

# Éléments de logique et de théorie des ensembles

Pour les exemples et exercices traités dans ce chapitre les ensembles usuels de nombres entiers, rationnels réels et complexes sont supposés connus, au moins de manière intuitive comme cela se passe au Lycée. Nous reviendrons plus loin sur les constructions de ces ensembles.

## 1.1 Quelques notions de logique

Nous allons préciser à un premier niveau quelques notions mathématiques qui sont relativement intuitives mais nécessitent quand même des définitions rigoureuses.

L'idée étant de préciser schématiquement comment se présente une théorie mathématique ainsi que la notion essentielle de démonstration.

La première notion est celle d'assertion. De manière intuitive, une assertion est un énoncé mathématique aussi rigoureux que possible qui ne peut prendre que deux valeurs de vérité à savoir « vrai » ou « faux » mais jamais entre les deux comme dans le langage courant.

Une assertion qui est toujours vraie est une tautologie.

Par exemple les énoncés suivantes sont des assertions :  $2 < 15$  (elle est vraie),  $\sqrt{2}$  est un nombre rationnel (elle est fausse),  $\cos(n\pi) = (-1)^n$  (vraie), ...

Deux assertions sont dites logiquement équivalentes, ou plus simplement équivalentes, si elles sont toutes deux vraies ou toutes deux fausses.

Il y a ensuite les énoncés qui se démontrent. Pour ce faire, on se donne des règles précises (que nous verrons par la pratique) qui permettent de construire de nouvelles assertions à partir d'assertions données.

**Remarque 1.1** *Il ne faut pas croire que dans une théorie donnée toute assertion  $P$  soit obligatoirement démontrable. En 1931 Kurt Gödel a démontré qu'il y a des assertions non démontrables (on dit aussi qu'elles sont indécidables) : il n'est pas possible de démontrer que  $P$  est vraie ni que  $P$  est fausse.*

À la base de toute théorie mathématique, on dispose d'un petit nombre d'assertions qui sont supposés vraies a priori (c'est-à-dire avant toute expérience) et que l'on nomme axiomes ou postulats. Ces axiomes sont élaborés par abstraction à partir de l'intuition et ne sont pas déduits d'autres relations.

Par exemple, la géométrie euclidienne est basée sur une quinzaine d'axiomes. L'un de ces axiomes est le postulat numéro 15 qui affirme que par un point donné passe une et une seule droite parallèle à une droite donnée.

Une autre exemple important est donné par la construction de l'ensemble noté  $\mathbb{N}$  des entiers naturels. Cette construction peut se faire en utilisant les axiomes de Peano suivants :

- 0 est un entier naturel ;
- tout entier naturel  $n$  a un unique successeur noté  $n + 1$  ;
- deux entiers naturels ayant même successeur sont égaux ;
- une partie  $P$  de  $\mathbb{N}$  qui contient 0 et telle que si  $n$  est dans  $P$  alors le successeur de  $n$  y est aussi, est égale à  $\mathbb{N}$  (axiome de récurrence).

Nous reviendrons au paragraphe 1.6 sur l'ensemble  $\mathbb{N}$  en partant sur une autre base.

La théorie des ensemble est basée sur le système d'axiomes de Zermelo-Fränkel.

La notion de définition nous permet de décrire un objet ou une situation précise à l'aide du langage courant.

Les énoncés qui se démontrent sont classés en fonction de leur importance dans une théorie comme suit :

- un théorème est une assertion vraie déduite d'autres assertions, il s'agit en général d'un résultat important à retenir ;
- un lemme est un résultat préliminaire utilisé pour démontrer un théorème ;
- un corollaire est une conséquence importante d'un théorème ;
- une proposition est de manière générale un résultat auquel on peut attribuer la valeur vraie ou fausse sans ambiguïté.

Pour rédiger un énoncé mathématique, on utilise le langage courant et les objets manipulés sont représentés en général par des lettres de l'alphabet latin ou grec. Usuellement, on utilise :

- les lettres minuscules  $a, b, c, \dots$  pour des objets fixés ;
- les lettres minuscules  $x, y, z, t, \dots$  pour des objets inconnus à déterminer ;
- les lettres majuscules  $E, F, G, H, \dots$  pour des ensembles ;
- des lettres de l'alphabet grecques minuscules ou majuscules  $\alpha, \beta, \varepsilon, \delta, \dots \Lambda, \Gamma, \Omega, \dots$

## 1.2 Les connecteurs logiques de base

L'élaboration de nouvelles assertions à partir d'autres se fait en utilisant les connecteurs logiques de négation, de conjonction, de disjonction, d'implication et d'équivalence définis comme suit, où  $P$  et  $Q$  désignent des assertions.

- La négation de  $P$ , notée  $\neg P$ , ou non  $P$  ou  $\overline{P}$ , est l'assertion qui est vraie si  $P$  est fausse et fausse si  $P$  est vraie.

Par exemple la négation de l'assertion : «  $x$  est strictement positif » est «  $x$  est négatif ou nul ».

En théorie des ensembles on admet qu'il n'existe pas d'assertion  $P$  telle que  $P$  et  $\overline{P}$  soient toutes deux vraies. On dit que cette théorie est non contradictoire.

- La conjonction de  $P$  et  $Q$ , notée  $P \wedge Q$  (lire  $P$  et  $Q$ ), est l'assertion qui est vraie uniquement si  $P$  et  $Q$  sont toutes deux vraies (et donc fausse dans les trois autres cas).

Par exemple  $P \wedge \overline{P}$  est toujours faux (on se place dans des théories non contradictoires).

- La disjonction de  $P$  et  $Q$ , notée  $P \vee Q$  (lire  $P$  ou  $Q$ ), est l'assertion qui est vraie uniquement si l'une des deux assertions  $P$  ou  $Q$  est vraie (donc fausse si  $P$  et  $Q$  sont toutes deux fausses).

Par exemple  $P \vee \overline{P}$  est toujours vraie (c'est une tautologie).

Il faut remarquer que le « ou » pour « ou bien » est inclusif, c'est-à-dire que  $P$  et  $Q$  peuvent être toutes deux vrais dans le cas où  $P \vee Q$  est vraie.

On peut aussi introduire le « ou exclusif », noté  $W$ , qui est vrai uniquement lorsque l'une des deux assertions, mais pas les deux simultanément, est vraie.

- L'implication, notée  $P \rightarrow Q$ , est l'assertion qui est fausse uniquement si  $P$  est vraie et  $Q$  fausse (donc vraie dans les trois autres cas).

On peut remarquer que si  $P$  est fausse, alors  $P \rightarrow Q$  est vraie indépendamment de la valeur de vérité de  $Q$ .

L'implication est à la base du raisonnement mathématique. En partant d'une assertion  $P$  (ou de plusieurs), une démonstration aboutit à un résultat  $Q$ . Si cette démonstration est faite sans erreur, alors  $P \rightarrow Q$  est vraie et on notera  $P \Rightarrow Q$  (ce qui signifie que si  $P$  est vraie, alors  $Q$  est vraie). Dans ce cas, on dit que  $P$  est une condition suffisante et  $Q$  une condition nécessaire.

On peut remarquer que l'implication est transitive, c'est-à-dire que si  $P$  implique  $Q$  et  $Q$  implique  $R$ , alors  $P$  implique  $R$ .

- L'équivalence de  $P$  et  $Q$ , notée  $P \leftrightarrow Q$ , est l'assertion qui est vraie uniquement si  $P \rightarrow Q$  et  $Q \rightarrow P$  sont toutes deux vraies. Dans le cas où  $P \leftrightarrow Q$  est vraie on dit que  $P$  et  $Q$  sont équivalentes et on note  $P \Leftrightarrow Q$  (ce qui signifie que  $P$  et  $Q$  sont, soit toutes deux vraies, soit toutes deux fausses). Dans ce cas, on dit que  $Q$  est une condition nécessaire et suffisante de  $P$ .

On peut résumer ce qui précède, en utilisant la table de vérité suivante :

$P$	$Q$	$\bar{P}$	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
$V$	$V$	$F$	$V$	$V$	$V$	$V$
$V$	$F$	$F$	$F$	$V$	$F$	$F$
$F$	$V$	$V$	$F$	$V$	$V$	$F$
$F$	$F$	$V$	$F$	$F$	$V$	$V$

Les tables de vérité peuvent être utilisées pour faire certaines démonstrations. On rappelle que deux assertions qui ont même table de vérité sont équivalentes.

Avec le théorème qui suit, on résume quelques règles de calcul.

**Théorème 1.1** Soient  $P, Q, R$  des propositions. On a les équivalences :

1. commutativité :

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

$$(P \vee Q) \Leftrightarrow (Q \vee P)$$

2. associativité

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

$$(P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$$

3. distributivité :

$$(P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$$

$$(P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$$

4. négations :

$$\overline{(\bar{P})} \Leftrightarrow (P)$$

$$\overline{(P \wedge Q)} \Leftrightarrow (\bar{P} \vee \bar{Q})$$

$$\overline{(P \vee Q)} \Leftrightarrow (\bar{P} \wedge \bar{Q})$$

$$(P \rightarrow Q) \Leftrightarrow (\bar{Q} \rightarrow \bar{P})$$

$$(P \rightarrow Q) \Leftrightarrow (\bar{P} \vee Q)$$

$$\overline{(P \rightarrow Q)} \Leftrightarrow (P \wedge \bar{Q})$$

**Démonstration.** On utilise les tables de vérité (exercices). ■

Les équivalences  $(\overline{P \wedge Q}) \Leftrightarrow (\overline{P} \vee \overline{Q})$  et  $(\overline{P \vee Q}) \Leftrightarrow (\overline{P} \wedge \overline{Q})$  sont appelées lois de Morgan.

**Exercice 1.1** Montrer que les assertions  $P \rightarrow Q$  et  $\overline{P} \vee Q$  sont équivalentes.

**Solution 1.1** On montre qu'elles ont même table de vérité.

$P$	$Q$	$\overline{P}$	$\overline{P} \vee Q$	$P \rightarrow Q$
$V$	$V$	$F$	$V$	$V$
$V$	$F$	$F$	$F$	$F$
$F$	$V$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$

**Exercice 1.2** Montrer que les assertions  $\overline{P \rightarrow Q}$  et  $P \wedge \overline{Q}$  sont équivalentes.

**Solution 1.2** On montre qu'elles ont même table de vérité.

$P$	$Q$	$P \wedge \overline{Q}$	$\overline{P \rightarrow Q}$
$V$	$V$	$F$	$F$
$V$	$F$	$V$	$V$
$F$	$V$	$F$	$F$
$F$	$F$	$F$	$F$

**Exercice 1.3** Montrer que les assertions  $P \leftrightarrow P$ ,  $(P \wedge Q) \rightarrow P$ ,  $P \rightarrow (P \vee Q)$ ,  $P \vee (P \rightarrow Q)$ ,  $P \rightarrow (Q \rightarrow P)$  et  $((P \rightarrow Q) \rightarrow P) \rightarrow P$  sont des tautologies (i. e. toujours vraies).

**Solution 1.3** Pour  $P \leftrightarrow P$ ,  $(P \wedge Q) \rightarrow P$ ,  $P \rightarrow (P \vee Q)$ , c'est évident et pour les autres, on utilise la table de vérité :

$P$	$Q$	$P \rightarrow Q$	$Q \rightarrow P$	$P \vee (P \rightarrow Q)$	$P \rightarrow (Q \rightarrow P)$	$((P \rightarrow Q) \rightarrow P) \rightarrow P$
$V$	$V$	$V$	$V$	$V$	$V$	$V$
$V$	$F$	$F$	$V$	$V$	$V$	$V$
$F$	$V$	$V$	$F$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$	$V$	$V$

**Exercice 1.4** Simplifier l'expression :

$$R = (\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q}) \vee (P \wedge Q).$$

**Solution 1.4** En utilisant les tables de vérité, on a :

$P$	$Q$	$\overline{P} \wedge Q$	$\overline{P} \wedge \overline{Q}$	$(\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q})$	$P \wedge Q$	$R$
$V$	$V$	$F$	$F$	$F$	$V$	$V$
$V$	$F$	$F$	$F$	$F$	$F$	$F$
$F$	$V$	$V$	$F$	$V$	$F$	$V$
$F$	$F$	$F$	$V$	$V$	$F$	$V$

Donc  $R$  a la même table de vérité que  $P \rightarrow Q$ , ce qui signifie que  $R$  est équivalent à  $P \rightarrow Q$ .

**Exercice 1.5** Soient  $P, Q, R$  trois assertions.

1. Écrire la négation de chacune de ces assertions :  $\overline{P \wedge Q}$ ,  $\overline{P \vee Q}$ ,  $P \vee (Q \wedge R)$ ,  $P \wedge (Q \vee R)$ ,  $P \rightarrow \overline{Q}$ ,  $P \leftrightarrow Q$ ,  $\overline{P \vee Q} \rightarrow R$ ,  $P \vee Q \rightarrow \overline{R}$ ,  $\overline{P \wedge Q} \Rightarrow R$  et  $\overline{P \vee Q} \rightarrow \overline{R}$ .
2. Traduire chacune de ces assertions, ainsi sa négation, en langage courant où  $P$  correspond à « j'écris »,  $Q$  à « je pense » et  $R$  à « je chante ».

**Solution 1.5** On a :

$$\overline{\overline{P \wedge Q}} = P \vee Q$$

ce qui peut se traduire par la négation de « je n'écris pas et je pense » est « j'écris ou je ne pense pas » ;

$$\overline{\overline{P \vee Q}} = P \wedge Q$$

$$\overline{P \vee (Q \wedge R)} = \overline{P} \wedge \overline{Q \wedge R} = \overline{P} \wedge (\overline{Q} \vee \overline{R}) = (\overline{P} \wedge \overline{Q}) \vee (\overline{P} \wedge \overline{R})$$

et ainsi de suite.

**Exercice 1.6** Montrer les équivalences qui suivent.

1.  $(P \rightarrow (Q \rightarrow R)) \Leftrightarrow ((P \wedge Q) \rightarrow R)$
2.  $((P \vee Q) \rightarrow R) \Leftrightarrow ((P \rightarrow R) \wedge (Q \rightarrow R))$
3.  $((P \wedge Q) \rightarrow R) \Leftrightarrow ((P \rightarrow R) \vee (Q \rightarrow R))$
4.  $(P \rightarrow (Q \wedge R)) \Leftrightarrow ((P \rightarrow Q) \wedge (P \rightarrow R))$
5.  $(P \rightarrow (Q \vee R)) \Leftrightarrow ((P \rightarrow Q) \vee (P \rightarrow R))$

**Solution 1.6** On peut utiliser les tables de vérité ou utiliser l'équivalence  $(P \rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$ . Par exemple, on a :

$$(P \rightarrow (Q \rightarrow R)) \Leftrightarrow \overline{P} \vee (\overline{Q} \vee R) \Leftrightarrow \overline{P \wedge Q} \vee R \Leftrightarrow ((P \wedge Q) \rightarrow R)$$

**Exercice 1.7** Montrer que les assertions  $P \vee Q$  (ou exclusif) et  $(P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$  sont équivalentes.

**Solution 1.7** On montre qu'elles ont même table de vérité.

$P$	$Q$	$P \vee Q$	$(P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	F

**Exercice 1.8** Soient  $a, b$  deux entiers naturels.

1. Donner un équivalent de  $(a < b) \rightarrow (a = b)$
2. Donner la négation de  $(a \leq b) \rightarrow (a > b)$

**Solution 1.8**

1.  $(a < b) \rightarrow (a = b)$  est équivalent à  $(a \geq b) \vee (a = b)$  encore équivalent à  $a \geq b$ .
2. La négation de  $(a \leq b) \rightarrow (a > b)$  est  $(a \leq b) \wedge (a \leq b)$ , soit  $(a \leq b)$ .

**Exercice 1.9** On dispose de 6 pièces de 1 euro dont une seule est fautive et plus lourde que les autres. Montrer qu'on peut la détecter en utilisant une balance de type Roberval en effectuant au plus deux pesées. Même question avec 8 pièces.

**Solution 1.9** On numérote de 1 à 6 les pièces. On place les pièces 1, 2, 3 sur le plateau  $P_1$  de la balance et les pièces 4, 5, 6 sur le plateau  $P_2$ . L'un des deux plateaux, disons  $P_1$  est plus chargé, il contient donc la fausse pièce. On isole la pièce 3 et on place la pièce 1 sur le plateau  $P_1$  et la pièce 2 sur  $P_2$ . Si les plateaux sont équilibrés c'est 3 qui est fausse, sinon le plateau le plus chargé contient la fausse pièce.

Pour 8 pièces, on isole les pièces 7 et 8 et on place les pièces 1, 2, 3 sur le plateau  $P_1$  et les pièces 4, 5, 6 sur le plateau  $P_2$ . Si les plateaux sont équilibrés, on compare 7 et 8 avec la balance et on détermine la fausse pièce, sinon l'un des deux plateaux, disons  $P_1$  est plus chargé, il contient donc la fausse pièce et le procédé utilisé pour les 6 pièces nous permet de trouver la fausse pièce.

**Exercice 1.10** Des cannibales proposent à un touriste de décider lui même de son sort en faisant une déclaration : si celle-ci est vraie, il sera rôti, sinon il sera bouilli. Quelle déclaration peut faire ce touriste (malin) pour imposer une troisième solution ?

**Solution 1.10** ♠♠♠

**Exercice 1.11** Les habitants d'un village sont partagés en deux clans : ceux du clan A disent toujours la vérité et ceux du clan B mentent toujours. Un touriste passant par ce village rencontre trois habitants et souhaite savoir à quel clan appartient chacun d'eux. Il n'entend pas la réponse du premier, le deuxième répète ce qu'il a entendu, selon lui, du premier et le troisième lui indique le clan du premier et du second. Le touriste a la réponse à sa question. Pouvez-vous faire de même.

**Solution 1.11** ♠♠♠

On dit qu'une théorie est non contradictoire si  $P \wedge \bar{P}$  est faux pour toute proposition  $P$ .

**Exercice 1.12** Montrer que si dans une théorie une propriété  $P$  est contradictoire, c'est-à-dire si  $P \wedge \bar{P}$  est vraie, alors  $Q \wedge \bar{Q}$  est vraie pour toute propriété  $Q$ .

**Solution 1.12** Nous allons montrer que s'il existe un énoncé contradictoire  $P$ , alors tout énoncé  $Q$  est vrai, donc  $\bar{Q}$  aussi et  $Q \wedge \bar{Q}$  est vraie.

On vérifie tout d'abord que  $R = \bar{P} \rightarrow (P \rightarrow Q)$  est une tautologie avec la table de vérité :

$P$	$Q$	$\bar{P}$	$P \rightarrow Q$	$\bar{P} \rightarrow (P \rightarrow Q)$
V	V	F	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

Comme  $R$  et  $\bar{P}$  sont vraies,  $P \rightarrow Q$  est vraie et  $Q$  est vraie puisque  $P$  est vraie.

### 1.3 Quelques méthodes de raisonnement

En général l'énoncé d'une proposition à démontrer est formé d'une ou plusieurs hypothèses qui constituent l'assertion  $H$  et d'une ou plusieurs conclusions qui constituent l'assertion  $C$ . Il s'agit donc de montrer l'implication  $H \implies C$ .

Si de plus, on peut montrer que  $C \implies H$ , on dira alors que la réciproque de la proposition est vraie.

Les idées de base que l'on peut utiliser sont les suivantes.

- Une assertion peut toujours être remplacée par n'importe quelle assertion qui lui est équivalente.
- On peut effectuer une démonstration directe, c'est à dire de déduire logiquement  $C$  de  $H$ .
- L'implication étant transitive, on peut essayer de montrer que  $C \implies C'$  sachant par ailleurs que  $C' \implies H$ .
- Dans le cas où une démonstration directe semble difficile, on peut essayer une démonstration par l'absurde qui consiste à étudier l'assertion  $H \wedge \overline{C}$  équivalente à  $\overline{H \implies C}$  et on montre qu'on aboutit à une impossibilité si cette dernière assertion est vraie (pratiquement, on suppose que la conclusion est fautive avec les hypothèses et on aboutit à une absurdité). Il en résulte alors que  $\overline{H \implies C}$  est fautive, c'est à dire que  $H \implies C$  est vraie, soit  $H \implies C$ .
- On peut aussi essayer de montrer la contraposée  $\overline{C} \implies \overline{H}$  puisque les implications  $H \implies C$  et  $\overline{C} \implies \overline{H}$  sont équivalentes.
- La démonstration par contre-exemple permet de montrer qu'une implication  $H \implies C$ , où  $H$  et  $C$  sont des propriétés portant sur des variables  $x$ , est fautive. Pour ce faire on cherche une ou des valeurs de  $x$  pour lesquels  $H(x)$  est vraie et  $C(x)$  est fautive.
- La démonstration par récurrence permet de montrer qu'une propriété portant sur des entiers naturels est toujours vraie. Cette méthode de démonstration est décrite au paragraphe 1.6, où elle apparaît comme un théorème basé sur le fait que l'ensemble des entiers naturels est bien ordonné. Si on accepte l'axiome de Péano, le principe de récurrence en est une conséquence immédiate.

**Exercice 1.13** *En raisonnant par l'absurde, montrer que  $\sqrt{2}$  est irrationnel.*

**Solution 1.13** *Supposons que  $\sqrt{2} = \frac{p}{q}$  avec  $p, q$  entiers naturels non nuls premiers entre eux. On a alors  $p^2 = 2q^2$  qui entraîne que  $p$  est pair, soit  $p = 2p'$  et  $q^2 = 2p'^2$  entraîne  $q$  pair, ce qui contredit  $p$  et  $q$  premiers entre eux.*

**Exercice 1.14** *En raisonnant par l'absurde, montrer que  $\frac{\ln(2)}{\ln(3)}$  est irrationnel.*

**Solution 1.14** *Supposons que  $\frac{\ln(2)}{\ln(3)} = \frac{p}{q}$  avec  $p, q$  entiers naturels non nuls premiers entre eux. On a alors  $\ln(2^q) = \ln(3^p)$  et  $2^q = 3^p$ , ce qui est impossible puisque  $2^q$  est un entier pair et  $3^p$  est un entier impair.*

**Exercice 1.15** *Soit  $n$  un entier naturel non carré, c'est-à-dire ne s'écrivant pas sous la forme  $n = p^2$  avec  $p$  entier. En raisonnant par l'absurde et en utilisant le théorème de Bézout, montrer que  $\sqrt{n}$  est irrationnel.*

**Solution 1.15** *Si  $n$  est non carré, on a alors  $n \geq 2$ .*

*Supposons que  $\sqrt{n} = \frac{p}{q}$  avec  $p, q$  premiers entre eux dans  $\mathbb{N}^*$ . Le théorème de Bézout nous dit qu'il existe un couple  $(u, v)$  d'entiers relatifs tels que  $up + vq = 1$ . On a alors :*

$$1 = (up + vq)^2 = u^2p^2 + 2uvpq + v^2q^2$$

*avec  $u^2p^2 = u^2nq^2$ . L'égalité précédente s'écrit alors  $qr = 1$  avec  $r = u^2nq + 2uvp + v^2q$  dans  $\mathbb{Z}$ , ce qui implique que  $q = 1$  et  $\sqrt{n} = p$ , en contradiction avec  $n$  non carré.*

**Exercice 1.16** *Sachant que tout entier supérieur ou égal à 2 admet un diviseur premier, montrer que l'ensemble  $\mathcal{P}$  des nombres premiers est infini.*

**Solution 1.16** *On sait déjà que  $\mathcal{P}$  est non vide (il contient 2). Supposons que  $\mathcal{P}$  soit fini avec :*

$$\mathcal{P} = \{p_1, \dots, p_r\}.$$

*L'entier  $n = p_1 \cdots p_r + 1$  est supérieur ou égal à 2, il admet donc un diviseur premier  $p_k \in \mathcal{P}$ . L'entier  $p_k$  divise alors  $n = p_1 \cdots p_r + 1$  et  $p_1 \cdots p_r$ , il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion  $\mathcal{P}$  est infini.*

**Exercice 1.17** *Montrer que  $x = \sqrt[3]{45 + 29\sqrt{2}} + \sqrt[3]{45 - 29\sqrt{2}}$  est un entier.*

**Solution 1.17** *En posant  $a = \sqrt[3]{45 + 29\sqrt{2}}$  et  $b = \sqrt[3]{45 - 29\sqrt{2}}$ , on a :*

$$\begin{cases} a^3 + b^3 = 90 \\ ab = \sqrt[3]{45^2 - 2 \cdot 29^2} = \sqrt[3]{343} = 7 \end{cases}$$

*ce qui donne :*

$$\begin{aligned} 90 &= (a + b)(a^2 - ab + b^2) \\ &= (a + b)((a + b)^2 - 3ab) = x(x^2 - 21) \end{aligned}$$

*donc  $x$  est racine du polynôme :*

$$P(X) = X(X^2 - 21) - 90$$

*On regarde si ce polynôme a des racines entières. Comme  $n^2 - 21$  est négatif pour  $n \leq 4$ , on cherche ces racines à partir de  $n = 5$ . On a  $P(5) = -70$  et  $P(6) = 0$ . On a alors  $P(X) = (X - 6)(X^2 + 6X + 15)$  et  $x = 6$ , puis c'est la seule racine réelle de  $P$ .*

## 1.4 Notions de base sur les ensembles. Quantificateurs

Nous nous contenterons d'une définition intuitive de la notion d'ensemble.

Un ensemble est une collection d'objets possédant des propriétés communes, ces objets sont les éléments de l'ensemble.

On utilisera les notations suivantes, pour les ensembles de nombres usuels :

- $\mathbb{N}$  est ensemble des entiers naturels ;
- $\mathbb{Z}$  est l'ensemble des entiers relatifs ;
- $\mathbb{Q}$  est l'ensemble des nombres rationnels
- $\mathbb{R}$  est l'ensemble des nombres réels ;
- $\mathbb{C}$  est l'ensemble des nombres complexes.

On admet l'existence d'un ensemble qui ne contient aucun élément. Cet ensemble est noté  $\emptyset$  et on dit que c'est l'ensemble vide.

Nous serons souvent amenés à décrire un ensemble en précisant les propriétés que doivent vérifier tous ses éléments, ce que nous noterons de la façon suivante :

$$E = \{\text{description des propriétés des éléments de } E\}$$

(on dit que l'ensemble  $E$  est défini en compréhension).

Cette notion d'ensemble défini en compréhension peut conduire à des paradoxes liés au problème de « l'ensemble de tous les ensembles », mais à un premier niveau, on se contente de ce point de vue intuitif. Une étude approfondie de la théorie des ensembles peut mener assez loin. Le lecteur intéressé peut consulter le volume de Bourbaki sur les ensembles, ou tout autre ouvrage spécialisé.

On peut aussi décrire un ensemble en donnant la liste finie ou infinie de tous ces éléments, quand cela est possible, ce qui se note :

$$E = \{x_1, x_2, \dots, x_n\}$$

s'il s'agit d'un ensemble fini ou :

$$E = \{x_1, x_2, \dots, x_n, \dots\}$$

s'il s'agit d'un ensemble infini pour lequel on peut numéroter les éléments (un tel ensemble est dit dénombrable). On dit alors que l'ensemble  $E$  est défini en extension.

Un singleton est un ensemble qui ne contient qu'un élément, soit  $E = \{a\}$ .

Si  $n, m$  sont deux entiers relatifs, l'ensemble des entiers relatifs compris entre  $n$  et  $m$  sera noté  $\{n, \dots, m\}$ . Dans le cas où  $m < n$ , il ne peut y avoir d'entiers entre  $n$  et  $m$  et cet ensemble est tout simplement l'ensemble vide. Dans le cas où  $n = m$ , cet ensemble est le singleton  $\{n\}$ . Pour  $n < m$ , on notera aussi  $\{n, n+1, \dots, m\}$  cet ensemble.

Nous nous contentons dans un premier temps de définitions intuitives de ces notions d'ensemble fini ou dénombrable (voir les paragraphes 2.1 et 2.2 pour des définitions plus rigoureuses).

Si  $E$  est un ensemble, on notera  $a \in E$  pour signifier que  $a$  est un élément de  $E$ , ce qui se lit «  $a$  appartient à  $E$  ». La négation de cette assertion est «  $a$  n'appartient pas à  $E$  » et se notera  $a \notin E$ .

Pour signifier qu'un ensemble  $F$  est contenu dans un ensemble  $E$ , ce qui signifie que tout élément de  $F$  est dans  $E$ , nous noterons  $F \subset E$  qui se lit «  $F$  est contenu dans  $E$  ». On peut écrire de manière équivalent que  $E \supset F$  pour dire que  $E$  contient  $F$ . La négation de cette assertion est notée  $F \not\subset E$ .

Deux ensembles  $E$  et  $F$  sont égaux si, et seulement si, ils ont les mêmes éléments, ce qui se traduit par  $E \subset F$  et  $F \subset E$ .

On admet que si  $E$  est un ensemble, il existe un ensemble dont tous les éléments sont formés de tous les sous-ensembles (ou parties) de  $E$ . On note  $\mathcal{P}(E)$  cet ensemble et on dit que c'est l'ensemble des parties de  $E$ . Ainsi  $F \subset E$  est équivalent à  $F \in \mathcal{P}(E)$ . L'ensemble vide et  $E$  sont des éléments de  $\mathcal{P}(E)$ .

Par exemple pour  $E = \{1, 2, 3\}$ , on a :

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

Pour décrire des ensembles, ou faire des raisonnements, nous utiliseront les deux quantificateurs suivants.

- Le quantificateur universel « quel que soit » ou « pour tout » noté  $\forall$  utilisé pour signifier que tout élément  $x$  d'un ensemble  $E$  vérifie une propriété  $P(x)$ , la syntaxe étant :

$$(\forall x \in E) (P(x)). \tag{1.1}$$

- Le quantificateur existentiel « il existe » noté  $\exists$  pour signifier qu'il existe au moins un élément  $x$  de  $E$  vérifiant la propriété  $P(x)$ , la syntaxe étant :

$$(\exists x \in E) | (P(x)). \tag{1.2}$$

Pour signifier qu'il existe un et un seul  $x$  dans  $E$  vérifiant la propriété  $P(x)$ , on utilisera la syntaxe :

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

La négation de l'assertion 1.1 est :

$$(\exists x \in E) \mid (\overline{P(x)})$$

en utilisant le symbole  $\mid$  qui se lit « tel que » utilisé pour traduire le fait que  $x$  est tel que la propriété  $\overline{P(x)}$  est vérifiée et la négation de 1.2 est :

$$(\forall x \in E) (\overline{P(x)}).$$

Nous verrons qu'il n'est pas toujours facile de traduire la négation d'une assertion en utilisant les quantificateurs.

Par exemple pour traduire le fait qu'une suite  $(u_n)_{n \in \mathbb{N}}$  de nombres réels est convergente vers un réel  $\ell$  nous écrirons :

$$(\exists \ell \in \mathbb{R}) \mid (\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0, |u_n - \ell| < \varepsilon)$$

ce qui signifie qu'il existe un réel  $\ell$  tel que quel que soit la précision  $\varepsilon > 0$  que l'on choisisse l'écart entre  $u_n$  et  $\ell$  (soit  $|u_n - \ell|$ ) est inférieur à  $\varepsilon$  à partir d'un certain rang  $n_0$ .

La négation de cette assertion s'écrit :

$$(\forall \ell \in \mathbb{R}), (\exists \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \geq n_0 \mid |u_n - \ell| \geq \varepsilon)$$

Nous étudierons plus loin les suites réelles ou complexes.

En utilisant les quantificateurs, il faudra faire attention à l'ordre d'apparition de ces derniers. Par exemple les assertions suivantes, où  $f$  est une fonction à valeurs réelles définie sur un ensemble  $E$  :

$$\forall x \in E, \exists M > 0 \mid f(x) < M$$

et

$$\exists M > 0 \mid \forall x \in E, f(x) < M.$$

ne sont pas équivalentes. La première assertion signifie que pour tout élément  $x$  de  $E$  il existe un réel  $M > 0$  qui dépend à priori de  $x$  (il faudrait donc le noter  $M(x)$ ) tel que  $f(x) < M$  (par exemple  $M(x) = f(x) + 1$  convient), alors que la seconde signifie qu'il existe un réel  $M > 0$ , indépendant de  $x$  dans  $E$ , tel que  $f(x) < M$ , ce qui n'est pas la même chose.

## 1.5 Les symboles $\sum$ et $\prod$

Si  $n$  est un entier naturel non nul et  $x_1, x_2, \dots, x_n$  des entiers, rationnels, réels ou complexes, on notera :

$$\sum_{k=1}^n x_k = x_1 + x_2 + \dots + x_n \text{ et } \prod_{k=1}^n x_k = x_1 \cdot x_2 \cdot \dots \cdot x_n$$

la somme et le produit des  $x_k$ .

Dans une telle somme ou produit l'indice est muet, c'est-à-dire que  $\sum_{k=1}^n x_k = \sum_{i=1}^n x_i$  et  $\prod_{k=1}^n x_k =$

$$\prod_{i=1}^n x_i.$$

La manipulation d'un produit de réels strictement positifs se ramène à une somme en utilisant la fonction logarithme :

$$\ln \left( \prod_{k=1}^n x_k \right) = \sum_{k=1}^n \ln(x_k)$$

On peut également effectuer des changements d'indice. Par exemple, en posant  $i = k + 1$ , on aura :

$$\sum_{k=1}^n x_k = \sum_{i=2}^{n+1} x_{i-1} = \sum_{k=2}^{n+1} x_{k-1}$$

On peut ajouter ou multiplier de telles sommes (ou produits). Par exemple, on a :

$$\sum_{k=1}^n x_k + \sum_{k=1}^n y_k = \sum_{k=1}^n (x_k + y_k)$$

$$\lambda \sum_{k=1}^n x_k = \sum_{k=1}^n \lambda x_k$$

$$\left( \sum_{k=1}^n x_k \right) \left( \sum_{k=1}^m y_k \right) = \left( \sum_{j=1}^n x_j \right) \left( \sum_{k=1}^m y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k.$$

Pour vérifier ce résultat, on écrit que :

$$\begin{aligned} S &= \left( \sum_{k=1}^n x_k \right) \left( \sum_{k=1}^m y_k \right) \\ &= (x_1 + x_2 + \cdots + x_n) \left( \sum_{k=1}^m y_k \right) \\ &= x_1 \sum_{k=1}^m y_k + \cdots + x_n \sum_{k=1}^m y_k \\ &= \sum_{j=1}^n x_j \left( \sum_{k=1}^m y_k \right) = \sum_{j=1}^n \left( \sum_{k=1}^m x_j y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k. \end{aligned}$$

**Exercice 1.18** Montrer que pour tout entier  $n \geq 1$ , on a :

$$P_n = \prod_{k=1}^n \left( 1 + \frac{1}{k} \right)^k = \frac{(n+1)^n}{n!}.$$

**Solution 1.18** Il revient au même de calculer  $S_n = \ln(P_n)$ . On a :

$$\begin{aligned} S_n &= \ln \left( \prod_{k=1}^n \left( \frac{k+1}{k} \right)^k \right) = \sum_{k=1}^n (k \ln(k+1) - k \ln(k)) \\ &= \sum_{k=1}^n k \ln(k+1) - \sum_{k=1}^n k \ln(k) \end{aligned}$$

et le changement d'indice  $j = k + 1$  dans la première somme donne :

$$\begin{aligned}
 S_n &= \sum_{j=2}^{n+1} (j-1) \ln(j) - \sum_{k=1}^n k \ln(k) \\
 &= \sum_{j=2}^{n+1} j \ln(j) - \sum_{j=2}^{n+1} \ln(j) - \sum_{k=1}^n k \ln(k) \\
 &= \sum_{k=2}^{n+1} k \ln(k) - \sum_{k=2}^{n+1} \ln(k) - \sum_{k=1}^n k \ln(k) \\
 &= (n+1) \ln(n+1) - \sum_{k=2}^{n+1} \ln(k)
 \end{aligned}$$

(on a utilisé le fait que l'indice est muet dans une somme).

On a donc en définitive :

$$\begin{aligned}
 S_n &= \ln(P_n) = \ln((n+1)^{n+1}) - \sum_{k=2}^{n+1} \ln(k) \\
 &= \ln((n+1)^{n+1}) - \ln\left(\prod_{k=2}^n k\right) = \ln((n+1)^{n+1}) - \ln(n!) \\
 &= \ln\left(\frac{(n+1)^{n+1}}{n!}\right)
 \end{aligned}$$

$$\text{et } P_n = \frac{(n+1)^n}{n!}.$$

Une autre solution consiste à effectuer directement un changement d'indice dans le produit. Soit :

$$\begin{aligned}
 P &= \prod_{k=1}^n \left(\frac{k+1}{k}\right)^k = \frac{\prod_{k=1}^n (k+1)^k}{\prod_{k=1}^n k^k} \\
 &= \frac{\prod_{j=2}^{n+1} j^{j-1}}{\prod_{k=1}^n k^k} = \frac{\prod_{k=2}^{n+1} k^{k-1}}{\prod_{k=1}^n k^k} = \frac{2 \cdot 3^2 \cdot 4^3 \cdot \dots \cdot n^{n-1} \cdot (n+1)^n}{2^2 \cdot 3^3 \cdot 4^4 \cdot \dots \cdot (n-1)^{n-1} \cdot n^n} \\
 &= \frac{(n+1)^n}{2 \cdot 3 \cdot 4 \cdot \dots \cdot (n-1) \cdot n} = \frac{(n+1)^n}{n!}.
 \end{aligned}$$

## 1.6 Les théorèmes de récurrence

On désigne par  $\mathbb{N}$  l'ensemble des entiers naturels, soit :

$$\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}.$$

La construction de cet ensemble avec les opérations usuelles d'addition et de multiplication est admise.

On note  $\mathbb{N}^*$  l'ensemble  $\mathbb{N}$  privé de 0.

Notre point de départ est l'axiome du bon ordre suivant : toute partie non vide de  $\mathbb{N}$  admet un plus petit élément, ce qui signifie que si  $A$  est une partie non vide de  $\mathbb{N}$ , il existe alors un entier  $m$  tel que :

$$\begin{cases} m \in \mathbb{N}, \\ \forall n \in A, m \leq n. \end{cases}$$

**Exercice 1.19** On peut montrer que  $\sqrt{3}$  est irrationnel en utilisant seulement le fait que  $\mathbb{N}$  est bien ordonné. Pour ce faire on raisonne par l'absurde en supposant qu'il existe deux entiers strictement positifs  $a$  et  $b$  tels que  $\sqrt{3} = \frac{a}{b}$ .

On introduit l'ensemble :

$$A = \left\{ q \in \mathbb{N} - \{0\} \mid \exists p \in \mathbb{N} \mid \sqrt{3} = \frac{p}{q} \right\}.$$

1. Montrer que  $A$  a un plus petit élément  $q_1$ . On a donc  $\sqrt{3} = \frac{p_1}{q_1}$  avec  $p_1 \in \mathbb{N}$ .
2. Montrer que  $\sqrt{3} = \frac{3q_1 - p_1}{p_1 - q_1}$  et conclure.

### Solution 1.19

1. Si on suppose  $\sqrt{3}$  rationnel alors l'ensemble  $A$  est non vide dans  $\mathbb{N}$  et en conséquence il admet un plus petit élément  $q_1$ . Comme  $q_1 \in A$ , il existe un entier  $p_1 \geq 1$  tel que  $\sqrt{3} = \frac{p_1}{q_1}$ .
2. On a :

$$\sqrt{3} + 1 = \frac{2}{\sqrt{3} - 1} = \frac{2q_1}{p_1 - q_1}$$

et :

$$\sqrt{3} = \frac{2q_1}{p_1 - q_1} - 1 = \frac{3q_1 - p_1}{p_1 - q_1} = \frac{p_2}{q_2}$$

où on a posé :

$$\begin{cases} p_2 = 3q_1 - p_1, \\ q_2 = p_1 - q_1. \end{cases}$$

Comme  $1 < \sqrt{3} = \frac{p_1}{q_1} < 2$  (puisque  $1 < 3 = \sqrt{3}^2 < 4$ ) on a  $p_1 < 2q_1$ , donc  $p_2 > 0$  et  $q_2 < q_1$ . On a donc  $\sqrt{3} = \frac{p_2}{q_2}$  avec  $q_2 \in A$  et  $q_2 < q_1$ , ce qui contredit le fait que  $q_1$  est le plus petit élément de  $A$ . On peut donc conclure à l'irrationalité de  $\sqrt{3}$ .

En fait l'exercice précédent peut se généraliser comme suit.

**Exercice 1.20** Soit  $n$  un entier naturel non carré (i. e. il n'existe pas d'entier  $p$  tel que  $n = p^2$ ). On se propose, comme dans l'exercice précédent, de montrer que  $\sqrt{n}$  est irrationnel en utilisant seulement le fait que  $\mathbb{N}$  est bien ordonné.

Pour ce faire on raisonne par l'absurde en supposant qu'il existe deux entiers strictement positifs  $a$  et  $b$  tels que  $\sqrt{n} = \frac{a}{b}$ .

On introduit l'ensemble :

$$A = \left\{ q \in \mathbb{N} - \{0\} \mid \exists p \in \mathbb{N} \mid \sqrt{n} = \frac{p}{q} \right\}.$$

1. Montrer que  $A$  a un plus petit élément  $q_1$ . On a donc  $\sqrt{n} = \frac{p_1}{q_1}$  avec  $p_1 \in \mathbb{N}$ .
2. Montrer qu'il existe un entier  $m_1 \in [1, \sqrt{n}[$  tel que  $\sqrt{n} = \frac{nq_1 - m_1p_1}{p_1 - m_1q_1}$  et conclure.

### Solution 1.20

1. Si on suppose  $\sqrt{n}$  rationnel alors l'ensemble  $A$  est non vide dans  $\mathbb{N}$  et en conséquence il admet un plus petit élément  $q_1$ . Comme  $q_1 \in A$ , il existe un entier  $p_1 \geq 1$  tel que  $\sqrt{n} = \frac{p_1}{q_1}$ .
2. L'ensemble :

$$B = \{m \in \mathbb{N}^* \mid m^2 < n\}$$

étant non vide dans  $\mathbb{N}^*$  (1 est dans  $B$  car  $n$  non carré dans  $\mathbb{N}$  entraîne  $n \geq 2$ ) et majoré par  $n$  admet un plus grand élément  $m_1 \in \mathbb{N} \cap [1, \sqrt{n}[$  et on a :

$$m_1^2 < n < (m_1 + 1)^2$$

( $m_1$  est en fait la partie entière de  $\sqrt{n}$ ). On a alors :

$$\sqrt{n} + m_1 = \frac{n - m_1^2}{\sqrt{n} - m_1} = \frac{(n - m_1^2) q_1}{p_1 - m_1 q_1}$$

et :

$$\sqrt{n} = \frac{(n - m_1^2) q_1}{p_1 - m_1 q_1} - m_1 = \frac{nq_1 - m_1 p_1}{p_1 - m_1 q_1} = \frac{p_2}{q_2}$$

où on a posé :

$$\begin{cases} p_2 = nq_1 - m_1 p_1, \\ q_2 = p_1 - m_1 q_1. \end{cases}$$

En tenant compte de  $\sqrt{n} = \frac{p_1}{q_1}$ , on a :

$$p_2 = p_1 \left( n \frac{q_1}{p_1} - m_1 \right) = p_1 (\sqrt{n} - m_1) > 0,$$

soit  $p_2 \geq 1$  et  $q_2 \geq 1$  puisque  $\sqrt{n} = \frac{p_2}{q_2} > 0$ . Ensuite de :

$$\sqrt{n} = \frac{p_1}{q_1} < m_1 + 1,$$

on déduit que :

$$q_2 = p_1 - m_1 q_1 < q_1.$$

On a donc  $q_2 \in A$  et  $q_2 < q_1$ , ce qui contredit le fait que  $q_1$  est le plus petit élément de  $A$ . On peut donc conclure à l'irrationalité de  $\sqrt{n}$ .

De l'axiome du bon ordre, on déduit les deux théorèmes fondamentaux qui suivent. Le premier résultat est souvent appelé théorème de récurrence faible et le second théorème de récurrence forte.

**Théorème 1.2** Soient  $n_0 \in \mathbb{N}$  et  $\mathcal{P}(n)$  une propriété portant sur les entiers  $n \geq n_0$ . La propriété  $\mathcal{P}(n)$  est vraie pour tout entier  $n \geq n_0$  si et seulement si :

- (i)  $\mathcal{P}(n_0)$  est vraie ;

(ii) pour tout  $n \geq n_0$  si  $\mathcal{P}(n)$  est vrai alors  $\mathcal{P}(n+1)$  est vraie.

**Démonstration.** La condition nécessaire est évidente.

En supposant les conditions (i) et (ii) vérifiées, on note  $A$  l'ensemble des entiers  $n \geq n_0$  pour lesquels  $\mathcal{P}(n)$  est faux. Si  $A$  est non vide il admet alors un plus petit élément  $n > n_0$  (puisque  $\mathcal{P}(n_0)$  est vraie). Mais alors  $\mathcal{P}(n-1)$  est vraie ce qui implique, d'après (ii), que  $\mathcal{P}(n)$  est vraie, soit une contradiction. En définitive  $A$  est vide et la propriété est vraie pour tout entier  $n \geq n_0$ . ■

**Théorème 1.3** Soient  $n_0 \in \mathbb{N}$  et  $\mathcal{P}(n)$  une propriété portant sur les entiers  $n \geq n_0$ . La propriété  $\mathcal{P}(n)$  est vraie pour tout entier  $n \geq n_0$  si et seulement si :

(i)  $\mathcal{P}(n_0)$  est vraie ;

(ii) pour tout  $n \geq n_0$  si  $\mathcal{P}(k)$  est vrai pour tout entier  $k$  compris entre  $n_0$  et  $n$ , alors  $\mathcal{P}(n+1)$  est vraie.

**Démonstration.** La condition nécessaire est évidente.

En supposant les conditions (i) et (ii) vérifiées, on note  $A$  l'ensemble des entiers  $n \geq n_0$  pour lesquels  $\mathcal{P}(n)$  est faux. Si  $A$  est non vide il admet alors un plus petit élément  $n > n_0$  et  $\mathcal{P}(k)$  est vraie pour tout  $k$  compris entre  $n_0$  et  $n-1$ , ce qui implique que  $\mathcal{P}(n)$  est vraie, soit une contradiction. En définitive  $A$  est vide et la propriété est vraie pour tout entier  $n \geq n_0$ . ■

**Exercice 1.21** Montrer que  $2^n > n^2$  pour tout entier  $n \geq 5$ .

**Solution 1.21** Pour  $n = 5$ , on a  $2^5 = 32 > 5^2 = 25$ .

Supposant le résultat acquis au rang  $n \geq 5$ , on a :

$$2^{n+1} = 2 \cdot 2^n > 2n^2 > (n+1)^2$$

puisque :

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2 > 0$$

pour  $n \geq 5$ . Le résultat est donc vrai au rang  $n+1$  et il est vrai pour tout  $n \geq 5$ .

**Exercice 1.22** Montrer que si  $\varphi$  est une fonction strictement croissante de  $\mathbb{N}$  dans  $\mathbb{N}$ , on a alors  $\varphi(n) \geq n$  pour tout  $n$ .

**Solution 1.22** Comme  $\varphi$  est une fonction de  $\mathbb{N}$  dans  $\mathbb{N}$ ,  $\varphi(0)$  est un entier naturel et donc  $\varphi(0) \geq 0$ . Supposant le résultat acquis pour  $n \geq 0$ , sachant que  $\varphi$  est strictement croissante, on a  $\varphi(n+1) > \varphi(n) \geq n$ , donc  $\varphi(n+1) > n$ , ce qui équivaut à  $\varphi(n+1) \geq n+1$  puisque  $\varphi(n+1)$  est un entier.

Le théorème de récurrence faible peut être utilisé pour montrer quelques identités classiques comme celles qui apparaissent avec les exercices qui suivent.

**Exercice 1.23** Montrer par récurrence que pour tout entier naturel non nul  $n$ , on a :

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

$$V_n = \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6},$$

$$W_n = \sum_{k=1}^n k^3 = \left( \frac{n(n+1)}{2} \right)^2 = U_n^2.$$

**Solution 1.23** Pour  $n = 1$  c'est clair.

En supposant les résultats acquis pour  $n \geq 1$ , on a :

$$U_{n+1} = \frac{n(n+1)}{2} + n + 1 = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

$$\begin{aligned} V_{n+1} &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

$$\begin{aligned} W_{n+1} &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \frac{(n+1)^2(n^2 + 4n + 4)}{4} \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 \end{aligned}$$

On a aussi :

$$\begin{aligned} U_n &= 1 + 2 + \dots + (n-1) + n \\ &= n + (n-1) + \dots + 2 + 1 \end{aligned}$$

et en additionnant terme à terme on obtient :

$$2U_n = n(n+1).$$

Le calcul de  $U_n$  peut aussi se faire en passant par  $V_{n+1}$  et en utilisant l'identité :

$$(k+1)^2 = k^2 + 2k + 1$$

Précisément, en effectuant le changement d'indice  $k = j + 1$ , on a :

$$V_{n+1} = \sum_{k=1}^{n+1} k^2 = \sum_{j=0}^n (j+1)^2 = \sum_{j=0}^n j^2 + 2 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit :

$$V_{n+1} = V_n + 2U_n + n + 1$$

et :

$$2U_n = V_{n+1} - V_n - (n+1) = (n+1)^2 - (n+1) = n(n+1)$$

ce qui donne bien  $U_n = \frac{n(n+1)}{2}$ .

De même, le calcul de  $V_n$  peut aussi se faire en passant par  $W_{n+1}$  et en utilisant l'identité :

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

Précisément, en effectuant le changement d'indice  $k = j + 1$ , on a :

$$W_{n+1} = \sum_{k=1}^{n+1} k^3 = \sum_{j=0}^n (j+1)^3 = \sum_{j=0}^n j^3 + 3 \sum_{j=0}^n j^2 + 3 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit :

$$W_{n+1} = W_n + 3V_n + 3U_n + n + 1$$

et :

$$\begin{aligned} 3V_n &= W_{n+1} - W_n - 3U_n - (n + 1) = (n + 1)^3 - 3\frac{n(n + 1)}{2} - (n + 1) \\ &= \frac{n(n + 1)(2n + 1)}{2} \end{aligned}$$

ce qui donne bien  $V_n = \frac{n(n + 1)(2n + 1)}{6}$ .

Ce procédé peut en fait se généraliser.

**Exercice 1.24** Calculer, pour tout entier naturel  $n$ , la somme :

$$I_n = 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1).$$

**Solution 1.24** On a :

$$\begin{aligned} I_n &= \sum_{k=0}^n (2k + 1) = 2 \sum_{k=0}^n k + \sum_{k=0}^n 1 = n(n + 1) + (n + 1) \\ &= (n + 1)^2. \end{aligned}$$

**Exercice 1.25** On appelle nombres triangulaires les sommes  $U_n = \sum_{k=1}^n k$  et nombres pyramidaux les sommes  $P_n = \sum_{k=1}^n U_k$ . Montrer que :

$$P_n = \frac{n(n + 1)(n + 2)}{6}.$$

**Solution 1.25** Pour  $n = 1$  on a  $P_1 = U_1 = 1$  et le résultat est acquis est vrai pour  $n = 1$ . En le supposant acquis pour  $n \geq 1$ , on a :

$$\begin{aligned} P_{n+1} &= \frac{n(n + 1)(n + 2)}{6} + \frac{(n + 1)(n + 2)}{2} \\ &= \frac{(n + 1)(n + 2)}{2} \left( \frac{n}{3} + 1 \right) = \frac{(n + 1)(n + 2)(n + 3)}{6}. \end{aligned}$$

**Exercice 1.26** Montrer par récurrence, que pour tout entier naturel  $n$  et tout nombre complexe  $\lambda$  différent de 1, on a :

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

**Solution 1.26** Pour  $n = 0$ , c'est clair. Si c'est vrai pour  $n \geq 0$ , alors :

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

Plus généralement, on a l'identité (dite remarquable) suivante.

**Exercice 1.27** Montrer que pour tout entier naturel  $n$  et tous nombres complexes  $a$  et  $b$  on a :

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

**Solution 1.27** Pour  $n = 0$ , c'est évident. En supposant le résultat acquis au rang  $n \geq 0$ , on a :

$$\begin{aligned} b^{n+2} - a^{n+2} &= (b^{n+1} - a^{n+1})b + ba^{n+1} - a^{n+2} \\ &= (b - a) \sum_{k=0}^n a^k b^{n+1-k} + (b - a)a^{n+1} \\ &= (b - a)(b^{n+1} + ab^n + \dots + a^{n-1}b^2 + a^n b) + (b - a)a^{n+1} \\ &= (b - a) \sum_{k=0}^{n+1} a^k b^{n+1-k}. \end{aligned}$$

Le résultat est donc vrai pour tout  $n \geq 0$ .

Le théorème de récurrence nous permet de définir la fonction factorielle sur l'ensemble des entiers naturels de la façon suivante :

$$\begin{cases} 0! = 1 \\ \forall n \in \mathbb{N}, (n+1)! = (n+1)n! \end{cases}$$

De manière plus générale, c'est le théorème de récurrence qui nous assure de l'existence et de l'unicité d'une suite (réelle ou complexe) définie par :

$$\begin{cases} u_0 \text{ est un scalaire donné,} \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

où  $f$  est une fonction définie sur un ensemble  $I$  et à valeurs dans le même ensemble  $I$ . Une telle suite est dite définie par une relation de récurrence (d'ordre 1).

Une telle suite peut aussi se définir en donnant les premières valeurs  $u_0, u_1, \dots, u_p$  et une relation  $u_{n+1} = f(u_n, \dots, u_{n-(p-1)})$  pour  $n \geq p-1$ . Une telle suite est dite définie par une relation de récurrence d'ordre  $p$ .

**Exercice 1.28** Montrer que pour tout entier naturel  $n$  et tous nombres complexes  $a$  et  $b$  on a :

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

où  $C_n^k = \frac{n!}{k!(n-k)!}$  pour  $k$  compris entre 0 et  $n$  avec la convention  $0! = 1$  (formule du binôme de Newton).

**Solution 1.28** Pour  $n = 0$  et  $n = 1$ , c'est évident. En supposant le résultat acquis au rang  $n \geq 1$ , on a :

$$\begin{aligned} (a+b)^{n+1} &= (a+b)^n (a+b) = \left( \sum_{k=0}^n C_n^k a^{n-k} b^k \right) (a+b) \\ &= \sum_{k=0}^n C_n^k a^{n-(k-1)} b^k + \sum_{k=0}^n C_n^k a^{n-k} b^{k+1} \\ &= \sum_{k=0}^n C_n^k a^{n-(k-1)} b^k + \sum_{k=1}^{n+1} C_n^{k-1} a^{n-(k-1)} b^k \\ &= a^{n+1} + \sum_{k=1}^n (C_n^k + C_n^{k-1}) a^{n+1-k} b^k + b^{n+1} \end{aligned}$$

et tenant compte de  $C_n^k + C_n^{k-1} = C_{n+1}^k$  (triangle de Pascal), cela s'écrit :

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

Le résultat est donc vrai pour tout  $n \geq 0$ .

Les coefficients  $C_n^k$  se notent aussi  $\binom{n}{k}$ .

On peut remarquer que, pour  $k$  fixé :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

est un polynôme en  $n$  de degré  $k$ , ce qui permet d'étendre cette définition à  $\mathbb{R}$  ou même  $\mathbb{C}$ .

Comme  $(a+b)^n$ , on a aussi :

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

**Exercice 1.29** Montrer par récurrence, que pour tout entier naturel non nul  $n$  et tout nombre complexe  $\lambda$  différent de 1, on a :

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

**Solution 1.29** Pour  $n = 1$ , c'est clair. Si c'est vrai pour  $n \geq 1$ , alors :

$$\begin{aligned} \sum_{k=1}^{n+1} k\lambda^k &= n \frac{\lambda^{n+1}}{\lambda-1} + \lambda \frac{1-\lambda^n}{(\lambda-1)^2} + (n+1)\lambda^{n+1} \\ &= n \frac{\lambda^{n+1}}{\lambda-1} + \lambda \frac{1-\lambda^n}{(\lambda-1)^2} + n\lambda^{n+1} \frac{\lambda-1}{\lambda-1} + \lambda^{n+1} \frac{(\lambda-1)^2}{(\lambda-1)^2} \\ &= \frac{n\lambda^{n+2}}{\lambda-1} + \frac{\lambda}{(\lambda-1)^2} (1 + \lambda^{n+1}(\lambda-2)) \\ &= \frac{(n+1)\lambda^{n+2}}{\lambda-1} + \frac{\lambda}{(\lambda-1)^2} (1 - \lambda^{n+1}). \end{aligned}$$

**Exercice 1.30** Montrer que pour tout entier  $n \geq 1$ , on a :

$$\sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}} = 2 \cos\left(\frac{\pi}{2^{n+1}}\right)$$

(le nombre 2 apparaissant  $n$  fois sous la racine).

**Solution 1.30** Notons  $x_n = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}}$ . Pour  $n = 1$ , on a :

$$x_1 = \sqrt{2} = 2 \cos\left(\frac{\pi}{4}\right).$$

Supposant le résultat acquis au rang  $n \geq 1$ , on a :

$$x_{n+1}^2 = 2 + x_n = 2 + 2 \cos\left(\frac{\pi}{2^{n+1}}\right)$$

et utilisant la formule  $\cos(2\theta) = 2 \cos^2(\theta) - 1$ , il vient :

$$\cos\left(\frac{\pi}{2^{n+1}}\right) = \cos\left(2 \frac{\pi}{2^{n+2}}\right) = 2 \cos^2\left(\frac{\pi}{2^{n+2}}\right) - 1$$

on a :

$$x_{n+1}^2 = 4 \cos^2\left(\frac{\pi}{2^{n+2}}\right).$$

Comme  $x_{n+1}$  est positif, on en déduit que  $x_{n+1} = 2 \cos\left(\frac{\pi}{2^{n+2}}\right)$ .

**Exercice 1.31** Soit  $x_1, x_2, \dots, x_n$  des réels dans  $[0, 1]$ . Montrer par récurrence que  $\prod_{k=1}^n (1 - x_k) \geq$

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

**Solution 1.31** Notons :

$$u_n = \prod_{k=1}^n (1 - x_k) \quad \text{et} \quad v_n = 1 - \sum_{k=1}^n x_k.$$

Pour  $n = 1$ , on a  $u_1 = v_1$ .

Supposant le résultat acquis au rang  $n \geq 1$  et tenant compte de  $1 - x_{n+1} \geq 0$ , on a :

$$\begin{aligned} u_{n+1} &= u_n (1 - x_{n+1}) \geq \left(1 - \sum_{k=1}^n x_k\right) (1 - x_{n+1}) \\ &\geq 1 - \sum_{k=1}^n x_k - x_{n+1} + x_{n+1} \sum_{k=1}^n x_k \geq 1 - \sum_{k=1}^{n+1} x_k = v_{n+1}. \end{aligned}$$

puisque tous les  $x_k$  sont positifs.

Les théorèmes de récurrence peuvent aussi être utilisés pour montrer les résultats fondamentaux d'arithmétique suivants.

**Exercice 1.32** Soit  $a, b$  deux entiers naturels avec  $b$  non nul. Montrer qu'il existe un unique couple d'entiers  $(q, r)$  tel que :

$$\begin{cases} a = bq + r, \\ 0 \leq r \leq b - 1. \end{cases}$$

**Solution 1.32** On montre tout d'abord l'existence du couple  $(q, r)$  par récurrence sur l'entier  $a \geq 0$ .

Pour  $a = 0$ , le couple  $(q, r) = (0, 0)$  convient.

Supposant le résultat acquis pour tous les entiers  $a'$  compris entre 0 et  $a - 1$ , où  $a$  est un entier naturel non nul, on distingue deux cas. Si  $a$  est compris entre 1 et  $b - 1$ , le couple  $(q, r) = (0, a)$  convient, sinon on a  $a \geq b$ , donc  $0 \leq a - b \leq a - 1$  et l'hypothèse de récurrence nous assure de l'existence d'un couple d'entiers  $(q, r)$  tels que  $a - b = bq + r$  et  $0 \leq r \leq b - 1$ , ce qui nous fournit le couple d'entiers  $(q', r) = (q + 1, r)$ .

L'unicité se montre facilement par l'absurde.

**Exercice 1.33** Soit  $n$  un entier naturel supérieur ou égal à 2. Montrer, par récurrence, que soit  $n$  est premier, soit  $n$  admet un diviseur premier  $p \leq \sqrt{n}$ .

**Solution 1.33** Pour  $n = 2$  et  $n = 3$ , le résultat est évident ( $n$  est premier).

Supposons le acquis pour tous les entiers strictement inférieurs à  $n \geq 3$ . Si  $n$  est premier, c'est terminé, sinon il existe deux entiers  $a$  et  $b$  compris entre 2 et  $n - 1$  tels que  $n = ab$  et comme ces deux entiers jouent des rôles symétriques, on peut supposer que  $a \leq b$ . L'hypothèse de récurrence nous dit que soit  $a$  est premier et c'est alors un diviseur premier de  $n$  tel que  $a^2 \leq ab \leq n$ , soit  $a$  admet un diviseur premier  $p \leq \sqrt{a}$  et  $p$  divise aussi  $n$  avec  $p \leq \sqrt{n}$ .

**Exercice 1.34** Montrer que tout entier naturel  $n$  supérieur ou égal à 2 se décompose de manière unique sous la forme :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

où les  $p_k$  sont des nombres premiers vérifiant :

$$2 \leq p_1 < p_2 < \cdots < p_r$$

et les  $\alpha_k$  sont des entiers naturels non nuls (décomposition en nombres premiers).

**Solution 1.34** On démontre tout d'abord l'existence d'une telle décomposition par récurrence sur  $n \geq 2$ .

Pour  $n = 2$ , on a déjà la décomposition.

Supposons que, pour  $n \geq 2$ , tout entier  $k$  compris entre 2 et  $n$  admet une telle décomposition. Si  $n + 1$  est premier, on a déjà la décomposition, sinon on écrit  $n + 1 = ab$  avec  $a$  et  $b$  compris entre 2 et  $n$  et il suffit d'utiliser l'hypothèse de récurrence pour  $a$  et  $b$ .

L'unicité d'une telle décomposition se montre également par récurrence sur  $n \geq 2$ . Le résultat est évident pour  $n = 2$ . Supposons le acquis pour tout entier  $k$  compris entre 2 et  $n \geq 2$ . Si  $n + 1$  a deux décompositions :

$$n + 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s},$$

où les  $p_j$  [resp.  $q_i$ ] sont premiers deux à deux distincts et les  $\alpha_j$  [resp.  $\beta_i$ ] entiers naturels non nuls. L'entier  $p_1$  est premier et divise le produit  $q_1^{\beta_1} \cdots q_s^{\beta_s}$ , il divise donc nécessairement l'un des  $q_k$ . L'entier  $q_k$  étant également premier la seule possibilité est  $p_1 = q_k$ . En simplifiant par  $p_1$  on se ramène à la décomposition d'un entier inférieur ou égal à  $n$  et il suffit d'utiliser l'hypothèse de récurrence pour conclure.

**Exercice 1.35** Pour tout entier naturel  $n$  supérieur ou égal à 2, on note  $H_n = \sum_{k=1}^n \frac{1}{k}$ .

1. Soit  $p$  un entier naturel non nul. Montrer que  $H_{2p} = \frac{1}{2}H_p + \frac{a}{2b+1}$  où  $a, b$  sont des entiers naturels avec  $a$  non nul.
2. Montrer par récurrence que pour tout entier naturel non nul  $H_n$  est le quotient d'un entier impair par un entier pair et qu'en conséquence ce n'est pas un entier.

**Solution 1.35**

1. On a :

$$H_{2p} = \sum_{k=1}^p \frac{1}{2k} + \sum_{k=0}^{p-1} \frac{1}{2k+1} = \frac{1}{2}H_p + \frac{N}{D}$$

avec  $D = \text{ppcm}(1, 3, \dots, 2p-1)$  qui est impair et  $N$  entier naturel non nul.

2. On a  $H_2 = \frac{3}{2} \notin \mathbb{N}$ . Supposons le résultat acquis au rang  $n \geq 2$ . Si  $n = 2p$ , on a alors :

$$\begin{aligned} H_{n+1} &= H_n + \frac{1}{2p+1} = \frac{2a+1}{2b} + \frac{1}{2p+1} \\ &= \frac{(2a+1)(2p+1) + 2b}{2b(2p+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec  $a' = a + b + p + 2ap$  et  $b' = b(2p+1)$ . Si  $n = 2p+1$ , on a alors :

$$\begin{aligned} H_{n+1} &= H_{2(p+1)} = \frac{c}{2d+1} + \frac{1}{2}H_{p+1} \\ &= \frac{c}{2d+1} + \frac{1}{2} \frac{2a+1}{2b} = \frac{4bc + (2d+1)(2a+1)}{4b(2d+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec  $a' = a + d + 2ad + 2bc$  et  $b' = 2b(2d+1)$ .

Dans tous les cas,  $H_n$  est le quotient d'un entier impair par un entier pair et en conséquence, ce n'est pas un entier.

## 1.7 L'algèbre des parties d'un ensemble

Nous allons définir sur l'ensemble  $\mathcal{P}(E)$  des parties d'un ensemble  $E$  des opérations qui vont traduire les idées intuitives de partie complémentaire, d'intersection et de réunion.

L'ensemble  $E$  étant donné et  $A, B, C, \dots$  désignant des parties de  $E$  (donc des éléments de  $\mathcal{P}(E)$ ), on définit les ensembles suivant.

- le complémentaire de  $A$  dans  $E$  est l'ensemble noté  $C_E A$ , ou  $E \setminus A$  (lire  $E$  moins  $A$ ) ou  $\bar{A}$  des éléments de  $E$  qui ne sont pas dans  $A$ , ce qui peut se traduire par :

$$(x \in \bar{A}) \Leftrightarrow ((x \in E) \wedge (x \notin A))$$

ou encore par :

$$\bar{A} = \{x \in E \mid x \notin A\}$$

- L'intersection de  $A$  et  $B$ , notée  $A \cap B$ , est l'ensemble des éléments de  $E$  qui sont dans  $A$  et dans  $B$ , soit :

$$(x \in A \cap B) \Leftrightarrow ((x \in A) \wedge (x \in B))$$

ou encore :

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$

Si  $A \cap B = \emptyset$ , on dit alors que  $A$  et  $B$  sont disjointes.

Par exemple  $A$  et  $\bar{A}$  sont disjointes.

- La réunion de  $A$  et  $B$ , notée  $A \cup B$ , est l'ensemble des éléments de  $E$  qui sont soit dans  $A$ , soit dans  $B$  (éventuellement dans  $A$  et  $B$ ) soit :

$$(x \in A \cup B) \Leftrightarrow ((x \in A) \vee (x \in B))$$

ou encore :

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$

- La différence de  $A$  et  $B$ , notée  $A \setminus B$ , est l'ensemble des éléments de  $E$  qui sont dans  $A$  et qui ne sont pas dans  $B$ , soit :

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

ou encore :

$$A \setminus B = \{x \in A \mid x \notin B\}$$

Ainsi  $\bar{A} = E \setminus A$ .

- La différence symétrique de  $A$  et  $B$ , notée  $A \Delta B$ , est l'ensemble des éléments de  $E$  qui sont soit dans  $A$  et pas dans  $B$  soit dans  $B$  et pas dans  $A$  (c'est-à-dire dans  $A$  ou exclusif dans  $B$ ), soit :

$$(x \in A \Delta B) \Leftrightarrow ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$$

Par exemple, on a  $A \Delta \emptyset = A$ ,  $A \Delta E = \bar{A}$ .

Ces opérateurs de complémentarité, intersection, réunion et différence symétrique sont décrits à l'aide des connecteurs logiques non de négation,  $\wedge$  de conjonction,  $\vee$  de disjonction et  $\Delta$  de disjonction exclusive.

Avec le théorème qui suit, on résume les résultats essentiels relatifs à ces opérateurs ensemblistes.

**Théorème 1.4** Soient  $E$  un ensemble et  $A, B, C, \dots$  des sous-ensembles de  $E$ . On a :

1. commutativité :

$$A \cap B = B \cap A$$

$$A \cup B = B \cup A$$

$$A \Delta B = B \Delta A$$

2. associativité :

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

3. distributivité :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4. différence symétrique :

$$\begin{aligned} A\Delta A &= \emptyset \\ A\Delta B &= (A \setminus B) \cup (B \setminus A) \\ A\Delta B &= (A \cap \overline{B}) \cup (B \cap \overline{A}) \\ A\Delta B &= (A \cup B) \setminus (A \cap B) \end{aligned}$$

5. négations :

$$\begin{aligned} \overline{\overline{A}} &= A \\ (A \subset B) &\Leftrightarrow (\overline{B} \subset \overline{A}) \\ \overline{A \cap B} &= \overline{A} \cup \overline{B} \\ \overline{A \cup B} &= \overline{A} \cap \overline{B} \end{aligned}$$

**Démonstration.** Laissée au lecteur. ■

On notera l'analogie entre ce théorème et le théorème 1.1 sur les règles de calculs avec les connecteurs logiques.

Toutes ces égalités entre ensembles se visualisent bien en utilisant les diagrammes d'Euler-Venn.

La propriété d'associativité de l'intersection et de la réunion nous permet d'écrire  $A \cap B \cap C$  et  $A \cup B \cup C$  l'intersection et la réunion de trois ensembles sans se soucier de parenthèses. De manière plus générale, grâce à cette associativité, on peut définir l'intersection ou la réunion de  $n$  sous-ensembles  $A_1, A_2, \dots, A_n$  de  $E$  par :

$$(x \in A_1 \cap A_2 \cap \dots \cap A_n) \Leftrightarrow ((x \in A_1) \wedge (x \in A_2) \wedge \dots \wedge (x \in A_n))$$

et :

$$(x \in A_1 \cup A_2 \cup \dots \cup A_n) \Leftrightarrow ((x \in A_1) \vee (x \in A_2) \vee \dots \vee (x \in A_n))$$

De façon condensée, on écrira  $(A_k)_{1 \leq k \leq n}$  une telle famille de sous ensembles de  $E$  et :

$$\bigcap_{k=1}^n A_k = A_1 \cap A_2 \cap \dots \cap A_n$$

l'intersection et :

$$\bigcup_{k=1}^n A_k = A_1 \cup A_2 \cup \dots \cup A_n$$

la réunion.

On vérifie facilement que pour tout entier  $j$  compris entre 1 et  $n$ , on a :

$$\bigcap_{k=1}^n A_k \subset A_j \subset \bigcup_{k=1}^n A_k.$$

**Définition 1.1** On dit qu'une famille  $(A_k)_{1 \leq k \leq n}$  de parties d'un ensemble  $E$  forme une partition de  $E$  si les  $A_k$  sont deux à deux disjoints, c'est-à-dire que  $A_k \cap A_j = \emptyset$  pour  $1 \leq k \neq j \leq n$  de réunion égale à  $E$ , soit  $\bigcup_{k=1}^n A_k = E$ .

Dans le cas où  $(A_1, A_2)$  forme une partition de  $E$ , on a nécessairement  $A_2 = \overline{A_1}$ .

**Exercice 1.36** Simplifier les expressions suivantes, où  $A$  et  $B$  sont des sous-ensembles d'un ensemble  $E$  :

1.  $C = (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B}) \cup (A \cap B)$
2.  $\overline{C}$
3.  $D = \overline{\overline{\overline{A \cap B} \cap (\overline{A} \cap B)} \cup (A \cap B) \cap (A \cap B)}$

**Solution 1.36**

1. Avec la distributivité de  $\cap$  sur  $\cup$ , on a :

$$\overline{A} = \overline{A} \cap E = \overline{A} \cap (B \cup \overline{B}) = (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B})$$

(on a mis  $\overline{A}$  en facteur) et avec la distributivité de  $\cup$  sur  $\cap$ , on a :

$$C = \overline{A} \cup (A \cap B) = (\overline{A} \cup A) \cap (\overline{A} \cup B) = E \cap (\overline{A} \cup B) = \overline{A} \cup B.$$

2.  $\overline{C} = A \cap \overline{B}$ .

3. En posant :

$$X = A \cap \overline{B}, Y = \overline{X} \cap (\overline{A} \cap B), Z = \overline{Y} \cup (A \cap B), T = \overline{Z} \cap (A \cap B)$$

on a :

$$\begin{aligned} D = \overline{T} &= Z \cup (\overline{A} \cup \overline{B}) = \overline{Y} \cup (A \cap B) \cup (\overline{A} \cup \overline{B}) \\ &= X \cup (A \cup \overline{B}) \cup (A \cap B) \cup (\overline{A} \cup \overline{B}) \end{aligned}$$

avec  $(A \cup \overline{B}) \cup (\overline{A} \cup \overline{B}) = E$ , donc  $D = E$ .

**Exercice 1.37** Soient  $A_1, A_2, \dots, A_p$  des ensembles deux à deux distincts. Montrer que l'un de ces ensembles ne contient aucun des autres.

**Solution 1.37** On raisonne par l'absurde, c'est-à-dire qu'on suppose que chacun des ensembles  $A_k$  contient un ensemble  $A_j$  différent de  $A_k$ . Donc  $A_1$  contient un ensemble  $A_{j_1} \neq A_1$ , soit  $A_{j_1} \subsetneq A_1$ ,  $A_{j_1}$  contient un ensemble  $A_{j_2} \neq A_{j_1}$ , soit  $A_{j_2} \subsetneq A_{j_1}$ , et on peut continuer indéfiniment, ce qui est impossible puisque la famille d'ensembles est finie.

**Exercice 1.38** Que dire de deux ensembles  $A$  et  $B$  tels que  $A \cap B = A \cup B$  ?

**Solution 1.38** On a toujours  $A \cap B \subset A \cup B$ . Si de plus  $A \cup B \subset A \cap B$ , on a alors :

$$A \subset A \cup B \subset A \cap B \subset B \text{ et } B \subset A \cup B \subset A \cap B \subset A$$

ce qui donne  $A = B$ .

**Exercice 1.39** Soient  $A, B, C$  trois ensembles. Montrer que  $A \cap C = A \cup B$  si, et seulement si,  $B \subset A \subset C$ .

**Solution 1.39** Si  $A \cap C = A \cup B$ , alors :

$$B \subset A \cup B = A \cap C \subset A \text{ et } A \subset A \cup B = A \cap C \subset C.$$

Réciproquement si  $B \subset A \subset C$ , alors :

$$A \cap C = A = A \cup B$$

**Exercice 1.40** Soient  $A, B, C$  trois ensembles. Montrer que si  $A \cup B \subset A \cup C$  et  $A \cap B \subset A \cap C$ , alors  $B \subset C$ .

**Solution 1.40** Soit  $x \in B$ . Comme  $A \cup B \subset A \cup C$ ,  $x$  est dans  $A \cup C$ . S'il est dans  $C$  c'est fini, sinon il est dans  $A$ , donc dans  $A \cap B \subset A \cap C$ , donc dans  $C$ .

**Exercice 1.41** Soient  $A, B, C$  trois ensembles. Montrer que :

$$(A \cup B) \cap (B \cup C) \cap (C \cup A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$$

**Solution 1.41** On a :

$$(A \cup B) \cap (B \cup C) = B \cup (A \cap C)$$

et, en notant  $D = (A \cup B) \cap (B \cup C) \cap (C \cup A)$ , on a :

$$D = ((B \cap C) \cup (A \cap B)) \cup (C \cap A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$$

Où alors on part de  $x \in D$  et on montre que  $x \in E = (A \cap B) \cup (B \cap C) \cup (C \cap A)$ , puis partant de  $x \in E$ , on montre que  $x \in D$ .

La notion de produit cartésien de deux ensembles sera très souvent utilisée. Elle correspond à l'idée de couples et se généralise pour aboutir à la notion de liste.

**Définition 1.2** Étant donné deux ensembles  $E$  et  $F$ , on appelle produit cartésien de  $E$  par  $F$  l'ensemble  $E \times F$  des couples  $(x, y)$  formés d'un élément  $x$  de  $E$  et d'un élément  $y$  de  $F$ .

Il est à noter que les couples sont ordonnés, c'est-à-dire que  $(x, y) = (y, x)$   $E \times F$  si, et seulement si  $x = y$ . De manière plus générale, on a  $(x, y) = (x', y')$  dans  $E \times F$  si, et seulement si  $x = x'$  et  $y = y'$ .

Dans le cas où  $F = E$ , on note  $E^2$  pour  $E \times E$ .

On peut itérer le procédé et définir le produit cartésien  $E_1 \times E_2 \times \cdots \times E_n$  de  $n$  ensembles comme l'ensemble des listes (ordonnées)  $(x_1, x_2, \cdots, x_n)$  formées d'un élément  $x_1$  de  $E_1$  suivi d'un élément  $x_2$  de  $E_2$ ,  $\cdots$ , suivi d'un élément  $x_n$  de  $E_n$ . On notera de façon condensé :

$$\prod_{k=1}^n E_k = E_1 \times E_2 \times \cdots \times E_n.$$

Là encore, on a  $(x_1, x_2, \cdots, x_n) = (x'_1, x'_2, \cdots, x'_n)$  dans  $E \times F$  si, et seulement si  $x_k = x'_k$  pour tout  $k$  compris entre 1 et  $n$ .

Dans le cas où tous les  $E_k$  sont égaux à un même ensemble  $E$ , on notera  $E^n$  pour  $E \times E \times \cdots \times E$  ( $n$  fois).

**Exercice 1.42** Montrer que l'ensemble :

$$C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$

ne peut pas s'écrire comme produit cartésien de deux parties de  $\mathbb{R}$ .

**Solution 1.42** Si  $C = E \times F$ , où  $E$  et  $F$  sont deux parties de  $\mathbb{R}$ , on a alors  $(1, 0) \in C = E \times F$  et  $(1, 0) \in C = E \times F$ , donc  $1 \in E \cap F$  et  $(1, 1) \in E \times F = C$ , ce qui est faux.

## 1.8 Applications. Notions d'injectivité, surjectivité et bijectivité

Les notations  $E, F, G$  désignent des ensembles.

**Définition 1.3** On appelle application, ou fonction, de  $E$  dans  $F$  (ou de  $E$  vers  $F$ ) toute partie  $\Gamma$  du produit cartésien  $E \times F$  telle que :

$$\forall x \in E, \exists ! y \in F \mid (x, y) \in \Gamma.$$

En notant  $f$  une application de  $E$  dans  $F$  (c'est en réalité le triplet  $(E, F, \Gamma)$  avec la propriété énoncée ci-dessus), on notera pour tout  $x \in E$ ,  $f(x)$  l'unique élément de  $F$  tel que  $(x, f(x)) \in \Gamma$  et on dira que  $f(x)$  est l'image de  $x$  par  $f$  et  $x$  est un antécédent de  $y$  par  $f$ . Un antécédent de  $y$  par  $f$  n'est pas unique a priori.

On dira aussi que  $E$  est l'ensemble de départ (ou l'ensemble de définition),  $F$  l'ensemble d'arrivée et  $\Gamma$  le graphe de l'application  $f$ .

Deux applications  $f$  et  $g$  sont égales si, et seulement si, elles ont même ensemble de départ  $E$ , même ensemble d'arrivée  $F$  et même graphe  $\Gamma$ , c'est-à-dire que :

$$\forall x \in E, g(x) = f(x)$$

On a tout simplement précisé l'idée d'un procédé qui associe à tout élément de  $E$  un unique élément de  $F$ .

On notera :

$$\begin{aligned} f : E &\rightarrow F \\ x &\mapsto f(x) \end{aligned}$$

une telle application (ou fonction). On utilisera aussi les notation  $f : E \rightarrow F$  ou  $f : x \mapsto f(x)$ .

**Remarque 1.2** Nous ne faisons pas la distinction ici entre fonction et application. Usuellement, on distingue ces notions en disant qu'une fonction de  $E$  dans  $F$  toute partie  $\Gamma$  du produit cartésien  $E \times F$  telle que pour tout élément  $x$  de  $E$ , il existe au plus un élément  $y$  de  $F$  tel que  $(x, y) \in \Gamma$ . Le sous-ensemble  $D$  de  $E$  pour lequel il existe un unique élément  $y$  de  $F$  tel que  $(x, y) \in \Gamma$  est appelé l'ensemble de définition de la fonction. Une application est donc une fonction pour laquelle tout élément de l'ensemble de départ  $E$  a une image dans  $F$ .

On notera  $\mathcal{F}(E, F)$  ou  $F^E$  l'ensemble de toutes les applications de  $E$  dans  $F$  (la deuxième notation sera justifiée plus loin).

L'application qui associe à tout  $x$  d'un ensemble  $E$  le même  $x$  est l'application identique notée  $Id_E$ , où  $Id$  si l'ensemble  $E$  est fixé.

Si  $f$  est une fonction de  $E$  dans  $F$  et  $D$  un sous-ensemble non vide de  $E$ , on définit une application  $g$  de  $D$  dans  $F$  en posant :

$$\forall x \in D, g(x) = f(x)$$

et on dit que  $g$  est la restriction de  $f$  à  $D$ , ce qui se note  $g = f|_D$ .

**Définition 1.4** Soit  $f$  une application de  $E$  dans  $F$ . Pour toute partie  $A$  de  $E$ , l'image de  $A$  par  $f$  est le sous ensemble de  $F$  noté  $f(A)$  et défini par :

$$f(A) = \{f(x) \mid x \in A\}.$$

Pour toute partie  $B$  de  $F$ , l'image réciproque de  $B$  par  $f$  est le sous ensemble de  $E$  noté  $f^{-1}(B)$  et défini par :

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

On a donc, pour tout  $y \in F$  :

$$y \in f(A) \Leftrightarrow \exists x \in A \mid y = f(x)$$

et pour tout  $x \in E$  :

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$

L'ensemble  $f(E)$  est appelé l'image de  $f$ .

À propos de la notation  $f^{-1}(B)$ , on pourra lire la remarque 1.3 (qui n'engage que moi) plus loin.

**Exemple 1.1** On a  $f(\emptyset) = \emptyset$ ,  $f(\{x\}) = \{f(x)\}$  pour tout  $x \in E$ ,  $f^{-1}(\emptyset) = \emptyset$  et  $f^{-1}(F) = E$ .

Pour tout  $y \in F$ ,  $f^{-1}\{y\}$  est l'ensemble des  $x \in E$  tels que  $f(x) = y$  et cet ensemble peut être vide ou formé de un ou plusieurs éléments. En fait  $f^{-1}\{y\}$  est l'ensemble des solutions dans  $E$  de l'équation  $f(x) = y$ , où  $y$  est donné dans  $F$  et  $x$  l'inconnue dans  $E$ . Cette équation peut avoir 0 ou plusieurs solutions.

**Exemple 1.2** Pour  $f : x \mapsto x^2$  avec  $E = F = \mathbb{R}$ , on a  $f^{-1}\{0\} = \{0\}$ ,  $f^{-1}\{-1\} = \emptyset$  et  $f^{-1}\{1\} = \{-1, 1\}$ .

On vérifie facilement le résultat suivant.

**Théorème 1.5** Soit  $f$  une application de  $E$  dans  $F$ . Pour toutes parties  $A, B$  de  $E$  et  $C, D$  de  $F$ , on a :

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

**Démonstration.** Vérification immédiate.

Par exemple, pour le point 2, on peut écrire que  $y$  est dans  $f(A \cup B)$  si, et seulement si, il existe  $x$  dans  $A \cup B$  tel que  $y = f(x)$ , ce qui implique que  $y \in f(A)$  dans le cas où  $x \in A$  ou  $y \in f(B)$  dans le cas où  $x \in B$ , soit  $y \in f(A) \cup f(B)$  dans tous les cas. Réciproquement si  $y \in f(A) \cup f(B)$ , il est dans  $f(A)$  ou  $f(B)$  et s'écrit donc  $y = f(x)$  avec  $x$  dans  $A$  ou  $B$ , ce qui signifie que  $y \in f(A \cup B)$ . On a donc les inclusions  $f(A \cup B) \subset f(A) \cup f(B)$  et  $f(A) \cup f(B) \subset f(A \cup B)$ , c'est-à-dire l'égalité souhaitée.

Pour le point 3, on a seulement une inclusion. Dire que  $y \in f(A \cap B)$  équivaut à dire qu'il existe  $x \in A \cap B$  tel que  $y = f(x)$  et  $y \in f(A) \cap f(B)$ . Réciproquement, si  $y \in f(A) \cap f(B)$ , il existe  $x_1 \in A$  et  $x_2 \in B$  tels que  $y = f(x_1) = f(x_2)$  et, a priori, il n'y a aucune raison pour que  $x_1 = x_2$ . ■

**Exercice 1.43** Vérifier sur un exemple que l'égalité  $f(A \cap B) = f(A) \cap f(B)$  n'est pas toujours vérifiée.

**Solution 1.43** Considérer  $f : x \mapsto \sin(x)$  avec  $A = [-\pi, \pi]$  et  $B = [0, 2\pi]$ . On a :

$$f(A \cap B) = f([0, \pi]) = [0, 1] \subsetneq f(A) \cap f(B) = [-1, 1].$$

**Exercice 1.44** Soit  $f$  une application de  $E$  dans  $F$ . Vérifier que :

1. pour toute partie  $A$  de  $E$ ,  $A \subset f^{-1}(f(A))$
2. pour toute partie  $B$  de  $F$ ,  $f(f^{-1}(B)) = B \cap f(E)$ .

**Solution 1.44** Vérification immédiate.

**Exercice 1.45** Soient  $E$  un ensemble et  $f$  une application de  $\mathcal{P}(E)$  dans  $\mathbb{R}$  telle que pour toutes parties disjointes de  $E$  on ait  $f(A \cup B) = f(A) + f(B)$ .

1. Montrer que  $f(\emptyset) = 0$ .
2. Montrer que pour toutes parties  $A, B$  de  $E$ , on a :

$$f(A \cup B) + f(A \cap B) = f(A) + f(B).$$

**Solution 1.45**

1. On a  $f(\emptyset) = f(\emptyset \cup \emptyset) = f(\emptyset) + f(\emptyset)$  dans  $\mathbb{R}$ , donc  $f(\emptyset) = 0$ .
2. Avec les partitions  $A \cup B = A \cup (B \setminus A)$  et  $B = (A \cap B) \cup (B \setminus A)$ , on a :

$$\begin{cases} f(A \cup B) = f(A) + f(B \setminus A) \\ f(B) = f(A \cap B) + f(B \setminus A) \end{cases}$$

et par soustraction :

$$f(A \cup B) - f(B) = f(A) - f(A \cap B)$$

qui donne le résultat.

Après avoir défini le cardinal d'un ensemble et la notion d'ensemble fini (qui est quand même intuitive), nous verrons que si  $E$  est un ensemble fini alors la fonction  $f$  qui associe à une partie  $A$  de  $E$  son cardinal (c'est-à-dire le nombre de ses éléments) vérifie l'équation fonctionnelle de l'exercice précédent.

On dispose d'une opération importante sur les fonctions, c'est la composition des fonctions qui permet de construire de nouvelles fonctions à partir de fonctions données.

**Définition 1.5** Soient  $f$  une application de  $E$  dans  $F$  et  $g$  une application de  $F$  dans  $G$ . La composée de  $f$  par  $g$  est la fonction de  $E$  dans  $G$  notée  $g \circ f$  et définie par :

$$\forall x \in E, g \circ f(x) = g(f(x)).$$

Ce qui peut se schématiser par :

$$\begin{array}{ccccc} E & \xrightarrow{f} & F & \xrightarrow{g} & G \\ x & \mapsto & f(x) & \mapsto & g(f(x)) \end{array}$$

On remarquera que  $f \circ g$  n'est pas définie a priori (dans la situation de la définition).

Dans le cas où  $f$  est définie de  $E$  dans  $F$  et  $g$  de  $F$  dans  $E$ , on peut définir les applications  $f \circ g$  (de  $F$  dans  $F$ ) et  $g \circ f$  (de  $E$  dans  $E$ ) et il n'y a aucune raison pour que ces applications soient égales, même si  $F = E$ .

Dans le cas où  $E = F$ , on dit que les applications  $f$  et  $g$  (définies de  $E$  dans  $E$ ) commutent si  $f \circ g = g \circ f$ .

On vérifie facilement que la loi de composition est associative, c'est-à-dire que  $f \circ (g \circ h) = (f \circ g) \circ h$ , quand toutes ces composées ont un sens.

Cette propriété d'associativité permet de définir la composée de  $n$  applications  $f_1 \circ f_2 \circ \dots \circ f_n$  sans se soucier de parenthèses.

Si  $f$  est une application de  $E$  dans  $E$ , on peut définir la suite de ses itérées par la relation de récurrence suivante :

$$\begin{cases} f^1 = f \\ \forall n \in \mathbb{N}^*, f^{n+1} = f^n \circ f \end{cases}$$

On convient que  $f^0 = Id_E$ .

On vérifie facilement que  $f^p \circ f^q = f^q \circ f^p = f^{p+q}$  pour tous entiers naturels  $p, q$ .

**Exercice 1.46** Soient  $E$  et  $F$  deux ensembles. Déterminer toutes les applications  $f$  de  $E$  dans  $E$  telles que  $f \circ g = g \circ f$  pour toute application  $g$  de  $E$  dans  $E$ .

**Solution 1.46** Soit  $x \in E$  et  $g$  la fonction définie sur  $E$  par  $g(y) = x$  pour tout  $y \in E$  (la fonction constante égale à  $x$ ). On a alors  $x = g(f(x)) = f(g(x)) = f(x)$ . Comme  $x$  est quelconque dans  $E$ , on déduit que  $f = Id_E$ .

Les notions suivantes d'injectivité et de surjectivité sont aussi très importantes.

**Définition 1.6** Soient  $E, F$  deux ensembles et  $f$  une application de  $E$  dans  $F$ . On dit que  $f$  est :

1. *injective* (ou que c'est une injection) si deux éléments distincts de  $E$  ont deux images distinctes dans  $F$ , soit :

$$x_1 \neq x_2 \text{ dans } E \Rightarrow f(x_1) \neq f(x_2) \text{ dans } F \quad (1.3)$$

2. *surjective* (ou que c'est une surjection) si tout élément de  $F$  a au moins un antécédent dans  $E$ , soit :

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

3. *bijection* (ou que c'est une bijection) si elle est à la fois injective ou surjective.

Une injection peut aussi se caractériser en disant que tout élément de  $F$  a au plus un antécédent par  $f$ , encore équivalent à dire que pour tout  $y \in F$  l'équation  $y = f(x)$  a au plus une solution  $x$  dans  $E$ , ce qui revient à dire que si  $x_1$  et  $x_2$  sont deux éléments de  $E$  tels que  $f(x_1) = f(x_2)$ , alors  $x_1 = x_2$  (contraposée de (1.3)).

Une surjection peut se caractériser en disant que pour tout  $y \in F$  l'équation  $y = f(x)$  a au moins une solution  $x$  dans  $E$ , encore équivalent à dire que  $f(E) = F$ .

Si  $f$  est une surjection de  $E$  dans  $F$ , on dit parfois que  $f$  est une surjection de  $E$  sur (pour surjection)  $F$ .

Une bijection peut se caractériser en disant que tout élément de  $F$  a un unique antécédent par  $f$ , encore équivalent à dire que pour que pour tout  $y \in F$  l'équation  $y = f(x)$  a une et une seule solution  $x$  dans  $E$ , ce qui permet de définir l'application réciproque de  $f$ , notée  $f^{-1}$ , de  $F$  dans  $E$  par :

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

Cette application  $f^{-1}$  est une bijection de  $F$  dans  $E$ .

L'application  $f \circ f^{-1}$  est alors l'application identité  $y \mapsto y$  de  $F$  dans  $F$  et l'application  $f^{-1} \circ f$  est alors l'application identité  $x \mapsto x$  de  $E$  dans  $E$ , ce qui se note  $f \circ f^{-1} = Id_F$  et  $f^{-1} \circ f = Id_E$ .

**Définition 1.7** On appelle permutation d'un ensemble  $E$  toute bijection de  $E$  dans lui même.

On note en général  $\mathfrak{S}(E)$  l'ensemble des permutations de  $E$ .

**Exemple 1.3** L'application  $x \mapsto x^2$  est surjective de  $\mathbb{R}$  dans  $\mathbb{R}^+$ , mais non injective. Elle est bijective de  $\mathbb{R}^+$  dans  $\mathbb{R}^+$ .

**Remarque 1.3** Dans le cas où  $f$  est une application de  $E$  dans  $F$ , on a noté pour toute partie  $B$  de  $F$ ,  $f^{-1}(B)$  l'image réciproque de  $B$  par  $f$ , sans aucune hypothèse de bijectivité pour  $f$ . Dans le cas où  $f$  est bijective,  $f^{-1}(B)$  est aussi l'image directe de  $B$  par  $f^{-1}$ , mais dans le cas général, il faut bien prendre garde, malgré la notation, que  $f$  n'a aucune raison d'être bijective. Il faudrait en réalité utiliser un autre symbole que  $f^{-1}$  (par exemple  $f^*(B)$ ,  $f^{(-1)}(B)$ , ou  $f^{\zeta\boxtimes}(f)$ ), mais je préfère utiliser la notation  $f^{-1}(B)$  rencontrée le plus souvent. Si l'on sait de quoi l'on parle il n'y a pas de véritable problème, il s'agit seulement d'une notation.

On peut lire dans *An introduction to the theory of numbers* de Hardy et Wright, p. 7 : «We shall very often use  $A$  as in (vi), viz. an unspecified positive constant. Different  $A$ 's have usually different values, even when they occur in the same formula; and even when definite values can be assigned to them, these values are irrelevant to the argument.» C'est peut être excessif, mais l'essentiel est toujours de savoir de quoi l'on parle, on pourra ensuite écrire les choses en toute rigueur.

**Exercice 1.47** Montrer qu'une application  $f$  strictement monotone de  $\mathbb{R}$  dans  $\mathbb{R}$  est injective.

**Solution 1.47** Supposons que  $f$  soit strictement croissante (au besoin on remplace  $f$  par  $-f$ ). Si  $x \neq y$ , on a nécessairement  $x > y$  ou  $y > x$  et donc  $f(x) > f(y)$  ou  $f(x) < f(y)$ , soit  $f(x) \neq f(y)$  dans tous les cas.

**Exercice 1.48** Soit  $m$  un entier naturel. Montrer que s'il existe un entier naturel  $n$  et une injection  $\varphi$  de  $E_n = \{1, \dots, n\}$  dans  $E_m = \{1, \dots, m\}$ , on a alors nécessairement  $n \leq m$ .

**Solution 1.48** On procède par récurrence sur  $m \geq 0$ .

Si  $m = 0$ , on a alors  $E_m = \emptyset$  et  $E_n = \emptyset$  (en effet, si  $E_n \neq \emptyset$ , l'ensemble  $f(E_n)$  est alors non vide et contenu dans l'ensemble vide, ce qui est impossible), donc  $n = 0$ .

Supposons le résultat acquis pour  $m \geq 0$ . Soit  $\varphi$  une injection de  $E_n$  dans  $E_{m+1}$ . Si  $n = 0$ , on a bien  $n \leq m + 1$ . Si  $n \geq 1$ , on distingue alors deux cas de figure :

- soit  $\varphi(n) = m + 1$  et dans ce cas  $\varphi$  induit une bijection de  $E_{n-1}$  dans  $E_m$  (la restriction de  $\varphi$  à  $E_{n-1}$ ) et  $n - 1 \leq m$ , soit  $n \leq m + 1$  ;
- soit  $\varphi(n) \neq m + 1$  et dans ce cas, en désignant par  $\psi$  l'application de  $E_{m+1}$  dans lui même définie par  $\psi(\varphi(n)) = m + 1$ ,  $\psi(m + 1) = \varphi(n)$  et  $\psi(k) = k$  pour  $k \in E_{m+1} \setminus \{\varphi(n), m + 1\}$ , l'application  $\psi \circ \varphi$  est injective de  $E_n$  dans  $E_{m+1}$  (composée de deux injections puisque  $\varphi$  est injective et  $\psi$  bijective) avec  $\psi \circ \varphi(n) = m + 1$ , ce qui nous ramène au cas précédent.

On déduit de l'exercice précédent que pour  $n > m$  dans  $\mathbb{N}$ , il n'existe pas d'injection de  $\{1, \dots, n\}$  dans  $\{1, \dots, m\}$ .

**Exercice 1.49** Soient  $n, m$  deux entiers naturels. Montrer que s'il existe une bijection  $\varphi$  de  $E_n = \{1, \dots, n\}$  sur  $E_m = \{1, \dots, m\}$ , on a alors nécessairement  $n = m$ .

**Solution 1.49** On a  $n \leq m$  puisque  $\varphi$  est une injection de  $E_n$  dans  $E_m$  et  $m \leq n$  puisque  $\varphi^{-1}$  est une injection de  $E_m$  dans  $E_n$ , ce qui donne  $n = m$ .

Le résultat des deux exercices précédents nous seront utiles pour définir le cardinal (c'est-à-dire le nombre d'éléments) d'un ensemble fini.

**Exercice 1.50** Soient  $E, F$  deux ensembles et  $f$  une bijection de  $E$  sur  $F$ . Montrer que si  $g$  [resp.  $h$ ] est une application de  $F$  sur  $E$  telle que  $g \circ f = Id_E$  [resp.  $f \circ h = Id_F$ ], alors  $g$  [resp.  $h$ ] est bijective et  $g = f^{-1}$  [resp.  $h = f^{-1}$ ].

**Solution 1.50** Résulte de  $g = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$  et  $h = f^{-1} \circ (f \circ h) = f^{-1} \circ Id_F = f^{-1}$ .

On vérifie facilement le résultat suivant.

**Théorème 1.6** Soient  $E, F, G$  des ensembles,  $f$  une application de  $E$  dans  $F$  et  $g$  une application de  $F$  dans  $G$ .

1. Si  $f$  et  $g$  sont injectives, alors  $g \circ f$  est injective (la composée de deux injections est une injection).
2. Si  $f$  et  $g$  sont surjectives, alors  $g \circ f$  est surjective (la composée de deux surjections est une surjection).
3. Si  $f$  et  $g$  sont bijectives, alors  $g \circ f$  est bijective (la composée de deux injections est une bijection) et  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

**Démonstration.**

1. Supposons  $f$  et  $g$  injectives. Si  $g \circ f(x_1) = g \circ f(x_2)$ , alors  $g(f(x_1)) = g(f(x_2))$ , donc  $f(x_1) = f(x_2)$  puisque  $g$  est injective et  $x_1 = x_2$  puisque  $f$  est injective.
2. Supposons  $f$  et  $g$  surjectives. Pour tout  $z \in G$ , il existe  $y \in F$  tel que  $z = g(y)$  puisque  $g$  est surjective et  $y \in F$  s'écrit  $y = f(x)$  avec  $x \in E$  puisque  $f$  est surjective. On a donc  $z = g \circ f(x)$  avec  $x \in E$ . L'application  $g \circ f$  est donc surjective.  
De manière plus compacte, on peut écrire que :

$$(g \circ f)(E) = g(f(E)) = g(F) = G.$$

3. Les deux premiers points nous disent que  $g \circ f$  est bijective si  $f$  et  $g$  le sont. Puis avec  $(f^{-1} \circ g^{-1}) \circ g \circ f = f^{-1} \circ Id_F \circ f = f^{-1} \circ f = Id_E$ , on déduit que  $f^{-1} \circ g^{-1}$  est l'inverse de  $g \circ f$ .

■

**Exercice 1.51** Soient  $E, F, G$  des ensembles,  $f$  une application de  $E$  dans  $F$  et  $g$  une application de  $F$  dans  $G$ . Montrer que :

1. si  $g \circ f$  est injective, alors  $f$  est injective ;
2. si  $g \circ f$  est surjective, alors  $g$  est surjective ;
3. si  $g \circ f$  est surjective et  $g$  injective, alors  $f$  est surjective ;
4. Si  $g \circ f$  est injective et  $f$  surjective, alors  $g$  est injective.

**Solution 1.51**

1. Si  $x, x'$  dans  $E$  sont tels que  $f(x) = f(x')$ , alors  $g \circ f(x) = g \circ f(x')$  et  $x = x'$  puisque  $g \circ f$  est injective. L'application  $f$  est donc injective.

2. Pour tout  $z$  dans  $G$ , il existe  $x$  dans  $E$  tel que  $z = g \circ f(x)$  puisque  $g \circ f$  est surjective et en notant  $y = f(x)$ , on a  $y \in F$  et  $z = g(y)$ , ce qui prouve que  $g$  est surjective.
3. Soit  $y \in F$ . Comme  $g \circ f$  est surjective, il existe  $x \in E$  tel que  $z = g(y) = (g \circ f)(x) = g(f(x))$  et  $y = f(x)$  si on suppose de plus que  $g$  est injective. En conséquence,  $f$  est surjective.
4. Soient  $y, y'$  dans  $F$  tels que  $g(y) = g(y')$ . Comme  $f$  est surjective, il existe  $x, x'$  dans  $E$  tels que  $y = f(x)$  et  $y' = f(x')$ , ce qui donne  $g \circ f(x) = g \circ f(x')$  et  $x = x'$  puisque  $g \circ f$  est injective, donc  $y = y'$ .

Le résultat qui suit peut parfois être utile pour montrer l'injectivité, la surjectivité ou la bijectivité d'une application.

**Théorème 1.7** Soient  $E, F$  deux ensembles et  $f$  une application de  $E$  dans  $F$ .

1. S'il existe une application  $g$  de  $F$  dans  $E$  telle que  $g \circ f = Id_E$ , alors  $f$  est injective.
2. S'il existe une application  $h$  de  $F$  dans  $E$  telle que  $f \circ h = Id_F$ , alors  $f$  est surjective.
3. S'il existe deux applications  $g$  et  $h$  de  $F$  dans  $E$  telles que  $g \circ f = Id_E$  et  $f \circ h = Id_F$ , alors  $f$  est bijective et  $g = h = f^{-1}$ .

**Démonstration.**

1. Si  $x, x'$  dans  $E$  sont tels que  $f(x) = f(x')$ , alors  $x = g \circ f(x) = g \circ f(x') = x'$  et  $f$  est injective.
2. Pour tout  $y \in F$ , on a  $y = (f \circ h)(y) = f(h(y))$  avec  $x = h(y) \in E$ , donc  $f$  est surjective.
3. Les deux premiers points nous disent que  $f$  est bijective et de  $g \circ f = Id_E$ , on déduit que  $f^{-1} = (g \circ f) \circ f^{-1} = g$ . De même  $h = g^{-1}$ .

■

**Exercice 1.52** Soient  $m$  un entier naturel non nul et  $E$  un ensemble non vide. Montrer que s'il existe une surjection  $\varphi$  de  $E_m = \{1, \dots, m\}$  sur  $E$ , on peut alors construire une injection de  $E$  dans  $E_m$ .

**Solution 1.52** Comme  $\varphi$  est surjective de  $E_m$  sur  $E$ , on a  $\varphi^{-1}\{x\} \neq \emptyset$  pour tout  $x \in E$  et chacun de ces sous-ensembles de  $E_m$  a un plus petit élément  $j_x = \min \varphi^{-1}\{x\} \in E_m$ , ce qui permet de définir l'application  $\psi$  de  $E$  dans  $E_m$  par :

$$\forall x \in E, \psi(x) = j_x$$

On a alors :

$$\forall x \in E, \varphi \circ \psi(x) = \varphi(j_x) = x$$

c'est-à-dire que  $\varphi \circ \psi = Id_E$  et l'application  $\psi$  est injective (théorème précédent).

**Exercice 1.53** Soient  $n, m$  deux entiers naturels non nuls. Montrer que s'il existe une surjection  $\varphi$  de  $E_n = \{1, \dots, n\}$  sur  $E_m = \{1, \dots, m\}$ , on a alors nécessairement  $n \geq m$ .

**Solution 1.53** En utilisant le résultat de l'exercice précédent, on peut construire une injection de  $E_m$  dans  $E_n$  et nécessairement  $m \leq n$  (exercice 1.48).

**Exercice 1.54** Soient  $E$  un ensemble et  $f$  une application de  $E$  dans  $E$ . Montrer que  $f$  est injective si, et seulement si,  $f(A \cap B) = f(A) \cap f(B)$  pour toutes parties  $A$  et  $B$  de  $E$ .

**Solution 1.54** On a toujours  $f(A \cap B) \subset f(A) \cap f(B)$  pour toutes parties  $A$  et  $B$  de  $E$ , que  $f$  soit injective ou pas. En effet un élément  $y$  de  $f(A \cap B)$  s'écrit  $y = f(x)$  avec  $x \in A \cap B$  et donc  $y \in f(A) \cap f(B)$ . Réciproquement si  $y \in f(A) \cap f(B)$ , il existe  $x \in A$  et  $x' \in B$  tels que  $y = f(x) = f(x')$  et dans le cas où  $f$  est injective, on a nécessairement  $x = x' \in A \cap B$ , donc  $y \in f(A \cap B)$ .

On a donc  $f(A \cap B) = f(A) \cap f(B)$  pour toutes parties  $A$  et  $B$  de  $E$ , si  $f$  est injective.

Réciproquement supposons que  $f(A \cap B) = f(A) \cap f(B)$  pour toutes parties  $A$  et  $B$  de  $E$ . Si  $f$  n'est pas injective, il existe  $x \neq x'$  dans  $E$  tels que  $f(x) = f(x')$  et :

$$\emptyset = f(\emptyset) = f(\{x\} \cap \{x'\}) = f(\{x\}) \cap f(\{x'\}) = f(\{x\}) = \{f(x)\}$$

ce qui est impossible. Donc  $f$  est injective.

**Exercice 1.55** Soient  $E$  un ensemble et  $f$  une application de  $E$  dans  $E$ . Montrer que  $f$  est bijective si, et seulement si,  $f(\overline{A}) = \overline{f(A)}$  pour toute partie  $A$  de  $E$ .

**Solution 1.55** Supposons  $f$  bijective. Un élément  $y$  de  $E$  est dans  $f(\overline{A})$  si, et seulement si, il s'écrit  $y = f(x)$  où  $x$  est uniquement déterminé dans  $\overline{A}$ , ce qui implique  $y \notin f(A)$  (sinon  $y = f(x') = f(x)$  avec  $x' \in A$  et  $x = x' \in A$ , ce qui contredit  $x \in \overline{A}$ ). On a donc  $f(\overline{A}) \subset f(A)$ . Si  $y \notin f(A)$ , il s'écrit  $y = f(x)$  ( $f$  est bijective) et  $x \notin A$ , donc  $y \in f(\overline{A})$ . On a donc  $f(\overline{A}) \subset f(A)$  et  $f(\overline{A}) = \overline{f(A)}$ .

Supposons que  $f(\overline{A}) = \overline{f(A)}$  pour toute partie  $A$  de  $E$ . En particulier, on a  $f(E) = f(\overline{\emptyset}) = \overline{f(\emptyset)} = \overline{\emptyset} = E$  et  $f$  est surjective. Si  $x \neq x'$  dans  $E$ , en remarquant que  $x' \in \overline{\{x\}}$ , on a  $f(x') \in f(\overline{\{x\}}) = \overline{f(\{x\})} = \overline{\{f(x)\}}$  et  $f(x) \neq f(x')$ . Donc  $f$  est injective.

**Exercice 1.56** Soient  $E, F, G, H$  des ensembles,  $f$  une application de  $E$  dans  $F$ ,  $g$  une application de  $F$  dans  $G$  et  $h$  une application de  $G$  dans  $H$ . Montrer que si  $g \circ f$  et  $h \circ g$  sont bijectives, alors  $f, g$  et  $h$  sont bijectives.

**Solution 1.56** Si  $g \circ f$  est bijective, elle est alors surjective et il en est de même de  $g$  (exercice 1.51). Si  $h \circ g$  est bijective, elle est alors injective et il en est de même de  $g$  (exercice 1.51). Donc  $g$  est bijective. Il en résulte que  $f = g^{-1} \circ (g \circ f)$  et  $h = (h \circ g) \circ g^{-1}$  sont bijectives comme composées.

**Exercice 1.57** On désigne par  $f$  l'application définie sur  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$  par :

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

Montrer que  $f$  est injective. Il résulte que  $\mathbb{N}^2$  est en bijection avec le sous ensemble  $f(\mathbb{N}^2)$  de  $\mathbb{N}$ . Ce résultat se traduit en disant que  $\mathbb{N}^2$  est dénombrable.

**Solution 1.57** L'égalité  $f(n, m) = f(n', m')$  avec  $(n, m)$  et  $(n', m')$  dans  $\mathbb{N}^2$  équivaut à  $2^n 3^m = 2^{n'} 3^{m'}$  et l'unicité de la décomposition en facteurs premiers d'un entier naturel non nul nous dit que  $(n, m) = (n', m')$ . L'application  $f$  est donc injective de  $\mathbb{N}^2$  dans  $\mathbb{N}$  et bijective de  $\mathbb{N}^2$  dans  $f(\mathbb{N}^2) \subset \mathbb{N}$ .

**Exercice 1.58** Montrer que l'application  $f : (n, m) \mapsto 2^{n+m+1} + 2^m$  est injective de  $\mathbb{N}^2$  dans  $\mathbb{N}$ .

**Solution 1.58** L'égalité  $f(n, m) = f(n', m')$  avec  $(n, m)$  et  $(n', m')$  dans  $\mathbb{N}^2$  équivaut à  $2^m (2^{n+1} + 1) = 2^{m'} (2^{n'+1} + 1)$ . Si  $m > m'$ , on a alors  $2^{m-m'} (2^{n+1} + 1) = 2^{n'+1} + 1$  qui est à la fois pair et impair, ce qui est impossible. De manière analogue, on voit que  $m' > m$  est impossible. On a donc  $m = m'$  et  $2^{n+1} + 1 = 2^{n'+1} + 1$ , ce qui équivaut à  $n = n'$ . L'application  $f$  est donc injective.