neutre et $-x$ l'inverse de $x \in A$ pour l'addition.*
2. *$A$ est stable par multiplication.*
3. *La multiplication est associative.*
4. *Il existe un élément neutre $e'$ pour la multiplication.*
5. *Pour tout $x, y, z \in A$, on a :*

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

**Remarque 3.40.** Si, en plus, la multiplication est commutatif, on dit que $A$ est un *anneau commutatif*.

**Exemples 3.41.**
1. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ sont des anneaux commutatifs,
2. $\mathbf{Z}/n\mathbf{Z}$ est un anneau commutatif,
3. $\mathscr{S}_3$ n'est pas un anneau (car il n'y a pas de seconde opération).

### 3.2.2 Sous-anneaux

**Définition 3.42.** *Soit $(A, +, \cdot)$ un anneau et $B \subset A$. On dit que $B$ est un* sous-anneau *de $A$ si $(B, +, \cdot)$ est un anneau.*

**Proposition 3.43.** *Soit $(A, +, \cdot)$ un anneau et $B \subset A$. $(B, +, \cdot)$ est un sous-anneau si et seulement si*

*(i) $(B, +) \subset (A, +)$ est un sous-groupe,*

*(ii) $B$ est stable par multiplication,*

*(iii) et, si on note $e'_A$ l'élément neutre multiplicatif de $A$, $e'_A \in B$.*

**Exemple 3.44.** $(\mathbf{Z}, +, \cdot)$ et $(\mathbf{Q}, +, \cdot)$ sont des sous-anneaux de $(\mathbf{R}, +, \cdot)$.

# 3.3 Corps

## 3.3.1 Corps

**Définition 3.45** (Corps)**.** *Soit $(K, +, \cdot)$ un anneau. On dit que $K$ est un* corps *si tout élément non nul de $K$ est inversible par multiplication et $(K^\times, \cdot)$ est un groupe. On dit que $K$ est un* corps commutatif *si la multiplication dans $K$ est commutative.*

**Exemple 3.46.** $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont des corps commutatifs.

## 3.3.2 Sous-corps

**Définition 3.47.** *Soient $(K, +, \cdot)$ un corps et $L \subset K$. $L$ est un* sous-corps *si $(L, +, \cdot)$ est un corps.*

**Proposition 3.48.** *Soient $(K, +, \cdot)$ un corps et $L \subset K$. $(L, +, \cdot)$ est un corps si et seulement si :*

1. *$(L, +, \cdot) \subset (K, +, \cdot)$ est un sous-anneau,*
2. *pour tout $x \in L^\times$, $x^{-1} \in L$.*

# 3.4 Exercices

**Exercice 3.1.** Dans $\mathbf{R}$, on définit l'opération $\cdot$ par

$$x \cdot y = \mathrm{e}^{x+y}$$

où $x + y$ est la somme usuelle de deux réels. $(\mathbf{R}, \cdot)$ est-il un groupe ?

**Exercice 3.2.** Soient $G$ un groupe et $H$ et $K$ deux sous-groupes de $G$.

1. Montrer que $H \cap K$ est un sous-groupe de $G$.
2. Montrer que $H \cup K$ est un sous-groupe de $G$ si et seulement si $H \subset K$ ou $K \subset H$.

**Exercice 3.3.** Montrer que l'ensemble

$$\left\{ \frac{1+2n}{1+2m},\ n, m \in \mathbf{Z} \right\}$$

est un sous-groupe de $(\mathbf{Q}^*, \cdot)$.

**Exercice 3.4.** Soit $G$ un groupe fini de cardinal un nombre premier $p$. Montrer que $G$ est cyclique et déterminer le nombre de générateurs de $G$.

**Exercice 3.5.** Écrire la table d'addition de $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$ et $\mathbf{Z}/8\mathbf{Z}$.

**Exercice 3.6.**
1. Déterminer le cardinal de $\mathbf{Z}/7\mathbf{Z}$, $(\mathbf{Z}/7\mathbf{Z})^\times$, $(\mathbf{Z}/30\mathbf{Z})^\times$, $(\mathbf{Z}/100\mathbf{Z})^\times$.
2. Écrire la table de multiplication $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$ et $\mathbf{Z}/8\mathbf{Z}$.

**Exercice 3.7.** Soit l'application

$$\begin{array}{rccc} f & : & \mathbf{Z} & \to & \mathbf{Q}^* \\ & & n & \mapsto & 2^n \end{array}.$$

Montrer que $f$ est un homomorphisme de groupes. Déterminer $\ker(f)$, $\mathrm{Im}(f)$ et $f^{-1}(\mathbf{N})$. Est-ce que $f$ est injecitve ? surjective ?

**Exercice 3.8.**
1. Décrire les éléments du groupe symétrique $\mathscr{S}_3$.
2. Montrer que, pour tout $\sigma \in \mathscr{S}_3$, le sous-groupe engendré par $\sigma$ est différent de $\mathscr{S}_3$.
3. Montrer que les groupes $\mathbf{Z}/6\mathbf{Z}$ et $\mathscr{S}_3$ ne sont pas isomorphes.
4. Montrer qu'il existe deux éléments $\rho, \sigma \in \mathscr{S}_3$, tels que le sous-groupe engendré par $\rho$ et $\sigma$ est égal à $\mathscr{S}_3$.

**Exercice 3.9.**
1. Soit $\mathbf{Z}[\mathrm{i}] = \{a + \mathrm{i}b,\ a, b \in \mathbf{Z}\}$ (appelé l'*ensemble des entiers de Gauss*). Montrer que $(\mathbf{Z}[\mathrm{i}], +, \cdot)$ est un anneau. Est-il un corps ? Déterminer les éléments inversibles pour la multiplication de $\mathbf{Z}[\mathrm{i}]$.
2. Soit $\mathbf{Q}[i] = \{a + \mathrm{i}b,\ a, b \in \mathbf{Q}\}$. Montrer que $\mathbf{Q}[\mathrm{i}]$ est un corps (on dit que $\mathbf{Q}[i]$ est le corps des fractions de $\mathbf{Z}[\mathrm{i}]$).
3. Soit $\mathbf{Q}[\sqrt{3}] = \left\{a + b\sqrt{3},\ a, b \in \mathbf{Q}\right\}$. Montrer que $(\mathbf{Q}[\sqrt{3}], +, \cdot)$ est un corps.

# Chapitre 4

# Nombres complexes

## 4.1 Introduction

Il y a deux raisons pour justifier la construction d'un ensemble beaucoup plus grand que $\mathbf{R}$ :

1. Considérons l'équation $x^2 = 1$ : cette équation a deux solutions dans $\mathbf{R}$ qui sont $1$ et $-1$. Que se passe-t-il si on remplace $1$ par $-1$ ? On est un plus embêté car aucun nombre réel admet un carré négatif. Alors décidons que $\mathrm{i}$ serait une des solutions de cette équation, c'est-à-dire que $\mathrm{i}^2 = -1$. L'équation aurait donc deux solutions dans un autre ensemble de nombres : $\mathrm{i}$ et $-\mathrm{i}$ car $x^2 + 1 = 0$ équivaudrait à $x^2 - \mathrm{i}^2 = 0$ ou soit $(x - \mathrm{i})(x + \mathrm{i}) = 0$. On posera donc $\mathbf{C} = \{a + \mathrm{i}b,\ a, b \in \mathbf{R}\}$ et l'élément $a + \mathrm{i}b$ serait solution de l'équation $x^2 = -b^2 + a^2$.
2. Dans le courant du XVI$^{\mathrm{e}}$ siècle, la formule de Cartan-Tartaglia donnant les racines du polynôme $x^3 + px + q$ posa un problème au mathématicien Raphaël Bombelli. Il essaya la formule pour le polynôme $x^3 - 15x = 4$ et obtient :
$$x = \sqrt[3]{2 - 11\sqrt{-1}} + \sqrt[3]{2 + 11\sqrt{-1}}.$$
Se retrouver avec une racine carré négatif est impensable dans $\mathbf{R}$ !

## 4.2 Définition de l'ensemble $\mathbf{C}$

**Définition 4.1** ($\mathbf{C}$)**.** *On définit l'*ensemble des complexes

$$\mathbf{C} = \{a + \mathrm{i}b,\ a, b \in \mathbf{R}\}$$

*avec* $\mathrm{i}^2 = -1$.

**Définition 4.2** (Interprétation géométrique)**.** *On peut aussi identifier* $\mathbf{C}$ *comme* $\mathbf{R}^2$*, c'est-à-dire que à un point* $M : (a, b)$*, on peut lui faire correspondre un* $z = a + \mathrm{i}b$ *et vice et versa. On dira que* $z = a + \mathrm{i}b$ *est l'*affixe *du point* $M : (a, b)$.

**Définition 4.3** (Opérations dans $\mathbf{C}$)**.** *On définit une* addition *et une* multiplication *dans* $\mathbf{C}$*. Si* $z = a + \mathrm{i}b \in \mathbf{C}$ *et* $z' = a' + \mathrm{i}b' \in \mathbf{C}$*, on a :*

$$z + z' = (a + \mathrm{i}b) + (c + \mathrm{i}d) = (a + c) + \mathrm{i}(b + d),$$
$$z \cdot z' = (a + \mathrm{i}b) \cdot (c + \mathrm{i}d) = ac - bd + \mathrm{i}(ad + bc)$$

**Définition 4.4** (Inverse)**.** *Si* $z = a + \mathrm{i}b \neq 0$*, l'*inverse *de* $z$ *est :*

$$\frac{1}{z} = \frac{1}{a + \mathrm{i}b} = \frac{a - \mathrm{i}b}{(a + \mathrm{i}b)(a - \mathrm{i}b)} = \frac{a - \mathrm{i}b}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \mathrm{i}\frac{b}{a^2 + b^2}.$$

**Définition 4.5** (Partie réelle et imaginaire)**.** *Soit* $z = a + \mathrm{i}b \in \mathbf{C}$*. On appelle* $a$*, la* partie réelle *de* $z$ *(qu'on note* $\mathrm{Re}(z)$*) et* $b$*, la* partie imaginaire *(qu'on note* $\mathrm{Im}(z)$*).*

**Définition 4.6** (Conjugé complexe)**.** *Si* $z = a + \mathrm{i}b \in \mathbf{C}$*, on définit le* conjugué complexe *de* $z$*,*

$$\overline{z} = a - \mathrm{i}b.$$

**Propriétés 4.7.** *Soit* $z, z' \in \mathbf{C}$*,*

1. $z = \overline{z}$ *si et seulement si* $z \in \mathbf{R}$.
2. $\overline{\overline{z}} = z$.
3. $2\,\mathrm{Re}(z) = z + \overline{z}$ *et* $2\mathrm{i}\,\mathrm{Im}(z) = z - \overline{z}$.
4. $\overline{z + z'} = \overline{z} + \overline{z'}$.
5. $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$.
6. $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}}$.

*Démonstration.* On démontre la propriété 4.7-3. On pose : $z = a + b\mathrm{i}$ et $\overline{z} = a - b\mathrm{i}$. On a donc :

$$z + \overline{z} = 2a = 2\,\mathrm{Re}(z),$$
$$z - \overline{z} = 2\mathrm{i}b = 2\mathrm{i}\,\mathrm{Im}(z).$$

□

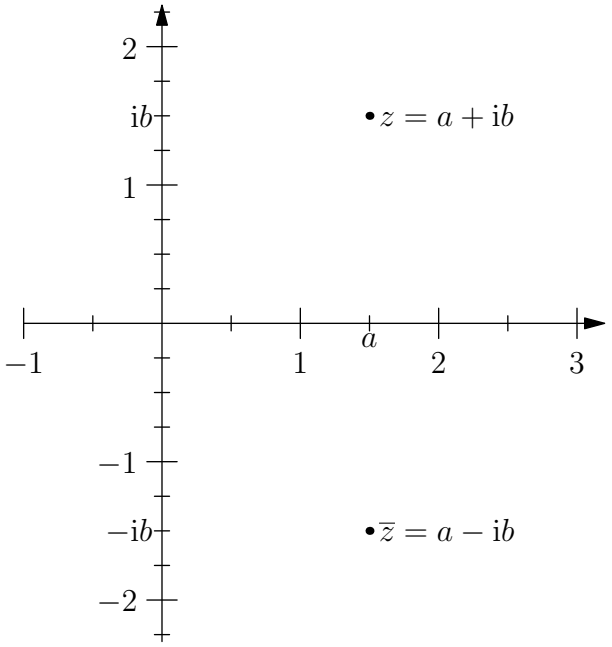


FIGURE 4.1 – $\overline{z}$ : Conjugué complexe de $z$. Géométriquement, cela correspond à une symétrie axiale par rapport à l'axe $Ox$.

## 4.3 Modules et arguments

**Définition 4.8** (Module)**.** *Soit $z = a + ib \in \mathbf{C}$. On appelle* module *de $z$ (noté $|z|$) la distance euclidienne qui sépare l'origne au point d'affixe $M : (a, b)$, c'est-à-dire $|z| = \sqrt{a^2 + b^2}$.*

**Remarque 4.9.** On a :

$$z\overline{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2 .$$

**Propriétés 4.10.** *1. Le module prolonge la valeur absolue dans les nombres réels, c'est-à-dire que, pour $x \in \mathbf{R}$, on a : $|x| = \sqrt{x^2 + 0^2} = x + i0$.*

*2. Pour tout $z \in \mathbf{C}$, le module $z$ est positif et est égal à zéro si et seulement $z = 0$.*

*3. Pour tout $z, w \in \mathbf{C}$,*

$$|zw| = |z| \cdot |w| ,$$

*et, si $z \neq 0$,*

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}.$$

4. *On a l'*inégalité triangulaire *:*

$$||z| - |w|| \leq |z + w| \leq |z| + |w|\,.$$

**Définition 4.11** (Argument)**.** *On note $O$ l'origine du plan $\mathrm{R}^2$ et $Ox$ l'axe des $x$. On appelle* argument *d'un nombre complexe $z$ non nul, l'angle $(Ox, \overrightarrow{OM})$ (défini à un multiple de $2\pi$ près). On notera $\theta = \mathrm{Arg}(z)$ où $\mathrm{Arg}(z) \in ]-\pi\,, \pi]$ est la détermination principale de l'argument.*

**Propriétés 4.12.** *Pour tout $z \in \mathrm{C}^*$.*

1. $\arg(\overline{z}) = -\arg(z) \pmod{2\pi}$.
2. $\arg(-z) = \arg(z) + \pi \pmod{2\pi}$.
3. $\arg(-\overline{z}) = \pi - \arg(z) \pmod{2\pi}$.

**Définition 4.13** (Exponentielle complexe)**.** *Soit $z = a + \mathrm{i}b \in \mathrm{C}$, on a alors :*

$$\mathrm{e}^{\mathrm{i}z} = \cos z + \mathrm{i}\sin z$$

*qui est l'*exponentielle complexe*.*

**Définition 4.14** (Écriture d'un nombre complexe)**.** *Soit $z \in \mathrm{C}$. On appelle* forme algébrique *du nombre complexe $z$, toute écriture de la forme $z = a + \mathrm{i}b$. Comme $a = |z|\cos\theta$ et $b = |z|\sin\theta$, on appelle* forme trigonométrique*, l'écriture $z = |z|\,(\cos\theta + \mathrm{i}\sin\theta)$. D'après la définition ,*

$$\mathrm{e}^{\mathrm{i}z} = \cos z + \mathrm{i}\sin z,$$

*d'où une nouvelle écriture :*

$$z = |z|\,\mathrm{e}^{\mathrm{i}\theta}$$

*qu'on appelle* forme exponentielle*.*

**Propriétés 4.15.** *Pout tout $z, z' \in \mathrm{C}^*$ :*

1. $\arg(zz') = \arg(z) + \arg(z') \pmod{2\pi}$*,*
2. $\arg\left(\frac{1}{z}\right) = -\arg(z) \pmod{2\pi}$*,*
3. $\arg\left(\frac{z}{z'}\right) = \arg(z) - \arg(z') \pmod{2\pi}$*,*
4. $\arg(z^n) = n\arg(z) \pmod{2\pi}$.

**Proposition 4.16** (Formule de Moivre)**.** *Pour tout $\theta \in \mathrm{R}$,*

$$(\cos\theta + \mathrm{i}\sin\theta)^n = \cos(n\theta) + \mathrm{i}\sin(n\theta),$$

*et sous forme exponentielle, la formule (dite* de Moivre*) s'exprime de la manière suivante :*

$$(\mathrm{e}^{\mathrm{i}\theta})^n = \mathrm{e}^{\mathrm{i}n\theta}.$$

**Remarque 4.17.** On a : $r_1 e^{i\theta_1} = r_2 e^{i\theta_2}$ si et seulement si $|r_1| = |r_2|$ et $\theta_1 = \theta_2 + 2k\pi$, pour tout $k \in \mathbf{Z}$.

**Proposition 4.18** (Formule d'Euler)**.** *La* formule d'Euler *permet d'exprimer* $\cos(\theta)$ *et* $\sin(\theta)$ *en fonction d'exponentielle complexe :*

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

## 4.4 Résolution algébrique d'équations avec les nombres complexes

### 4.4.1 Racines carrées d'un nombre complexe

**Définition 4.19** (Racine carrée d'un nombre complexe)**.** *Soit* $w = a + ib \in \mathbf{C}$ *alors* $z$ *est une* racine carrée *de* $w$ *si* $z^2 = w$.

On propose deux méthodes de résolution d'une équation du type $z^2 = w$ avec $z, w \in \mathbf{C}$.

**Algébrique** On écrit $z$ comme $x + iy$ et $w$ comme $a + ib$, avec $x, y, a, b \in \mathbf{R}$. On a :

$$\begin{aligned} z^2 = w &\Leftrightarrow (x+iy)^2 = a + ib \\ &\Leftrightarrow x^2 - y^2 + 2xyi = a + ib \text{ et } |z|^2 = |w|, \\ &\Leftrightarrow \begin{cases} x^2 - y^2 = a \\ 2xyi = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases} \end{aligned}$$

Notons :

$$x^2 - y^2 = a \tag{4.1}$$
$$2xyi = b \tag{4.2}$$
$$x^2 + y^2 = \sqrt{a^2+b^2} \tag{4.3}$$

Si on fait (4.1) + (4.3), on obtient :

$$2x^2 = a + \sqrt{a^2+b^2},$$

et si on fait (4.3) – (4.1), on a :

$$2y^2 = -a + \sqrt{a^2+b^2}.$$

D'où, les solutions sont :

$$x = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}, \quad y = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$$

avec le signe de $xy$ est le même que le signe de $b$, c'est-à-dire
– si $b$ est positif alors $x$ et $y$ ont même signe,
– si $b$ est négatif alors $x$ et $y$ sont de signe opposé.

**Géométrique** On écrit $z = r\mathrm{e}^{\mathrm{i}\theta}$ et $w = R\mathrm{e}^{\mathrm{i}\varphi}$ avec $r, R \geq 0$. On a donc :

$$z^2 = w \Leftrightarrow r^2\mathrm{e}^{2\mathrm{i}\theta} = R\mathrm{e}^{\mathrm{i}\varphi}$$
$$\Leftrightarrow \begin{cases} r^2 = R \\ 2\theta = \varphi + 2k\pi, \\ k \in \mathbf{Z} \end{cases} \Leftrightarrow \begin{cases} r = \sqrt{R} & \text{(et non } r = -\sqrt{R} \text{ car } r \geq 0) \\ \theta = \frac{\varphi}{2} + k\pi, & k \in \mathbf{Z}. \end{cases}$$

Ainsi, il y a deux solutions :

$$z_1 = \sqrt{R}\mathrm{e}^{\mathrm{i}\varphi/2}, \quad z_2 = \sqrt{R}\mathrm{e}^{\mathrm{i}\varphi/2+\pi\mathrm{i}} = -z_1.$$

**Remarque 4.20. Attention !** Il serait incongru d'écrire $\sqrt{z}$ si $z \in \mathbf{C} \setminus \mathbf{R}_+$.

### 4.4.2 Racines $n^{\mathrm{e}}$ d'un nombre complexe

**Définition 4.21** (Racines $n^{\mathrm{e}}$)**.** *Soient* $w \in \mathbf{C}$ *et* $n \in \mathbf{N}$. *Les* racines $n^{\mathrm{e}}$ *de* $w$ *sont les solutions de l'équation*

$$z^n = w. \tag{$E$}$$

On donne une méthode géométrique pour trouver les solutions de l'équation. On écrit $z = r\mathrm{e}^{\mathrm{i}\theta}$ et $w = R\mathrm{e}^{\mathrm{i}\varphi}$, on a alors

$$(E) \Leftrightarrow r^n\mathrm{e}^{\mathrm{i}n\theta} = R\mathrm{e}^{\mathrm{i}\varphi}$$
$$\Leftrightarrow \begin{cases} r^n = R \\ n\theta = \varphi + 2k\pi, \quad k \in \mathbf{Z} \end{cases} \Leftrightarrow \begin{cases} r = \sqrt[n]{R} \\ \theta = \frac{\varphi}{n} + \frac{2k\pi}{n}, \quad k \in \mathbf{Z} \end{cases}.$$

D'où cette équation admet $n$ solutions :

$$z_k = \sqrt[n]{R} \cdot \mathrm{e}^{\varphi/n+2k\pi/n} \quad \text{avec } k \in \{0, \ldots, n-1\}.$$

Soit l'équation :

$$z^n = 1. \tag{4.4}$$

**Définition 4.22** (Racines $n^{\text{e}}$ de l'unité)**.** *Les solutions de* (4.4) *sont appelés les* racines $n^{\text{e}}$ de l'unité *:*

$$z_k = \mathrm{e}^{2k\pi \mathrm{i}/n}, \quad \textit{pour } k = \{0, \ldots, n-1\}.$$

Les points $z_k$ sont les points d'un polyèdre régulier inscrit sur le cercle circonscrit unité. La figure 4.2 nous montre comment sont réparties les racines cinquième et septième de l'unité sur le cercle circonscrit unité.

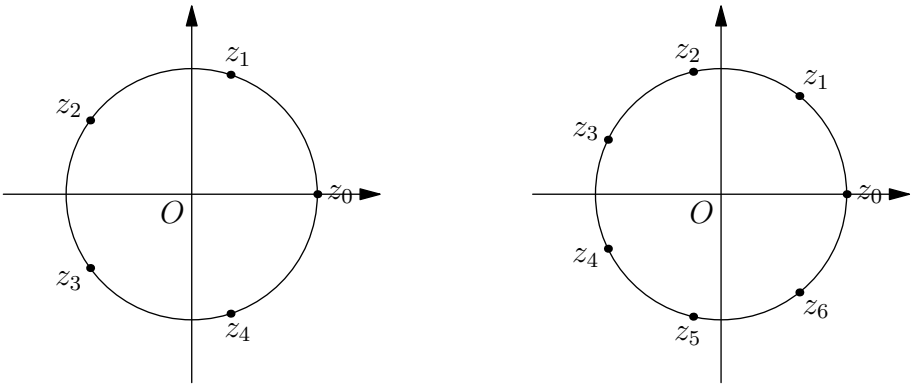


FIGURE 4.2 – Racines cinquième et septième de l'unité

### 4.4.3 Équations du second degré

Soient $a, b, c \in \mathbf{C}$ et $a \neq 0$. On considère l'équation :

$$az^2 + bz + c = 0. \tag{4.5}$$

On met l'équation (4.5) sous la forme canonique :

$$\begin{aligned}(4.5) &\Leftrightarrow a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = 0 \\ &\Leftrightarrow a \cdot \left(z + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0 \Leftrightarrow \left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.\end{aligned}$$

On pose $\Delta = b^2 - 4ac$ (qu'on appelle *discriminant*) et $w = z + \frac{b}{2}$. D'où :

$$(4.5) \Leftrightarrow w^2 = \frac{\Delta}{4a^2}.$$

Soit $\delta$ une racine carrée de $\Delta$, les deux solutions de (4.5) sont donc :

$$z_1 = \frac{-b + \delta}{2a}, \quad z_2 = \frac{-b - \delta}{2a}.$$

## 4.5 Exercices

**Exercice 4.1.** Mettre sous la forme $a + \mathrm{i}b$ (où $a, b \in \mathbf{R}$) les nombres :

$$\frac{3+6\mathrm{i}}{3-4\mathrm{i}},\ \left(\frac{1+\mathrm{i}}{2-\mathrm{i}}\right)^2 + \frac{3+6\mathrm{i}}{3-4\mathrm{i}},\ \frac{2+5\mathrm{i}}{1-\mathrm{i}} + \frac{2-5\mathrm{i}}{1+\mathrm{i}}.$$

**Exercice 4.2 ([19]).**
1. Linéariser $\sin^3(\theta)$ et $\cos^4(\theta)$.
2. Calculer $\cos(3\theta)$ en fonction de $\cos(\theta)$ et $\sin(3\theta)$ en fonction de $\sin(\theta)$.

**Exercice 4.3.** Soient $z_1, \ldots, z_n$ les racines $n^{\mathrm{e}}$ de l'unité. Calculer $z_1 + \cdots + z_n$ et $z_1 \times \cdots \times z_n$.

**Exercice 4.4.** Résoudre les équations suivantes :
1. $z^2 + z + 1 = 0$,
2. $z^2 + z - 2 = 0$,
3. $z^2 - (5 - 14\mathrm{i})z - 2(5\mathrm{i} + 12) = 0$,
4. $z^2 + 4z + 5 = 0$,
5. $z^2 - (3 + 4\mathrm{i})z - 1 + 5\mathrm{i} = 0$.

# Bibliographie


[1] R. CHILL, *Logique et théorie des ensembles*, Laboratoire de Mathématiques et Applications de Metz, Licence de Mathématiques, 1ère année, 1er semestre. URL : http://www.math.univ-metz.fr/~chill/logique.pdf.

[2] EXO7, *Logique, ensembles, raisonnements*, URL : http://exo7.emath.fr

[3] C. BOULONNE, *Notes de cours MAN : Axiomes et nombres*, Licence de Mathématiques.

[4] WIKIPEDIA, *Implication (logique)*.

[5] WIKIPEDIA, *Équivalence logique*.

[6] WIKIPEDIA, *Injection (mathématiques)*.

[7] S. DE BIÈVRE, *Une invitation aux mathématiques*, Novembre 2005.

[8] G. CONSTANTINI, *Dénombrement, combinatoire, lois de probabilités discrètes*, URL : http://pagesperso-orange.fr/gilles.constantini/.

[9] EXO7, *Relation d'équivalence, relation d'ordre*, URL : http://exo7.emath.fr

[10] EXO7, *Dénombrement*, URL : http://exo7.emath.fr

[11] EXO7, *Arithmétique dans* Z, URL : http://exo7.emath.fr

[12] G. CONSTANTINI, *PGCD, PPCM dans* Z*, Théorème de Bezout, Applications*, URL : http://pagesperso-orange.fr/gilles.constantini/.

[13] C. BERTAULT, *Arithémtique des entiers relatifs*, URL : http://bkristof.free.fr.

[14] C. BERTAULT, *Groupes, anneaux et corps*, URL : http://bkristof.free.fr.

[15] EXO7, *Structure de groupe, permutations*, URL : http://exo7.emath.fr.

[16] S. GONNORD, *Structures algébriques : groupes, anneaux et corps*, Math PCSI.

[17] R. FERRRÉOL, *Nombres complexes*, Cours MPSI, 2009-2010.

[18] D. FELDMANN, *Nombres complexes*.

[19] G. CONSTANTINI, *Nombres complexes*, URL : http://pagesperso-orange.fr/gilles.constantini/.

[20] WIKIPEDIA, *Nombres complexes*.

[21] EXO7, *Nombres complexes*.

# Index