

# RAISONNEMENTS MATHÉMATIQUES ET PREUVES (MAT 1762)

CORENTIN CORREIA

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE  
UNIVERSITÉ D'OTTAWA

AUTOMNE 2026

Dernières modifications : le 8 octobre 2026.



# Table des matières

|          |                                                                                |            |
|----------|--------------------------------------------------------------------------------|------------|
| <b>1</b> | <b>Éléments de logique</b>                                                     | <b>7</b>   |
| 1.1      | Un ensemble ? . . . . .                                                        | 7          |
| 1.2      | Assertion . . . . .                                                            | 7          |
| 1.3      | Négation . . . . .                                                             | 8          |
| 1.4      | Conjonction et disjonction . . . . .                                           | 9          |
| 1.5      | Implication . . . . .                                                          | 12         |
| 1.6      | Équivalence . . . . .                                                          | 15         |
| 1.7      | Quantificateurs . . . . .                                                      | 16         |
| <b>2</b> | <b>Notions de théorie des ensembles</b>                                        | <b>25</b>  |
| 2.1      | Ensemble, opérations entre ensembles . . . . .                                 | 25         |
| 2.2      | Un mot sur le paradoxe du barbier et l'axiomatique de Zermelo-Fraenkel . . . . | 39         |
| 2.3      | Fonctions . . . . .                                                            | 42         |
| 2.4      | Relation d'équivalence . . . . .                                               | 51         |
| 2.5      | Problèmes . . . . .                                                            | 55         |
| <b>3</b> | <b>Entiers, entiers positifs, ordre, induction</b>                             | <b>59</b>  |
| 3.1      | Axiomatique de $\mathbb{Z}$ et $\mathbb{N}$ . . . . .                          | 59         |
| 3.2      | Premières conséquences . . . . .                                               | 60         |
| 3.3      | Ordre sur les entiers . . . . .                                                | 64         |
| 3.4      | Raisonnement par induction et principe du bon ordre . . . . .                  | 70         |
| 3.5      | Problèmes . . . . .                                                            | 79         |
| <b>4</b> | <b>Séries finies</b>                                                           | <b>81</b>  |
| 4.1      | Preliminaires . . . . .                                                        | 81         |
| 4.2      | Premières propriétés des sommes . . . . .                                      | 84         |
| 4.3      | Exemples classiques de sommes . . . . .                                        | 86         |
| 4.4      | Somme et produit sur un ensemble fini . . . . .                                | 88         |
| 4.5      | Coefficients binomiaux et formule du binôme . . . . .                          | 91         |
| 4.6      | Problèmes . . . . .                                                            | 96         |
| <b>5</b> | <b>Arithmétique modulaire</b>                                                  | <b>99</b>  |
| 5.1      | Division euclidienne . . . . .                                                 | 99         |
| 5.2      | Entiers modulo $n$ . . . . .                                                   | 100        |
| 5.3      | Nombres premiers, PGCD . . . . .                                               | 105        |
| 5.4      | Problèmes . . . . .                                                            | 114        |
| <b>6</b> | <b>L'ensemble des nombres réels</b>                                            | <b>117</b> |
| 6.1      | Axiomatique de $\mathbb{R}$ et $\mathbb{R}_{>0}$ . . . . .                     | 117        |
| 6.2      | Premières conséquences . . . . .                                               | 119        |
| 6.3      | Ordre sur les réels . . . . .                                                  | 120        |

|          |                                                  |            |
|----------|--------------------------------------------------|------------|
| 6.4      | $\mathbb{Z}$ comme sous-ensemble de $\mathbb{R}$ | 124        |
| 6.5      | Supremum et infimum                              | 126        |
| 6.6      | $\mathbb{Z}$ non borné dans $\mathbb{R}$         | 129        |
| 6.7      | Racine carrée                                    | 131        |
| 6.8      | Problèmes                                        | 132        |
| <b>7</b> | <b>Suites réelles, limites</b>                   | <b>135</b> |
| 7.1      | Valeur absolue, distance                         | 135        |
| 7.2      | Limites                                          | 138        |
| 7.3      | Problèmes                                        | 147        |
| <b>8</b> | <b>Nombres rationnels, nombres irrationnels</b>  | <b>149</b> |
| 8.1      | Nombres rationnels                               | 149        |
| 8.2      | Nombres irrationnels                             | 152        |
| 8.3      | Problèmes                                        | 153        |

# Préface

Qu'est-ce qu'un énoncé ? Comment prouve-t-on un énoncé ? Comment s'articule une preuve ? Un mathématicien ne pourrait pas s'en sortir sans une idée claire sur ces interrogations.

Il s'avère qu'il a vraiment fallu se poser ce genre de questions à la fin du XIXe siècle, lorsque des paradoxes apparurent, laissant planer le doute sur le fondement des mathématiques (cf. le paradoxe du barbier, section 2.2.1 du chapitre 2). On a alors tout reconstruit, en partant de fondations que l'on appelle les « axiomes » dans le jargon. En d'autres termes, on a établi des règles pour que les mathématiciens arrêtent de faire les choses n'importe comment. L'édifice qui en résulte est notre théorie moderne des mathématiques. Les fondations sont très solides et le bâtiment ne semble pas vouloir s'écrouler (les axiomes ne fournissent pas une théorie contradictoire *a priori*), enfin, on espère...

Cette théorie, c'est la **théorie des ensembles**. Dans ce cours, nous n'en adopterons qu'une vision naïve. Cependant, pour des raisons d'honnêteté, nous expliquerons brièvement dans la section 2.2 du chapitre 2 ses axiomes et pourquoi cette théorie résout le paradoxe du barbier.

Maintenant que nous doutons de tout, on pourrait aussi se demander « Est-ce que tout énoncé se démontre ? ». Non, ce n'est pas qu'un sujet de philosophie. Les mathématiciens se sont vraiment intéressés à cette question, avec beaucoup d'inquiétude, la sueur au front. Mais c'est une autre histoire dont nous ne parlerons pas ici. Le lecteur curieux pourra s'intéresser aux travaux de Kurt Gödel sur l'indécidabilité.

Dans ce cours, il sera question de savoir rédiger et structurer une preuve, selon le type d'énoncé à démontrer (conjonction, disjonction, implication, équivalence, etc.). Pour cela, on commencera par le formalisme de base en logique et en théorie des ensembles. Les chapitres 1 et 2 seront donc les plus importants, car ils posent les fondements sur les raisonnements mathématiques et les objets que nous manipulons.

Il n'est plus question de mener des calculs ou d'appliquer des méthodes selon des règles que l'on a prises pour acquises. Le but est de comprendre comment les choses sont définies et pourquoi certains énoncés sont vrais. Ainsi, à partir d'axiomes, nous redécouvrirons l'ensemble des entiers dans le chapitre 3. Par le raisonnement, nous aboutirons aux résultats les plus classiques (ordre sur les entiers, raisonnement par induction, calculs de sommes au chapitre 4, arithmétique dans le chapitre 5).

Ce sera également la démarche adoptée pour définir et étudier l'ensemble des nombres réels dans le chapitre 6. L'axiome de complétude jouera un rôle majeur dans notre compréhension de la structure de l'ensemble des nombres réels.

Sans le chapitre 6, le contenu du chapitre 7 ne serait que très limité. Dans ce chapitre, nous pourrions ainsi faire de l'analyse, définir rigoureusement la notion de limite d'une suite réelle, et établir avec rigueur certains résultats cruciaux. Faute de définitions et de rigueur, on se contentait auparavant d'une approche intuitive pour se convaincre de la limite  $\frac{1}{n} \xrightarrow{n \rightarrow \infty} 0$ , nous serons maintenant en mesure de montrer ce fait.

Le dernier chapitre sera une étude rapide des nombres rationnels et irrationnels. Nous comprendrons enfin la différence cruciale entre l'ensemble des nombres réels et l'ensemble des nombres rationnelles.

Des exercices sont proposés tout au long du cours, et des problèmes figurent à la fin de chaque chapitre. Ces derniers sont des exercices plus approfondis, utilisant les outils du cours et menant à de jolis résultats. Les résultats admis ou démontrés dans ces problèmes ne font pas partie des connaissances exigibles du cours.

Ces notes de cours s'inspirent en grande partie du livre The Art of Proof par Matthias Beck and Ross Geoghegan. Springer, 2010. <http://dx.doi.org/10.1007/978-1-4419-7023-7>.

# Chapitre 1

## Éléments de logique

Commençons par aborder les fondamentaux en logique. Nous allons apprendre des méthodes de preuve, et plus généralement la façon dont on structure une preuve.

### 1.1 Un ensemble ?

Dans ce chapitre, on aura besoin de parler d'*ensemble*, une notion que nous aborderons plus en détail dans le chapitre 2. Tout ce qu'il faut savoir sur un ensemble, c'est que c'est une collection d'objets, appelés « éléments » ou « membres ». Si  $E$  est un ensemble, on dit que  $x$  appartient à  $E$ , noté  $x \in E$ , si  $x$  est un élément de  $E$ , sinon on écrit  $x \notin E$ . Par exemple :

1.  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  est l'ensemble des entiers ;
2.  $\mathbb{N} = \{1, 2, 3, \dots\}$  est l'ensemble des entiers positifs ;
3.  $\mathbb{R}$  est l'ensemble des nombres réels, par exemple  $3, \pi, \dots$  ;
4. et on peut en construire plein d'autres, par exemple l'ensemble  $E$  composé de trois éléments :  $1, \mathbb{R}$  et la fonction racine carrée  $x \in \mathbb{R}_{\geq 0} \mapsto \sqrt{x} \in \mathbb{R}$ . Si on note  $f$  la fonction racine carrée, alors  $E = \{1, \mathbb{R}, f\}$ .

Nous donnerons plus de détails dans le prochain chapitre. Parlons maintenant des fondements de la logique.

### 1.2 Assertion

**Définition 1.1.** Une *assertion*, ou un *énoncé*, ou une *proposition*, est une déclaration qui est soit fausse, soit vraie. Elle ne peut pas être vraie et fausse en même temps.

**Exemple 1.2.** Les propositions suivantes sont des assertions :

1. « Ottawa se situe dans la province de l'Ontario ». L'assertion est vraie.
2. « Il existe un nombre réel dont le carré est négatif ». C'est faux, mais c'est quand même une assertion.
3. « Il pleut » est une assertion, mais sa vérité dépend du contexte.
4. « Si  $1 < 0$ , alors 1 n'est pas un entier. » Réflexion : ici l'hypothèse «  $1 < 0$  » est fausse, est-ce qu'on en déduit que l'assertion est vraie ou fausse ? Nous répondrons bientôt à cette question (cf. exemple 1.27).
5. «  $\sqrt{2}$  » n'est pas une assertion.

L'avant-dernier exemple est une combinaison entre deux assertions «  $1 < 0$  » et « 1 n'est pas un entier », appelée *implication*. C'est un exemple d'opérations qu'on peut faire entre énoncés, qu'il va falloir définir rigoureusement pour déterminer si l'avant-dernier exemple est vrai ou faux.

Présentons les exemples importants d'opérations entre énoncés.

### 1.3 Négation

**Définition 1.3.** Étant donnée une assertion  $P$ , sa *négation* est l'assertion qui est fausse si  $P$  est vraie, vraie si  $P$  est fausse. On la note *non*  $P$ , ou  $\neg P$ .

Sur quoi repose la définition de cette opération ? L'opération  $\neg$  se définit par la valeur qu'on associe à  $\neg P$  (vraie ou fausse) en fonction de la valeur de l'assertion  $P$ . On peut résumer la définition de la négation d'une assertion par la table de vérité suivante :

| $P$ | $\neg P$ |
|-----|----------|
| V   | F        |
| F   | V        |

**Remarque 1.4.** L'opération  $\neg$  ne prend en entrée qu'une seule assertion, la table de vérité n'a donc qu'une entrée.

Dans la suite, nous allons voir des exemples d'opérations entre plusieurs assertions. Il faudra cette fois-ci une table de vérité à plusieurs entrées (autant qu'il n'y a d'assertions) pour connaître la valeur de l'opération en fonction de la valeur des assertions.

**Exemple 1.5.** Si  $P$  est l'assertion «  $1 < 0$  », alors  $\neg P$  est «  $1 \geq 0$  ». On remarque bien que  $P$  est fausse et  $\neg P$  est vraie.

**Proposition 1.6** (Double négation). *Soit  $P$  une assertion. Alors  $\neg\neg P$  est équivalente à  $P$ , en d'autres termes, ils admettent la même table de vérité.*

**Preuve.** On dresse la table de vérité de  $\neg\neg P$ . Il faut donc d'abord calculer  $\neg P$  en fonction de la valeur de  $P$ , puis ensuite  $\neg(\neg P)$  en fonction de la valeur de  $\neg P$  :

| $P$ | $\neg P$ | $\neg\neg P$ |
|-----|----------|--------------|
| V   | F        | V            |
| F   | V        | F            |

En résumé, la table de vérité de  $\neg\neg P$  vaut :

| $P$ | $\neg\neg P$ |
|-----|--------------|
| V   | V            |
| F   | F            |

donc l'opération  $\neg\neg$  a la même table de vérité que l'opération consistant à ne rien faire.  $\square$

Une première utilité de la négation est le raisonnement par l'absurde.

**Méthode de preuve 1.7** (Raisonnement par l'absurde). *Pour montrer qu'une assertion  $P$  est vraie, on suppose que  $P$  est fausse (autrement dit que  $\neg P$  est vraie) et on cherche une contradiction.*

**Exemple 1.8.** Montrons que  $\sqrt{2}$  est un nombre irrationnel.<sup>1</sup>

Par l'absurde, supposons que  $\sqrt{2}$  est un nombre rationnel. Il existe donc  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}$  tels que  $\sqrt{2} = \frac{a}{b}$ . On peut en plus supposer que  $a$  et  $b$  sont premiers entre eux, quitte à écrire la fraction  $\frac{a}{b}$  sous forme irréductible<sup>2</sup>. En élevant au carré, on obtient  $2 = \frac{a^2}{b^2}$ , c'est-à-dire  $a^2 = 2b^2$ . Cela signifie que l'entier  $a^2$  est pair, donc que  $a$  est pair (cf. l'exemple 1.32 plus loin pour une démonstration de ce fait). Il existe donc un entier  $k$  tel que  $a = 2k$ . L'égalité  $a^2 = 2b^2$  donne donc  $4k^2 = 2b^2$ , c'est-à-dire  $b^2 = 2k^2$ . Cela signifie que  $b^2$  est également pair et donc que  $b$  est pair. On avait supposé  $a$  et  $b$  premiers entre eux, et on vient de montrer qu'ils sont divisibles par 2, c'est absurde.

Donc  $\sqrt{2}$  est irrationnel.

## 1.4 Conjonction et disjonction

**Définition 1.9.** Soient  $P$  et  $Q$  deux assertions

- Leur *conjonction*, notée  $P$  et  $Q$ , ou  $P \wedge Q$ , est l'assertion qui est vraie si  $P$  et  $Q$  sont vraies, fausse si au moins l'une des deux est fausse. La table de vérité vaut donc :

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

- Leur *disjonction*, notée  $P$  ou  $Q$ , ou  $P \vee Q$ , est l'assertion qui est vraie si au moins l'une des deux est vraie, fausse si les deux sont fausses. La table de vérité vaut donc :

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

1.  $\sqrt{2}$  est l'unique nombre réel positif dont le carré vaut 2. Nous construirons ce nombre dans le chapitre 6.7. Un nombre est irrationnel s'il n'est pas rationnel, et un nombre est rationnel s'il s'écrit  $\frac{a}{b}$  avec  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}$ .

2. Ce qu'on veut dire, c'est que si  $a$  et  $b$  ne sont pas premiers entre eux, alors on peut remarquer qu'on peut écrire  $\frac{a}{b} = \frac{a'}{b'}$  avec de nouveaux entiers  $a'$  et  $b'$  premiers entre eux, puis continuer le raisonnement avec  $a'$  et  $b'$  (en oubliant  $a$  et  $b$ ). De manière générale, lorsqu'une propriété n'est pas vérifiée mais qu'on peut s'y ramener facilement (par exemple ici la propriété « être premiers entre eux »), les raisonnements en « quitte à » ou « sans perte de généralité, supposons » signifie qu'on va éviter d'introduire de nouvelles notations (ici  $a', b'$  pour remplacer  $a, b$ ) et supposer directement que la propriété est vérifiée, afin de ne pas alourdir la preuve.

**Remarque 1.10.** À méditer : pour ne pas confondre les symboles  $\wedge$  et  $\vee$ , penser à la ressemblance entre  $\wedge$  et  $\cap$  (symbole d'intersection d'ensembles), et entre  $\vee$  et  $\cup$  (symbole d'union d'ensembles). Mais quel est le rapport ? Réponse dans le prochain chapitre, dans la remarque 2.20.

**Exemple 1.11.**

1. «  $1 > 0$  et 5 est pair » est fausse.
2. «  $1 > 0$  ou 5 est pair » est vraie.

**Proposition 1.12.**

1.  $\neg P \vee P$  est toujours vraie.
2.  $\neg P \wedge P$  est toujours fausse.

**Remarque 1.13.** Le symbole  $\neg$  est prioritaire sur  $\vee$  et  $\wedge$ .  $\neg P \vee P$  signifie  $(\neg P) \vee P$  et non pas  $\neg(P \vee P)$ , ce dernier étant la même chose que  $\neg P$ .

**Preuve.** Dresser les tables de vérité (exercice). □

**Exercice 1.14.** Démontrer la proposition ci-dessus.

**Proposition 1.15.** Soient  $P, Q, R$  trois assertions.

1. Idempotence :  $P \wedge P$ ,  $P \vee P$  et  $P$  sont équivalentes.
2. Commutativité :
  - (a)  $P \wedge Q$  et  $Q \wedge P$  sont équivalentes.
  - (b)  $P \vee Q$  et  $Q \vee P$  sont équivalentes.
3. Absorption, neutre :
  - (a) « faux et  $P$  » est toujours fausse (faux est absorbant pour  $\wedge$ ) ;
  - (b) « vrai et  $P$  » a la même valeur de vérité que  $P$  (vrai est neutre pour  $\wedge$ ) ;
  - (c) « vrai ou  $P$  » est toujours vraie (vrai est absorbant pour  $\vee$ ) ;
  - (d) « faux ou  $P$  » a la même valeur de vérité que  $P$  (faux est neutre pour  $\vee$ ).
4. Associativité :
  - (a)  $(P \wedge Q) \wedge R$  et  $P \wedge (Q \wedge R)$  sont équivalentes, et on notera plutôt  $P \wedge Q \wedge R$ .
  - (b)  $(P \vee Q) \vee R$  et  $P \vee (Q \vee R)$  sont équivalentes, et on notera plutôt  $P \vee Q \vee R$ .
5. Distributivité :
  - (a)  $(P \vee Q) \wedge R$  et  $(P \wedge R) \vee (Q \wedge R)$  sont équivalentes.
  - (b)  $(P \wedge Q) \vee R$  et  $(P \vee R) \wedge (Q \vee R)$  sont équivalentes.

**Preuve.** L'idempotence s'obtient en dressant les tables de vérité.

Pour la commutativité, on remarque également que les tables de vérité sont les mêmes ( $P$  et  $Q$  jouent des rôles symétriques).

Pour les propriétés d'absorption et de neutralité : par définition (on peut aussi comparer les tables de vérité).

Pour l'associativité, il faut dresser la table de vérité. Mais cette table comporte trois entrées, donc on va réduire le champ des possibles en fixant la valeur d'une des entrées. Faisons l'exemple de l'associativité de  $\wedge$  (pour  $\vee$  : exercice). Dans le cas où  $P$  est fausse, on utilise la loi d'absorption : d'une part  $P \wedge (Q \wedge R)$  est fausse, et d'autre part  $P \wedge Q$  est fausse donc  $(P \wedge Q) \wedge R$  est fausse. Donc quelles que soient les valeurs de  $Q$  et  $R$ , on sait que  $P \wedge (Q \wedge R)$  et  $(P \wedge Q) \wedge R$  sont fausses dès que  $P$  est fausse. Supposons maintenant que  $P$  est vraie et utilisons la neutralité :  $P \wedge (Q \wedge R)$  a la même valeur de vérité que  $Q \wedge R$ , ensuite  $P \wedge Q$  a la même valeur de vérité que  $Q$  donc  $(P \wedge Q) \wedge R$  a la même valeur de vérité que  $Q \wedge R$ . On a donc prouvé que dans le cas où  $P$  est vraie,  $(P \wedge Q) \wedge R$  et  $P \wedge (Q \wedge R)$  partagent la même valeur de vérité (celle de  $Q \wedge R$ ) quelles que soient les vérités de  $Q$  et  $R$ .

La distributivité est laissée en exercice. Indication pour le premier point : comme  $R$  est isolée dans  $(P \vee Q) \wedge R$ , on peut judicieusement faire une disjonction de cas sur la valeur de vérité de  $R$  et utiliser les règles d'absorption et de neutralité.  $\square$

**Exercice 1.16.** Montrer les propriétés dont la justification a été laissée en exercice dans la preuve ci-dessus.

La prochaine proposition est la deuxième méthode de preuve que nous voyons. L'exemple qui suit décortique la structure de la preuve.

**Méthode de preuve 1.17** (Preuve d'une disjonction). *Soient  $P$  et  $Q$  deux assertions. Démontrer que  $P \vee Q$  est vraie, c'est équivalent à supposer que  $P$  est fausse et à montrer que  $Q$  est vraie (par symétrie, on peut aussi supposer que  $Q$  est fausse et montrer que  $P$  est vraie).*

Évidemment, si on peut d'emblée montrer que  $P$  est vraie (ou alors que  $Q$  est vraie), on n'a pas besoin d'utiliser cette méthode.

**Exemple 1.18.** On fixe un entier  $x$ . Montrons que «  $x$  n'est pas divisible par 4 ou  $x$  est pair » est vraie.

On suppose que «  $x$  n'est pas divisible par 4 » est fausse et on montre que «  $x$  est pair » est vraie.

Par hypothèse, la négation de «  $x$  n'est pas divisible par 4 » est vraie, c'est-à-dire qu'on sait que  $x$  est divisible par 4. Il existe donc un entier  $k$  tel que  $x = 4k$ . Ainsi  $x = 2 \times (2k)$  donc  $x$  s'écrit bien sous la forme  $2k'$  où  $k'$  est un entier (ici  $k' = 2k$ ). Donc  $x$  est pair, ce qu'on voulait démontrer.

**Preuve.** Si  $P$  est vraie, il n'y a rien à démontrer pour obtenir que  $P \vee Q$  est vraie. On peut donc se restreindre au cas où  $P$  est fausse,  $P \vee Q$  aura donc la même valeur de vérité que  $Q$  par propriété de neutralité.  $\square$

Un énoncé analogue existe pour la conjonction. C'est une traduction littérale de la définition,

mais qui a toute son importance.

**Proposition 1.19.** Soient  $P$  et  $Q$  deux assertions. Montrer que  $P \wedge Q$  est vraie consiste exactement à montrer séparément que  $P$  est vraie et que  $Q$  est vraie.

**Preuve.** Par définition. □

Enfin, la conjonction et la disjonction sont reliées de la manière suivante.

**Proposition 1.20.** Soient  $P$  et  $Q$  deux assertions.

1.  $\neg(P \wedge Q)$  est équivalente à  $\neg P \vee \neg Q$ .
2.  $\neg(P \vee Q)$  est équivalente à  $\neg P \wedge \neg Q$ .

**Preuve.** Comparer les tables de vérité. □

**Exercice 1.21.** Prouver la proposition ci-dessus.

**Exemple 1.22.** Reprenons l'exemple précédent. On fixe un entier  $x$ . La négation de «  $x$  n'est pas divisible par 4 ou  $x$  est pair » vaut «  $x$  divisible par 4 et  $x$  n'est pas pair ». Étant donné qu'un multiple de 4 est forcément pair, on en déduit que c'est faux.

On peut également définir le « ou exclusif ».

**Définition 1.23.** Soient  $P$  et  $Q$  deux assertions. On définit leur *disjonction exclusive*, notée  $P \oplus Q$ , par la table de vérité

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

Autrement dit,  $P \oplus Q$  est vraie si ou bien  $P$  est vraie, ou bien  $Q$  est vraie (pas les deux simultanément),  $P \oplus Q$  est fausse dans le cas contraire.

**Exercice 1.24.**

1. Définir  $P \oplus Q$  à partir de  $\neg$ ,  $\wedge$  et  $\vee$ .
2. Montrer que  $\oplus$  est commutative et associative.
3. Que dire de l'assertion «  $P \oplus \neg P$  » ?

## 1.5 Implication

On cherche maintenant à définir l'implication. Intuitivement, on voudrait une notion de conséquence.

Rappelons la quatrième assertion donnée dans l'exemple 1.2 : « Si  $1 < 0$ , alors 1 n'est pas un entier ». Comment parler de la conséquence d'une hypothèse qui n'est déjà pas valable ?

La bonne manière de formuler les choses est de se dire que  $P$  implique  $Q$  si, **dès que  $P$  est vraie**, alors  $Q$  est nécessairement vraie aussi. Comment l'écrire mathématiquement ? Cela voudrait dire qu'il n'est pas possible que  $P$  soit vraie et que  $Q$  soit fausse, en d'autres termes  $P \wedge \neg Q$  est fausse. Donc on définit «  $P$  implique  $Q$  » comme étant la négation de  $P \wedge \neg Q$ .

**Définition 1.25.** Étant données deux assertions  $P$  et  $Q$ , on définit l'*implication* de  $P$  vers  $Q$ , notée «  $P$  implique  $Q$  » ou  $P \Rightarrow Q$ , comme étant l'assertion  $\neg P \vee Q$ . La table de vérité est la suivante :

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

Si  $P \Rightarrow Q$  est vraie, alors

- $P$  est appelée une *condition suffisante* (pour que  $Q$  soit vraie, il **suffit** que  $P$  soit vraie) ;
- $Q$  est appelée une *condition nécessaire* (si  $P$  est vraie, alors **nécessairement**  $Q$  est vraie).

L'assertion  $Q \Rightarrow P$  est appelée la *réciproque* de  $P \Rightarrow Q$ .

**Exemple 1.26.** Étant donné un réel  $x$ , l'assertion  $x = 1 \Rightarrow x^2 = 1$  est vraie. Mais la réciproque  $x^2 = 1 \Rightarrow x = 1$  est fausse ( $x = -1$  satisfait aussi  $x^2 = 1$ ).

**Exemple 1.27.** Réponse à l'interrogation sur « Si  $1 < 0$ , alors 1 n'est pas un entier » (cf. exemple 1.2). Cette assertion est vraie, c'est ce que nous dit la table de vérité dès que l'hypothèse est fausse.

L'idée de conséquence est finalement trompeuse puisqu'on n'arrive pas à se l'imaginer lorsque la cause n'est pas valable. Voici un autre point de vue : si on notait 0 à la place de  $F$  et 1 à la place de  $V$ , alors  $P \Rightarrow Q$  est vraie si la valeur de  $P$  est plus petite que la valeur de  $Q$ , fausse sinon.

**Remarque 1.28.** Le symbole  $\Rightarrow$  ne doit jamais remplacer un « donc » lorsqu'on rédige une preuve. En effet, contrairement à «  $P$  donc  $Q$  », l'implication «  $P \Rightarrow Q$  » ne sous-entend pas que  $P$  est vraie, mais compare les vérités de  $P$  et de  $Q$ .

Voici deux méthodes pour montrer une implication.

**Méthode de preuve 1.29** (Preuve d'une implication). Soient  $P$  et  $Q$  deux assertions. Montrer que  $P \Rightarrow Q$  est vraie, c'est la même chose que supposer que  $P$  est vraie et de montrer que  $Q$  est vraie.

**Preuve.**  $P \Rightarrow Q$  correspond exactement à  $\neg P \vee Q$ . D'après la proposition 1.17, il faut donc supposer que  $\neg\neg P$  est vraie (c'est-à-dire que  $P$  est vraie) et montrer que  $Q$  est vraie.  $\square$

**Méthode de preuve 1.30** (Raisonnement par contraposée). Soient  $P$  et  $Q$  deux assertions. Alors  $P \Rightarrow Q$  et  $\neg Q \Rightarrow \neg P$  sont équivalents. En d'autres termes, on peut démontrer que  $P \Rightarrow Q$  est vraie en supposant que  $Q$  est fausse et en montrant que  $P$  est fausse.

**Preuve.** Par définition,  $\neg Q \Rightarrow \neg P$  est l'assertion  $\neg(\neg Q) \vee (\neg P)$ , c'est-à-dire  $Q \vee \neg P$ , c'est-à-dire  $P \Rightarrow Q$ .  $\square$

**Définition 1.31.** L'assertion  $\neg Q \Rightarrow \neg P$  est appelée la *contraposée* de  $P \Rightarrow Q$ .

**Attention.** Ne pas confondre la contraposée et la réciproque.

**Exemple 1.32.** Soit  $n \in \mathbb{Z}$ . Si  $n^2$  est pair, alors  $n$  est pair.

Montrons-le par contraposée. Supposons donc que  $n$  n'est pas pair. Il existe donc un entier  $k$  tel que  $n = 2k + 1$ . Ainsi, on a  $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \times (2k^2 + 2k) + 1$ . Donc on a écrit  $n^2$  sous la forme  $2k' + 1$  où  $k'$  est l'entier  $2k^2 + 2k$ . Donc on a démontré que  $n^2$  n'est pas pair.

**Proposition 1.33.** Soient  $P, Q, R$  trois assertions.

1. *Modus ponens* :  $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$  est toujours vraie. (« Il pleut. Or s'il pleut, le sol est mouillé. Donc le sol est mouillé. »)
2. *Syllogisme* :  $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$  est toujours vraie. (« Socrate est un homme et tous les hommes sont mortels, donc Socrate est mortel »)

**Preuve.** Utiliser la définition de  $\Rightarrow$  et les propriétés de base vérifiées par  $\wedge$  et  $\vee$ , ou alors par raisonnement déductif, c'est-à-dire en utilisant les méthodes de preuve (exercice).  $\square$

**Exercice 1.34.** Démontrer la proposition ci-dessus.

**Exercice 1.35.** En utilisant la définition de  $\Rightarrow$ , ainsi que les propriétés de base vérifiées par  $\wedge$  et  $\vee$ , montrer que «  $P \Rightarrow (Q \Rightarrow R)$  » et «  $(P \wedge Q) \Rightarrow R$  » sont équivalentes.

**Exercice 1.36.** Par un raisonnement déductif, c'est-à-dire avec les méthodes de preuve et non les tables de vérité, montrer que les assertions suivantes sont vraies.

1.  $P \Rightarrow (Q \Rightarrow P)$ .
2.  $(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$ .
3.  $(P \Rightarrow Q) \Rightarrow ((R \Rightarrow P) \Rightarrow (R \Rightarrow Q))$ .

## 1.6 Équivalence

Terminons avec l'équivalence, que nous avons en fait un peu déjà croisée dans les propositions précédentes, puisqu'on employait le mot « équivalents » pour exprimer le fait que deux assertions avaient les mêmes tables de vérité.

**Définition 1.37.** Soient  $P$  et  $Q$  deux assertions. On définit l'*équivalence* entre  $P$  et  $Q$ , notée «  $P$  équivalente à  $Q$  », ou «  $P$  si et seulement si  $Q$  », ou  $P \iff Q$ , comme étant l'assertion  $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ . La table de vérité est la suivante :

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

### Remarque 1.38.

1. De même que l'implication  $\Rightarrow$ , l'équivalence  $\iff$  compare les valeurs logiques (et détecte même lorsqu'elles coïncident). Par conséquent,  $P \iff Q$  ne suppose ni la véracité de  $P$ , ni celle de  $Q$ . Le symbole  $\iff$  n'est donc pas un mot à écrire dans une phrase.
2. On remarquera que  $P$  et  $Q$  jouent des rôles symétriques : «  $P \iff Q$  » et «  $Q \iff P$  » sont équivalentes.
3. Enfin, «  $P \iff Q$  » est équivalente à «  $\neg(P \oplus Q)$  » (comparer les tables de vérité).

**Méthode de preuve 1.39** (Méthode de preuve : preuve par double implication). Soient  $P$  et  $Q$  deux assertions. Montrer que  $P \iff Q$  est vraie revient à faire les deux choses suivantes :

- supposer que  $P$  est vraie et montrer que  $Q$  est vraie ;
- supposer que  $Q$  est vraie et montrer que  $P$  est vraie.

**Preuve.** Cela découle de la définition de  $\iff$  en fonction de  $\Rightarrow$ . □

**Exemple 1.40.** Soit  $x \in \mathbb{R}$ . Montrons l'équivalence suivante : «  $x^2 = 1 \iff (x = 1 \text{ ou } x = -1)$  ». On la démontre par double implication.<sup>3</sup>

**Étape 1 :** Preuve de «  $x^2 = 1 \Rightarrow (x = 1 \text{ ou } x = -1)$  ». Supposons que  $x^2 = 1$  et montrons «  $x = 1 \text{ ou } x = -1$  ». On sait que  $x^2 - 1 = 0$ . Une identité remarquable donne  $x^2 - 1 = (x + 1)(x - 1)$ . Ce produit étant nul, l'un des deux facteurs doit être nul. Ou bien  $x + 1 = 0$ , et on a donc montré que  $x = -1$ . Ou bien  $x - 1 = 0$ , et on a donc montré que  $x = 1$ .

**Étape 2 :** Preuve de «  $x^2 = 1 \Leftarrow (x = 1 \text{ ou } x = -1)$  ». Supposons «  $x = 1 \text{ ou } x = -1$  » et montrons que  $x^2 = 1$ . On sait qu'au moins une des assertions «  $x = 1$  » et «  $x = -1$  » est vraie. Si  $x = 1$ , alors  $x^2 = 1^2 = 1$ , ce qu'on voulait. Sinon, on a  $x = -1$  et donc  $x^2 = (-1)^2 = 1$ , ce qu'on voulait.

**Exercice 1.41.** Les assertions suivantes :

1.  $(P \iff Q) \wedge (Q \iff R)$  ;
2.  $(P \iff Q) \iff (Q \iff R)$ ,

sont-elles équivalentes ? On dressera leur table de vérité (à trois entrées).

## 1.7 Quantificateurs

Les propriétés sur  $\wedge$  et  $\vee$  peuvent aussi s'exprimer lorsqu'on a bien plus d'assertions. Soyons plus précis. Soit  $n$  un entier positif, ainsi que  $n$  assertions  $P(1), P(2), \dots, P(n)$ .

- L'associativité permet de définir  $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ . Elle est vraie si et seulement si toutes les assertions  $P(1), P(2), \dots, P(n)$  sont vraies (pas une seule ne doit être fausse).
- L'associativité permet aussi de définir  $P(1) \vee P(2) \vee \dots \vee P(n)$ . Elle est vraie si et seulement si au moins l'une des assertions  $P(1), P(2), \dots, P(n)$  est vraie.
- Les règles avec la négation se généralisent aisément :
  - $\neg(P(1) \wedge P(2) \wedge \dots \wedge P(n))$  est équivalente à  $\neg P(1) \vee \neg P(2) \vee \dots \vee \neg P(n)$  ;
  - $\neg(P(1) \vee P(2) \vee \dots \vee P(n))$  est équivalente à  $\neg P(1) \wedge \neg P(2) \wedge \dots \wedge \neg P(n)$ .

Dans cet exemple, les propriétés sont indexées<sup>4</sup> sur l'ensemble  $\{1, \dots, n\}$  des entiers entre 1 et  $n$ , c'est-à-dire qu'à un élément  $i$  de cet ensemble, j'associe l'assertion  $P(i)$ . On écrira de manière plus compacte :

- «  $\forall i \in \{1, \dots, n\}, P(i)$  » au lieu de  $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ , se lit « pour tout  $i \in \{1, \dots, n\}, P(i)$  » ;
- «  $\exists i \in \{1, \dots, n\}, P(i)$  » au lieu de  $P(1) \vee P(2) \vee \dots \vee P(n)$ , se lit « il existe  $i \in \{1, \dots, n\}$  tel que  $P(i)$  ».

$\forall$  et  $\exists$  sont respectivement appelés *quantificateurs universel* et *existentiel*.

**Remarque 1.42.** La variable  $i$  n'est pas un élément fixé de  $\{1, \dots, n\}$ , c'est un nom générique qu'on donne lorsqu'on balaye tous les éléments de cet ensemble. On dit que la variable est muette. On aurait pu écrire «  $\forall j \in \{1, \dots, n\}, P(j)$  », voire «  $\forall \Sigma \in \{1, \dots, n\}, P(\Sigma)$  ». En revanche, on n'aurait pas pu appeler la variable muette  $n$ , vu qu'on a déjà déclaré une variable (non muette)  $n$ .

On obtient ainsi que

- «  $\neg(\forall i \in \{1, \dots, n\}, P(i))$  » est équivalente à «  $\exists i \in \{1, \dots, n\}, \neg P(i)$  » ;
- «  $\neg(\exists i \in \{1, \dots, n\}, P(i))$  » est équivalente à «  $\forall i \in \{1, \dots, n\}, \neg P(i)$  ».

On peut en fait indexer les assertions sur des ensembles plus généraux. Exemples :

- Pour tout  $x \in \mathbb{R}$ , on peut définir  $P(x)$  comme étant l'assertion «  $x^2 = 1$  ».
- Pour tout  $x \in \mathbb{N}$ , on peut définir  $P(x)$  comme étant l'assertion «  $x$  est un nombre premier ».

Généralisons donc tout le propos dans ce cadre.

3. La rédaction est certes un peu exagérée, mais a pour but d'illustrer sur un exemple la structure d'une preuve.

4. À méditer : Il est tentant de dire « numérotées ». Or on pourrait très bien les indexer sur un ensemble dont on ne peut énumérer les éléments (élément numéro 1, élément numéro 2, etc.). Cf problème 2.5.3 du chapitre 2.

**Définition 1.43.** Soit  $E$  un ensemble. Soit, pour tout  $x \in E$ , une assertion  $P(x)$ .

- L'assertion «  $\forall x \in E, P(x)$  » se lit « pour tout  $x \in E, P(x)$  » et est vraie si pour tout élément  $x$  de  $E$ ,  $P(x)$  est vraie.
- L'assertion «  $\exists x \in E, P(x)$  » se lit « il existe  $x \in E$  tel que  $P(x)$  » et est vraie s'il existe un élément  $x$  de  $E$  tel que  $P(x)$  est vraie.

On a naturellement les propriétés suivantes :

- «  $\neg(\forall x \in E, P(x))$  » est équivalente à «  $\exists x \in E, \neg P(x)$  » ;
- «  $\neg(\exists x \in E, P(x))$  » est équivalente à «  $\forall x \in E, \neg P(x)$  ».

**Remarque 1.44.**

1. «  $\forall x \in E, P(x)$  » est la généralisation du « et » qu'on retrouvait dans «  $P \wedge Q$  » ou dans «  $P(1) \wedge \dots \wedge P(n)$  ». En revanche, on ne peut pas reformuler la véracité de «  $\forall x \in E, P(x)$  » avec des « et », puisqu'on ne peut *a priori* pas énumérer les assertions.
2. De même, «  $\exists x \in E, P(x)$  » est la généralisation du « ou » qu'on retrouvait dans «  $P \vee Q$  » ou dans «  $P(1) \vee \dots \vee P(n)$  ».

Dans la définition 1.43, la variable  $x$  est muette, on aurait pu écrire «  $\forall y \in E, P(y)$  ».

**Attention.** La négation de «  $\forall x \in E, P(x)$  » ne vaut pas «  $\forall x \notin E, P(x)$  ». La négation ne se reporte que sur  $P(x)$ , pas sur «  $x \in E$  » (on reste dans le cadre de l'ensemble  $E$ , on n'en sort pas). Et bien sûr  $\forall$  se transforme en  $\exists$ .

**Exemple 1.45.** Si  $x$  est un entier plus grand ou égal à 2, l'assertion «  $x$  est un nombre premier » s'écrit

$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, x = nm \Rightarrow (n = 1 \text{ ou } m = 1).$$

Quelques commentaires :

- Attention à la structure de l'assertion. Elle doit se lire comme

$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, (x = nm \Rightarrow (n = 1 \text{ ou } m = 1)),$$

et non pas comme «  $(\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, x = nm) \Rightarrow (n = 1 \text{ ou } m = 1)$  ». La dernière assertion n'a pas de sens vu que les variables  $m$  et  $n$  du membre de gauche de l'implication sont muettes, alors que dans le membre de droite,  $m$  et  $n$  n'ont jamais été déclarées, on ne sait pas ce que c'est.

- Une fois qu'on saura manipuler le produit cartésien, on pourra écrire de manière plus compacte «  $\forall(n, m) \in \mathbb{N} \times \mathbb{N}$  ». Plus généralement, une juxtaposition de symboles  $\forall$  peut se voir comme un unique  $\forall$ . Cela est aussi valable pour  $\exists$ . Tout cela est expliqué dans la remarque 2.45

En revanche, une assertion de la forme «  $\forall \dots, \exists \dots, \forall \dots, \dots$  » ne peut *a priori* pas se simplifier.

- La négation de «  $x$  est premier », c'est-à-dire l'assertion «  $x$  n'est pas premier », se calcule étape par étape. On commence par la négation du quantificateur universel en  $n$ , on obtient :

$$\exists n \in \mathbb{N}, \neg(\forall m \in \mathbb{N}, x = nm \Rightarrow (n = 1 \text{ ou } m = 1)).$$

On considère ensuite la négation du quantificateur en  $m$  :

$$\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, \neg(x = nm \Rightarrow (n = 1 \text{ ou } m = 1)).$$

À l'avenir, on pourra aller beaucoup plus vite en regroupant ces deux étapes en une, ceci est aussi valable lorsqu'on a une juxtaposition de  $\exists$ . Traitons maintenant la négation de l'implication :

$$\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, x = nm \text{ et } \neg(n = 1 \text{ ou } m = 1).$$

Il ne reste plus qu'à traiter la négation de la disjonction. Noter que la négation de «  $n = 1$  » est «  $n \neq 1$  », mais peut aussi s'écrire «  $n \geq 2$  » vu que  $n$  est un entier positif. Ainsi l'assertion «  $x$  n'est pas premier » s'écrit

$$\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, x = nm \text{ et } n \geq 2 \text{ et } m \geq 2.$$

#### Remarque 1.46.

1. On peut encore simplifier l'expression de l'assertion obtenue. On peut montrer (exercice) que si  $E$  est l'ensemble des entiers plus grands ou égaux à 2, alors l'assertion «  $\exists n \in \mathbb{N}, \exists m \in \mathbb{N}, x = nm \text{ et } n \geq 2 \text{ et } m \geq 2$  » que nous venons d'obtenir est équivalente à

$$\exists n \in E, \exists m \in E, x = nm.$$

Autrement dit, la propriété «  $n \geq 2$  et  $m \geq 2$  » donne une restriction supplémentaire au fait qu'on doit trouver  $n$  et  $m$  dans  $\mathbb{N}$ .

2. Par abus, on peut même écrire

$$\exists n \geq 2, \exists m \geq 2, x = nm.$$

L'abus vient du fait qu'on ne sait pas où se situent les variables muettes  $n$  et  $m$ . Sont-ce des réels ? des entiers ? On fera cet abus seulement si le contexte est clair.

**Exemple 1.47.** Étant donnée une fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  et étant donné un réel  $x$ , la continuité de  $f$  en  $x$  s'écrit :

$$\forall \varepsilon > 0, \exists \delta > 0, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon.$$

Quelques commentaires :

- Ici, «  $\forall \varepsilon > 0$  » doit être compris comme «  $\forall \varepsilon \in \mathbb{R}_{>0}$  » où  $\mathbb{R}_{>0}$  est l'ensemble des réels positifs, de même pour «  $\exists \delta > 0$  ».
- Attention à la structure de l'assertion. Elle doit se lire comme

$$\forall \varepsilon > 0, \exists \delta > 0, \forall y \in \mathbb{R}, \left( |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon \right),$$

et non pas comme «  $\left( \forall \varepsilon > 0, \exists \delta > 0, \forall y \in \mathbb{R}, |y - x| < \delta \right) \Rightarrow |f(y) - f(x)| < \varepsilon$  ». La dernière assertion n'a pas de sens vu que la variable  $\varepsilon > 0$  du membre de gauche de l'implication est muette, alors que dans le membre de droite,  $\varepsilon$  n'a jamais été déclarée, on ne sait pas ce que c'est.

- La négation de l'assertion se calcule étape par étape. On commence par la négation du «  $\forall \varepsilon > 0, \dots$  » :

$$\exists \varepsilon > 0, \neg \left( \exists \delta > 0, \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon \right),$$

puis la négation du «  $\exists \delta > 0, \dots$  » :

$$\exists \varepsilon > 0, \forall \delta > 0, \neg \left( \forall y \in \mathbb{R}, |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon \right),$$

puis la négation du «  $\forall y \in \mathbb{R}, \dots$  » :

$$\exists \varepsilon > 0, \forall \delta > 0, \exists y \in \mathbb{R}, \neg \left( |y - x| < \delta \Rightarrow |f(y) - f(x)| < \varepsilon \right),$$

et enfin la négation de l'implication. On obtient ainsi que le fait que  $f$  ne soit pas continue en  $x$  s'écrit :

$$\exists \varepsilon > 0, \forall \delta > 0, \exists y \in \mathbb{R}, |y - x| < \delta \text{ et } |f(y) - f(x)| \geq \varepsilon.$$

**Exemple 1.48.** Démontrons l'assertion «  $\forall x > 0, \frac{x+2}{x} \neq 1$  ».

On procède par l'absurde. On suppose donc que la négation est vraie. Or la négation vaut exactement :

$$\exists x > 0, \frac{x+2}{x} = 1.$$

Comme on la suppose vraie, on sait donc qu'il existe un réel  $x > 0$  tel que  $\frac{x+2}{x} = 1$ , on en fixe un. Ainsi, on obtient  $x + 2 = x$ , c'est-à-dire  $2 = 0$ . C'est une contradiction.

Donc l'assertion «  $\forall x > 0, \frac{x+2}{x} \neq 1$  » est vraie.

**Exercice 1.49.** Écrire les énoncés suivants à l'aide de quantificateurs, puis donner leur négation.

1. Il existe un plus grand entier.
2. Chaque entier est la somme de deux entiers.
3. Il existe un entier qui, lorsqu'on l'ajoute à n'importe quel entier, ne change pas cet entier.

**Méthode de preuve 1.50.** Pour montrer que «  $\forall x \in E, P(x)$  » est vrai, il faut fixer un élément **arbitraire**  $x$  de  $E$ , et montrer que  $P(x)$  est vrai.

Par « arbitraire », on entend que la seule information que nous exploitons sur  $x$ , c'est son appartenance à  $E$ ,  $x$  incarne donc un élément quelconque de  $E$ . Ce n'est pas comme «  $\exists x \in E, P(x)$  », où on choisit un élément  $x \in E$  bien spécifique, pour lequel cela va fonctionner.

**Exemple 1.51.** Reprenons l'exemple 1.47 sur la continuité d'une fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  en un réel  $x$ . Nous considérons la fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  définie par  $f(t) = t^2$  pour tout  $t \in \mathbb{R}$ , et nous nous concentrons sur le point 0. Montrons que  $f$  est continue en 0 (la rédaction sera exagérée afin de bien comprendre comment s'articule la preuve). Comme  $f(0) = 0$ , on doit démontrer

$$\forall \varepsilon > 0, \exists \delta > 0, \forall y \in \mathbb{R}, |y| < \delta \Rightarrow |y^2| < \varepsilon.$$

Étant donné le «  $\forall \varepsilon > 0$  », on fixe  $\varepsilon > 0$ , et pour celui-ci, on doit démontrer

$$\exists \delta > 0, \forall y \in \mathbb{R}, |y| < \delta \Rightarrow |y^2| < \varepsilon.$$

Il n'est pas toujours facile de démontrer l'existence d'un élément ayant la propriété voulue (ici  $\exists \delta > 0, \dots$ ). Il faut donc faire place à la réflexion et à l'intuition.

**Brouillon :** Pour trouver un tel  $\delta > 0$ , je me dis que si je fixe un  $\delta > 0$  et je prends un réel  $y$  vérifiant  $|y| < \delta$ , alors j'aurais nécessairement  $|y^2| < \delta^2$ . Si  $\delta^2 \leq \varepsilon$ , alors j'ai ce que je veux. On va donc prendre  $\delta = \sqrt{\varepsilon}$ .

**Rédaction après avoir réfléchi au brouillon :** Considérons  $\delta = \sqrt{\varepsilon}$  et montrons

$$\forall y \in \mathbb{R}, |y| < \sqrt{\varepsilon} \Rightarrow |y^2| < \varepsilon.$$

Au vu du «  $\forall y \in \mathbb{R}$  », nous allons fixer un certain  $y \in \mathbb{R}$  et montrer

$$|y| < \sqrt{\varepsilon} \Rightarrow |y^2| < \varepsilon.$$

Or si on a  $|y| < \sqrt{\varepsilon}$ , alors nécessairement  $|y^2| < \sqrt{\varepsilon}^2 = \varepsilon$ . Ceci achève la preuve. Donc  $f$  est continue en 0.

**Exercice 1.52.** Montrer la continuité de  $f$  en tout point  $x \in \mathbb{R}$  (l'existence de  $\delta$  demande un peu plus de travail).

**Exemple 1.53.** Reprenons l'exemple 1.47 sur la continuité d'une fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  en un réel  $x$ .

Ici, nous considérons la fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  définie par  $f(t) = 1$  si  $t \geq 0$ ,  $f(t) = 0$  si  $t < 0$ , et nous nous concentrons sur le point  $x = 0$ . Montrons que  $f$  n'est pas continue en 0 (avec une rédaction moins exagérée que celle de l'exemple précédent).

$f(0)$  étant égal à 1, on doit démontrer l'assertion suivante :

$$\exists \varepsilon > 0, \forall \delta > 0, \exists y \in \mathbb{R}, |y| < \delta \text{ et } |f(y) - 1| \geq \varepsilon.$$

**Brouillon :** On doit chercher un bon  $\varepsilon$ . La propriété nous dit qu'avec un tel  $\varepsilon > 0$ , on pourrait choisir un  $y$  aussi proche qu'on veut de 0, on n'aurait quand même  $f(y)$  loin de 1 à plus de  $\varepsilon$ . Or, si on trace le graphe de  $f$ , on remarque que les réels  $y$  strictement négatifs, arbitrairement proche de 0, vérifient toujours  $|f(y) - 1| = 1$ , en particulier  $|f(y) - 1| \geq 1/2$ . On va donc montrer que  $\varepsilon = 1/2$  convient (évidemment, tout  $\varepsilon$  strictement entre 0 et 1 conviendrait).

**Rédaction après avoir réfléchi au brouillon :** Considérons  $\varepsilon = 1/2$ . Fixons  $\delta > 0$  et démontrons :

$$\exists y \in \mathbb{R}, |y| < \delta \text{ et } |f(y) - 1| \geq 1/2.$$

On choisit un réel  $y$  arbitraire strictement compris entre  $-\delta$  et 0 (par exemple  $y = -\delta/2$ ) et ce  $y$  vérifie bien «  $|y| < \delta$  » ainsi que «  $|f(y) - 1| \geq 1/2$  » (vu que  $f(y) = 0$ ), ce qu'on voulait. Donc la propriété est bien vraie pour  $\varepsilon = 1/2$ , donc  $f$  n'est pas continue en 0.

**Exercice 1.54.** Soit  $E$  un ensemble et soit  $P(x)$  et  $Q(x)$  des assertions pour tout  $x \in E$ . Par un raisonnement déductif, montrer que les assertions suivantes sont vraies.

1.  $(\forall x \in E, P(x)) \Rightarrow (\exists x \in E, P(x))$ .
2.  $(\forall x \in E, (P(x) \Rightarrow Q(x))) \Rightarrow ((\exists x \in E, P(x)) \Rightarrow (\exists x \in E, Q(x)))$ .
3.  $(\exists x \in E, (P(x) \Rightarrow Q(x))) \Rightarrow ((\forall x \in E, P(x)) \Rightarrow (\exists x \in E, Q(x)))$ .

Qu'en est-il de

$$(\exists x \in E, (P(x) \Rightarrow Q(x))) \Rightarrow ((\exists x \in E, P(x)) \Rightarrow (\exists x \in E, Q(x))) ?$$

**Exercice 1.55.** Soit  $P(n)$  une assertion pour tout  $n \in \mathbb{N}$ . Exprimer avec des quantificateurs les assertions suivantes.

1. À partir d'un certain entier positif  $n$ , on a  $P(n)$ ,  $P(n+1)$ ,  $P(n+2)$ ,  $P(n+3)$ , etc.
2. Il existe un nombre fini d'entiers positifs  $n$  tel que  $P(n)$ .
3. Il existe une infinité d'entiers positifs  $n$  tel que  $P(n)$ .

Dans les exemples précédents, il était question de démontrer des «  $\exists x \in E, \dots$  ». En général, il peut être difficile de prouver une existence. Voici une méthode, appelée *analyse-synthèse*

**Méthode de preuve 1.56** (Analyse-synthèse). Pour démontrer que «  $\exists x \in E, P(x)$  » est vraie, la méthode d'analyse-synthèse est une stratégie consistant à suivre la démarche suivante.

1. On part du principe qu'il existe bien un élément  $x$  de  $E$  tel que  $P(x)$ . On fixe un tel  $x$ .
2. ANALYSE (« si un tel  $x$  existe, à quoi ressemble-t-il ? ») : Le fait que  $P(x)$  soit vraie donne des informations sur  $x$ , qu'on essaye d'affiner le plus possible pour avoir le plus d'indices sur ce que pourrait être  $x$ .
3. SYNTHÈSE : Si on a obtenu assez d'indices sur la manière de construire un tel candidat  $x$ , on le construit, on montre qu'il appartient bien à  $E$ <sup>5</sup> et on montre que la propriété  $P(x)$  est vraie.

La phase d'analyse peut aussi révéler une expression explicite de  $x$  (les informations obtenues sont tellement restrictives qu'il ne peut y en avoir qu'un seul). Dans ce cas, sous réserve d'existence, la phase d'analyse nous fournit en bonus qu'un tel  $x$  est unique.

**Remarque 1.57.** L'existence d'un **unique**  $x \in E$  tel que  $P(x)$  est vraie, se note

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

Dans le même esprit que la remarque 1.44, «  $\exists! x \in E, P(x)$  » est la généralisation de la disjonction exclusive.

**Exemple 1.58.** Montrons que toute fonction  $f: \mathbb{R} \rightarrow \mathbb{R}$  admet une unique décomposition  $f = g + h$  où  $g: \mathbb{R} \rightarrow \mathbb{R}$  est une fonction paire et  $h: \mathbb{R} \rightarrow \mathbb{R}$  est une fonction impaire<sup>6</sup>.

5. Ne pas oublier cette étape!

Autrement dit, on notant  $E$  l'ensemble des fonctions de  $\mathbb{R}$  dans  $\mathbb{R}$ ,  $E_p$  l'ensemble des fonctions  $g \in E$  qui sont paires et  $E_i$  l'ensemble des fonctions  $h \in E$  qui sont impaires, on veut montrer :

$$\forall f \in E, \exists! (g, h) \in E_p \times E_i, f = g + h.^7$$

Soit  $f \in E$ . On cherche à montrer qu'il existe une unique fonction paire  $g$  et une unique fonction impaire  $h$  telles que  $f = g + h$ . On procède par analyse-synthèse. Supposons que de telles fonctions  $g$  et  $h$  existent.

**Analyse :** On sait que  $f = g + h$ , c'est-à-dire que pour tout  $x \in \mathbb{R}$ ,  $f(x) = g(x) + h(x)$  (définition de l'égalité entre fonctions). Étant donné  $x \in \mathbb{R}$ , et en utilisant le fait que  $g$  et  $h$  sont respectivement paire et impaire, on a

$$f(-x) = g(-x) + h(-x) = g(x) - h(x).$$

On remarque alors que

$$f(x) + f(-x) = 2g(x) \text{ et } f(x) - f(-x) = 2h(x).$$

$x$  étant arbitraire, on a donc obtenu que nécessairement  $g$  et  $h$  sont les fonctions définies par, pour tout  $x \in \mathbb{R}$ ,

$$g(x) = \frac{f(x) + f(-x)}{2} \text{ et } h(x) = \frac{f(x) - f(-x)}{2}.$$

Sous réserve d'existence, on sait donc que  $g$  et  $h$  sont **uniques**.

**Synthèse :** Définissons deux fonctions  $g, h: \mathbb{R} \rightarrow \mathbb{R}$  par, pour tout  $x \in \mathbb{R}$ ,

$$g(x) = \frac{f(x) + f(-x)}{2} \text{ et } h(x) = \frac{f(x) - f(-x)}{2}.$$

Vérifions que  $g$  est paire et que  $h$  est impaire<sup>8</sup>. Soit  $x \in \mathbb{R}$ . On a :

$$\begin{aligned} g(-x) &= \frac{f(-x) + f(-(-x))}{2} = \frac{f(-x) + f(x)}{2} = g(x) \\ \text{et } h(-x) &= \frac{f(-x) - f(-(-x))}{2} = \frac{f(-x) - f(x)}{2} = -\left(\frac{f(x) - f(-x)}{2}\right) = -h(x). \end{aligned}$$

Ceci est valable pour tout  $x \in \mathbb{R}$  donc  $g$  est paire et  $h$  est impaire. Enfin, étant donné  $x \in \mathbb{R}$ , on a

$$g(x) + h(x) = \frac{f(x) + f(-x) + f(x) - f(-x)}{2} = \frac{2f(x)}{2} = f(x).$$

Ainsi  $f = g + h$ . Donc  $g$  et  $h$  conviennent.

On a donc démontré l'existence de telles fonctions  $g$  et  $h$ , et l'unicité découle de la phase d'analyse.

6. Une fonction  $g: \mathbb{R} \rightarrow \mathbb{R}$  est paire si pour tout  $x \in \mathbb{R}$ , on a  $g(-x) = g(x)$ . Une fonction  $h: \mathbb{R} \rightarrow \mathbb{R}$  est impaire si pour tout  $x \in \mathbb{R}$ , on a  $h(-x) = -h(x)$ .

7. Comme nous n'avons pas encore vu le produit cartésien entre ensembles, on pourra pour l'instant comprendre «  $\exists! (g, h) \in E_p \times E_i, \dots$  » comme «  $\exists! g \in E_p, \exists! h \in E_i, \dots$  ».

8. Ce qui correspond à l'étape « on montre qu'il appartient bien à  $E$  » dans l'encadré expliquant la méthode d'analyse-synthèse. À ne pas oublier !

**Exercice 1.59.** Déterminer toutes les fonctions  $f: \mathbb{R} \rightarrow \mathbb{R}$  vérifiant pour tout  $x \in \mathbb{R}$ ,

$$f(x) + 2f(-x) = x^2.$$

**Exercice 1.60.** Soit  $E$  un ensemble et  $P(x)$  une assertion pour tout  $x \in E$ . Exprimer «  $\exists! x \in E, P(x)$  » sans  $\exists!$ .



# Chapitre 2

## Notions de théorie des ensembles

Il est temps de se familiariser avec le vocabulaire de la théorie des ensembles. Le but ne sera pas de mettre l'accent sur les axiomes qui en sont à l'origine. Pour la culture, nous évoquerons quand même quelques éléments fondateurs de la théorie des ensembles, notamment son rôle pour appréhender certains paradoxes tels que le paradoxe du barbier (cf. section 2.2).

### 2.1 Ensemble, opérations entre ensembles

On peut d'emblée se mettre en tête que les notions ensemblistes que nous allons voir sont l'analogue des notions logiques qu'on a vues dans le chapitre précédent.

| Comparaisons et opérations entre ensembles         | Analogues logiques                                 |
|----------------------------------------------------|----------------------------------------------------|
| Inclusion $A \subset B$                            | Implication $\Rightarrow$                          |
| Égalité $A = B$                                    | Équivalence $\Longleftrightarrow$                  |
| Intersection $A \cap B$                            | Conjonction $\wedge$                               |
| Union $A \cup B$                                   | Disjonction $\vee$                                 |
| Union disjointe $A \sqcup B$                       | Disjonction $\oplus$                               |
| Intersection quelconque $\bigcap_{E \in X} E$      | Quantificateur universel $\forall$                 |
| Union quelconque $\bigcup_{E \in X} E$             | Quantificateur existentiel $\exists$               |
| Union disjointe quelconque $\bigsqcup_{E \in X} E$ | Quantificateur existentiel avec unicité $\exists!$ |
| Complémentaire $A^c$                               | Négation $\neg$                                    |
| Produit cartésien $A \times B$                     | Difficile à trouver, cf. remarque 2.45             |

#### 2.1.1 Inclusion, égalité

Un *ensemble*, c'est une collection de choses appelées *éléments* ou *membres*. Si  $E$  est un ensemble et  $x$  un élément de  $E$ , on notera  $x \in E$ . Si  $x$  n'est pas un élément de  $E$ , on notera  $x \notin E$ .

Comme indiqué au début de la section 1.1 du chapitre 1, il existe des exemples d'ensembles bien connus auxquels on a déjà donné un nom, comme  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{R}$ . On peut aussi considérer l'ensemble des entiers pairs, ou même l'ensemble dont les éléments sont tous les entiers sauf l'entier 5. Il n'existe pas que des ensembles constitués de nombres. On peut par exemple fabriquer l'ensemble  $E = \{1, \mathbb{R}, f\}$  constitué de trois éléments : 1, l'ensemble  $\mathbb{R}$  des réels et  $f$  la fonction racine carrée de  $\mathbb{R}_{\geq 0}$  dans  $\mathbb{R}$ .

**Remarque 2.1.** On utilise des accolades  $\{\dots\}$  pour définir un ensemble. Entre ces accolades, on peut lister les éléments de l'ensemble. Par exemple :

- l'ensemble  $\{1, 2, 3\}$  dont les éléments sont les entiers 1, 2 et 3 ;

- on peut aussi lister les éléments à l'aide de points de suspension :
  - l'ensemble  $\mathbb{N} = \{1, 2, 3, \dots\}$  qui a un nombre infini d'éléments ;
  - un autre exemple mais pour un ensemble fini : si  $a$  et  $b$  sont des entiers tels que  $a \leq b$ , alors l'ensemble des entiers compris (au sens large) entre  $a$  et  $b$  peut se noter  $\{a, a+1, \dots, b-1, b\}$ , voire  $\{a, \dots, b\}$ .

Il n'est parfois pas possible de lister les éléments d'un ensemble.

- C'est le cas lorsqu'il s'agit d'un ensemble dont on ne peut pas décrire les éléments par énumération, ce qu'on appelle un ensemble non dénombrable (c'est le cas de  $\mathbb{R}$ , voir par exemple le problème 2.5.3 à la fin de ce chapitre). Dans ce cas, l'ensemble en question n'est pas défini avec des accolades, sa définition repose sur une construction à partir d'ensembles déjà connus.
- C'est aussi le cas lorsqu'on pourrait quand même énumérer les éléments de l'ensemble, mais que la notation avec des points de suspension est ambiguë car on ne devine pas le motif. Par exemple, est-ce assez clair que  $\{2, 3, 5, 7, 11, \dots\}$  désigne l'ensemble des nombres premiers ? Comme nous le verrons, on utilise alors une notation plus compacte. Par exemple l'ensemble des nombres premiers peut s'écrire  $\{x \in \mathbb{N} \mid P(x)\}$  où pour tout  $x \in \mathbb{N}$ ,  $P(x)$  est l'assertion «  $x$  est un nombre premier ». On fait donc usage d'une variable muette  $x$  pour balayer l'ensemble des éléments de  $\mathbb{N}$ , et on n'accepte que ceux vérifiant la propriété, cela nous donne notre nouvel ensemble.

**Attention.**  $\mathbb{R}$  est un ensemble, mais il peut aussi être un élément d'un ensemble. Par exemple, si on reprend l'exemple de l'ensemble  $E = \{1, \mathbb{R}, f\}$ ,  $\mathbb{R}$  est un élément de  $E$ . L'ensemble  $E$  est lui-même un élément de l'ensemble  $\{E\}$  (c'est le seul). Remarquons enfin que  $1 \in E$ , mais  $1 \notin \{E\}$ .

**Exercice 2.2.** Soit  $E$  un ensemble. Déterminer les éléments de l'ensemble  $\{1, \{1, 2, 3\}, E, \{E\}\}$ .

### Définition 2.3.

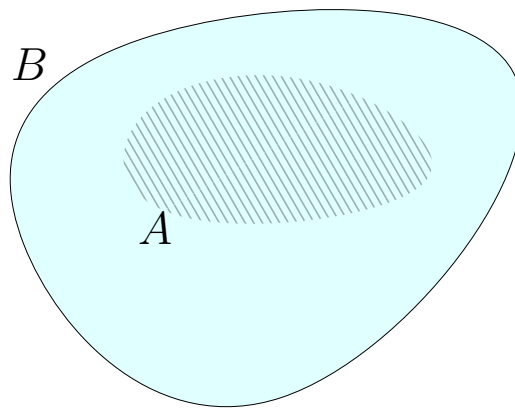
- L'*ensemble vide* est l'ensemble qui ne contient aucun élément, on le note  $\emptyset$ . On admet son existence.<sup>a</sup>
- Un ensemble ne contenant qu'un seul élément est appelé un *singleton*. L'ensemble  $\{x\}$  est appelé le *singleton*  $x$ .
- Un ensemble contenant deux éléments distincts est appelé une *paire*. Par exemple, la paire  $\{1, 2\}$ .

<sup>a</sup>. L'existence d'un tel ensemble est en fait un des axiomes de la théorie des ensembles.

Comparons maintenant les ensembles entre eux.

**Définition 2.4.** Soient  $A$  et  $B$  deux ensembles. On dit que  $A$  est *inclus* dans  $B$ , ou  $A$  est *contenu* dans  $B$ , ou  $B$  *contient*  $A$ , ou  $A$  est un *sous-ensemble*/une *partie* de  $B$ , noté  $A \subset B$ , si tout élément de  $A$  appartient à  $B$ . Autrement dit,  $A \subset B$  si et seulement si

$$\forall x \in A, x \in B.$$



**Exemple 2.5.**  $\mathbb{N}$  est un sous-ensemble de  $\mathbb{Z}$ .

**Notation.** Étant donné un ensemble  $A$  et pour tout  $x \in A$ , une assertion  $P(x)$ , on peut définir un sous-ensemble, noté  $\{x \in A \mid P(x)\}$ , ou  $\{x \in A : P(x)\}$ , ou  $\{x \in A, P(x)\}$ , qui est l'ensemble des éléments  $x$  de  $A$  pour lesquels  $P(x)$  est vrai.

**Exemple 2.6.**

1.  $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$ .
2. L'ensemble des entiers positifs pairs s'écrit  $\{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, n = 2k\}$ .

**Notation.** On peut se permettre quelques raccourcis dans l'écriture  $\{x \in A \mid P(x)\}$  lorsque les éléments s'écrivent d'une certaine forme. Contentons-nous de l'expliquer sur des exemples.

1. Reprenons le dernier exemple des entiers pairs. Au lieu d'écrire  $\{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, n = 2k\}$ , on peut directement écrire  $\{2k \in \mathbb{N} \mid k \in \mathbb{N}\}$ .
2. L'ensemble  $\{x \in \mathbb{N} \mid \exists n \geq 2, \exists m \geq 2, x = nm\}$  des entiers plus grands ou égaux à 2 qui ne sont pas premiers peut également s'écrire  $\{nm \in \mathbb{N} \mid n \geq 2, m \geq 2\}$ . Noter qu'ici, on se permet d'écrire «  $n \geq 2$  » au lieu de «  $n$  entier plus grand ou égal à 2 », c'est un abus qu'on se permet quand le contexte est clair. Ici on se doute qu'on considère des entiers.
3. On peut définir l'ensemble des nombres réels rationnelles par  $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists a \in \mathbb{Z}, \exists b \in \mathbb{N}, x = \frac{a}{b}\}$ , mais on peut directement écrire  $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ .

**Exercice 2.7.** Définir avec des accolades l'ensemble des carrés d'entiers.

**Proposition 2.8.** Soient  $A, B$  et  $C$  trois ensembles. Alors l'assertion suivante est vraie :

$$A \subset B \text{ et } B \subset C \Rightarrow A \subset C.$$

**Remarque 2.9.** Cette proposition ressemble beaucoup au syllogisme énoncé dans la proposition 1.33. L'inclusion peut en fait être vue comme une implication : si un élément  $x$  est dans  $A$ , alors il est dans  $B$ . En fait, si  $A$  et  $B$  sont contenus dans un ensemble  $E$  ambiant, alors  $A \subset B$  peut aussi s'écrire :

$$\forall x \in E, x \in A \Rightarrow x \in B.$$

**Preuve.** Pour démontrer l'implication, on suppose  $A \subset B$  et  $B \subset C$  et on montre  $A \subset C$ . Soit  $x \in A$ , montrons que  $x \in C$ . On sait que  $A \subset B$ , donc  $x \in B$ . Mais on sait aussi que  $B \subset C$ , donc  $x \in C$ , ce qu'on voulait.  $\square$

**Définition 2.10.** Deux ensembles  $A$  et  $B$  sont *égaux*, noté  $A = B$ , si et seulement si

$$A \subset B \text{ et } B \subset A.$$

On parle de « méthode par double-inclusion » pour démontrer une égalité entre ensembles, même si c'est plus une définition qu'une méthode.

Les ensembles  $A$  et  $B$  ayant des rôles symétriques dans la définition, on montre facilement que  $A = B$  et  $B = A$  sont équivalents. De plus, la proposition précédente montre que si  $A = B$  et  $B = C$ , alors  $A = C$ .

**Exemple 2.11.** La définition indique que lorsqu'on décrit un ensemble, l'ordre et la répétition des éléments entre les accolades n'ont aucune importance. Ainsi, les ensembles  $\{a, b\}$ ,  $\{b, a\}$ ,  $\{a, b, a\}$  et  $\{b, a, a, b, b, b\}$  sont les mêmes.

**Remarque 2.12.** De même que l'inclusion est similaire à une implication, l'égalité entre ensembles peut être vue comme l'analogue de l'équivalence. En fait, si  $A$  et  $B$  sont contenus dans un ensemble  $E$  ambiant, alors  $A = B$  peut aussi s'écrire :

$$\forall x \in E, x \in A \iff x \in B.$$

**Exercice 2.13.** Considérons les ensembles suivants :

$$A = \{x \in \mathbb{Z} \mid x > 3\},$$

$$B = \{3x^2 + 1 \mid x \in \mathbb{Z}\},$$

$$C = \{n \in \mathbb{N} \mid n > 3\},$$

$$D = \{k \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z}, k = 3\ell + 1\}.$$

Déterminer les inclusions qui ont lieu entre ces ensembles.

**Proposition 2.14.** Soit  $A$  un ensemble. Alors  $\emptyset$  et  $A$  sont des sous-ensembles de  $A$ . Si  $A$  est non vide, et si  $x$  est un élément de  $A$ , alors  $\{x\}$  est un sous-ensemble de  $A$ .

Vu que  $A \subset A$ , on en déduit que tout ensemble  $A$  est égal à lui-même.

**Attention** à bien faire la distinction entre  $\in$  et  $\subset$ . Par exemple, avec les notations de l'énoncé, on a  $x \in A$  et  $\{x\} \subset A$ . De même, on a  $A \subset A$  et  $A \in \{A\}$ .

**Preuve.** Pour  $A \subset A$ , on doit démontrer

$$\forall x \in A, x \in A,$$

on doit donc fixer un élément  $x$  de  $A$  et montrer que  $x \in A$ , ce qui est trivialement le cas.

Pour  $\emptyset \subset A$ , on doit démontrer que tout élément  $x \in \emptyset$  est un élément de  $A$ . Comment

démontrer cela sachant qu'il n'y a aucun élément  $x$  dans  $\emptyset$ ? Une manière de se convaincre que c'est toujours vrai est de considérer la négation :

$$\exists x \in \emptyset, x \notin A.$$

Comme on ne peut pas trouver d'élément  $x$  dans  $\emptyset$ , on ne peut *a fortiori* pas trouver d'élément  $x$  dans  $\emptyset$  vérifiant  $x \notin A$ . Donc la négation de  $\emptyset \subset A$  est fausse.

Supposons maintenant que  $A$  n'est pas l'ensemble vide et considérons un élément  $x$  de  $A$ . On veut montrer  $\{x\} \subset A$ . Soit donc  $y \in \{x\}$  et montrons que  $y$  est dans  $A$ . Mais l'assertion  $y \in \{x\}$  nous dit trivialement que  $y = x$ . Donc  $y$  est un élément de  $A$ . D'où  $\{x\} \subset A$ .  $\square$

**Corollaire 2.15.** *Il y a une unicité de l'ensemble vide.*

Voilà pourquoi nous ne parlions pas d'un ensemble vide, mais bien de l'ensemble vide.

**Preuve.** Soient  $\emptyset_1$  et  $\emptyset_2$  deux ensembles ne contenant aucun élément. En appliquant la proposition précédente à  $A = \emptyset_2$ , on obtient  $\emptyset_1 \subset \emptyset_2$ . Puis en l'appliquant à  $A = \emptyset_1$ , on obtient  $\emptyset_2 \subset \emptyset_1$ . Ainsi  $\emptyset_1 = \emptyset_2$ .  $\square$

**Définition 2.16.** Soit  $A$  un ensemble. L'ensemble des sous-ensembles de  $A$  est noté  $\mathcal{P}(A)$  (on admet qu'il existe <sup>a</sup>).

<sup>a</sup>. C'est en fait un des axiomes de la théorie des ensembles

**Proposition 2.17.**

1. *L'ensemble des sous-ensembles du vide vaut*

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

2. *L'ensemble des sous-ensembles d'un singleton  $\{x\}$  vaut*

$$\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}.$$

**Preuve.** On procède par double inclusion.

La proposition 2.14 énonce que si  $A$  est un ensemble, alors  $\emptyset$  et  $A$  sont des éléments de  $\mathcal{P}(A)$ . En appliquant cela à  $A = \emptyset$  et  $A = \{x\}$ , on obtient donc  $\{\emptyset\} \subset \mathcal{P}(\emptyset)$  et  $\{\emptyset, \{x\}\} \subset \mathcal{P}(\{x\})$ . Démontrons les inclusions réciproques.

Considérons  $A \in \mathcal{P}(\emptyset)$  et montrons  $A \in \{\emptyset\}$ , c'est-à-dire que  $A = \emptyset$ . Par définition,  $A \subset \emptyset$ . Mais la proposition 2.14 énonce qu'on a aussi  $\emptyset \subset A$ . Donc  $A = \emptyset$  comme voulu. Ceci démontre  $\mathcal{P}(\emptyset) \subset \{\emptyset\}$ . D'où  $\mathcal{P}(\emptyset) = \{\emptyset\}$ .

Considérons enfin  $A \in \mathcal{P}(\{x\})$ , c'est-à-dire  $A \subset \{x\}$ , et montrons  $A \in \{\emptyset, \{x\}\}$ , c'est-à-dire que  $A = \emptyset$  ou  $A = \{x\}$  (on doit donc démontrer une disjonction). Supposons donc  $\neg(A = \emptyset)$  et montrons que  $A = \{x\}$ . Le fait que  $\neg(A = \emptyset)$  soit vrai signifie que  $A$  admet au moins un élément. Soit  $y$  un élément de  $A$ . Par définition de  $A$ , on sait que  $A \subset \{x\}$ . Donc  $y$  est dans  $\{x\}$ , c'est-à-dire  $y = x$ . Donc  $x$  est un élément de  $A$ , ce qui donne  $\{x\} \subset A$ . Par double inclusion, on a donc  $A = \{x\}$ . Ceci démontre  $\mathcal{P}(\{x\}) \subset \{\emptyset, \{x\}\}$ .

D'où  $\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}$ . □

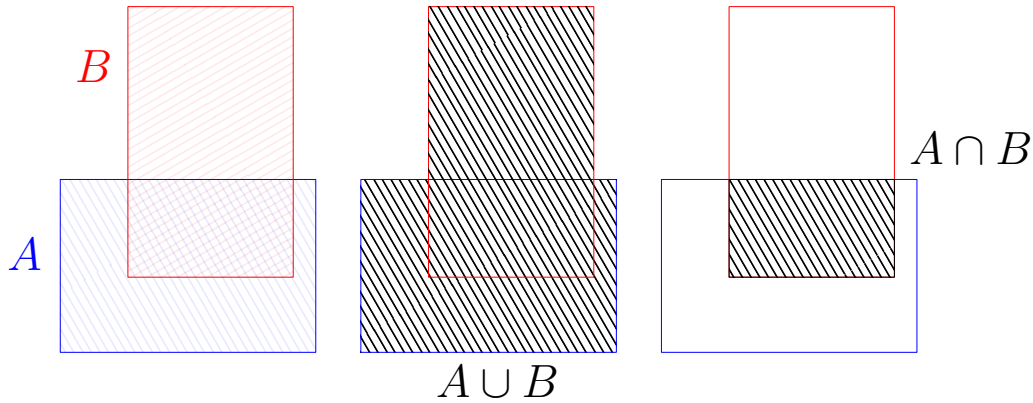
**Exercice 2.18.**

1. Soit  $E$  une paire  $\{a, b\}$  (avec  $a$  et  $b$  distincts). Déterminer  $\mathcal{P}(E)$ .
2. Soit  $E = \{a, b, c\}$  un ensemble à trois éléments  $a, b$  et  $c$  distincts. Déterminer  $\mathcal{P}(E)$ .
3. Déterminer  $\mathcal{P}(\mathcal{P}(\emptyset))$ , puis  $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ .

### 2.1.2 Intersection, union

**Définition 2.19.** Soient  $A$  et  $B$  deux ensembles.

- L'*intersection* entre  $A$  et  $B$ , notée  $A \cap B$ , ou «  $A$  inter  $B$  », est l'ensemble dont les éléments sont exactement ceux qui appartiennent à  $A$  et à  $B$ .
- L'*union* entre  $A$  et  $B$ , notée  $A \cup B$ , ou «  $A$  union  $B$  », est l'ensemble dont les éléments sont exactement ceux qui appartiennent à  $A$  ou à  $B$ .



**Remarque 2.20.**

1. L'intersection se définit avec une conjonction, et l'union avec une disjonction. La remarque 1.10 fait maintenant sens.
2. L'intersection  $A \cap B$  est trivialement un sous-ensemble de  $A$  et de  $B$ . Les ensembles  $A$  et  $B$  sont trivialement des sous-ensembles de l'union  $A \cup B$ . À vérifier, exercice.
3. En admettant que  $A$  et  $B$  sont des sous-ensembles d'un même ensemble ambiant  $E$ , on montre que l'intersection et l'union sont caractérisées par les assertions suivantes :

$$\forall x \in E, x \in A \cap B \iff (x \in A \wedge x \in B),$$

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

**Exercice 2.21.** Considérons les ensembles suivants :

$$A = \{2x \mid x \in \mathbb{N}\},$$

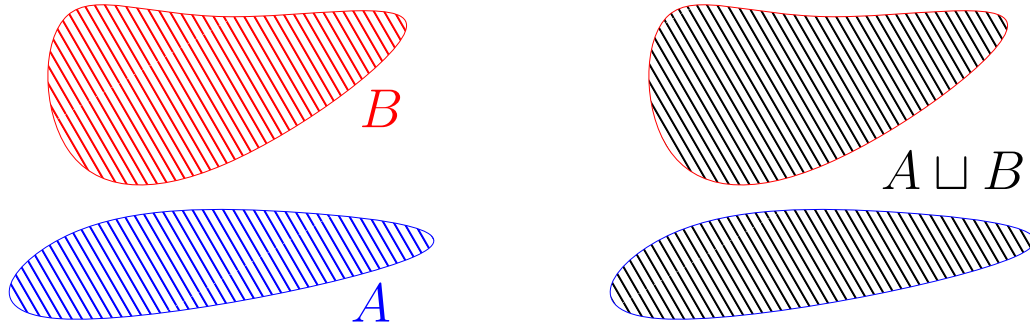
$$B = \{3x \mid x \in \mathbb{N}\},$$

$$C = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid \forall x \in \mathbb{R}, f(x) = f(-x)\},$$

$$D = \{f: x \in \mathbb{R} \mapsto x^k \in \mathbb{R} \mid k \in \mathbb{N}\}.$$

Déterminer  $A \cap B$ ,  $A \cap C$  et  $C \cap D$ . A-t-on l'égalité  $A \cup B = \mathbb{N}$ ?

**Définition 2.22.** Si deux ensembles  $A$  et  $B$  vérifient  $A \cap B = \emptyset$ , autrement dit  $\forall x \in A, x \notin B$  (ou  $\forall x \in B, x \notin A$ ), on dit que  $A$  et  $B$  sont *disjoints*. On dit alors que l'union  $A \cup B$  est une *union disjointe*, notée  $A \sqcup B$ .



**Remarque 2.23.** Alors que l'union est l'analogue de la disjonction, l'union disjointe se rattache plus particulièrement à la disjonction exclusive. En effet,  $A$  et  $B$  sont disjoints si et seulement si

$$\forall x \in A \cup B, x \in A \oplus x \in B$$

**Proposition 2.24.** Soient  $A$ ,  $B$  et  $C$  trois ensembles.

1. *Commutativité* :  $A \cup B = B \cup A$  et  $A \cap B = B \cap A$ .
2. *Associativité* :  $(A \cap B) \cap C = A \cap (B \cap C)$  et  $(A \cup B) \cup C = A \cup (B \cup C)$ . On notera ainsi  $A \cap B \cap C$  et  $A \cup B \cup C$ .
3. *Distributivité* :  $C \cap (A \cup B) = (C \cap A) \cup (C \cap B)$  et  $C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$ .
4. *Neutre* :  $A \cup \emptyset = A$ .
5. *Absorption* :  $A \cap \emptyset = \emptyset$ .
6.  $A \subset B \iff A \cap B = A$ .
7.  $A \subset B \iff A \cup B = B$ .
8. *Maximalité* :  $A \cap B$  est l'unique ensemble satisfaisant les deux propriétés suivantes :
  - (a)  $A \cap B$  est un sous-ensemble de  $A$  et de  $B$  ;
  - (b) si  $C$  est un autre sous-ensemble de  $A$  et de  $B$ , alors  $C \subset A \cap B$ .
 ( $A \cap B$  est « le plus grand » ensemble qui soit un sous-ensemble de  $A$  et de  $B$ ) ;
9. *Minimalité* :  $A \cup B$  est l'unique ensemble satisfaisant les deux propriétés suivantes :
  - (a)  $A \cup B$  contient  $A$  et  $B$  ;
  - (b) si  $C$  est un autre ensemble contenant  $A$  et  $B$ , alors  $A \cup B \subset C$
 ( $A \cup B$  est « le plus petit » ensemble qui contient  $A$  et  $B$ ).

Concernant les deux dernières propriétés, nous reparlerons de plus petit élément et plus grand élément lorsque nous introduirons les relations d'ordre (cf. section 3.3.1).

**Preuve.** La commutativité, l'associativité et la distributivité sont conséquences directes de la commutativité, l'associativité et la distributivité vérifiées par  $\wedge$  et  $\vee$  (proposition 1.15). À faire, exercice.

Preuve de  $A \cup \emptyset = A$ . L'ensemble  $A \cup \emptyset$  est l'ensemble constitué des éléments  $x$  vérifiant  $x \in A \vee x \in \emptyset$ . C'est équivalent à  $x \in A$ , l'assertion  $x \in \emptyset$  étant fausse.

Preuve de  $A \cap \emptyset = \emptyset$ . Même méthode que  $A \cup \emptyset = A$ , exercice.

Preuve de  $A \subset B \iff A \cap B = A$ . Supposons  $A \subset B$  et montrons  $A \cap B = A$ . On sait déjà que  $A \cap B \subset A$ . Pour l'inclusion réciproque, considérons  $x \in A$ . Étant donné que  $A \subset B$ , on obtient également  $x \in B$ . Donc  $x \in A$  et  $x \in B$ , donc  $x \in A \cap B$ . Ceci prouve l'inclusion réciproque, on a donc montré  $A \cap B = A$ . Ceci achève la preuve de l'implication  $A \subset B \Rightarrow A \cap B = A$ . Démontrons l'implication réciproque, c'est-à-dire supposons  $A \cap B = A$  et démontrons  $A \subset B$ . Soit  $x \in A$ , montrons que  $x \in B$ .  $A$  vaut  $A \cap B$ , donc  $x \in A \cap B$ , donc  $x \in A$  et  $x \in B$ , ce qu'on voulait. On a donc démontré l'implication réciproque. D'où l'équivalence.

Preuve de  $A \subset B \iff A \cup B = B$ . Mêmes idées (exercice).

Preuve de la propriété de maximalité. Introduisons une notation pour ne pas alourdir la preuve. Étant donné un ensemble  $D$ , on note  $P(D)$  la conjonction des deux assertions suivantes :

1.  $D$  est un sous-ensemble de  $A$  et de  $B$  ;
2. si  $C$  est un autre sous-ensemble de  $A$  et de  $B$ , alors  $C \subset D$ .

On doit donc démontrer que l'assertion  $P(A \cap B)$  est vraie, et que si  $D$  est un ensemble tel que  $P(D)$  est vraie, alors  $D = A \cap B$ .

On sait déjà que  $A \cap B$  est un sous-ensemble de  $A$  et de  $B$ . Soit  $C$  un autre sous-ensemble de  $A$  et de  $B$ . Montrons  $C \subset A \cap B$ . Soit  $x \in C$ , montrons que  $x \in A \cap B$ . On a  $C \subset A$  donc  $x \in A$ , puis  $C \subset B$  donc  $x \in B$ . Ainsi  $x \in A$  et  $x \in B$ , ce qui donne  $x \in A \cap B$  par définition. Ainsi  $P(A \cap B)$  est vraie.

Soit  $D$  un ensemble tel que  $P(D)$  est vraie. On sait que  $D$  est un sous-ensemble de  $A$  et de  $B$ , donc on peut appliquer à  $C = D$  la deuxième assertion figurant dans  $P(A \cap B)$ , pour ainsi obtenir  $D \subset A \cap B$ . De même,  $A \cap B$  est un sous-ensemble de  $A$  et de  $B$ , donc on peut appliquer à  $C = A \cap B$  la deuxième assertion figurant dans  $P(D)$ , pour ainsi obtenir  $A \cap B \subset D$ . D'où  $D = A \cap B$  et donc l'unicité.

Preuve de la propriété de minimalité. Mêmes idées (exercice). □

**Exercice 2.25.** Démontrer ce qui a été laissé en exercice dans la preuve ci-dessus.

**Exercice 2.26.** Si  $C$  est un sous-ensemble de  $A \cup B$ , a-t-on  $C \subset A$  et  $C \subset B$ ? Si  $A \cap B$  est un sous-ensemble de  $C$ , a-t-on  $A \subset C$  et  $B \subset C$ ?

Enfin, les quantificateurs universel et existentiel (généralisations de la conjonction et la disjonction de deux assertions) permettent de définir l'intersection et l'union de plus de deux ensembles.

**Définition 2.27.** Soit  $X$  un ensemble d'ensembles. On définit alors

- l'*intersection*  $\bigcap_{A \in X} A$  comme étant l'ensemble formé des éléments  $x$  vérifiant : pour tout  $A \in X$ ,  $x \in A$  ;
- l'*union*  $\bigcup_{A \in X} A$  comme étant l'ensemble formé des éléments  $x$  vérifiant : il existe  $A \in X$  tel que  $x \in A$ .

Autrement dit, si  $E$  est un ensemble *ambiant* aux éléments de  $X$ , c'est-à-dire que  $A \subset E$  pour tout  $A \in X$ , alors  $\bigcap_{A \in X} A$  et  $\bigcup_{A \in X} A$  sont caractérisés par :

$$\forall x \in E, \left( x \in \bigcap_{A \in X} A \iff \forall A \in X, x \in A \right)$$

et

$$\forall x \in E, \left( x \in \bigcup_{A \in X} A \iff \exists A \in X, x \in A \right).$$

Si on a un paramétrage des éléments de  $X$ , par exemple  $X = \{A_i \mid i \in I\}$  pour un certain ensemble  $I$ , alors on écrira plutôt

$$\bigcap_{i \in I} A_i \text{ et } \bigcup_{i \in I} A_i.$$

**Exemple 2.28.** Tout ensemble  $E$  est union de ses singletons :

$$E = \bigcup_{x \in E} \{x\}.$$

Ici il s'agit de  $\bigcup_{A \in X} A$  avec  $X = \{\{x\} \mid x \in E\}$ .

**Définition 2.29.** Soit  $X$  un ensemble d'ensembles. On dit que les éléments de  $X$  forment une famille *disjointe* si pour tout  $A, B \in X$  tels que  $A \neq B$ , on a  $A \cap B = \emptyset$ . Autrement dit, cela signifie :

$$\forall x \in \bigcup_{A \in X} A, \exists! A \in X, x \in A.$$

Dans ce cas, l'union des  $A \in X$  est notée  $\bigsqcup_{A \in X} A$  (*union disjointe*).

**Attention.** Le fait que la famille est disjointe n'est pas équivalent à  $\bigcap_{A \in X} A = \emptyset$ .

Voici un contre-exemple. Pour tout  $n \in \mathbb{Z}$ , posons  $A_n = \{i \in \mathbb{Z}, i \geq n\}$ . On vérifie que si  $n$  et  $m$  sont des entiers tels que  $m > n$ , alors  $A_m \cap A_n = A_m$  (exercice). Donc la famille n'est pas disjointe. Pourtant, l'intersection  $\bigcap_{n \in \mathbb{Z}} A_n = \emptyset$  est vide : si ce n'était pas vrai, un élément dedans serait un entier plus grand que tous les entiers, ce qui est exclu<sup>1</sup>.

Néanmoins, l'implication suivante est vraie :

$$\text{famille disjointe} \Rightarrow \bigcap_{A \in X} A = \emptyset.$$

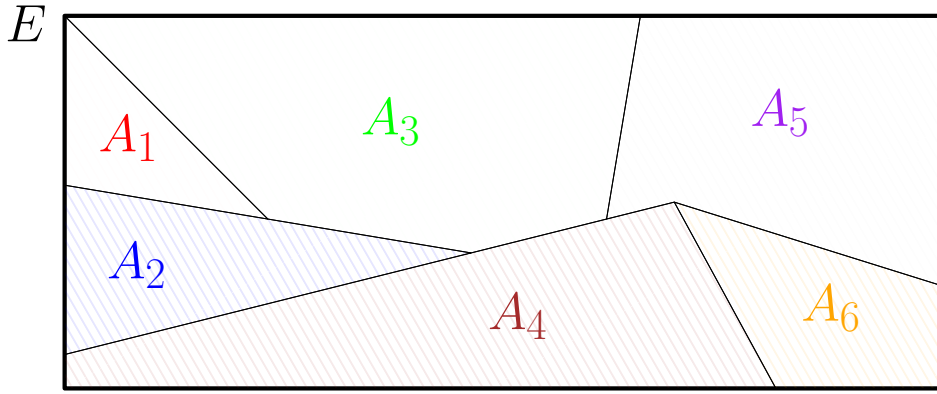
**Définition 2.30.** Soit  $E$  un ensemble. Considérons un ensemble  $X$  de sous-ensembles de  $E$ . On dit que  $X$  est une *partition* de  $E$  si les deux conditions sont vérifiées :

- les éléments de  $X$  forment une famille disjointe ;
- $E = \bigsqcup_{A \in X} A$ .

Cela peut aussi être résumé par l'assertion suivante :

$$\forall x \in E, \exists! A \in X, x \in A.$$

1. Conséquence de l'axiomatique de  $\mathbb{Z}$ , ce que nous allons voir dans le chapitre 3



$\{A_1, A_2, A_3, A_4, A_5, A_6\}$  est une partition de  $E$ .

### Exemple 2.31.

1. Les singletons de  $E$  forment une partition de  $E$ .
2. De manière triviale, si  $X$  est un ensemble d'ensembles et si ses éléments forment une famille disjointe, alors  $X$  est une partition de  $\bigsqcup_{A \in X} A$ .

### 2.1.3 Différence, complémentaire

Nous avons vu les notions d'inclusion, d'égalité, d'intersection et d'union, chacune étant respectivement l'analogue de  $\Rightarrow$ ,  $\iff$ ,  $\wedge$  et  $\vee$ . Regardons maintenant ce qui peut se rapprocher de la négation  $\neg$ .

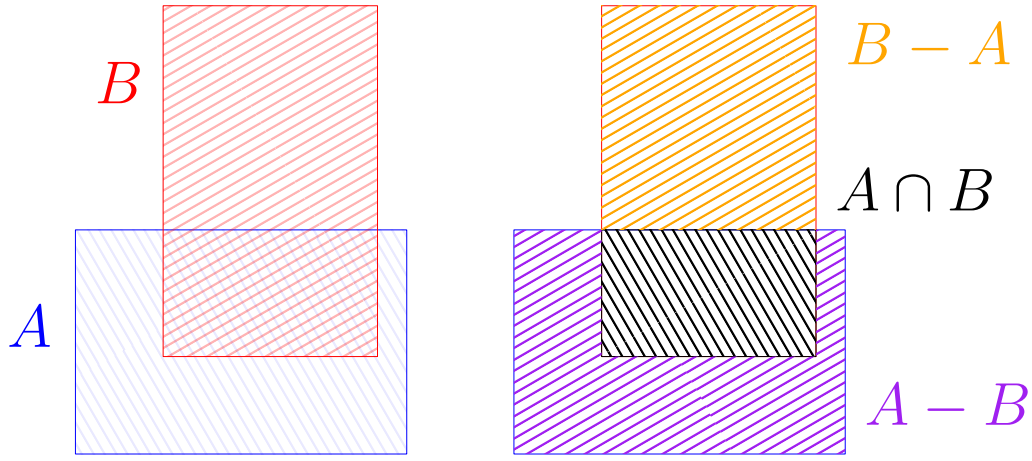
**Définition 2.32.** Soient  $A$  et  $E$  deux ensembles.

- La *différence* de  $E$  par  $A$ , noté  $E - A$ , ou  $E \setminus A$ , ou «  $E$  privé de  $A$  », est le sous-ensemble de  $E$  dont les éléments sont ceux de  $E$  qui ne sont pas dans  $A$ . Autrement dit, on a  $E - A = \{x \in E \mid x \notin A\}$ .
- Si  $A \subset E$ , alors  $E - A$  est aussi appelé le *complémentaire* de  $A$  dans  $E$ . On le notera  $A^c$  si l'ensemble  $E$  ambiant est clair.

**Attention** avec la notation  $A^c$ . Le complémentaire de  $A$  dépend de l'ensemble  $E$  ambiant.

**Proposition 2.33.** Soient  $A$ ,  $B$  et  $E$  trois ensembles.

1.  $A - \emptyset = A$ ;
2.  $A \subset E \iff A - E = \emptyset$  (en particulier  $A - A = \emptyset$ );
3.  $E - (E - A) = E \cap A$  (en particulier, si  $A \subset E$ ,  $E - (E - A) = A$ , propriété d'involution de l'opération «  $E -$  »);
4. Si  $A$  et  $B$  sont des sous-ensembles de  $E$ , alors  $A \subset B \iff E - B \subset E - A$ ;
5.  $A \cup B = (A - B) \sqcup (A \cap B) \sqcup (B - A)$ ;
6.  $E = (E \cap A) \sqcup (E - A)$ .



**Preuve.** Étant donné  $x \in A$ , on sait que  $x \notin \emptyset$  par définition de l'ensemble vide, donc  $x \in A - \emptyset$ . Réciproquement, on sait que  $A - \emptyset$  est un sous-ensemble de  $A$ . On a donc obtenu  $A - \emptyset = A$ .

Montrons  $A \subset E \iff A - E = \emptyset$ . Nous allons démontrer les deux implications par contraposée. Supposons  $A \not\subset E$  et montrons que  $A - E$  n'est pas vide. La négation de  $A \subset E$  s'écrit «  $\exists x \in A, x \notin E$  ». Soit donc  $x \in A$  tel que  $x \notin E$ . Par définition de  $A - E$ ,  $x$  est donc un élément de cet ensemble, donc cet ensemble n'est pas vide. Maintenant, si on suppose que  $A - E$  n'est pas vide, les mêmes idées permettent de montrer que  $A \not\subset E$ .

Preuve de  $E - (E - A) = E \cap A$ . Soit  $x \in E - (E - A)$ , montrons que  $x \in E \cap A$ .  $E - (E - A) \subset E$  donc on sait déjà que  $x \in E$ , il reste à démontrer que  $x \in A$ . Or par définition de  $E - (E - A)$ , on sait que  $x \notin E - A$ . Cette dernière assertion signifie que  $x \in E$  vérifie  $\neg(x \notin A)$ , c'est-à-dire  $x \in A$ , ce qu'on voulait. Maintenant, si on considère  $x \in E \cap A$ , les mêmes idées permettent de montrer  $x \in E - (E - A)$ .

Montrons  $A \subset B \iff E - B \subset E - A$  dans le cas où  $A$  et  $B$  sont des sous-ensembles de  $E$ . Supposons donc  $A \subset B$  et montrons  $E - B \subset E - A$ . Soit  $x \in E - B$ . Par définition,  $x \in E$  et  $x \notin B$ . Comme  $A \subset B$ , on obtient donc  $x \notin A$  (en effet,  $A \subset B$  peut s'écrire «  $\forall x \in E, x \in A \Rightarrow x \in B$  », ou de manière équivalente «  $\forall x \in E, x \notin B \Rightarrow x \notin A$  » par contraposée). Donc  $x \in E$  et  $x \notin A$ , c'est-à-dire  $x \in E - A$ . On a donc démontré  $A \subset B \iff E - B \subset E - A$ . Pour la réciproque, remarquons que  $A$  et  $B$  sont choisis arbitrairement parmi les sous-ensembles de  $E$ . Autrement dit, on a démontré que pour tout  $\tilde{A} \subset E$  et tout  $\tilde{B} \subset E$ ,  $\tilde{A} \subset \tilde{B} \iff E - \tilde{B} \subset E - \tilde{A}$ . Appliquons cela à  $A = E - B$  et  $B = E - A$ , et utilisons les égalités  $E - (E - A) = A$  et  $E - (E - B) = B$ , on obtient alors  $E - B \subset E - A \Rightarrow A \subset B$ , c'est-à-dire réciproque. D'où l'équivalence.

Démontrons  $A \cup B = (A - B) \sqcup (A \cap B) \sqcup (B - A)$ . On montre d'abord que l'union est bien disjointe (à faire, exercice). Montrons ensuite  $A \cup B \subset (A - B) \sqcup (A \cap B) \sqcup (B - A)$ . Soit  $x \in A \cup B$ . Cela signifie que  $x \in A$  ou  $x \in B$ . Sans perte de généralité, supposons  $x \in A$  (sinon  $x \in B$  et on appliquera le même raisonnement). Deux cas possibles : ou bien  $x \in B$ , ou bien  $x \notin B$ . Dans le premier cas, cela signifie que  $x \in A \cap B$ , dans le second, que  $x \in A - B$ . Donc au total,  $x$  est un bien élément de  $(A - B) \sqcup (A \cap B) \sqcup (B - A)$ . Pour l'inclusion réciproque, remarquons que chacun des membres  $A - B$ ,  $A \cap B$  et  $B - A$  sont des sous-ensembles de  $A \cup B$ , donc leur union aussi. D'où l'égalité.

Preuve de  $E = (E \cap A) \sqcup (E - A)$ . On applique la propriété précédente à des ensembles bien choisis : on remplace  $A$  par  $A \cap E$  et  $B$  par  $E$ . On obtient ainsi  $(A \cap E) \cup E = ((A \cap E) - E) \sqcup (A \cap E \cap E) \sqcup (E - (A \cap E))$ . Vu que  $A \cap E \subset E$ , on obtient  $(A \cap E) \cup E = E$  et  $(A \cap E) - E = \emptyset$ . Ensuite, on a  $A \cap E \cap E = A \cap E$ . Enfin, on a  $E - (A \cap E) = E - A$  : en effet, il suffit de passer au complémentaire dans la troisième propriété pour obtenir  $E - (E - (E - A)) = E - (E \cap A)$ , puis la propriété d'involution (vu que  $E - A \subset E$ ).

permet d'obtenir  $E - (E - (E - A)) = E - A$ . Au total, on a bien  $E = (E \cap A) \sqcup (E - A)$ .  $\square$

**Exercice 2.34.** Montrer ce qui n'a pas été vérifié dans la preuve :  $(A - B) \sqcup (A \cap B) \sqcup (B - A)$  est une union disjointe.

Enfin, la prochaine proposition est un analogue de la proposition 1.20 ou plus généralement des propriétés qui suivent la définition 1.43.

**Proposition 2.35.** Soit  $E$  un ensemble. Soit  $X$  un ensemble d'ensembles.

1.  $E - \bigcap_{A \in X} A = \bigcup_{A \in X} (E - A)$ .
2.  $E - \bigcup_{A \in X} A = \bigcap_{A \in X} (E - A)$ .

**Exemple 2.36.**

1. Supposons que les éléments de  $X$  sont des sous-ensembles de  $E$ . Alors les égalités de la proposition s'écrivent  $(\bigcap_{A \in X} A)^c = \bigcup_{A \in X} A^c$  et  $(\bigcup_{A \in X} A)^c = \bigcap_{A \in X} A^c$  si le contexte est clair, c'est-à-dire si on connaît bien l'ensemble  $E$  ambiant.
2. Par exemple si  $A$  et  $B$  sont des sous-ensembles de  $E$ , on a  $(A \cap B)^c = A^c \cup B^c$  et  $(A \cup B)^c = A^c \cap B^c$ .

**Preuve.** Utiliser la négation d'assertions de la forme «  $\forall A \in X, \dots$  » ou «  $\exists A \in X, \dots$  ». Exercice.  $\square$

**Exercice 2.37.** Démontrer la proposition ci-dessus.

### 2.1.4 Produit cartésien

**Définition 2.38.** Étant donnés deux ensembles  $A$  et  $B$ , on définit leur *produit cartésien* comme étant le nouvel ensemble

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

Les éléments  $(x, y)$  sont appelés des *couples*. L'égalité entre couples est définie par la règle suivante : pour tout  $x, x' \in A$ , pour tout  $y, y' \in B$ ,

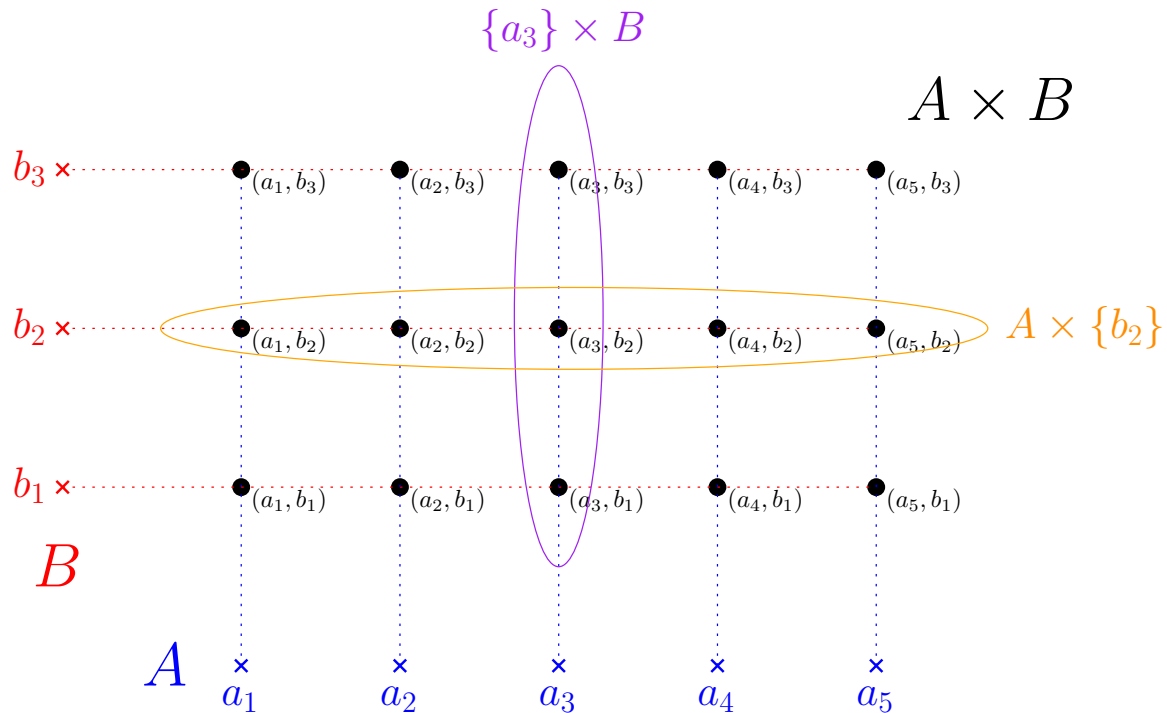
$$(x, y) = (x', y') \iff x = x' \text{ et } y = y'.$$

Le produit cartésien  $A \times A$  sera noté  $A^2$ .

Ceci ne constitue pas une définition rigoureuse puisqu'on n'a pas construit les couples. On explique seulement la condition d'égalité entre ces objets. Pour la culture, nous expliquerons la construction dans la section 2.2, qui repose sur les axiomes de la théorie des ensembles.

**Attention.** Le couple  $(x, y)$  ne doit pas être confondu avec la paire  $\{x, y\}$ . L'ordre est important pour un couple :  $(x, y) \neq (y, x)$  (sauf si  $x = y$ ) ; alors que  $\{x, y\} = \{y, x\}$ .

**Remarque 2.39.** Les produits cartésiens  $\emptyset \times A$  et  $A \times \emptyset$  sont vides. En effet, si  $A \times \emptyset$  n'était pas vide, alors il admettrait un élément qui par définition s'écrirait  $(x, y)$  pour  $x \in A$  et  $y \in \emptyset$ , ce qui n'est pas possible. Ainsi le produit cartésien n'a d'intérêt que pour les ensembles non vides.



**Remarque 2.40.**

1. Si  $A = \{a_1, a_2\}$  et  $B = \{b_1, b_2, b_3\}$ , alors

$$A \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3)\}.$$

On remarque que le nombre d'éléments de  $A \times B$  est le produit entre le nombre d'éléments de  $A$  et le nombre d'éléments de  $B$ . D'où le nom **produit** cartésien.

2. S'il y a un nombre infini d'éléments dans  $A$  ou dans  $B$ , la remarque qu'on vient de faire ne tient plus. Mais on peut encore trouver l'intuition d'un produit, avec le point de vue suivant. En classant les éléments de  $A \times B$  selon la coordonnée en  $B$ , on obtient

$$A \times B = \bigsqcup_{y \in B} \{(x, y) \mid x \in A\} = \bigsqcup_{y \in B} (A \times \{y\}).$$

Or, intuitivement  $A$  et  $A \times \{y\}$  sont pareil (notion rendue rigoureuse dans la section 2.3 grâce à la notion de bijection). Ainsi, de manière informelle,  $A \times B$  est constitué d'autant de copies de  $A$  qu'il n'y a d'éléments dans  $B$ . Et de manière similaire,  $A \times B$  est constitué d'autant de copies de  $B$  qu'il n'y a d'éléments dans  $A$ .

3. « Cartésien » fait référence à René Descartes qui a popularisé ce formalisme et montré tout son intérêt pour les équations (cartésiennes) d'une droite, d'un cercle, etc. On considère ainsi le produit cartésien  $\mathbb{R}^2$  quand on veut travailler en dimension 2, chaque point est un couple  $(x, y)$  où la coordonnée  $x \in \mathbb{R}$  est l'abscisse et la coordonnée  $y \in \mathbb{R}$  est l'ordonnée. On peut avoir besoin d'une dimension supplémentaire (pour représenter l'altitude, le temps, etc.) et ainsi se placer dans  $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ , à condition d'avoir défini le produit cartésien de plus de deux ensembles (ce dont on ne parlera pas ici).

**Proposition 2.41.** Soient  $A$  et  $B$  deux ensembles non vides. Alors on a

$$A \times B = B \times A \iff A = B.$$

**Preuve.** Supposons que  $A \times B = B \times A$  et montrons  $A = B$ . Soit  $x \in A$ . Si  $y$  est un élément de  $B$ , alors par définition  $(x, y) \in A \times B$ , donc  $(x, y) \in B \times A$ , ce qui signifie que  $x \in B$ . Ceci prouve que  $A \subset B$ . L'inclusion réciproque s'obtient de la même manière. D'où  $A = B$ . La réciproque est triviale.  $\square$

**Attention.** Le produit cartésien n'est pas associatif : si  $A$ ,  $B$  et  $C$  sont trois ensembles, alors  $(A \times B) \times C$  et  $A \times (B \times C)$  ne sont pas les mêmes ensembles. En effet, les éléments de  $(A \times B) \times C$  sont des couples  $(x, y)$  avec  $x \in A \times B$  et  $y \in C$ , ce qui n'est pas la même chose que  $A \times (B \times C)$  dont les éléments sont des couples  $(x, y)$  avec  $x \in A$  et  $y \in B \times C$ .

**Proposition 2.42** (Distributivité). Si  $A$ ,  $B$  et  $C$  sont trois ensembles, alors

1.  $A \times (B \cup C) = (A \times B) \cup (A \times C)$  ;
2.  $(B \cup C) \times A = (B \times A) \cup (C \times A)$  ;
3.  $A \times (B \cap C) = (A \times B) \cap (A \times C)$  ;
4.  $(B \cap C) \times A = (B \times A) \cap (C \times A)$ .

**Preuve.** Exercice.  $\square$

**Exercice 2.43.** Démontrer la proposition ci-dessus.

**Exercice 2.44.** L'égalité  $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$  est-elle toujours vraie ?

**Remarque 2.45.**

1. «  $\forall x \in A, \forall y \in B$ , » peut s'écrire «  $\forall (x, y) \in A \times B$ , », de même pour  $\exists$ . Si  $A = B$ , on pourra aussi se permettre «  $\forall x, y \in A$  », de même pour  $\exists$ .
2. La déclaration « Soit  $x \in A$ , soit  $y \in B$  » peut aussi s'écrire « Soit  $(x, y) \in A \times B$  ». Si  $A = B$ , on pourra aussi se permettre « Soient  $x, y \in A$  ».
3. C'est compliqué de trouver un analogue logique au produit cartésien. *Grosso modo*, le produit cartésien consiste à travailler avec deux variables indépendantes au lieu d'une. De plus, si  $A \subset E$  et  $B \subset F$ , et si  $A$  et  $B$  sont caractérisés par des propriétés :

$$A = \{x \in E \mid P(x)\} \text{ et } B = \{y \in F \mid Q(y)\},$$

alors on aura

$$A \times B = \{(x, y) \in E \times F \mid P(x) \wedge Q(y)\}.$$

C'est en quelque sorte une conjonction de deux propriétés chacune fonction d'une variable, où les deux variables sont en plus indépendantes.

La notion de couple peut être généralisée, avec plus que deux coordonnées. On parlera alors de triplet  $(a, b, c)$ , ou plus généralement de  $k$ -uplet  $(a_1, \dots, a_k)$ . La règle d'égalité est similaire :

deux  $k$ -uplets  $(a_1, \dots, a_k)$  et  $(a'_1, \dots, a'_k)$  sont égaux s'il y a égalité coordonnée, à savoir  $a_i = a'_i$  pour tout  $1 \leq i \leq k$ .

Si  $A_1, \dots, A_k$  sont des ensembles, on notera

$$A_1 \times \dots \times A_k = \{(a_1, \dots, a_k) \mid \forall 1 \leq i \leq k, a_i \in A_i\}.$$

## 2.2 Un mot sur le paradoxe du barbier et l'axiomatique de Zermelo-Fraenkel

Cette section ne fait pas partie des connaissances exigibles du cours.

Pour la culture, parlons quand même des fondations de la théorie des ensembles. En effet, bien qu'elle paraisse intuitive avec des opérations que l'on peut expliquer avec des dessins (union, intersection, sous-ensembles, etc.), tous les coups ne sont pas permis. Georg Cantor et Bertrand Russell l'avaient très bien compris, ce qui a plongé la communauté mathématique dans une crise des fondements sans précédent.

### 2.2.1 Paradoxe du barbier

Avant de présenter le paradoxe formulé par Cantor, commençons par sa reformulation due à Russell.

#### Paradoxe du barbier.

« Dans une ville, un barbier rase tous les hommes qui ne se rasent pas eux-mêmes. Est-ce que le barbier se rase lui-même ? »

Si le barbier ne se rase pas lui-même, alors le barbier doit le raser, donc il se rase lui-même. Et s'il se rase lui-même, c'est-à-dire si le barbier le rase, alors il ne se rase pas lui-même. Dans les deux cas, on a une contradiction.

Pour proposer une solution à ce paradoxe, il faut en fait se rendre compte qu'on a implicitement commencer le raisonnement avec l'hypothèse selon laquelle le barbier est un homme de la ville concernée. La contradiction qui suit signifie donc que l'hypothèse de départ n'est pas valable. Ainsi le barbier n'habite pas dans la ville, ou n'est pas un homme. C'est exactement ce qu'on appelle le principe d'exclusion, ou de compréhension, et la théorie des ensembles reposent en partie sur ce principe afin d'éviter ce type de paradoxe.

Avec des symboles mathématiques, voici ce qu'avait formulé Cantor.

« Soit  $\Omega$  l'ensemble de tous les ensembles. Posons

$$R = \{x \in \Omega \mid x \notin x\}.$$

L'ensemble  $R$  appartient-il à lui-même ? »

Si  $R \notin R$ , alors en appliquant la définition de  $R$  à la variable muette  $x = R$ , on obtient  $R \in R$ . Et si  $R \in R$ , alors par définition de  $R$ ,  $R \notin R$ . Dans les deux cas, on a une contradiction.

Implicitement, nous avons supposé que  $\Omega$  existait et qu'on pouvait former l'ensemble  $R$ . Donc le paradoxe suggère que l'ensemble de tous les ensembles n'existe pas, ou qu'on ne peut pas former l'ensemble  $R$ . Cet argument, dû à Cantor, s'appelle un « argument diagonal »<sup>2</sup>.

### 2.2.2 Axiomatique de Zermelo-Fraenkel

Avec ces paradoxes, on s'aperçoit que notre approche des ensembles n'est pas rigoureuse et ne repose sur rien de solide. C'est alors qu'apparurent Ernst Zermelo et Abraham Fraenkel. Ils proposèrent les axiomes<sup>3</sup> de la théorie des ensembles, qu'on continue encore d'utiliser aujourd'hui. Dans cette théorie, tout est défini comme un ensemble, même les entiers (nous l'expliquons brièvement ci-dessous), les fonctions, etc. Les éléments d'un ensemble sont des ensembles eux-mêmes. Voici la liste de ces axiomes.

1. Axiome d'extensionnalité : détermine l'égalité entre ensembles. C'est donc sur cet axiome que repose la définition 2.10.
2. Axiome de l'ensemble vide : existence d'un ensemble qui ne contient pas d'élément, appelé l'ensemble vide. En particulier, il existe bien un ensemble (sinon ce serait dommage...). La définition 2.3 de l'ensemble vide repose donc sur cet axiome.
3. Axiome de la paire : si  $A$  et  $B$  sont des ensembles, alors on peut former l'ensemble  $\{A, B\}$  qui n'est composé que des éléments  $A$  et  $B$ . À partir de deux ensembles  $x$  et  $y$  distincts, on peut donc former l'ensemble  $\{x, x\}$ , c'est-à-dire le singleton  $\{x\}$ , ainsi que la paire  $\{x, y\}$ , comme dans la définition 2.3
4. Axiome de l'union : étant donné  $E$  un ensemble, cet axiome assure l'existence de l'union des éléments de  $E$  (l'ensemble dont les éléments sont exactement ceux qui appartiennent à un moins un élément de  $E$ ). Ainsi, étant donnés deux ensembles  $A$  et  $B$ , l'axiome de la paire permet de construire  $E = \{A, B\}$ , puis l'axiome de l'union permet de construire  $A \cup B$ . La définition 2.19 de l'union repose donc sur cet axiome. Il en est de même plus généralement pour la définition 2.27 de l'union quelconque.
5. Axiome des parties : étant donné  $E$  un ensemble, il assure l'existence de l'ensemble  $\mathcal{P}(E)$ , c'est-à-dire qu'on peut former un ensemble dont les éléments sont exactement les sous-ensembles de  $E$ . La définition 2.16 est fondée sur cet axiome.
6. Axiome de compréhension : étant donnés une propriété et  $E$  un ensemble, on peut définir le sous-ensemble des éléments de  $E$  vérifiant cette propriété. Par exemple, si  $A$  est un ensemble, l'ensemble des éléments de  $E$  vérifiant la propriété « appartenir à  $A$  » est un ensemble, il s'agit exactement de  $E \cap A$ .
7. Axiome de l'infini : brièvement, il assure que l'infini a sa place dans cette théorie.
8. Axiome de remplacement : brièvement, étant donné  $E$  un ensemble, si chaque  $x \in E$  est relié à un unique  $y$ , alors on peut former l'ensemble des  $y$  qui sont reliés à un moins un élément de  $E$  (penser à l'image d'une fonction, cf. section 2.3).
9. Axiome de fondation : brièvement, on ne peut pas définir un ensemble qui se contient lui-même. On ne veut pas d'ensemble  $E$  avec une chaîne infinie d'appartenance  $E \ni E \ni E \ni E \ni \dots$

---

2. Pour comprendre pourquoi on parle de « diagonale », il faut imaginer l'expression  $x \notin y$  comme ayant deux variables  $x$  et  $y$ , l'une qu'on représente en abscisse, l'autre en ordonnée. Ici, on regarde seulement les expressions du type  $x \notin x$ , c'est-à-dire qu'on se place sur la diagonale, d'équation  $y = x$ .

3. Les axiomes sont des assertions qu'on suppose vraies, qu'on ne démontre pas. On part de ces axiomes pour former une théorie, c'est-à-dire l'ensemble des propriétés, propositions, théorèmes, qui en découlent. Une mauvaise axiomatique est un ensemble d'axiomes qui aboutit à une contradiction. Toute la difficulté est donc de proposer une axiomatique cohérente.

L'axiome de fondation interdit l'existence d'un ensemble de tous les ensembles. Cela résout donc le paradoxe formulé par Cantor. Par contre, l'axiome de compréhension permet toujours, étant donné un ensemble  $E$ , de considérer  $R = \{x \in E \mid x \notin x\}$ . On obtient donc que  $R$  n'est pas dans  $E$ , puisque si  $R \in E$ , on a la contradiction  $R \in R \iff R \notin R$ . C'est exactement le principe d'exclusion qu'on a illustré avec le paradoxe du barbier (ou bien le barbier est dans une autre ville, ou bien le barbier n'est pas un homme, sinon on a une contradiction).

L'idée de la théorie de ZF est de démarrer avec l'ensemble vide (en utilisant l'axiome de l'ensemble vide) et de considérer tous les ensembles qu'on peut construire à partir de  $\emptyset$  en utilisant les opérations de base (paire, union, compréhension, etc.). On peut ainsi construire  $\{\emptyset\}$  (axiome de la paire ou axiome des parties), puis la paire constituée de  $\emptyset$  et  $\{\emptyset\}$ , etc. On peut en fait construire tous les objets que nous manipulons depuis la primaire. Voici un exemple.

- Considérons  $\emptyset$ ;
- puis  $\emptyset \cup \{\emptyset\}$ , c'est-à-dire  $\{\emptyset\}$ ;
- puis  $\{\emptyset\} \cup \{\{\emptyset\}\}$ ;
- on a compris le schéma, à chaque étape, on a un ensemble  $A$  et on construit le nouvel ensemble  $A \cup \{A\}$ <sup>4</sup> qu'on appelle le successeur de  $A$ .

Puis l'axiome de l'infini nous permet de considérer l'ensemble de ces éléments que nous venons de construire algorithmiquement. Bravo ! L'ensemble  $\mathbb{N}$  a été créé : le premier ensemble  $\emptyset$  est ce qu'on appelle l'entier 1, puis si  $n \in \mathbb{N}$ , son successeur  $n + 1$  est construit comme étant  $n \cup \{n\}$ . Nous n'irons pas plus loin sur la construction de  $\mathbb{N}$ , voire de  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ . Nous définirons ces ensembles à partir d'axiomes, nous ne démontrerons pas qu'ils existent bien (cf. chapitre 3 pour  $\mathbb{N}$  et  $\mathbb{Z}$ , chapitre 6 pour  $\mathbb{R}$ ).

Il est également intéressant de comprendre comment on retrouve le produit cartésien  $A \times B$  tel qu'on se l'« imaginait » dans la définition 2.38.

- Étant donnés  $a \in A$ ,  $b \in B$ , il faut déjà construire le couple  $(a, b)$ . Or l'axiome de la paire nous permet de construire dans un premier temps  $\{a, b\}$ , puis dans un second temps  $\{a, \{a, b\}\}$ . On définit alors  $(a, b) = \{a, \{a, b\}\}$ . Noter que la définition n'est pas symétrique en  $a$  et  $b$ , ainsi  $(a, b) \neq (b, a)$ , sauf si  $a = b$ . De manière générale, avec l'axiome d'extensionnalité, on obtient bien la définition de l'égalité entre deux couples, comme énoncée dans la définition 2.38.
- Si  $a \in A$ , on peut alors former l'ensemble  $B_a = \{(a, b) \mid b \in B\}$ . C'est une conséquence de l'axiome de remplacement : à chaque  $b \in B$ , on associe  $(a, b)$  (qu'on a construit à l'étape précédente).
- Puis en associant à chaque  $a \in A$  l'ensemble  $B_a$ , l'axiome de remplacement permet de construire l'ensemble  $E = \{B_a \mid a \in A\}$ .
- L'axiome de l'union permet alors de définir  $A \times B$  comme l'union des éléments de  $E$ . C'est exactement l'une des unions décrites dans le deuxième point de la remarque 2.40, mais cette fois-ci ce n'est pas une conséquence, c'est la définition même de  $A \times B$ .

### 2.2.3 La vie n'est qu'une question de choix

Il manque un petit quelque chose dans l'axiomatique de Zermelo-Fraenkel que nous utilisons tous les jours sans nous en rendre compte.

Sur un exemple très bref, supposons que  $A$  et  $B$  sont des ensembles non vides et qu'on veut montrer que  $A \times B$  est non vide. Rien de plus simple vu qu'on peut décrire ses éléments : on choisit  $a \in A$ , on choisit  $b \in B$ , et on forme le couple  $(a, b)$ . C'est un élément de  $A \times B$  donc l'ensemble n'est pas vide.

---

4. Pourquoi ce nouvel ensemble n'est pas égal aux autres ?

Mais qu'est-ce qui nous autorise à choisir un élément dans  $A$  puis un élément dans  $B$ ? On ajoute alors l'axiome du choix qui permet de faire cela. Il énonce que si  $E$  est un ensemble, alors on peut associer à tout  $x \in E$  un élément de  $x$ .<sup>5</sup> Dans l'exemple ci-dessus, on applique l'axiome du choix à  $E = \{A, B\}$ .

On parlera donc d'axiomatique de ZFC, C pour « choix ».

## 2.3 Fonctions

Nous allons maintenant définir la notion de fonction. Les fonctions sont des objets que nous manipulons depuis le plus jeune âge. On connaît par exemple les fonctions affines  $x \in \mathbb{R} \mapsto ax + b \in \mathbb{R}$  (étant donnés des réels  $a$  et  $b$ ), la fonction carrée  $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$ , etc. Ici ce sont des exemples où on associe un nombre réel à un autre nombre réel, mais on pourrait très bien considérer d'autres ensembles que  $\mathbb{R}$  et associer leurs éléments entre eux. De manière générale, c'est une machine qui prend en entrée un élément de l'ensemble de départ et renvoie un élément de l'ensemble d'arrivée.

Pour étudier une fonction simple (affine, polynomiale, etc.), on a toujours eu l'habitude de lui associer son graphe, une représentation visuelle nous permettant de comprendre le comportement de la fonction. Dans ce cours, la définition rigoureuse de la notion de fonction repose sur l'approche suivante : c'est d'abord le graphe qui est défini, puis la fonction qui lui est associée.

**Définition 2.46.** Soient  $A$  et  $B$  deux ensembles. Un *graphe* de *domaine*  $A$  et de *codomaine*  $B$  est un sous-ensemble  $G$  de  $A \times B$  vérifiant la propriété suivante :

$$\forall x \in A, \exists! y \in B, (x, y) \in G.$$

**Exemple 2.47.** Considérons  $A = \{1, 2, 3\}$  et  $B = \{s, t\}$ .

1.  $\{(1, s), (2, s), (3, t)\}$  est un graphe de domaine  $A$  et de codomaine  $B$ .
2.  $\{(1, t), (3, t)\}$  n'est pas un graphe de domaine  $A$  et de codomaine  $B$ . En effet, il n'y a pas de couple dont la coordonnée en  $A$  vaut 2. Par contre, c'est un graphe de domaine  $A - \{2\}$  et de codomaine  $B$ .
3.  $\{(1, t), (2, s), (3, u)\}$  n'est pas un graphe de domaine  $A$  et de codomaine  $B$  (sauf si  $u$  vaut  $s$  ou  $t$ ). Par contre, c'est un graphe de domaine  $A$  et de codomaine  $B \cup \{u\}$ .
4.  $\{(1, s), (2, s), (3, t), (1, t)\}$  n'est pas un graphe de domaine  $A$  et de codomaine  $B$ . En effet, il y a deux couples distincts dont la coordonnée en  $A$  vaut 1.

**Définition 2.48.** Soient  $A$  et  $B$  deux ensembles. Une *fonction*  $f$ , ou *application*, de  $A$  dans  $B$  est un triplet  $(A, B, G)$  où  $G$  est un graphe de domaine  $A$  et de codomaine  $B$ . On pourra noter  $f: A \rightarrow B$ .

Pour tout  $x \in A$ , on notera  $f(x)$  l'unique  $y \in B$  tel que  $(x, y) \in G$ , et on pourra écrire plus explicitement

$$f: \begin{array}{ccc} A & \rightarrow & B \\ x & \mapsto & f(x) \end{array} \quad \text{ou} \quad f: x \in A \mapsto f(x) \in B.$$

5. N'oublions pas que les éléments de  $E$  sont des ensembles. En théorie des ensembles, tout est construit et défini comme un ensemble!

L'ensemble des fonctions de  $A$  dans  $B$  est noté  $\mathcal{F}(A, B)$ .

**Exemple 2.49.**

1. Si  $A$  est un ensemble, on définit la fonction *identité*  $x \in A \mapsto x \in A$ . Par définition, c'est la fonction de domaine et codomaine  $A$ , et de graphe  $\{(x, x) \mid x \in A\}$ . L'identité sur  $A$  est noté  $\text{id}_A$ .
2. La fonction carrée de  $\mathbb{R}$  dans  $\mathbb{R}$  est définie par le triplet  $(\mathbb{R}, \mathbb{R}, G)$ , avec

$$G = \{(x, x^2) \mid x \in \mathbb{R}\}.$$

3. Soient  $A$  et  $B$  deux ensembles et  $a_0 \in A$ . On définit la fonction d'évaluation  $\Phi: f \in \mathcal{F}(A, B) \mapsto f(a_0) \in B$ . Formellement, il s'agit du triplet  $(\mathcal{F}(A, B), B, G)$  où  $G$  est le graphe de domaine  $\mathcal{F}(A, B)$  et de codomaine  $B$  défini par

$$G = \{(f, f(a_0)) \mid f \in \mathcal{F}(A, B)\}.$$

Il faut s'assurer que la fonction est bien définie, c'est-à-dire que  $\Phi(f)$  est un élément de  $B$  pour tout  $f \in \mathcal{F}(A, B)$  (autrement dit, que  $G$  est un sous-ensemble de  $\mathcal{F}(A, B) \times B$ ). Or  $\Phi(f) = f(a_0)$  avec  $f: A \rightarrow B$  une fonction et  $a_0 \in A$ , donc  $f(a_0) \in B$ .

**Remarque 2.50.** Si  $A$  est vide, alors  $A \times B$  est vide donc le seul graphe de domaine  $A$  et de codomaine  $B$  est l'ensemble vide. La fonction  $(\emptyset, B, \emptyset)$  est appelée la *fonction vide*.

Question : Pourquoi n'existe-t-il pas de fonction  $A \rightarrow \emptyset$  si  $A$  est non vide ? (Indication : examiner la définition d'un graphe)

**Proposition 2.51.** Soient  $A, B, C$  et  $D$  des ensembles. Soient  $f: A \rightarrow B$  et  $g: C \rightarrow D$  des fonctions. Alors  $f = g$  si et seulement si  $A = C$ ,  $B = D$  et pour tout  $x \in A$ ,  $f(x) = g(x)$ .

**Preuve.** Par définition,  $f$  et  $g$  sont respectivement des couples  $(A, B, G)$  et  $(C, D, G')$  où  $G$  et  $G'$  sont respectivement des graphes de domaine  $A$  et  $C$ , et de codomaine  $B$  et  $D$ . L'égalité entre  $f$  et  $g$  est donc équivalente à  $(A, B, G) = (C, D, G')$ , c'est-à-dire à

$$A = C \text{ et } B = D \text{ et } G = G'.$$

Or sous la condition «  $A = C$  », on a

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

et

$$G' = \{(x, g(x)) \mid x \in A\},$$

donc  $G = G'$  équivaut à «  $\forall x \in A, f(x) = g(x)$  ».

□

**Exemple 2.52.**

1. Les fonctions  $f: x \in \mathbb{R} \rightarrow x^2 \in \mathbb{R}$  et  $g: x \in \mathbb{R} \rightarrow x^2 \in \mathbb{R}_{\geq 0}$  sont bien définies sur le même ensemble  $\mathbb{R}$ , elles vérifient  $f(x) = g(x)$  pour tout  $x \in \mathbb{R}$ . Cependant  $f$  et  $g$  ne sont pas égales : le codomaine n'est pas le même ( $\mathbb{R}$  pour  $f$ ,  $\mathbb{R}_{\geq 0}$  pour  $g$ ).
2. Dans le même esprit que l'exemple précédent, si  $A$  et  $B$  sont deux ensembles tels que  $A \subset B$ , alors les fonctions  $\text{id}_A$  et  $x \in A \mapsto x \in B$  sont égales seulement si  $A = B$ .

**Remarque 2.53.** On parle souvent de fonctions à deux arguments, c'est-à-dire qu'on peut l'évaluer en deux variables  $x \in A$  et  $y \in B$  pour obtenir  $f(x, y)$ . Avec notre formalisme, il s'agit tout simplement d'une fonction définie sur  $A \times B$ , les deux arguments  $x$  et  $y$  ne sont en fait qu'un seul argument  $(x, y)$ . Pour faire simple, on pourra écrire  $f(x, y)$  au lieu de  $f((x, y))$ .

Le propos se généralise pour une fonction de plus de deux variables, à condition de définir le produit cartésien de plus de deux ensembles, qui existe mais dont on ne parlera pas dans ce cours.

**Définition 2.54.** Soient  $A$  et  $B$  deux ensembles et  $f: A \rightarrow B$  une fonction de  $A$  dans  $B$ .

- Étant donnés  $x \in A$  et  $y \in B$ , si  $f(x) = y$ , alors on dit que  $y$  est l'*image* de  $x$  par  $f$ , et que  $x$  est **un** *antécédent* de  $y$  par  $f$ .
- Si  $C$  est un sous-ensemble de  $A$ , l'*image* de  $C$  par  $f$  est le sous-ensemble de  $B$  défini par

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

**Attention** à bien faire la différence entre  $f(x)$  (élément de  $B$ ) et  $f(C)$  (sous-ensemble de  $B$ ) lorsque  $x \in A$  et  $C \subset A$ .

- L'*image* de  $f$ , notée  $\text{im}f$ , est le sous-ensemble de  $B$  défini par

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

- Si  $C$  est un sous-ensemble de  $B$ , alors sa *préimage*, ou *image réciproque*, est le sous-ensemble de  $A$  défini par

$$f^{-1}(C) = \{x \in A \mid f(x) \in C\}.$$

Si  $C$  est un singleton  $\{y\}$ , on pourra noter  $f^{-1}(y)$  au lieu de  $f^{-1}(\{y\})$ .

Concernant le premier point, on ne parle pas « d'une image » de  $x$ , mais bien de « l'image ». Il y a unicité de l'image par définition d'un graphe. En revanche, il peut y avoir plusieurs antécédents pour  $y$ , on ne dit pas que  $x$  est « l'antécédent » de  $y$  (sauf si on sait déjà qu'il est unique).

Intuitivement, si  $C \subset A$ ,  $f(C)$  est l'ensemble des points de  $B$  qu'on peut attraper à partir de  $C$ , et  $\text{im}f$  est l'ensemble des points qu'on peut attraper en toute généralité. Remarquons que dans le cas  $C = \{x\}$  avec  $x \in A$ , on a  $f(\{x\}) = \{f(x)\}$ .

Si  $C \subset B$ ,  $f^{-1}(C)$  est l'ensemble des points de  $A$  à partir desquels on peut obtenir un élément de  $C$ . Par définition,  $f^{-1}(C) = \emptyset$  dès que  $C \subset B - \text{im}f$ , et  $f^{-1}(y) = \emptyset$  dès que  $y \in B - \text{im}f$ .

**Exemple 2.55.**

1. Considérons  $f: x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$ .  
 $f([0, 4]) = f([-4, 4]) = [0, 16]$ .  
 $f^{-1}([25, 36]) = [-6, -5] \cup [5, 6]$ .
2. Considérons  $f: x \in \mathbb{R} \mapsto \sin x \in [-1, 1]$ .  
 $f^{-1}([0, 1]) = \bigcup_{k \in \mathbb{Z}} [2k\pi, (2k+1)\pi]$ .

**Exercice 2.56.** Soit  $f: A \rightarrow B$  une fonction. Soient  $X$  un ensemble de sous-ensembles de  $A$ , et  $Y$  un ensemble de sous-ensembles de  $B$

1. Comparer  $f(\bigcup_{E \in X} E)$  et  $\bigcup_{E \in X} f(E)$ .
2. Comparer  $f(\bigcap_{E \in X} E)$  et  $\bigcap_{E \in X} f(E)$ .
3. Comparer  $f^{-1}(\bigcup_{E \in Y} E)$  et  $\bigcup_{E \in Y} f^{-1}(E)$ .
4. Comparer  $f^{-1}(\bigcap_{E \in Y} E)$  et  $\bigcap_{E \in Y} f^{-1}(E)$ .

« Comparer » signifie « Déterminer si chacune des inclusions  $\subset$  et  $\supset$  a toujours lieu, ou trouver un contre-exemple ».

**Définition 2.57.** Soit  $f: A \rightarrow B$  une fonction.

- Pour  $E \subset A$ , la *restriction* de  $f$  à  $E$  est la fonction

$$f|_E: x \in E \mapsto f(x) \in B.$$

- Pour  $F \subset B$  tel que  $\text{im} f \subset F$ , la *corestriction* de  $f$  à  $F$  est la fonction

$$f|_F: x \in A \mapsto f(x) \in F.$$

On parle de *corestriction* d'une fonction à *son image* lorsqu'on considère  $F = \text{im} f$ .

- Dès que  $E \subset A$  et  $f(E) \subset F \subset B$ , on peut à la fois restreindre à  $E$  et corestreindre à  $F$  :

$$f|_E^F: x \in E \mapsto f(x) \in F.$$

**Attention.** Même si elles désignent les mêmes règles d'association, les fonctions  $f$  et  $f|_F$  ne sont pas égales, puisqu'elles n'ont pas le même ensemble d'arrivée (sauf si  $F = B$ ). De même,  $f$  et  $f|_E$  ne sont pas égales (sauf si  $E = A$ ). Noter que les conditions figurant à chaque point, à savoir «  $E \subset A$  », «  $\text{im} f \subset F \subset B$  » et «  $E \subset A$  et  $f(E) \subset F \subset B$  », sont indispensables pour la bonne définition des nouvelles fonctions construites à partir de  $f$ .

**Définition 2.58.** Soient  $A$  et  $B$  deux ensembles et  $f: A \rightarrow B$  une fonction de  $A$  dans  $B$ .

- On dit que  $f$  est *injective* si

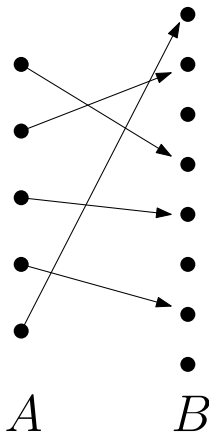
$$\forall (x, y) \in A^2, f(x) = f(y) \Rightarrow x = y.$$

- $f$  est dite *surjective* si

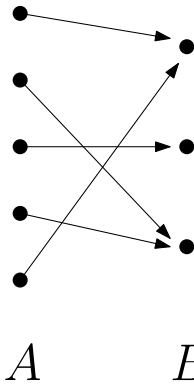
$$\forall y \in B, \exists x \in A, f(x) = y,$$

autrement dit si  $\text{im} f = B$ .

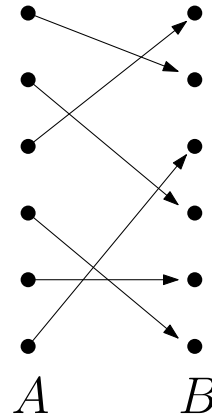
- $f$  est *bijjective* si elle est injective et surjective.



Injective, non surjective



Surjective, non injective



Bijjective

L'injectivité dit que lorsque  $y \in \text{im}f$ ,  $f^{-1}(y)$  est un singleton (il n'y a qu'un point de  $A$  qui permet d'obtenir  $y$ ). L'existence d'une injection de  $A$  vers  $B$  signifie intuitivement qu'il y a plus d'éléments dans  $B$  que dans  $A$ , et donc  $B$  est « plus grand » que  $A$ .

La surjectivité de  $f$  signifie qu'à partir de  $A$ , on peut obtenir tout l'ensemble  $B$ . Intuitivement, l'existence d'une surjection de  $A$  vers  $B$  signifie qu'il y a assez d'éléments dans  $A$  pour décrire tous les éléments de  $B$ , et donc  $A$  est « plus grand » que  $B$ .

Une bijection de  $A$  vers  $B$  est une correspondance exacte entre les éléments de  $A$  et les éléments de  $B$ . Intuitivement, les ensembles ont la même taille.

### Remarque 2.59.

1. Si  $A$  est un singleton, alors toute fonction  $A \rightarrow B$  est injective. Si  $B$  est un singleton, alors toute fonction  $A \rightarrow B$  est surjective.
2. Pour toute fonction  $f: A \rightarrow B$ ,  $f|_{\text{im}f}: A \rightarrow \text{im}f$  est surjective.
3. Toute restriction d'une fonction injective est injective. Toute corestriction d'une fonction injective est injective. Si  $f: A \rightarrow B$  est injective, alors  $f|_{\text{im}f}: A \rightarrow \text{im}f$  est bijective.
4. La fonction vide  $\emptyset \rightarrow B$  est injective. En effet, il n'existe pas d'éléments  $x, y$  dans  $A$ , donc encore moins d'éléments  $x, y$  dans  $A$  vérifiant  $f(x) = f(y)$  et  $x \neq y$ .

### Exemple 2.60.

1. Considérons  $f: x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$ .  
 $f$  n'est pas injective car  $f(-1) = f(1)$ . Elle n'est pas non plus surjective car aucun réel négatif ne peut s'écrire comme  $f(x)$  pour un certain  $x \in \mathbb{R}$  ( $\text{im}f = \mathbb{R}_{\geq 0} \neq \mathbb{R}$ ).  
 Par exemple, si on n'avait plutôt considéré  $\mathbb{R}_{\geq 0}$  comme ensemble de départ, alors  $f$  aurait été injective. Avec domaine  $\mathbb{R}$ , il aurait fallu que le codomaine soit  $\mathbb{R}_{\geq 0}$  pour que  $f$  soit surjective.
2.  $f: x \in \mathbb{R} \mapsto \sin x \in \mathbb{R}$  n'est pas surjective, mais  $g: x \in \mathbb{R} \mapsto \sin x \in [-1, 1]$  l'est.
3.  $f: x \in \mathbb{R} \mapsto \sin x \in \mathbb{R}$  n'est pas injective, mais  $g: x \in [-\pi/2, \pi/2] \mapsto \sin x \in \mathbb{R}$  l'est.
4. Si  $A$  est un ensemble, alors  $\text{id}_A$  est une bijection de  $A$  vers  $A$ . Démontrons-le. Commençons par l'injectivité. Soit  $x, y \in A$  tels que  $\text{id}_A(x) = \text{id}_A(y)$ . Vu que  $\text{id}_A(x) = x$

et  $\text{id}_A(y) = y$ , cela donne  $x = y$ . D'où l'injectivité. Montrons ensuite la surjectivité. Soit  $y \in A$ . Alors on peut écrire  $y = \text{id}_A(y)$  donc  $y$  est dans l'image de  $\text{id}_A$ , d'où la surjectivité. Donc l'application identité est une bijection.

5. Soient  $A$  et  $B$  deux ensembles et  $a_0 \in A$ . La fonction d'évaluation  $\Phi: f \in \mathcal{F}(A, B) \mapsto f(a_0) \in B$  est surjective. En effet, si  $b \in B$ , on peut trouver facilement une fonction  $f: A \rightarrow B$  telle que  $\Phi(f) = b$ , par exemple la fonction constante égale à  $b$ , c'est-à-dire  $f: x \in A \mapsto b \in B$ .

**Exercice 2.61.** Soit  $f: (x, y) \in \mathbb{R}^2 \mapsto x - y \in \mathbb{R}$ . La fonction est-elle injective ? surjective ? Soit  $z \in \mathbb{R}$ , tracer dans le plan l'ensemble  $f^{-1}(z)$ . Calculer les ensembles  $f(\mathbb{R} \times \{y\})$ , pour  $y \in \mathbb{R}$ .

**Exercice 2.62.** Soit  $f: (x, y) \in \mathbb{R}^2 \mapsto x^2 + y^2 \in \mathbb{R}$ . La fonction est-elle injective ? surjective ? Que dire des ensembles  $f^{-1}(z)$  lorsque  $z > 0$  ?  $z = 0$  ?  $z < 0$  ? Calculer les ensembles  $f(\mathbb{R} \times \{y\})$ , pour  $y \in \mathbb{R}$ .

**Exercice 2.63.** Déterminer si les fonctions suivantes sont injectives, surjectives, bijectives (on considérera à chaque fois  $\mathbb{N}$  comme ensemble d'arrivée). Dans le cas où la fonction est bijective, expliciter la réciproque.

1.  $f: n \in \mathbb{N} \mapsto \begin{cases} n^2 + 1 & \text{si } n \text{ est pair,} \\ n + 3 & \text{si } n \text{ est impair.} \end{cases}$
2.  $g: n \in \mathbb{N} \mapsto \begin{cases} n + 2 & \text{si } n \text{ est pair} \\ 2 & \text{si } n = 1, \\ n - 2 & \text{si } n \text{ est impair et } n \geq 3. \end{cases}$

**Remarque 2.64.** Soit  $A$  et  $B$  des ensembles. Pour tout  $b \in B$ , on disait dans la remarque 2.40 que  $A \times \{b\}$  est une copie de  $A$ . Mathématiquement, on voulait dire qu'il existe une bijection de  $A$  vers  $A \times \{b\}$ . On peut par exemple considérer

$$\begin{aligned} f: A &\rightarrow A \times \{b\} \\ x &\mapsto (x, b) \end{aligned},$$

c'est une bijection. Montrons d'abord l'injectivité. Soient  $a, a' \in A$  tels que  $f(a) = f(a')$ . Alors  $(a, b) = (a', b)$ , donc  $a = a'$ . D'où l'injectivité. Pour la surjectivité, considérons  $y \in A \times \{b\}$ . On dispose de  $a \in A$  tel que  $y = (a, b)$  donc  $y = f(a)$ . D'où la surjectivité.

**Exercice 2.65.** Soit  $f: A \rightarrow B$  une fonction. On définit une nouvelle fonction

$$\begin{aligned} \bar{f}: \mathcal{P}(A) &\rightarrow \mathcal{P}(B) \\ C &\mapsto f(C) \end{aligned}.$$

Montrer que

1.  $f$  est injective si et seulement si  $\bar{f}$  est injective ;
2.  $f$  est surjective si et seulement si  $\bar{f}$  est surjective ;
3.  $f$  est bijective si et seulement si  $\bar{f}$  est bijective.

**Exercice 2.66.** Soient  $A, A', B, B'$  des ensembles. On suppose qu'il existe des injections (resp. surjections, resp. bijections) de  $A$  dans  $A'$  et de  $B$  dans  $B'$ . Montrer qu'il existe une injection (resp. surjection, resp. bijection) de  $A \times B$  dans  $A' \times B'$ .

**Exercice 2.67.** Soit  $f: A \rightarrow B$  une fonction.

1. Si  $Y$  est une partition de  $B$ , est-ce que l'ensemble  $\{f^{-1}(F) \mid F \in Y\}$  est une partition de  $A$  ?
2. Si  $X$  est une partition de  $A$ , à quelle condition l'ensemble  $\{f(E) \mid E \in X\}$  est-il une partition de  $B$  ?

**Définition 2.68** (Composition de deux fonctions). Soient  $f: A \rightarrow B$  et  $g: C \rightarrow D$  deux applications. On suppose  $\text{im} f \subset C$ . On définit alors l'application  $g \circ f: A \rightarrow D$  par :

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

**Attention.** La composition n'est pas bien définie si  $\text{im} f \not\subset C$ . En effet, s'il existe  $y \in (\text{im} f) - C$  et si  $x$  est un élément de  $A$  tel que  $y = f(x)$  ( $x$  existe par définition de  $y$ ), alors  $(g \circ f)(x)$  n'est pas bien défini (cela vaudrait  $g(f(x)) = g(y)$ , or  $y$  n'est pas dans le domaine de  $g$ ). Par exemple, si  $g: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$  est la fonction racine carrée, et  $f: x \in \mathbb{R} \rightarrow -x^2 \in \mathbb{R}$ , alors  $g \circ f$  n'est pas bien défini (la racine carrée d'un nombre négatif n'est pas bien définie).

**Proposition 2.69.** Soient  $f: A \rightarrow B$  et  $g: C \rightarrow D$  deux applications. On suppose  $\text{im} f \subset C$ .

1. Si  $E$  est un sous-ensemble de  $A$ , alors  $(g \circ f)(E) = g(f(E))$ .
2.  $\text{im}(g \circ f) = g(\text{im} f)$ .
3. Si  $F$  est un sous-ensemble de  $D$ , alors  $(g \circ f)^{-1}(F) = f^{-1}(g^{-1}(F))$ .
4. Si  $f$  et  $g$  sont injectives, alors  $g \circ f$  est injective.
5. Si  $f$  et  $g$  sont surjectives et  $B = C$ , alors  $g \circ f$  est surjective.
6. Si  $f$  et  $g$  sont bijectives et  $\text{im} f = C$ , alors  $g \circ f$  est bijective.

**Preuve.**

1. Soit  $E \subset A$ . Soit  $y \in (g \circ f)(E)$ . Alors il existe  $x \in E$  tel que  $y = (g \circ f)(x)$ , c'est-à-dire  $y = g(f(x))$ . Or  $f(x) \in f(E)$ , donc  $g(f(x)) \in g(f(E))$ , donc  $y \in g(f(E))$ . Réciproquement, soit  $y \in g(f(E))$ . Il existe  $z \in f(E)$  tel que  $y = g(z)$ . Il existe  $x \in E$  tel que  $z = f(x)$ , donc  $y = g(f(x))$ , c'est-à-dire  $y = (g \circ f)(x)$ . Vu que  $x$  est dans  $E$ , on obtient  $y \in (g \circ f)(E)$ . D'où l'égalité  $(g \circ f)(E) = g(f(E))$ .
2. Appliquer l'égalité qu'on vient de démontrer à  $C = E$ .
3. Preuve de  $(g \circ f)^{-1}(F) = f^{-1}(g^{-1}(F))$  : exercice.
4. Supposons que  $f$  et  $g$  sont injectives. Considérons  $x, y \in A$  tels que  $(g \circ f)(x) = (g \circ f)(y)$ , montrons  $x = y$ . On a  $g(f(x)) = g(f(y))$ , donc l'injectivité de  $g$  entraîne  $f(x) = f(y)$ , puis l'injectivité de  $f$  entraîne  $x = y$ . D'où l'injectivité.
5. Si  $f$  et  $g$  sont surjectives et  $B = C$ , alors  $g \circ f$  est surjective : exercice.
6. Supposons  $f$  et  $g$  bijectives et  $B = C$ . En particulier,  $f$  et  $g$  sont injectives donc  $g \circ f$  est injective. Mais également  $f$  et  $g$  sont surjectives et  $B = C$ , donc  $g \circ f$  est

surjective. D'où la bijectivité de  $g \circ f$ . □

**Exercice 2.70.** Démontrer ce qui a été laissé en exercice dans la preuve ci-dessus.

**Exercice 2.71.** Soit  $f: A \rightarrow B$  une application.

1. Montrer que  $f$  est injective si et seulement s'il existe  $g: B \rightarrow A$  tel que  $g \circ f = \text{id}_A$ , et que dans ce cas,  $g$  est une surjection.
2. Montrer que  $f$  est surjective si et seulement s'il existe  $g: B \rightarrow A$  tel que  $f \circ g = \text{id}_B$ , et que dans ce cas,  $g$  est une injection.
3. Montrer que  $f$  est bijective si et seulement s'il existe  $g: B \rightarrow A$  tel que  $g \circ f = \text{id}_A$  et  $f \circ g = \text{id}_B$ , et que dans ce cas,  $g$  est une bijection.

L'exercice ci-dessus nous dit en fait que l'existence d'une injection  $A \rightarrow B$  est équivalente à l'existence d'une surjection  $B \rightarrow A$ , ce qui confirme l'intuition que  $A$  est un ensemble plus petit que  $B$ , puisqu'il y a assez de place dans  $B$  pour que  $A$  soit « injecté » dedans, ou puisqu'il y a assez de monde dans  $B$  pour « recouvrir »  $A$ .

**Théorème 2.72.** Soit  $f: A \rightarrow B$  une application de  $A$  vers  $B$ . Alors  $f$  est une bijection si et seulement s'il existe  $g: B \rightarrow A$  vérifiant :  $\forall (x, y) \in A \times B, f(x) = y \iff g(y) = x$ .

Si c'est le cas, alors  $g$  est unique et bijective. On l'appelle la réciproque de  $f$ , on la note  $f^{-1}: B \rightarrow A$ . On a les égalités  $f^{-1} \circ f = \text{id}_A$  et  $f \circ f^{-1} = \text{id}_B$ .

En conséquence, l'existence d'une bijection  $A \rightarrow B$  est équivalente à l'existence d'une bijection  $B \rightarrow A$ .

**Attention.** À ne pas confondre avec les notations  $f^{-1}(C)$  et  $f^{-1}(y)$  de la définition 2.54. Elles sont valables même quand  $f$  n'est pas bijective mais ne permettent pas de définir une application  $f^{-1}: B \rightarrow A$ .

Dans le cas d'une bijection  $f$ , la réciproque est une véritable application  $B \rightarrow A$ .

**Preuve.** Supposons que  $f: A \rightarrow B$  est bijective. Construisons  $g: B \rightarrow A$ . Pour tout  $y \in B$ , la surjectivité de  $f$  nous dit qu'il existe  $x \in A$  tel que  $y = f(x)$ , et l'injectivité nous dit qu'un tel  $x$  est unique, on le note donc  $g(y)$ . On pose donc  $g: y \in B \rightarrow g(y) \in A$ . Avec cette définition, on vérifie immédiatement l'assertion  $\forall (x, y) \in A \times B, f(x) = y \iff g(y) = x$ .

Pour la réciproque, supposons qu'une telle fonction  $g$  existe et montrons que  $f$  est bijective. Commençons par l'injectivité. Soient  $x, x' \in A$  tels que  $f(x) = f(x')$  (on note  $y$  la valeur commune) et montrons que  $x = x'$ . L'égalité  $y = f(x)$  donc  $x = g(y)$ , puis  $y = f(x')$  donne  $x' = g(y)$ . D'où  $x = x'$  et l'injectivité. Pour la surjectivité, remarquons que si  $y$  est un élément de  $B$ , et si  $x$  désigne  $g(y)$ , alors  $y = f(x)$ . D'où la surjectivité.

Nous avons donc démontré l'équivalence.

Supposons maintenant que  $f$  est bijective, et donc qu'une telle fonction  $g$  existe, et montrons l'unicité d'une telle fonction. Soit  $g, h: B \rightarrow A$  vérifiant la propriété en question. Soit  $y \in B$  et montrons que  $g(y) = h(y)$ . Soient  $x \in A$  l'unique élément vérifiant  $f(x) = y$ . Alors par la propriété vérifiée par  $g$ , l'égalité  $f(x) = y$  implique  $g(y) = x$ . Puis, par la propriété vérifiée par  $h$ , l'égalité  $f(x) = y$  implique  $h(y) = x$ . D'où  $g(y) = h(y)$ . Ceci est valable pour tout  $y \in B$  donc  $g = h$ .

Pour justifier que  $g$  est bijective, il suffit de remarquer que  $f$  est sa réciproque (l'assertion  $\forall (x, y) \in A \times B, f(x) = y \iff g(y) = x$  est symétrique en  $f$  et  $g$ ). Ainsi l'équivalence démontrée dans cette preuve nous permet d'affirmer que  $g$  est bijective.

Enfin, les égalités  $g \circ f = \text{id}_A$  et  $f \circ g = \text{id}_B$  se déduisent directement de la propriété «  $\forall (x, y) \in A \times B, f(x) = y \iff g(y) = x$  ».  $\square$

### Exemple 2.73.

1.  $f: x \in \mathbb{R} \rightarrow 2x \in \mathbb{R}$  est une bijection. En effet, si  $(x, y) \in \mathbb{R}^2$  vérifie  $y = 2x$ , alors  $x = y/2$ , et réciproquement. On vient de montrer que la fonction  $g: y \in \mathbb{R} \mapsto y/2 \in \mathbb{R}$  est la réciproque de  $f$ . Ainsi  $f$  est bijective.
2. Soient  $A$  et  $B$  des ensembles,  $b \in B$ . Pour montrer que  $f: A \rightarrow A \times \{b\}$  est une bijection, il suffit d'explicitier sa réciproque :

$$\begin{aligned} g: A \times \{b\} &\rightarrow A \\ x &\mapsto a \text{ tel que } x = (a, b) \end{aligned}$$

Les fonctions bijectives permettent de dire si deux ensembles sont les mêmes ou non à changement de point de vue près (le changement de point de vue est incarné par la fonction elle-même). Lorsqu'on veut étudier un ensemble compliqué, noté  $A$ , on lui cherche un ensemble qu'on comprend bien, noté  $B$ , avec lequel il est en bijection, et la fonction bijective donne elle-même une description de  $A$ , en encodant ses éléments à partir des éléments de l'ensemble  $B$ . Vu qu'on comprend bien l'ensemble  $B$ , on visualise beaucoup mieux l'ensemble  $A$ . Les exercices suivants donnent des exemples d'ensembles connus qui sont en bijection.

**Exercice 2.74.** Soit  $A$  un ensemble. Montrer que  $\mathcal{P}(A)$  et  $\mathcal{F}(A, \{0, 1\})$  sont en bijection.

Indication : Pour  $C \in \mathcal{P}(A)$  fixé, associer à tout élément  $x$  de  $A$  la valeur 1 si  $x \in C$ , 0 si  $x \in A - C$ .

**Exercice 2.75.** Soient  $A, B$  et  $C$  trois ensembles. Trouver une bijection de  $\mathcal{F}(A \times B, C)$  vers  $\mathcal{F}(A, \mathcal{F}(B, C))$ .

Indication : Étant donnée une fonction  $f(., .): A \times B \rightarrow C$  à deux variables, que dire si on gèle une coordonnée, c'est-à-dire que dire de l'objet  $f(a, .)$ , pour  $a \in A$  ?

C'est ce qu'on appelle la *curryfication*, très utilisée dans certains langages de programmation.

L'exercice suivant montre qu'étant donné  $A$ , il existe toujours un ensemble  $B$  qui est plus grand que  $A$ . Il est dû à Cantor et l'indication que nous proposons consiste à suivre sa preuve originale qui est un argument diagonal (comme dans le paradoxe qu'il a formulé, cf. section 2.2.1).

**Exercice 2.76.** Soit  $A$  un ensemble. Montrer qu'il n'existe pas de surjection de  $A$  dans  $\mathcal{P}(A)$ .

Indication : Par l'absurde, supposons qu'il existe une fonction  $f: A \rightarrow \mathcal{P}(A)$  surjective. Considérons  $C = \{x \in A \mid x \notin f(x)\}$ . Choisir judicieusement (en utilisant ce qu'on sait sur  $f$ ) un élément  $x_0$  de  $A$  pour lequel les assertions «  $x_0 \in C$  » et «  $x_0 \notin C$  » aboutissent à une contradiction.

Ainsi, partant de  $A$ , on obtient une suite  $A, \mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \mathcal{P}(\mathcal{P}(\mathcal{P}(A))), \dots$  d'ensembles de plus en plus grands.

Pour la culture, si on considère  $A = \mathbb{N}$ , alors on peut montrer que  $\mathcal{P}(\mathbb{N})$  est en bijection avec  $\mathbb{R}$  (cf. problème 2.5.4). Ainsi  $\mathbb{N}$  et  $\mathbb{R}$  ne sont pas en bijection (on le démontre également dans le problème 2.5.3). Comme  $n \in \mathbb{N} \mapsto n \in \mathbb{R}$  est une injection, on sait que  $\mathbb{N}$  est un ensemble « de plus petite taille » que  $\mathbb{R}$ .

## 2.4 Relation d'équivalence

**Motivation :** Si dans mon tiroir, j'ai des chaussettes unicolores et que je veux connaître toutes les couleurs dont je dispose, inutile de regarder les chaussettes individuellement. Je les classe par couleur et l'information qui m'intéresse sera l'ensemble de ces classes.

Une relation d'équivalence  $\sim$  sur un ensemble  $A$  consiste à classer ses éléments, de sorte à ensuite regarder l'ensemble des classes, noté  $A/\sim$ . On ne regarde plus individuellement les éléments (dans  $A$ ), mais leur classe (dans  $A/\sim$ ). On fait donc en sorte de ne plus pouvoir distinguer deux éléments d'une même classe.

On perd certes de l'information en faisant cela, mais parce qu'il y en avait plus que ce qui était nécessaire, on ne garde que l'information intéressante. Par exemple, dans  $\mathbb{Z}$ , nous ferons du calcul en ne considérant seulement le reste de la division par  $n$ , cette information est suffisante pour répondre à certaines questions d'arithmétique (cf. section 5.2 du chapitre 5).

Ne plus pouvoir distinguer des éléments entre eux en les classant permet aussi d'effacer des propriétés indésirables. Prenons l'exemple d'une fonction  $f: A \rightarrow B$  qui n'est pas injective. Cela signifie qu'il existe des éléments distincts  $x, y \in A$  tels que  $f(x) = f(y)$ . En classant les éléments de  $A$  selon leur image par  $f$ , on fait en sorte de ne plus distinguer les points qui ont la même image, et on « rend »  $f$  injective. Concrètement,  $f$  reste toujours la même fonction et ne devient pas injective à la fin, mais on construit naturellement une fonction injective  $(A/\sim) \rightarrow B$  à partir de  $f$ .

**Définition 2.77.** Une relation  $\mathcal{R}$  sur un ensemble  $A$  est un sous-ensemble de  $A \times A$ . Si  $(x, y) \in \mathcal{R}$  est dans ce sous-ensemble, alors on dit que  $x$  est *relié* à  $y$ , et on notera plutôt  $x\mathcal{R}y$ .

**Notations.** On utilise souvent d'autres symboles que  $\mathcal{R}$  pour désigner une relation, par exemple  $\sim, \equiv, \leq, \preceq$ , etc.

### Exemple 2.78.

1. La relation d'égalité entre éléments dans un ensemble  $A$ . Le graphe associé est  $\{(x, x) \mid x \in A\}$ .
2. Dans  $\mathcal{P}(A)$ , la relation  $\mathcal{R}$  définie par : pour tout  $B, C \in \mathcal{P}(A)$ ,  $B\mathcal{R}C$  si et seulement s'il existe une injection (resp. surjection, resp. bijection) de  $B$  dans  $C$ .
3. Dans  $\mathcal{P}(A)$ , la relation  $\mathcal{R}$  défini par : pour tout  $B, C \in \mathcal{P}(A)$ ,  $B\mathcal{R}C$  si et seulement si  $B \cap C$  est non vide.
4. La relation « être inclus dans » dans  $\mathcal{P}(A)$ , noté  $\subset$ .
5. La relation « plus petit que » dans  $\mathbb{R}$ , notée  $<$ , et la relation « plus petit ou égal à » dans  $\mathbb{R}$ , notée  $\leq$ .
6. Étant donnée une fonction  $f: A \rightarrow B$ , on peut définir une relation  $\mathcal{R}$  par : pour tout  $x, y \in A$ ,  $x\mathcal{R}y$  si et seulement si  $f(x) = f(y)$ .
7. La relation  $\equiv$  dans  $\mathbb{Z}$ , définie par : pour tout  $x, y \in \mathbb{Z}$ ,  $x \equiv y$  si et seulement si  $x - y$  est pair (relation très étudiée dans la section 5.2 du chapitre 5).

Étant donnée une relation sur  $A$ , on veut maintenant regrouper les éléments de  $A$  qui sont reliés entre eux. Mais le découpage en classe impose des conditions bien strictes sur la relation, notamment pour que les classes satisfassent ces propriétés absolument naturelles :

- tout élément  $x \in A$  doit être dans la même classe que lui-même ;
- si  $x$  est dans la même classe qu'un autre élément  $y$ , alors  $y$  doit être dans la même classe que  $x$  ;
- si  $x$  et  $y$  sont dans la même classe, et si  $y$  et  $z$  sont dans la même classe, alors  $x$  et  $z$  doivent être dans la même classe.

Voici donc les hypothèses supplémentaires que doit vérifier une relation pour que les classes sous-jacentes satisfassent ces trois propriétés.

**Définition 2.79.** Une *relation d'équivalence* sur  $A$  est une relation  $\sim$  sur  $A$  vérifiant les propriétés suivantes :

- (réflexivité) pour tout  $x \in A$ ,  $x \sim x$  ;
- (symétrie) pour tout  $x, y \in A$ , si  $x \sim y$ , alors  $y \sim x$  ;
- (transitivité) pour tout  $x, y, z \in A$ , si  $x \sim y$  et  $y \sim z$ , alors  $x \sim z$ .

**Exemple 2.80.** Reprenons les relations présentées dans l'exemple 2.78. La première, la relation d'égalité, est une relation d'équivalence. Il en est de même pour la sixième relation (exercice).

La relation  $\leq$  dans  $\mathbb{R}$  n'est pas symétrique ( $0 \leq 1$  mais  $1 \not\leq 0$ ), ce n'est donc pas une relation d'équivalence. En revanche, elle est réflexive et transitive. Noter bien que  $<$  n'est pas réflexive.

La relation d'inclusion dans  $\mathcal{P}(A)$  est réflexive et transitive. Mais elle n'est pas symétrique dès que  $A$  est non vide. En effet, on a  $\emptyset \subset A$  mais l'inclusion réciproque n'a pas lieu.

La relation sur  $\mathcal{P}(A)$  définie via l'existence d'une injection/surjection/bijection : exercice. La relation sur  $\mathcal{P}(A)$  définie par  $BRC \iff B \cap C \neq \emptyset$  est symétrique. Elle n'est cependant pas réflexive :  $\emptyset$  n'est pas relié à lui-même. Elle n'est pas transitive dès que  $A$  possède au moins deux éléments. En effet, si  $x$  et  $y$  sont deux éléments distincts, alors  $\{x\}$  est relié à  $\{x, y\}$ ,  $\{x, y\}$  est relié à  $\{y\}$ , mais  $\{x\}$  n'est pas relié à  $\{y\}$ .

Enfin, la dernière relation présentée dans l'exemple 2.78 est une relation d'équivalence. À vérifier, exercice.

**Exercice 2.81.** Traiter les passages laissés en exercice dans l'exemple ci-dessus.

**Définition 2.82.** Soit  $\sim$  une relation d'équivalence sur un ensemble  $A$ . Pour tout  $x \in A$ , sa *classe d'équivalence* est le sous-ensemble de  $A$  défini par

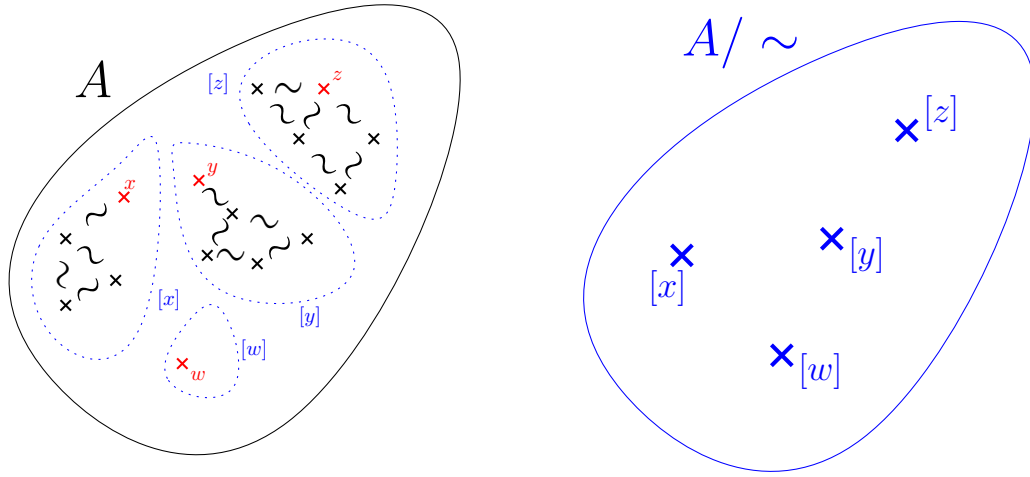
$$[x] = \{y \in A \mid x \sim y\}.$$

L'ensemble des classes d'équivalence est noté

$$A/\sim = \{[x] \mid x \in A\}.$$

On l'appelle le *quotient* de  $A$  par la relation d'équivalence  $\sim$ .

Si  $c$  est un élément de  $A/\sim$ , un *représentant* de  $c$  est un élément  $x \in A$  tel que  $c = [x]$ . Un *système de représentants* est un sous-ensemble  $R$  de  $A$  tel que pour tout  $c \in A/\sim$ , il existe un unique  $x \in R$  tel que  $c = [x]$ .



**Proposition 2.83.** Avec les mêmes notations que la définition précédente, on a les propriétés suivantes :

1. Pour tout  $x, y \in A$ ,

$$[x] = [y] \iff x \sim y;$$

2. Pour tout  $x, y \in A$ ,

$$[x] = [y] \iff [x] \cap [y] \neq \emptyset;$$

3.  $A/\sim$  est une partition de  $A$ .

Ainsi, si  $R$  est un système de représentant, on peut écrire

$$A = \bigsqcup_{x \in R} [x].$$

Remarquons aussi que si  $c \in A/\sim$ , alors l'ensemble des représentants de  $c$  est exactement l'ensemble des éléments de  $c$ . Autrement dit, on a  $\{x \in A \mid c = [x]\} = c$ .

**Preuve.** Soient  $x, y \in A$ . Montrons  $[x] = [y] \iff x \sim y$ . Supposons d'abord  $[x] = [y]$ .  $x$  est un élément de  $[x]$ , donc de  $[y]$ , ce qui signifie par définition que  $x \sim y$ . D'où l'implication directe. Supposons maintenant  $x \sim y$ . Si  $z$  est un élément de  $[x]$ , alors  $x \sim z$  par définition. Par transitivité, on a donc  $z \sim y$  donc  $z \in [y]$ . Cela prouve  $[x] \subset [y]$  et l'inclusion réciproque se démontre de la même manière. D'où l'implication réciproque, et l'équivalence.

Montrons maintenant  $[x] = [y] \iff [x] \cap [y] \neq \emptyset$ . Le sens direct est trivial. Pour la réciproque, supposons que l'ensemble  $[x] \cap [y]$  n'est pas vide et considérons un élément  $z$  dedans. D'une part,  $z \in [x]$  donc  $z \sim x$ . D'autre part,  $z \in [y]$  donc  $z \sim y$ . Ainsi, par transitivité,  $x \sim y$ . L'équivalence que nous avons montré nous permet donc d'obtenir  $[x] = [y]$ .

Montrons enfin que  $A/\sim$  partitionne  $A$ . La seconde équivalence nous dit exactement que deux classes d'équivalence distinctes ne s'intersectent pas, donc les éléments de  $A/\sim$  forment une famille disjointe. Il ne reste plus qu'à montrer que l'union des classes d'équivalence vaut  $A$ . Les classes d'équivalence étant des sous-ensembles de  $A$ , on sait déjà que leur union est incluse dans  $A$ . Réciproquement, si  $x \in A$ , alors la réflexivité nous dit que  $x$  est dans sa propre classe  $[x]$ , donc appartient à l'union des classes. D'où l'égalité. Ceci achève la preuve.  $\square$

**Exemple 2.84.**

1. Considérons la relation d'égalité « = » dans un ensemble  $A$  non vide. Si  $x \in A$ , alors  $[x] = \{x\}$  (le seul élément égal à  $x$  est lui-même). Ainsi le quotient vaut

$$A/_= = \{\{x\} \mid x \in A\},$$

c'est la partition en singletons. L'ensemble  $A$  est un système de représentants.

Cet exemple n'est pas intéressant car il ne permet pas d'identifier des éléments entre eux, on ne perd aucune information et on peut reconstruire  $A$  à partir de  $A/_=$  en « cassant » les singletons. D'ailleurs, la fonction  $x \in A \mapsto \{x\} \in A/_=$  est une bijection, de réciproque  $C \in A/_= \mapsto x \in A$  tel que  $C = \{x\}$ .

2. Considérons sur  $\mathbb{Z}$  la relation d'équivalence  $x \equiv y \iff x - y$  est pair.

Soit  $x \in \mathbb{Z}$ . Alors (à vérifier, exercice) sa classe d'équivalence vaut  $[x] = \{x + 2k \mid k \in \mathbb{Z}\}$ , ce qu'on peut aussi noter  $x + 2\mathbb{Z}$ .

Si  $x$  est pair, alors 0 est dans sa classe d'équivalence, sinon 1 est dans sa classe (on le montrera dans le chapitre 5). On en déduit que  $\mathbb{Z}/\equiv = \{[0], [1]\}$  et que  $\{0, 1\}$  est un système de représentant. L'ensemble  $\mathbb{Z}/\equiv$  sera noté  $\mathbb{Z}_2$  et sera très étudié dans la section 5.2 du chapitre 5.

3. Étant donnée  $f: A \rightarrow B$ , reprenons l'exemple de la relation d'équivalence définie par  $x \sim y \iff f(x) = f(y)$ .

Soit  $x \in A$ . Notons  $z = f(x)$ , c'est un élément de  $\text{im} f$ . La classe d'équivalence de  $x$  vaut

$$[x] = \{y \in A \mid f(y) = f(x)\} = \{y \in A \mid y \in f^{-1}(z)\} = f^{-1}(z).$$

Ainsi le quotient vaut  $A/_\sim = \{f^{-1}(z) \mid z \in \text{im} f\}$ , c'est la partition de  $A$  en préimages. Le passage de  $A$  vers  $A/_\sim$  consiste à agglomérer les éléments de  $A$  qui ont la même image par  $f$ . On ne peut plus distinguer deux éléments qui ont la même image, ils ne font qu'un. Ainsi cela permet de construire naturellement une fonction injective à partir de  $f$ , de la manière suivante. Considérons

$$\begin{array}{ccc} \bar{f}: & A/_\sim & \rightarrow B \\ & [x] & \mapsto f(x) \end{array}$$

Avant de vérifier que  $\bar{f}$  est injective, il faut d'abord d'assurer qu'elle est bien définie.

**Remarque 2.85.** Avant de s'assurer que  $\bar{f}$  est bien définie, il faut déjà comprendre pour quelle raison il se pourrait qu'elle ne soit pas bien définie. La définition de  $\bar{f}$  ci-dessus nous dit que si on lit  $[x]$ , on doit renvoyer  $f(x)$ . Mais  $[x]$  peut aussi s'écrire  $[y]$  pour un autre élément  $y$  (tel que  $y \sim x$ ). Donc si je lis  $[y]$ , je dois renvoyer  $f(y)$ . Mais  $[x]$  et  $[y]$  étant les mêmes éléments de  $A/_\sim$ ,  $f$  doit renvoyer la même chose quelle que soit l'écriture de cet élément. Il faut donc être sûr que  $f([x])$  ne dépend pas du représentant  $x$  qu'on a choisi pour la classe d'équivalence.

Si  $x$  et  $y$  sont des éléments de  $A$  tels que  $[x] = [y]$ , alors  $x \sim y$ . Par définition, cela signifie que  $f(x) = f(y)$ . Ainsi  $f([x])$  ne dépend pas de l'écriture de l'élément  $[x]$ . Donc  $\bar{f}$  est bien définie.

Montrons maintenant que  $\bar{f}$  est injective. Soient  $[x]$  et  $[y]$  deux éléments de  $A/_\sim$  tels que  $\bar{f}([x]) = \bar{f}([y])$ . Par définition, on a  $f(x) = f(y)$ . Cela signifie donc que  $x \sim y$ , donc que  $[x] = [y]$ . Ceci démontre l'injectivité.

**Exercice 2.86.** Soit  $A$  un ensemble non vide.  $\mathcal{P}(A)$ , on considère la relation d'équivalence  $\sim$  définie par : pour tout  $B, C \in \mathcal{P}(A)$ ,  $B \sim C$  si et seulement s'il existe une bijection de  $B$  dans  $C$ .

Déterminer les classes d'équivalence et un système de représentants dans les cas suivants.

1.  $A$  est un singleton.
2.  $A$  est une paire.
3.  $A$  est constitué de trois éléments deux à deux distincts.

Dans chacun des cas, qu'est-ce qui caractérise les classes ? Ce sera vrai plus généralement lorsque  $A$  est un ensemble fini (cf. problème 4.6.1 du chapitre 4).

## 2.5 Problèmes

### 2.5.1 Problème 1

Le but de ce problème est de démontrer le théorème de Cantor-Schröder-Bernstein.

**Théorème** (de Cantor-Schröder-Bernstein). *Soient  $A$  et  $B$  deux ensembles. On suppose qu'il existe une fonction injective de  $A$  vers  $B$ , et une fonction injective de  $B$  vers  $A$ . Alors il existe une bijection de  $A$  vers  $B$ .*

Cet énoncé va dans le sens de l'intuition qu'on avait sur les fonctions injectives. Il énonce le fait que s'il y a plus de place dans  $B$  que dans  $A$ , et plus de place dans  $A$  que dans  $B$ , alors  $A$  et  $B$  ont la même taille. Pour des ensembles finis, ce résultat est très facile à démontrer, à condition de connaître les résultats de base sur la théorie du cardinal (cf. problème 4.6.1 du chapitre 4). Pour des ensembles infinis, cela demande beaucoup plus d'effort.

Notons que ce théorème implique par exemple que les ensembles  $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$  et  $[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$  sont en bijection, puisque  $x \in [0, 1] \mapsto x/2 \in [0, 1)$  et  $x \in [0, 1) \mapsto x \in [0, 1]$  sont des injections.

Nous proposons ici deux preuves.

**Première preuve.** Cette démonstration du théorème de Cantor-Schröder-Bernstein démarre avec la preuve du résultat préliminaire suivant.

**Proposition.** *Soit  $A$  un ensemble et  $C$  un sous-ensemble de  $A$ . On suppose qu'il existe une injection  $A \rightarrow C$ . Alors il existe une bijection de  $A$  vers  $C$ .*

Soit  $f: A \rightarrow C$  une fonction injective. On définit une famille  $(D_n)_{n \in \mathbb{N}}$  de sous-ensemble de  $A$  de la manière suivante :

- $D_1 = A - C$ ;
- $\forall n \in \mathbb{N}, D_{n+1} = f(D_n)$ ,

ainsi que  $D = \bigcup_{n \in \mathbb{N}} D_n$ . On définit aussi la fonction

$$\begin{aligned} \varphi: A &\rightarrow C \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in D, \\ x & \text{si } x \notin D. \end{cases} \end{aligned}$$

1. Montrer que  $\varphi$  est bien définie.
2. Montrer que  $f(D) = \bigcup_{n \in \mathbb{N} - \{1\}} D_n = D \cap C$ .
3. Déterminer  $\varphi(D)$  et montrer que  $\varphi|_D^{\varphi(D)}: D \rightarrow \varphi(D)$  est une bijection.
4. Déterminer  $\varphi(A - D)$  et montrer que  $\varphi|_{A-D}^{\varphi(A-D)}: A - D \rightarrow \varphi(A - D)$  est une bijection.
5. En déduire que  $\varphi: A \rightarrow C$  est une bijection.

Le résultat préliminaire a donc été démontré. Soient maintenant  $f: A \rightarrow B$  et  $g: B \rightarrow A$  des fonctions injectives.

6. Trouver une fonction injective  $A \rightarrow g(B)$ .
7. Que dire de la corestriction  $g|_{g(B)}: B \rightarrow g(B)$  ?
8. En déduire le théorème de Cantor-Schröder-Bernstein.

**Seconde preuve.** Cette nouvelle preuve part d'un résultat du point fixe que nous allons démontrer.

**Théorème** (du point fixe de Knaster-Tarski). *Soit  $A$  un ensemble et  $f: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$  une fonction. On suppose que  $f$  est croissante, c'est-à-dire qu'elle vérifie :*

$$\forall E, F \in \mathcal{P}(A), E \subset F \Rightarrow f(E) \subset f(F).$$

*Alors il existe  $M \in \mathcal{P}(A)$  tel que  $f(M) = M$ .*

Soit  $f: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$  une fonction croissante. Posons

$$\mathcal{F} = \{E \in \mathcal{P}(A) \mid E \subset f(E)\} \text{ et } M = \bigcup_{E \in \mathcal{F}} E.$$

1. Montrer que  $\mathcal{F}$  est non vide.
2. Montrer que pour tout  $E \in \mathcal{F}$ , on a  $E \subset f(M)$ . En déduire  $M \subset f(M)$ .
3. Montrer que pour tout  $E \in \mathcal{F}$ , on a  $f(E) \in \mathcal{F}$ . En déduire  $f(M) \subset M$ .

On obtient ainsi  $f(M) = M$ . D'où le théorème du point fixe.

Démontrons maintenant le théorème de Cantor-Schröder-Bernstein. Considérons  $f: A \rightarrow B$  et  $g: B \rightarrow A$  des fonctions injectives.

4. En utilisant le théorème du point fixe, démontrer qu'il existe  $M \in \mathcal{P}(A)$  tel que  $A - M = g(B - f(M))$ .
5. Montrer que la restriction de  $f$  à  $M$ , corestreinte à  $f(M)$ , est une bijection.
6. Montrer que la restriction de  $g$  à  $B - f(M)$ , corestreinte à  $g(B - f(M))$  est une bijection. En déduire une bijection de  $A - M$  vers  $B - f(M)$ .
7. En déduire une bijection de  $A$  vers  $B$ .

### 2.5.2 Problème 2

On souhaite démontrer le résultat suivant, étonnant à première vue.

**Théorème.** *Il existe une bijection de  $\mathbb{R}^2$  vers  $\mathbb{R}$ .*

Pour démontrer ce théorème, nous utiliserons le théorème de Cantor-Schröder-Bernstein énoncé dans le problème 1, ainsi que le résultat suivant, qui va nous permettre de travailler avec l'ensemble des réels sans avoir besoin de les définir.

**Proposition.** Pour tout réel  $x \in [0, 1)$ , il existe une unique suite<sup>a</sup>  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant :

- il n'existe pas de  $N$  tel que pour tout  $n \geq N$ ,  $x_n = 9$  ;
- en écriture décimale, on a  $x = 0.x_1x_2x_3\dots$

Réciproquement, toute suite  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant la première condition constitue l'écriture décimale d'un élément  $x \in (0, 1)$ .

a. On anticipe sur la notion de suite. Une suite  $(x_n)_{n \in \mathbb{N}}$  n'est autre qu'une fonction  $f$  définie sur  $\mathbb{N}$  par  $f(n) = x_n$ .

On ne définira pas proprement ce qu'est l'écriture décimale d'un nombre réel.

1. Trouver une bijection de  $(0, 1)$  vers  $\mathbb{R}$  (la chercher en utilisant des fonctions usuelles simples).
2. Montrer alors qu'il existe une bijection de  $(0, 1)^2$  vers  $\mathbb{R}^2$ .
3. Trouver une injection de  $(0, 1)^2$  vers  $(0, 1)$ . Indication, si  $(x_n)_{n \in \mathbb{N}}$  et  $(y_n)_{n \in \mathbb{N}}$  sont les suites associées à  $x, y \in (0, 1)$  comme dans la proposition, définir un élément de  $(0, 1)$  dont l'écriture décimale comporte tous les termes  $x_n$  et  $y_n$  ( $n \in \mathbb{N}$ ).
4. En déduire, à l'aide du théorème de Cantor-Schröder-Bernstein, qu'il existe une bijection de  $\mathbb{R}^2$  vers  $\mathbb{R}$ .

### 2.5.3 Problème 3

Montrons que  $\mathbb{R}$  n'est pas dénombrable, c'est-à-dire qu'il n'existe pas de surjection de  $\mathbb{N}$  vers  $\mathbb{R}$ . L'existence d'une telle surjection, notée  $f$ , permettrait d'énumérer les éléments de  $\mathbb{R}$  : 1er élément  $f(1)$ , 2e élément  $f(2)$ , etc. Mais  $\mathbb{R}$  est beaucoup trop gros pour pouvoir lister ses éléments un par un.

Nous allons suivre la démonstration originale due à Cantor, c'est encore une fois un argument diagonal. Comme dans le problème 2.5.2, on utilisera le résultat suivant.

**Proposition.** Pour tout réel  $x \in [0, 1)$ , il existe une unique suite  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant :

- il n'existe pas de  $N$  tel que pour tout  $n \geq N$ ,  $x_n = 9$  ;
- en écriture décimale, on a  $x = 0.x_1x_2x_3\dots$

Réciproquement, toute suite  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant la première condition constitue l'écriture décimale d'un élément  $x \in (0, 1)$ .

Supposons par l'absurde qu'il existe une surjection  $f: \mathbb{N} \rightarrow \mathbb{R}$ .

1. Montrer qu'il existe alors une surjection  $g: \mathbb{N} \rightarrow [0, 1)$ . Indication, pour tout  $n \in \mathbb{Z}$ , ramener  $[n, n + 1)$  dans  $[0, 1)$  par une opération simple.

Ainsi, on peut écrire  $[0, 1) = \{g(i) \mid i \in \mathbb{N}\}$ . Par la proposition, pour tout  $i \in \mathbb{N}$ , on peut écrire  $g(i) = 0.x_1^{(i)}x_2^{(i)}x_3^{(i)}\dots$  (en écriture décimale) pour une unique suite  $(x_n^{(i)})_{n \in \mathbb{N}}$  qui ne stationne pas à 9.

2. Construire une suite  $(y_n)_{n \in \mathbb{N}}$  qui ne stationne pas à 9 et tel que pour tout  $i \in \mathbb{N}$ ,  $y_i \neq x_i^{(i)}$ .
3. En déduire que l'élément  $y = 0.y_1y_2y_3\dots$  n'est pas dans l'image de  $g$ . Conclure.

### 2.5.4 Problème 4

On veut montrer que  $\mathbb{R}$  et  $\mathcal{P}(\mathbb{N})$  sont en bijection. Pour cela, nous allons encore une fois admettre et exploiter le résultat suivant.

**Proposition.** *Pour tout réel  $x \in [0, 1)$ , il existe une unique suite  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant :*

- *il n'existe pas de  $N$  tel que pour tout  $n \geq N$ ,  $x_n = 9$  ;*
- *en écriture décimale, on a  $x = 0.x_1x_2x_3\dots$*

*Réciproquement, toute suite  $(x_n)_{n \in \mathbb{N}}$  d'éléments de  $\{0, 1, \dots, 9\}$  vérifiant la première condition constitue l'écriture décimale d'un élément  $x \in (0, 1)$ .*

Nous utiliserons également le théorème de Cantor-Schröder-Bernstein énoncé dans le problème 2.5.1. On admet également que  $\mathbb{R}$  et  $(0, 1)$  sont en bijection (c'est une question du problème 2.5.2).

1. En utilisant l'énoncé de l'exercice 2.74, montrer qu'on peut trouver une injection de  $\mathcal{P}(\mathbb{N})$  vers l'ensemble des suites d'éléments de  $\{0, 1, \dots, 9\}$  qui ne stationnent pas à 9.
2. En déduire une injection de  $\mathcal{P}(\mathbb{N})$  vers  $\mathbb{R}$ .
3. Montrer qu'il existe une injection de l'ensemble des suites d'éléments de  $\{0, 1, \dots, 9\}$  vers l'ensemble des suites d'éléments de  $\{0, 1\}$ . Indication : associer à chaque entier de  $\{0, 1, \dots, 9\}$  une séquence de 4 éléments de  $\{0, 1\}$ , de manière injective.
4. En déduire une injection de  $\mathbb{R}$  vers  $\mathcal{P}(\mathbb{N})$  et conclure à l'aide du théorème de Cantor-Schröder-Bernstein.

# Chapitre 3

## Entiers, entiers positifs, ordre, induction

Dans ce chapitre, nous étudions des objets que nous manipulons depuis notre plus tendre enfance. Le but ici est de partir des axiomes qui caractérisent les entiers, et d'en déduire toutes les propriétés que nous avons longtemps prises pour acquises.

Nous ne prouverons pas l'existence de tels ensembles à partir de l'axiomatique de ZFC. Le lecteur curieux pourra s'intéresser à l'axiomatique de Peano dont on a donné un bref aperçu dans la section 2.2.

### 3.1 Axiomatique de $\mathbb{Z}$ et $\mathbb{N}$

Dans ce chapitre, nous supposons l'existence

- d'un ensemble  $\mathbb{Z}$  dont les éléments sont appelés les *entiers* ;
- d'un sous-ensemble  $\mathbb{N} \subset \mathbb{Z}$  dont les éléments sont appelés les *entiers positifs* ;
- d'une *addition*  $+: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ , l'évaluation en un couple  $(a, b) \in \mathbb{Z}^2$  sera notée  $a + b$  plutôt que  $+(a, b)$  ;
- d'une *multiplication*  $\cdot: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ , l'évaluation en un couple  $(a, b) \in \mathbb{Z}^2$  sera notée  $a \cdot b$ , voire  $ab$ , plutôt que  $\cdot(a, b)$ ,

satisfaisant les axiomes qui suivent. Les axiomes A porteront sur  $\mathbb{Z}$ , et les axiomes B concerneront plus particulièrement  $\mathbb{N}$ .

**Axiome A.1** (Commutativité, associativité, distributivité). Pour tous entiers  $a$ ,  $b$  et  $c$ , on a

1.  $a + b = b + a$  ;
2.  $a \cdot b = b \cdot a$  ;
3.  $(a + b) + c = a + (b + c)$  ;
4.  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  ;
5.  $a \cdot (b + c) = a \cdot b + a \cdot c$ .

**Axiome A.2** (Élément neutre additif). Il existe un entier  $0$  tel que  $a + 0 = a$  pour tout  $a \in \mathbb{Z}$ . Cet élément  $0$  est appelé un *élément neutre additif*, ou un *élément identité de l'addition*.

**Axiome A.3** (Élément neutre multiplicatif). Il existe un entier 1 tel que  $1 \neq 0$  et  $a \cdot 1 = a$  pour tout  $a \in \mathbb{Z}$ . Cet élément 1 est appelé un *élément neutre multiplicatif*, ou un *élément identité de la multiplication*.

**Axiome A.4** (Inverse additif). Pour tout  $a \in \mathbb{Z}$ , il existe un entier, noté  $-a$  et appelé l'*inverse additif de  $a$* , tel que  $a + (-a) = 0$ .

**Attention.** L'élément  $-a$  est seulement défini par la propriété décrite par l'axiome, il n'est pas défini comme «  $a$  multiplié par  $-1$  » (une telle définition nécessiterait d'abord de définir  $-1$ ). Les axiomes permettront cependant d'aboutir à l'égalité  $-a = (-1) \cdot a$ .

**Axiome A.5** (Annulation (multiplicative à gauche)). Pour tout  $a, b, c$  dans  $\mathbb{Z}$ , si  $a \cdot b = a \cdot c$  et  $a \neq 0$ , alors  $b = c$ .

**Axiome B.1.**

1. Si  $a, b \in \mathbb{N}$ , alors  $a + b \in \mathbb{N}$  ( $\mathbb{N}$  est *fermé* sous l'addition).
2. Si  $a, b \in \mathbb{N}$ , alors  $ab \in \mathbb{N}$  ( $\mathbb{N}$  est *fermé* sous la multiplication).
3.  $0 \notin \mathbb{N}$ .
4. Pour tout  $a \in \mathbb{Z}$ , on a  $a \in \mathbb{N}$  ou  $a = 0$  ou  $-a \in \mathbb{N}$ .

**Attention.** Dans certaines références, 0 est un élément de  $\mathbb{N}$ .

**Axiome B.2** (Induction). Si  $A \subset \mathbb{Z}$  satisfait les propriétés suivantes :

- $1 \in A$ ;
- $\forall n \in \mathbb{Z}, n \in A \Rightarrow n + 1 \in A$ ,

alors  $\mathbb{N} \subset A$ .

On dira qu'un entier est *négatif* s'il n'appartient pas à  $\mathbb{N}$  et ne vaut pas 0. Ainsi, un entier est ou bien positif, ou bien négatif, ou bien nul (nul signifiant « égal à 0 »).

**Remarque 3.1.** Noter que, sans l'axiome d'induction, les ensembles  $\mathbb{N} \subset \mathbb{Z}$  pourraient très bien être les ensembles  $\mathbb{R}_{>0} \subset \mathbb{R}$ . L'axiome d'induction est donc indispensable pour caractériser  $\mathbb{N}$  et  $\mathbb{Z}$  comme on se l'imagine.

## 3.2 Premières conséquences

Dans cette section, on ne s'intéresse qu'aux axiomes A. Elles impliquent les propriétés suivantes que nous connaissons tous depuis longtemps.

**Proposition 3.2.** Soient  $a, b, c$  et  $d$  des entiers.

1.  $(b + c)a = ba + ca$ .
2.  $(a + b)(c + d) = ac + ad + bc + bd$ .
3.  $0 + a = a$  et  $1 \cdot a = a$ .

4.  $(-a) + a = 0$ .
5. Si  $a + b = a + c$ , alors  $b = c$ .
6. Si  $a + b = a$ , alors  $b = 0$ . Ainsi 0 est l'unique neutre additif.
7.  $a \cdot 0 = 0 \cdot a = 0$ .
8. Si  $a + b = 0$ , alors  $b = -a$ . Ainsi,  $a$  n'admet qu'un seul inverse additif.
9. Si  $ab = a$  et  $a \neq 0$ , alors  $b = 1$ . Ainsi, 1 est l'unique neutre multiplicatif.
10.  $ab = 0 \iff a = 0$  ou  $b = 0$ .
11.  $a \cdot a = a \iff a = 0$  ou  $a = 1$ .

**Preuve.**

1. Commutativité pour  $\cdot$  et distributivité :

$$(b + c)a = a(b + c) = ab + ac = ba + ca.$$

2. On applique d'abord la règle de distributivité  $A(B + C) = AB + AC$  à  $A = a + b$ ,  $B = c$  et  $C = d$ , ce qui donne

$$(a + b)(c + d) = (a + b)c + (a + b)d.$$

On applique ensuite le premier point de cette proposition à chacun des membres :  $(a + b)c = ac + bc$  et  $(a + b)d = ad + bd$ .

3. Commutativité et neutre pour l'addition. Commutativité et neutre pour la multiplication.
4. Commutativité pour l'addition et inverse additif.
5. Si  $a + b = a + c$ , alors  $-a + (a + b) = -a + (a + c)$ . L'associativité pour l'addition et la propriété de l'inverse additif donnent

$$-a + (a + b) = (-a + a) + b = b$$

et de même  $-a + (a + c) = c$ . D'où  $b = c$ .

6. Appliquer la propriété précédente à  $c = 0$ .
7.  $a \cdot 0 = 0 \cdot a$  par commutativité. 0 étant un neutre additif, on a  $0 = 0 + 0$ . Donc la distributivité donne  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ . On applique le dernier point «  $A + B = A \Rightarrow B = 0$  » à  $A = B = a \cdot 0$ , pour obtenir  $a \cdot 0 = 0$ .
8. Si  $a + b = 0$ , alors  $-a + (a + b) = -a + 0$ . D'une part, l'associativité pour l'addition et la propriété de l'inverse additif donnent

$$-a + (a + b) = (-a + a) + b = b.$$

D'autre part, 0 étant un neutre additif, on a  $-a + 0 = -a$ . D'où  $b = -a$ .

9. On remarque que «  $ab = a$  » s'écrit aussi «  $ab = a \cdot 1$  », et on applique l'axiome d'annulation multiplicative à gauche à  $c = 1$ .
10. L'implication indirecte est une conséquence de la propriété 7 de cette proposition. Supposons maintenant que  $ab = 0$  et montrons la disjonction  $a = 0$  ou  $b = 0$ . Supposons donc  $\neg(a = 0)$ , c'est-à-dire  $a \neq 0$ , et montrons  $b = 0$ . D'après la propriété 7,  $0 = a \cdot 0$ . Donc on a  $ab = a \cdot 0$ . Comme  $a \neq 0$ , on peut utiliser l'axiome d'annulation multiplicative à gauche pour obtenir ce qu'on voulait :  $b = 0$ . D'où l'implication directe, d'où l'équivalence.

11. L'implication indirecte est une conséquence de la propriété 7 de cette proposition, et de l'axiome du neutre multiplicatif. Supposons maintenant que  $a \cdot a = a$  et montrons la disjonction  $a = 0$  ou  $a = 1$ . Supposons donc  $\neg(a = 0)$ , c'est-à-dire  $a \neq 0$ , et montrons  $a = 1$ . L'axiome du neutre multiplicatif nous dit que  $a = a \cdot 1$ . Donc on a  $a \cdot a = a \cdot 1$ . Comme  $a \neq 0$ , on peut utiliser l'axiome d'annulation multiplicative à gauche pour obtenir ce qu'on voulait :  $a = 1$ . D'où l'implication directe, d'où l'équivalence.  $\square$

Continuons avec quelques règles de calculs portant sur l'inverse additif.

**Proposition 3.3.** *Soient  $a$  et  $b$  des entiers.*

1.  $-0 = 0$ .
2. *Involution* :  $-(-a) = a$ .
3.  $-(a + b) = (-a) + (-b)$ .
4.  $(-a)b = a(-b) = -(ab)$ . En particulier,  $(-1)a = -a$ .
5.  $(-a)(-b) = ab$ . En particulier,  $(-1)(-1) = 1$ .

**Preuve.**

1. L'égalité  $0 + a = 0$  est satisfaite pour  $a = 0$ , donc 0 est un inverse additif de 0, et c'est le seul d'après la propriété 8 de la proposition 3.2.
2. L'égalité  $(-a) + b = 0$  est satisfaite pour  $b = a$ , donc  $a$  est un inverse additif de  $-a$ , et c'est le seul d'après la propriété 8 de la proposition 3.2.
3. L'égalité  $(a + b) + c = 0$  est satisfaite pour  $c = (-a) + (-b)$  (utiliser l'associativité pour  $+$ , la commutativité pour  $+$ ,  $a + (-a) = 0$  et  $b + (-b) = 0$ ).
4. L'égalité  $(ab) + c = 0$  est satisfaite pour  $c = (-a)b$ , c'est une conséquence de la distributivité :  $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$ . La distributivité montre aussi que l'égalité  $(ab) + c = 0$  est satisfaite pour  $c = a(-b)$ . Ainsi, par unicité de l'inverse de  $ab$ , on a  $-(ab) = (-a)b = a(-b)$ .
5. L'égalité  $(-a)b = a(-b)$  que nous venons de montrer est valable pour tous entiers  $a$  et  $b$ . En remplaçant  $b$  par  $-b$ , on obtient  $(-a)(-b) = a(-(-b))$ . Or on a  $-(-b) = b$ , donc  $(-a)(-b) = ab$ .  $\square$

**Proposition/définition 3.4** (Soustraction). *Si  $a$  et  $b$  sont des entiers, alors il existe un unique entier  $c$  tel que  $a + c = b$ . Il s'agit de l'entier  $b + (-a)$ , on le note  $b - a$  (soustraction de  $b$  par  $a$ ).*

**Preuve. Existence.** On montre que l'entier  $b + (-a)$  fonctionne :  $a + (b + (-a)) = b + a + (-a) = b + 0 = b$ .

**Unicité.** Si  $c$  et  $c'$  sont deux entiers vérifiant la même propriété, à savoir  $a + c = b$  et  $a + c' = b$ , alors on a en particulier

$$a + c = a + c'.$$

La propriété 5 de la proposition 3.2 énoncé alors que  $c = c'$ , d'où l'unicité.  $\square$

**Proposition 3.5.** Soient  $a, b, c$  et  $d$  des entiers.

1.  $a - b = c - d \iff a + d = b + c$ .
2.  $(a - b) - c = (a - c) - b$ . On notera donc  $a - b - c$ . De manière générale, les additions et soustractions peuvent se faire dans n'importe quel ordre (cela découle de la commutativité de  $+$  et du fait que  $-$  se définit à partir de  $+$ ). Par exemple,  $a - b + c - d = a - d - b + c = (-d) - c + b + a = \dots$
3.  $-(a - b) = b - a$ .
4.  $(a - b) + (c - d) = (a + c) - (b + d)$ .
5.  $(a - b) - (c - d) = (a + d) - (b + c)$ .
6.  $(a - b)c = ac - bc$ .
7.  $(a - b)(c - d) = (ac + bd) - (ad + bc)$ .

**Preuve.** Exercice. □

**Exercice 3.6.** Démontrer la proposition ci-dessus.

Parlons enfin de divisibilité.

**Définition 3.7.** Soient  $a$  et  $b$  deux entiers. On dit que  $a$  est *divisible* par  $b$ , ou que  $b$  *divise*  $a$ , ou que  $A$  est un *multiple* de  $b$ , noté  $b|a$ , s'il existe  $c \in \mathbb{Z}$  tel que  $a = bc$ .

On définit  $2 = 1 + 1$ . On dit que  $a$  est *pair* si  $a$  est divisible par 2. Sinon, on dit que  $a$  est *impair*.

**Attention.** On ne sait pas encore que les entiers impairs sont exactement les  $2k + 1$  pour  $k \in \mathbb{Z}$ . Nous serons en mesure de montrer cette propriété dans le chapitre 5. Noter qu'on l'a utilisée plusieurs fois dans les chapitres précédents, mais seulement pour illustrer les notions introduites.

**Proposition 3.8.**

1. 0 est divisible par tout entier.
2. Si  $a$  est un entier non nul, alors 0 ne divise pas  $a$ .

**Preuve.**

1. Si  $b$  est un entier quelconque, alors la propriété 7 de la proposition 3.2 énonce que l'égalité  $b \cdot c = 0$  est satisfaite pour  $c = 0$ .
2. On procède par contraposée. Si  $a$  est un entier divisible par 0, alors il existe un entier  $c$  tel que  $a = c \cdot 0$ . Mais  $c \cdot 0 = 0$ , donc cela signifie que  $a = 0$ . □

**Proposition 3.9.** Soient  $a, b$  et  $k$  des entiers.

1. Si  $k$  divise  $a$ , alors  $k$  divise  $-a$ .
2. Si  $k$  divise  $a$  et  $b$ , alors  $k$  divise  $a + b$  et  $ab$ .

**Preuve.**

1. Supposons que  $k$  divise  $a$ . Alors il existe un entier  $c$  tel que  $a = kc$ . Par la propriété 4 de la proposition 3.3, on a  $-a = k(-c)$ . Ainsi  $k$  divise  $-a$ .
2. Supposons que  $k$  divise  $a$  et  $b$ . Alors il existe des entiers  $c$  et  $d$  tels que  $a = kc$  et  $b = kd$ . Ainsi, la distributivité donne

$$a + b = kc + kd = k(c + d)$$

et l'associativité et la commutativité pour  $\cdot$  donnent

$$ab = (kc)(kd) = k(kcd).$$

D'où le résultat. □

En reprenant les mêmes notations que la proposition précédente et sa preuve, on remarque même qu'on a  $ab = (k \cdot k)(cd)$ . Donc  $k \cdot k$  divise  $ab$ .

### 3.3 Ordre sur les entiers

Comme nous allons le voir, les axiomes nous permettent de retrouver la relation « être plus petit ou égal à » que nous manipulons depuis longtemps sur les entiers (voire sur les réels). Jusque-là nous n'avons utilisé que les axiomes A, nous allons maintenant exploiter l'axiome B.1.

Avant cela, nous avons besoin du vocabulaire concernant les relations d'ordre.

#### 3.3.1 Relation d'ordre sur un ensemble

**Définition 3.10.** Soit  $A$  un ensemble. Une *relation d'ordre*  $\leq$  sur  $A$  est une relation sur  $A$  (cf. définition 2.77) vérifiant les trois conditions suivantes :

- (réflexivité) pour tout  $x \in A$ ,  $x \leq x$  ;
- (antisymétrie) pour tout  $x, y \in A$ , si  $x \leq y$  et  $y \leq x$ , alors  $x = y$  ;
- (transitivité) pour tout  $x, y, z \in A$ , si  $x \leq y$  et  $y \leq z$ , alors  $x \leq z$ .

#### Exemple 3.11.

1. Nous allons construire la relation d'ordre sur  $\mathbb{Z}$  dont nous avons déjà une bonne intuition : la relation « être plus petit ou égal à ».
2. Dans  $\mathcal{P}(A)$ , la relation d'inclusion  $\subset$  est une relation d'ordre.
3. La relation « divise », noté  $|$ , est une relation réflexive et transitive (à vérifier, exercice). On montrera dans la proposition 3.45 qu'elle est aussi antisymétrique sur  $\mathbb{N}$ , c'est donc une relation d'ordre sur  $\mathbb{N}$ .

**Exercice 3.12.** Montrer que la relation « divise » sur  $\mathbb{Z}$  est réflexive et transitive.

**Définition 3.13.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ .

- On dit que la relation d'ordre  $\leq$  est *totale* si pour tout  $a, b \in A$ , on a  $a \leq b$  ou

$b \leq a$  (on peut toujours comparer deux éléments).

- On dit que  $A$  admet un *plus grand élément* (resp. *plus petit élément*) s'il existe  $a \in A$  vérifiant

$$\forall b \in A, b \leq a$$

(resp.  $\forall b \in A, a \leq b$ ).

**Proposition 3.14.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ . Si  $A$  admet un plus grand élément, alors il est unique, on le note  $\max A$ . De même, si  $A$  admet un plus petit élément, alors il est unique, on le note  $\min A$ .

**Preuve.** Supposons que  $a$  et  $a'$  sont des plus grands éléments de  $A$ . Relativement à  $a$ , la propriété appliquée à  $b = a'$  donne  $a' \leq a$ . Puis relativement à  $a'$ , la propriété appliquée à  $b = a$  donne  $a \leq a'$ . L'antisymétrie de  $\leq$  donne donc  $a = a'$ . D'où l'unicité du plus grand élément. L'unicité du plus petit élément se démontre de la même manière.  $\square$

### Exemple 3.15.

1. Nous verrons que la relation d'ordre « être plus petit ou égal à » sur  $\mathbb{Z}$ , que nous allons construire, est totale (si je prends deux entiers, je suis toujours capable de les comparer). À méditer : cette relation admet-elle un plus grand/petit élément ?
2. Soit  $E$  un ensemble. La relation d'ordre  $\subset$  sur  $\mathcal{P}(E)$  est total si et seulement si  $E$  est vide ou est un singleton. En effet, si  $E$  admet deux éléments distincts  $x$  et  $y$ , alors ni  $\{x\} \subset \{y\}$ , ni  $\{y\} \subset \{x\}$  n'est vrai. Dans le cas où  $E$  est vide ou vaut un singleton : exercice.  
Soit  $E$  un ensemble.  $E$  est le plus grand élément de  $\mathcal{P}(E)$  (par définition de  $\mathcal{P}(E)$ ) et  $\emptyset$  est le plus petit de  $\mathcal{P}(E)$  (tout ensemble contient l'ensemble vide).
3. Considérons la relation d'ordre  $\subset$  sur  $\mathcal{P}(E) - \{E\}$ . Tout élément  $A \in \mathcal{P}(E) - \{E\}$  vérifie  $A \subset E$ . Mais  $E$  n'est pas dans l'ensemble  $\mathcal{P}(E) - \{E\}$ , donc  $E$  n'est pas le plus grand élément.

**Remarque 3.16.** Comme on vient de le voir dans le dernier exemple, **attention** lorsqu'une relation d'ordre bien connue sur un ensemble  $A$  (par exemple  $\subset$  sur  $\mathcal{P}(E)$ ) est restreinte à un sous-ensemble  $B$ . La recherche du plus grand/petit élément doit maintenant se faire dans  $B$ .

4. Soit  $E$  un ensemble, soient  $A$  et  $B$  des sous-ensembles de  $E$ . Les deux derniers points de la proposition 2.24 énoncent exactement le fait que  $A \cup B$  est le plus petit élément (pour la relation d'ordre  $\subset$ ) de  $\{C \in \mathcal{P}(E) \mid A \subset C \text{ et } B \subset C\}$ , et que  $A \cap B$  est le plus grand élément de  $\{C \in \mathcal{P}(E) \mid C \subset A \text{ et } C \subset B\}$ .

**Exercice 3.17.** Soit  $A$  un ensemble muni d'une relation d'ordre  $\leq$ . Pour tout  $a, a' \in A$ , on note  $a < a'$  lorsque  $a \leq a'$  et  $a \neq a'$ . On définit une relation d'ordre  $\preccurlyeq$  sur  $A^2$  de la manière suivante : pour tout  $(a, b), (a', b') \in A^2$ ,

$$(a, b) \preccurlyeq (a', b') \iff a < a' \text{ ou } (a = a' \text{ et } b \leq b').$$

1. Vérifier que  $\preccurlyeq$  est une relation d'ordre sur  $A^2$ .
2. Montrer que la relation d'ordre  $\preccurlyeq$  sur  $A^2$  est totale si et seulement si la relation d'ordre  $\leq$  sur  $A$  est totale.

La relation  $\preccurlyeq$  est appelée l'ordre lexicographique sur  $A^2$  associée à la relation d'ordre  $\leq$ . Par exemple, avec l'ordre usuel sur les lettres de notre alphabet  $A$ , l'ordre lexicographique sur  $A^2$  est l'ordre des mots dans un dictionnaire ne contenant que des mots de longueur 2 (mais on peut généraliser pour des mots de longueur arbitraire).

**Définition 3.18.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ . Considérons un sous-ensemble  $B \subset A$ .

- On dit qu'un élément  $a \in A$  *major*e (resp. *minor*e)  $B$  dans  $A$ , ou est un *majorant* (resp. *minorant*) de  $B$  dans  $A$ , ou une *borne supérieure* (resp. *borne inférieure*) de  $B$ , si pour tout  $b \in B$ , on a  $b \leq a$  (resp.  $a \leq b$ ).
- On dit que  $B$  est *majoré* (resp. *minoré*) dans  $A$ , ou *borné supérieurement* (resp. *borné inférieurement*) si  $B$  admet un majorant (resp. minorant) dans  $A$ .
- On dit que  $B$  est borné dans  $A$  si  $B$  est à la fois majoré et minoré dans  $A$ .

**Remarque 3.19.**

1. Les notions de majorant et minorant d'un ensemble  $B$  sont relatives à l'ensemble ambiant  $A$ .  
Par exemple, étant donnée une paire  $E = \{x, y\}$ , l'ensemble  $\{\{x\}, \{y\}\}$  est majoré dans  $\mathcal{P}(E)$  pour la relation d'inclusion (car  $E$  est un majorant), mais pas dans  $\mathcal{P}(E) - \{E\}$  (aucun des éléments de cet ensemble, à savoir  $\{x\}$ ,  $\{y\}$  et  $\emptyset$  ne majore  $\{\{x\}, \{y\}\}$ ).
2. Si  $B$  est majoré dans  $A$ , alors il est majoré dans tout ensemble  $A'$  contenant  $A$  (un majorant de  $B$  dans  $A$  est majorant de  $B$  dans  $A'$ ).
3. Si  $a$  est un majorant de  $B$  dans  $A$ , et si  $a \in B$ , alors  $a$  est le plus grand élément de  $B$ . De manière générale, un ensemble  $A$  admet un plus grand élément s'il est majoré dans lui-même, et dans ce cas, il existe un unique majorant de  $A$  qui est le plus grand élément de  $A$ .

Lorsque le contexte est clair, on ne précisera pas l'ensemble ambiant  $A$  dans lequel un sous-ensemble serait majoré ou minoré.

Par exemple, si on travaille clairement dans  $\mathbb{Z}$ , et si on considère un sous-ensemble  $B$  de  $\mathbb{Z}$ , on dira simplement «  $B$  est majoré » plutôt que «  $B$  est majoré dans  $\mathbb{Z}$  ».

### 3.3.2 Ordre sur les entiers

En exploitant l'axiome B.1, nous allons définir l'ordre usuel sur les entiers. Avant cela, nous avons besoin d'un résultat préliminaire, fondamental car il nous dira qu'un entier non nul ne peut pas être positif et négatif en même temps, et que deux entiers inverses l'un de l'autre sont de signes opposés.

**Proposition 3.20.**

1. Pour tout  $a \in \mathbb{Z}$ , la disjonction «  $a \in \mathbb{N}$  ou  $a = 0$  ou  $-a \in \mathbb{N}$  » est une disjonction exclusive (seulement une des trois assertions est vraie).

$$2. \mathbb{Z} - (\mathbb{N} \cup \{0\}) = \{-k \mid k \in \mathbb{N}\}.$$

Par commodité, l'ensemble  $\{-k \mid k \in \mathbb{N}\}$  s'écrit  $-\mathbb{N}$ . On a donc l'union disjointe  $\mathbb{Z} = -\mathbb{N} \sqcup \{0\} \sqcup \mathbb{N}$ , qui décrit la décomposition « négatif – nul – positif ».

**Preuve.**

1. Soit  $a \in \mathbb{Z}$ . Si  $a$  est nul, alors il n'appartient pas  $\mathbb{N}$  (axiome B.1.3). L'élément  $-a$  est également nul donc n'appartient pas  $\mathbb{N}$  non plus. Supposons maintenant  $a$  non nul et supposons par l'absurde que  $a$  et  $-a$  appartiennent à  $\mathbb{N}$ . Alors la fermeture de  $\mathbb{N}$  sous l'addition (axiome B.1.1) entraînerait  $0 = a + (-a) \in \mathbb{N}$ , ce qui serait en contradiction avec l'axiome B.1.3. Donc il n'est pas possible que  $a$  et  $-a$  appartiennent à  $\mathbb{N}$ . Ainsi les trois assertions de la disjonction s'excluent mutuellement.
2. Soit  $a \in \mathbb{Z} - (\mathbb{N} \cup \{0\})$ . Les assertions «  $a \in \mathbb{N}$  » et «  $a = 0$  » sont fausses, donc l'axiome B.1.4 entraîne que  $-a$  est un élément de  $\mathbb{N}$ . Ainsi  $a$  s'écrit  $-k$  avec  $k = -a \in \mathbb{N}$  (on a utilisé la propriété 2 de la proposition 3.3). Ceci prouve l'inclusion  $\mathbb{Z} - (\mathbb{N} \cup \{0\}) \subset \{-k \mid k \in \mathbb{N}\}$ . Considérons maintenant  $k \in \mathbb{N}$ . La disjonction «  $k \in \mathbb{N}$  ou  $k = 0$  ou  $-k \in \mathbb{N}$  » étant exclusive, on obtient que  $k$  est non nul et que  $-k$  n'est pas un élément de  $\mathbb{N}$ . Autrement dit, on a  $-k \neq 0$  et  $-k \notin \mathbb{N}$ . Donc  $-k$  est un élément de  $\mathbb{Z} - (\mathbb{N} \cup \{0\})$ . D'où l'inclusion  $\mathbb{Z} - (\mathbb{N} \cup \{0\}) \supset \{-k \mid k \in \mathbb{N}\}$   $\square$

**Définition 3.21.** On définit la relation  $<$  sur  $\mathbb{Z}$  par

$$\forall a, b \in \mathbb{Z}, a < b \iff b - a \in \mathbb{N}.$$

**Corollaire 3.22.** Pour tout  $a, b \in \mathbb{Z}$ , l'assertion «  $a < b$  ou  $a = b$  ou  $b < a$  » est vraie, et c'est une disjonction exclusive.

**Preuve.** Soient  $a, b \in \mathbb{Z}$ . Remarquons que «  $a < b$  », «  $a = b$  » et «  $b < a$  » s'écrivent respectivement «  $b - a \in \mathbb{N}$  », «  $b - a = 0$  » et «  $-(b - a) \in \mathbb{N}$  ». Ainsi l'axiome B.1.4 appliqué à l'entier  $b - a$  entraîne que la disjonction est vraie, et la proposition précédente énonce qu'elle est exclusive.  $\square$

On remarque ainsi que la relation  $<$  n'est pas réflexive. Il faut lui ajouter quelque chose pour en faire une relation d'ordre.

**Proposition/définition 3.23.** On définit la relation  $\leq$  sur  $\mathbb{Z}$  par

$$\forall a, b \in \mathbb{Z}, a \leq b \iff a < b \text{ ou } a = b.$$

C'est une relation d'ordre totale.

**Preuve.** Réflexivité : Si  $a$  est un entier, alors  $a = a$ , donc l'assertion «  $a < a$  ou  $a = a$  » est vraie. D'où  $a \leq a$ .

Antisymétrie : Soient  $a$  et  $b$  des entiers tels que  $a \leq b$  et  $b \leq a$ , montrons que  $a = b$ .

Par distributivité entre  $\wedge$  et  $\vee$ , l'assertion «  $a \leq b$  et  $b \leq a$  » s'énonce :

$$a = b \text{ ou } (a < b \text{ et } b < a).$$

Or le corollaire précédent énonce en particulier que les assertions «  $a < b$  » et «  $b < a$  » s'excluent l'une de l'autre, donc «  $a < b$  et  $b < a$  » est fausse. La disjonction écrite ci-dessus étant supposée vraie, on en déduit  $a = b$ .

Transitivité : Soient  $a, b$  et  $c$  trois entiers tels que  $a \leq b$  et  $b \leq c$ . Montrons que  $a \leq c$ . D'abord, si  $a = b$ , alors «  $b \leq c$  » donne «  $a \leq c$  ». De même, si  $b = c$ , alors «  $a \leq b$  » donne «  $a \leq c$  ». Supposons maintenant  $a \neq b$  et  $b \neq c$ . Cela signifie donc que  $b - a$  et  $c - b$  sont des éléments de  $\mathbb{N}$ . Comme  $\mathbb{N}$  est fermé sous l'addition (axiome B.1.1), on obtient que  $(b - a) + (c - b)$ , c'est-à-dire  $c - a$ , est un élément de  $\mathbb{N}$ . Ainsi  $a \leq c$ .

Enfin, montrons que l'ordre est total. Soient  $a$  et  $b$  deux entiers. Montrons  $a \leq b$  ou  $b \leq a$ . Supposons que  $a \leq b$  est fausse. Cela signifie que ni  $a < b$ , ni  $a = b$  n'a lieu. Or l'assertion «  $a < b$  ou  $a = b$  ou  $b < a$  » est vraie (d'après le dernier corollaire), donc on a  $b < a$ , donc en particulier  $b \leq a$ . Ceci prouve que l'ordre est total.  $\square$

**Remarque 3.24.** Remarquons que lorsqu'on a démontré la transitivité de  $\leq$ , on a également montré que  $<$  est transitive.

On va maintenant pouvoir justifier les noms « entiers positifs » et « entiers négatifs » qu'on donne aux éléments de  $\mathbb{N}$  et  $-\mathbb{N}$  (ce dernier étant  $\mathbb{Z} - (\mathbb{N} \cup \{0\})$  d'après la proposition 3.20).

**Proposition 3.25.**

1.  $\mathbb{N} = \{a \in \mathbb{Z} \mid a > 0\}$ .
2.  $-\mathbb{N} = \{a \in \mathbb{Z} \mid a < 0\}$ .

On obtient ainsi  $\mathbb{N} \cup \{0\} = \{a \in \mathbb{Z} \mid a \geq 0\}$ . On notera  $\mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\}$ .

**Attention aux conventions.** Dans la littérature,  $\mathbb{N}$  peut correspondre à notre ensemble  $\mathbb{Z}_{\geq 0}$ .

**Preuve.**

1. Pour tout entier  $a$ , on a  $a = a - 0$  (neutre additif). Donc si  $a \in \mathbb{N}$ , alors  $a - 0 \in \mathbb{N}$  donc  $a > 0$ . Réciproquement, si  $a > 0$ , alors par définition  $a - 0 \in \mathbb{N}$  donc  $a \in \mathbb{N}$ .
2. Par le corollaire 3.22, un entier est ou bien  $> 0$ , ou bien nul, ou bien  $< 0$ . L'ensemble des entiers  $> 0$  vaut exactement  $\mathbb{N}$ , 0 est le seul entier nul, donc l'ensemble des entiers  $< 0$  correspond au reste  $\mathbb{Z} - \mathbb{Z}_{\geq 0}$ , c'est-à-dire  $-\mathbb{N}$ .  $\square$

**Proposition 3.26.** Pour tout entier  $a$  non nul,  $a \cdot a \in \mathbb{N}$ .

**Preuve.** Soit  $a$  un entier non nul. On utilise la décomposition  $\mathbb{Z} - \{0\} = -\mathbb{N} \sqcup \mathbb{N}$ . Premier cas :  $a \in \mathbb{N}$ , alors c'est une conséquence de la fermeture de  $\mathbb{N}$  sous la multiplication. Second cas :  $a \in -\mathbb{N}$ . Il existe donc  $k \in \mathbb{N}$  tel que  $a = -k$ . Ainsi les propriétés 4 et 2 de la proposition 3.3 donnent :

$$a \cdot a = (-k) \cdot (-k) = -(-k) \cdot k = k \cdot k.$$

On est donc revenu au premier cas et on peut conclure  $a \cdot a$  appartient à  $\mathbb{N}$ .  $\square$

**Corollaire 3.27.**  $1 \in \mathbb{N}$ .

**Preuve.** Comme  $1 = 1 \cdot 1$ , la proposition précédente permet de conclure.  $\square$

**Remarque 3.28.** Ainsi l'entier 2 défini par  $2 = 1 + 1$  est aussi dans  $\mathbb{N}$ , par fermeture sous addition.

On en déduit aussi que  $-1$  n'est pas dans  $\mathbb{N}$ . En particulier, comme  $-1$  n'est pas nul, il n'existe pas d'entier  $a$  tel que  $a \cdot a = -1$ .

**Corollaire 3.29.** *Pour tout entier  $a$ , on a  $a + 1 > a > a - 1$ . Ainsi  $\mathbb{Z}$  et  $\mathbb{N}$  n'admettent pas de plus grand élément, et  $\mathbb{Z}$  n'admet pas de plus petit élément.*

**Preuve.** Soit  $a \in \mathbb{Z}$ . On a

$$(a + 1) - a = a + 1 + (-a) = 1 + a + (-a) = 1 + 0 = 1.$$

Donc d'après la proposition précédente,  $(a + 1) - a \in \mathbb{N}$ , donc  $a + 1 > a$ .

Ainsi, si  $a \in \mathbb{Z}$ , l'entier  $a + 1$  est plus grand que  $a$ , donc  $a$  ne peut être le plus grand élément de  $\mathbb{Z}$ . De même, si  $a \in \mathbb{N}$ , alors comme  $1 \in \mathbb{N}$  et  $\mathbb{N}$  est fermé sous l'addition, on obtient que  $a + 1$  est un entier positif plus grand que  $a$ , donc  $a$  ne peut être un plus grand élément de  $\mathbb{N}$ .

Enfin, on a

$$a - (a - 1) = a + (1 - a) = a + 1 + (-a) = 1 + a + (-a) = 1 + 0 = 1 \in \mathbb{N},$$

donc  $a > a - 1$ . Ainsi, si  $a \in \mathbb{Z}$ , l'entier  $a - 1$  est plus petit que  $a$ , donc  $a$  ne peut être le plus petit élément de  $\mathbb{Z}$ .  $\square$

Nous verrons que  $\mathbb{N}$  admet un plus petit élément : il s'agit de 1.

On termine avec quelques règles de calcul. On a d'abord besoin d'établir le résultat préliminaire suivant.

**Proposition 3.30.** *Soient  $a \in \mathbb{N}$  et  $b \in \mathbb{Z}$ . Alors  $ab \in \mathbb{N} \iff b \in \mathbb{N}$ .*

**Preuve.** Soit  $a \in \mathbb{N}$  et  $b \in \mathbb{Z}$ .

L'implication indirecte se déduit de la fermeture de  $\mathbb{N}$  sous la multiplication.

On démontre l'implication directe par contraposée. Supposons  $b \notin \mathbb{N}$  et montrons  $ab \notin \mathbb{N}$ . Par la décomposition  $\mathbb{Z} = -\mathbb{N} \sqcup \{0\} \sqcup \mathbb{N}$ , on sait que  $b$  est nul ou  $b \in -\mathbb{N}$ . Si  $b$  est nul, alors  $ab$  est nul et donc n'est pas dans  $\mathbb{N}$ . Si  $b \in -\mathbb{N}$ , alors il existe  $k \in \mathbb{N}$  tel que  $b = -k$ . La propriété 4 de la proposition 3.3 donne  $ab = -(ak)$ . Par fermeture de  $\mathbb{N}$  sous la multiplication (axiome B.1.2),  $ak$  est dans  $\mathbb{N}$ . Ainsi,  $ab$  est dans  $-\mathbb{N}$ , donc n'est pas dans  $\mathbb{N}$ .  $\square$

**Proposition 3.31.** Soient  $a, b, c$  et  $d$  des entiers.

1. Si  $a < b$ , alors  $a + c < b + c$ .
2. Si  $a < b$  et  $c \leq d$ , alors  $a + c < b + d$ .
3. Si  $c > 0$ , alors  $a < b \iff ac < bc$ .
4.  $a > b \iff -a < -b$ .
5. Si  $c < 0$ , alors  $a < b \iff ac > bc$ .
6. Si  $0 < a < b$  et  $0 < c \leq d$ , alors  $ac < bd$ .

**Preuve.**

1. Écrire  $b - a = (b + c) - (a + c)$ .
2. Écrire  $(b + d) - (a + c) = (b - a) + (d - c)$ .
3. Si  $c \in \mathbb{N}$ , alors la proposition 3.30 implique l'équivalence  $(b - a)c \in \mathbb{N} \iff c \in \mathbb{N}$ .
4. Écrire  $-b - (-a) = a - b$ .
5. Si  $c < 0$ , alors  $-c > 0$ . Appliquer la propriété 3 à  $-c$  au lieu de  $c$ , et utiliser la propriété 4 de la proposition 3.3, cela donne  $a < b \iff -(ac) < -(bc)$ . La propriété 4 que nous venons de montrer, appliquer à  $ac$  au lieu de  $a$ ,  $bc$  au lieu de  $b$ , donne alors  $-(ac) < -(bc) \iff ac > bc$ . Par transitivité de  $\iff$ , on obtient ainsi  $a < b \iff ac > bc$ .
6. Si  $c = d$ , c'est une application directe de la propriété 3. Si  $c < d$ , alors on utilise cette propriété deux fois, l'une pour obtenir  $ac < bc$  à partir des hypothèses  $a < b$  et  $c > 0$ , l'autre pour obtenir  $bc < bd$  à partir des hypothèses  $c < d$  et  $b > 0$ . Ainsi, par transitivité de  $<$ , on obtient  $ac < bd$ .

□

On peut aussi placer des inégalités larges dans les énoncés. Par exemple, on peut démontrer

- $a \leq b$  et  $c \leq d \Rightarrow a + c \leq b + d$ ;
- $c > 0 \Rightarrow (a \leq b \iff ac \leq bc)$ ;
- $a \geq b \iff -a \leq -b$ ;
- etc.

### 3.4 Raisonnement par induction et principe du bon ordre

Il est temps d'exploiter l'axiome B.2, qui aboutit à l'un des raisonnements incontournables des mathématiques : le raisonnement par induction. Il permet aussi d'étudier un peu plus finement la relation d'ordre  $\leq$  sur  $\mathbb{Z}$ , et ainsi obtenir des propriétés fondamentales, bien qu'intuitives. Par exemple, nous allons établir le fait que pour tout entier  $n$ , il n'existe pas d'entier  $a$  vérifiant  $n < a < n + 1$ .

**Remarque 3.32.** Notons  $\mathcal{N}$  l'ensemble des  $A \in \mathcal{P}(\mathbb{Z})$  qui sont stables par l'addition  $+1$  et dont 1 est un élément.  $\mathcal{N}$  est un sous-ensemble de  $\mathcal{P}(\mathbb{Z})$ .

Pour la relation d'ordre  $\subset$  sur  $\mathcal{P}(\mathbb{Z})$ ,  $\mathbb{N}$  est le plus petit élément de l'ensemble  $\mathcal{N}$ . En effet, l'axiome d'induction énonce que  $\mathbb{N}$  est un minorant de  $\mathcal{N}$ . De plus, nous savons maintenant que  $1 \in \mathbb{N}$ , donc la fermeture de  $\mathbb{N}$  sous l'addition implique que  $\mathbb{N}$  est un élément de  $\mathcal{N}$ . C'est donc son plus petit élément.

Cela signifie que tous les entiers qu'on peut construire en partant de l'entier 1, et en n'utilisant que l'opération « +1 », est exactement  $\mathbb{N}$ . En particulier, tout entier positif s'écrit  $1 + 1 + \dots + 1$  (un certain nombre de fois).

**Méthode de preuve 3.33** (Raisonnement par induction, ou raisonnement par récurrence). Pour tout  $n \in \mathbb{N}$ , on considère une assertion  $P(n)$ . Alors «  $\forall n \in \mathbb{N}, P(n)$  » est équivalente à

$$P(1) \wedge \left( \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1) \right).$$

Ainsi, pour montrer «  $\forall n \in \mathbb{N}, P(n)$  », le raisonnement par induction consiste à

- (initialisation) montrer  $P(1)$  ;
- (étape d'induction) montrer que, pour un entier positif  $n$  quelconque, si  $P(n)$  est vraie (hypothèse d'induction), alors  $P(n+1)$  est vraie.

**Preuve.** Implication directe. Supposons «  $\forall n \in \mathbb{N}, P(n)$  » et montrons  $P(1) \wedge \left( \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1) \right)$ . D'une part,  $P(1)$  est vraie (car  $1 \in \mathbb{N}$ ). D'autre part, si  $n \in \mathbb{N}$ , alors  $n+1 \in \mathbb{N}$  par fermeture de  $\mathbb{N}$  sous l'addition, donc  $P(n)$  et  $P(n+1)$  sont vraies, donc l'implication  $P(n) \Rightarrow P(n+1)$  est vraie. Ceci achève la preuve.

Implication indirecte. Supposons  $P(1) \wedge \left( \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1) \right)$ . Alors l'ensemble  $A = \{n \in \mathbb{N} \mid P(n)\}$  vérifie :

- $1 \in A$  ;
- $\forall n \in \mathbb{Z}, n \in A \Rightarrow n+1 \in A$ .

Par l'axiome B.2, on obtient  $\mathbb{N} \subset A$ . Or  $A$  est un ensemble d'entiers positifs, d'où  $A = \mathbb{N}$ , c'est-à-dire qu'on a  $P(n)$  pour tout  $n \in \mathbb{N}$ .  $\square$

Le raisonnement par induction peut être vu intuitivement comme une réaction en chaîne.

- $P(1)$  est vraie ;
- $P(1)$  est vraie et  $P(1) \Rightarrow P(2)$ , donc  $P(2)$  est vraie (*modus ponens*, cf. proposition 1.33 du chapitre 1) ;
- $P(2)$  est vraie et  $P(2) \Rightarrow P(3)$ , donc  $P(3)$  est vraie ;
- et ainsi de suite.

Ne jamais écrire « et ainsi de suite » (comme ci-dessus) dans une preuve ! Si on a une idée de preuve en « et ainsi de suite », c'est qu'il y a moyen de faire une preuve par induction. Explications plus précises dans l'exemple 3.34.

Nous allons donner des exemples illustrant le raisonnement par induction. Ces exemples demandent cependant la définition de notions que nous introduirons dans le prochain chapitre.

Pour  $a \in \mathbb{Z}$ , on définit  $a^n$ , pour  $n \in \mathbb{N}$ , de la manière suivante :

- $a^1 = a$  ;
- étant donné  $n \in \mathbb{N}$ , si  $a^n$  a été défini, alors  $a^{n+1} = a^n \cdot a$ .

On peut aussi définir  $a^0 = 1$  afin d'élargir la définition de  $a^n$  aux entiers  $n$  dans  $\mathbb{N} \cup \{0\}$ . Noter que la relation de récurrence  $a^{n+1} = a^n \cdot a$  est alors vraie pour  $n = 0$ .

Enfin, donnons des noms aux entiers positifs. On connaît déjà 1. On a aussi défini  $2 = 1 + 1$ . On définit ensuite  $3 = 2 + 1$ , puis  $4 = 3 + 1$ , etc.

**Exemple 3.34.** Soit  $a$  un entier. Montrons que pour tout  $n \in \mathbb{N}$ ,  $a^n$  est bien défini et est un entier.

- **Raisonnement non rigoureux :**  $a$  est un entier. Puis  $a^2$  est défini comme la multiplication de  $a$  avec lui-même donc c'est un entier. Puis  $a^3$  est défini comme le produit de l'entier  $a^2$  avec l'entier  $a$ , donc  $a^3$  est un entier, et ainsi de suite.

Le « et ainsi de suite » suggère qu'il s'agit d'une réaction en chaîne. Une preuve par induction est donc cachée. Noter que le raisonnement non rigoureux que nous venons d'écrire contient quand même les idées essentielles pour la preuve rigoureuse qui va suivre, il est bon de commencer comme cela au brouillon pour comprendre globalement à quoi va ressembler l'étape d'induction.

- **Raisonnement rigoureux :** Par induction, montrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n) = \ll a^n \text{ est bien défini et est un entier } \gg^1$ .

**Initialisation :** On a  $a^1 = a$  par définition. Par hypothèse,  $a$  est un entier. D'où  $P(1)$ .

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . Par hypothèse,  $a$  est un entier, et par  $P(n)$ ,  $a^n$  est aussi un entier. La multiplication étant une application de  $\mathbb{Z}^2$  vers  $\mathbb{Z}$ , le produit des deux, c'est-à-dire  $a^{n+1}$ , est donc bien définie et c'est un entier. D'où  $P(n+1)$ .

D'où le résultat par induction.

On peut également montrer que si  $a \in \mathbb{N}$ , alors pour tout  $n \in \mathbb{N}$ ,  $a^n \in \mathbb{N}$  (l'étape d'induction applique la fermeture sous la multiplication).

**Exemple 3.35.** Démontrer que pour tout  $n \in \mathbb{N}$ , l'entier  $11^n - 6$  est divisible par 5.

Par induction, démontrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n) = \ll 11^n - 6 \text{ est divisible par } 5 \gg$ .

**Initialisation :**  $11^1 - 6 = 11 - 6 = 5$ . La propriété  $P(1)$  est vraie.

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . Par hypothèse d'induction, il existe un entier  $k$  tel que  $11^n - 6 = 5k$ , c'est-à-dire  $11^n = 5k + 6$ . On a donc

$$11^{n+1} - 6 = 11 \cdot 11^n - 6 = 11 \cdot (5k + 6) - 6 = 5 \cdot (11k) + 60 = 5 \cdot (11k + 12).$$

D'où  $P(n+1)$ .

D'où le résultat par induction.

**Exercice 3.36.** Montrons que pour tout  $n \in \mathbb{Z}$ ,  $n^2 + 1 \geq n$ .

**Exercice 3.37** (Inégalité de Bernoulli). Soit  $x \geq -1$  un réel. Montrer que pour tout  $n \in \mathbb{N}$ ,  $(1+x)^n \geq 1+nx$ .<sup>a</sup>

<sup>a</sup>. Ce sera plus généralement vrai pour un réel  $x \geq -1$ , avec la même preuve, mais nous n'avons pas encore vu les nombres réels...

Nous allons maintenant en déduire des propriétés cruciales sur la relation d'ordre  $\leq$  sur  $\mathbb{Z}$ .

1. Il est important de bien formuler la propriété  $P(n)$ , cela évite des erreurs de raisonnement

**Proposition 3.38.**  $\forall n \in \mathbb{N}, n \geq 1$ .

Ainsi, on a  $\mathbb{N} = \{a \in \mathbb{N} \mid a > 0\} = \{a \in \mathbb{N} \mid a \geq 1\}$ .

**Preuve.** Par induction, démontrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n) = \ll n \geq 1 \gg$ .

**Initialisation :**  $P(1)$  est vraie par réflexivité.

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons que  $P(n)$  est vraie et démontrons  $P(n+1)$ . D'une part, on a  $n \geq 1$  par hypothèse d'induction. D'autre part, on a  $1 \geq 0$  par le corollaire 3.27 et la proposition 3.25. La propriété 1 de la proposition 3.31 donne donc  $n+1 \geq 1+0$ , c'est-à-dire  $n+1 \geq 1$ , d'où  $P(n+1)$ .

D'où le résultat par induction.  $\square$

**Corollaire 3.39.**

1. Pour tous entiers  $n$  et  $a$ , si  $a > n$ , alors  $a \geq n+1$ .
2. Pour tous entiers  $n$  et  $a$ , si  $n \leq a \leq n+1$ , alors  $a = n$  ou  $a = n+1$ . Autrement dit, on ne peut pas avoir  $n < a < n+1$ .
3. Pour tout entier  $n$ , si  $A = \{a \in \mathbb{Z} \mid a \geq n\}$ , alors  $A \cup \{n-1\} = \{a \in \mathbb{Z} \mid a \geq n-1\}$  et  $A - \{n\} = \{a \in \mathbb{Z} \mid a \geq n+1\}$ .

**Exemple 3.40.**

1.  $\mathbb{N} - \{1\} = \{a \in \mathbb{Z} \mid a \geq 2\}$ .
2.  $\mathbb{N} - \{1, 2\} = \{a \in \mathbb{Z} \mid a \geq 3\}$ .
3.  $\mathbb{N} \cup \{0\} = \{a \in \mathbb{Z} \mid a \geq 0\}$ .
4.  $\mathbb{N} \cup \{0, -1\} = \{a \in \mathbb{Z} \mid a \geq -1\}$ .
5.  $\mathbb{N} \cup \{0, -1, -2\} = \{a \in \mathbb{Z} \mid a \geq -2\}$ .

**Preuve.**

1. Si  $n$  et  $a$  sont deux entiers tels que  $a > n$ , alors  $a - n \in \mathbb{N}$  (par définition), et la proposition 3.38 donne  $a - n \geq 1$ . Donc  $a \geq n+1$ .
2. Soient  $n$  et  $a$  deux entiers vérifiant  $n \leq a \leq n+1$ . Montrons que  $a = n$  ou  $a = n+1$ . Supposons  $a \neq n$  et montrons  $a = n+1$ . On a donc  $a > n$ , et on obtient par la propriété précédente que  $a \geq n+1$ . Or on sait par hypothèse que  $a \leq n+1$ , donc l'antisymétrie donne  $a = n+1$ .
3. Soit  $n$  un entier et  $A = \{a \in \mathbb{Z} \mid a \geq n\}$ . Soit  $k \in A \cup \{n-1\}$ . Ou bien  $k \in A$ , dans ce cas  $k \geq n \geq n-1$  (car  $-1 < 0$ ). Ou bien  $k = n-1$ , ce qui donne trivialement  $k \geq n-1$ . Réciproquement, supposons qu'un entier  $k$  vérifie  $k \geq n-1$ . Ou bien  $k = n-1$ , ou bien le contraire et la première propriété donne  $k \geq n$ , c'est-à-dire  $k \in A$ . D'où l'égalité concernant l'ensemble  $A \cup \{n-1\}$ .

Soit  $k \in A - \{n\}$ . Alors  $k \geq n$  et  $k \neq n$ , c'est-à-dire  $k > n$ . La première propriété nous permet donc d'obtenir  $k \geq n+1$ . Réciproquement, si  $k \geq n+1$ , alors  $k \neq n$  (sinon on obtient  $1 \leq 0$ ) et  $k \geq n$  (car  $n+1 \geq n$ ), autrement dit  $k \in A - \{n\}$ . D'où l'égalité concernant l'ensemble  $A - \{n\}$ .  $\square$

**Exercice 3.41.** On définit une relation  $\sim$  sur  $\mathbb{N}^2$  par : pour tout  $(n, m), (n', m') \in \mathbb{N}^2$ ,  $(n, m) \sim (n', m')$  si et seulement si  $n + m = n' + m'$ .

1. Montrer que  $\sim$  est une relation d'équivalence.
2. Déterminer les classes d'équivalence de  $(1, 1)$ , de  $(2, 1)$  et de  $(3, 1)$ . Les dessiner, en représentant  $\mathbb{N} \times \mathbb{N}$  dans le plan, avec la première coordonnée en abscisse et la seconde en ordonnée.
3. Montrer que l'ensemble  $\{(a, 1) \mid a \in \mathbb{N}\}$  est un système de représentants pour cette relation d'équivalence. En particulier, décrire toutes les classes, les représenter dans le plan, et montrer que pour tout  $a \in \mathbb{N}$ , la classe de  $(a, 1)$  est en bijection avec l'ensemble  $\{1, \dots, a\}$ .
4. En s'aidant de la partition en classes d'équivalence de  $\mathbb{N}^2$ , construire une bijection entre  $\mathbb{N}$  et  $\mathbb{N}^2$ .

On en déduit maintenant l'une des propriétés cruciales de  $\mathbb{N}$ .

**Théorème 3.42** (Principe du bon ordre). *Tout sous-ensemble non vide de  $\mathbb{N}$  admet un plus petit élément.*

**Preuve.** Par induction, démontrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n)$  = « tout sous-ensemble de  $\mathbb{N}$  contenant un élément  $\leq n$  admet un plus petit élément ».

**Initialisation :** Soit  $A$  un sous-ensemble de  $\mathbb{N}$  contenant un élément  $\leq 1$ . Par la proposition 3.38, cet élément est  $\geq 1$ , donc il s'agit de l'entier 1 par antisymétrie. L'entier 1 appartient donc à  $A$  et vérifie  $\forall a \in A, a \geq 1$  (conséquence de la proposition 3.38). Donc 1 est le plus petit élément de  $A$ . D'où  $P(1)$ .

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . Soit  $A$  un sous-ensemble de  $\mathbb{N}$  contenant un élément  $\leq n+1$ , noté  $x$ . Si  $A$  contient un élément  $\leq n$ , alors l'hypothèse d'induction nous dit que  $A$  admet un plus petit élément. Supposons maintenant que l'ensemble  $A$  ne contient aucun élément  $\leq n$ . Le corollaire 3.39 nous dit alors que tout élément de  $A$  est plus grand que  $n$ . De plus, comme l'élément particulier  $x$  est  $\leq n+1$ , on obtient  $x = n+1$ . Ainsi  $n+1$  est le plus petit élément de  $A$ . D'où  $P(n+1)$ .

Ainsi, par induction, toutes les propriétés  $P(n)$  sont vraies.

Il reste à conclure la preuve du théorème. Soit  $A$  un sous-ensemble non vide de  $\mathbb{N}$ . Par hypothèse, il existe un élément  $n$  dans  $A$ . Ainsi, la propriété  $P(n)$  nous permet d'obtenir que  $A$  admet un plus petit élément.  $\square$

**Corollaire 3.43.** *Tout sous-ensemble minoré de  $\mathbb{Z}$  admet un plus petit élément.*

L'énoncé est faux pour un sous-ensemble minoré de  $\mathbb{R}$ . Par exemple, l'ensemble  $\mathbb{R}_{>0}$  des réels strictement plus grand que 0 est minoré par 0, mais on verra que pour tout  $a \in \mathbb{R}_{>0}$ , il existe toujours  $a' \in \mathbb{R}_{>0}$  tel que  $a' < a$ .

**Preuve.** Soit  $A$  sous-ensemble de  $\mathbb{Z}$ , et  $b \in \mathbb{Z}$  tel que pour tout  $a \in A$ ,  $a \geq b$ . Considérons l'ensemble  $A - b + 1 = \{a - b + 1 \mid a \in A\}$ . Pour tout  $a \in A$ ,  $a \geq b$ , donc  $a > b - 1$ , c'est-à-dire  $a - b + 1 > 0$ . Ainsi  $A - b + 1$  est un sous-ensemble de  $\mathbb{N}$ . Par le principe du bon ordre,  $A - b + 1$  admet un plus petit élément, noté  $x$ . C'est un élément de  $A - b + 1$ , donc il existe  $y \in A$  tel que  $x = y - b + 1$ . Le fait que  $x$  soit le plus petit élément

de  $A - b + 1$  implique que pour tout  $a \in A$ ,  $a - b + 1 \geq x$ , c'est-à-dire  $a - b + 1 \geq y - b + 1$ , c'est-à-dire  $a \geq y$ . On a donc montré que  $y$  est un élément de  $A$  plus petit que tous les éléments de  $A$ . Donc  $y$  est le plus petit élément de  $A$ .  $\square$

**Corollaire 3.44.** *Tout sous-ensemble majoré de  $\mathbb{Z}$  admet un plus grand élément.*

**Preuve.** Soit  $A$  un ensemble majoré. On considère alors l'ensemble  $-A = \{-a \mid a \in A\}$ . On affirme alors qu'il est minoré. En effet, si  $k \in \mathbb{Z}$  est un majorant de  $A$ , alors pour tout  $a \in A$ , on a  $a \leq k$ , c'est-à-dire  $-a \geq -k$ , donc  $-k$  est un minorant de  $-A$ .

Par le corollaire précédent,  $-A$  admet un plus petit élément, noté  $x$ . On affirme alors que  $-x$  est le plus grand élément de  $A$ . En effet, on a tout d'abord  $-x \in A$  ( $x$  s'écrit  $-a$  pour un certain  $a \in A$ , donc  $-x = a \in A$ ), et enfin pour tout  $a \in A$ , on a  $x \leq -a$ , c'est-à-dire  $-x \geq a$ , donc  $-x$  est un majorant de  $A$ . C'est donc le plus grand élément.  $\square$

Enfin, les propriétés supplémentaires sur  $\leq$  que nous venons d'obtenir permettent également d'obtenir la propriété suivante.

**Proposition 3.45.** *Soient  $a \in \mathbb{Z}$  un entier non nul et  $b \in \mathbb{N}$  tels que  $b \mid a$ . Alors*

1. *si  $a > 0$ , alors  $a \geq b$ ,*
2. *si  $a < 0$ , alors  $a \leq -b$ .*

*Ainsi, si  $a$  et  $b$  sont dans  $\mathbb{N}$ , et si  $a \mid b$  et  $b \mid a$ , alors  $a = b$ .*

Dans la dernière phrase de l'énoncé, l'hypothèse «  $a, b \in \mathbb{N}$  » est important. En effet, on a  $a \mid -a$  et  $-a \mid a$ , pourtant  $a \nmid a$  dès que  $a$  est non nul.

La dernière phrase de l'énoncé nous dit alors que  $\mid$  est réflexive sur  $\mathbb{N}$ . En reprenant l'exercice 3.12, on obtient donc que c'est une relation d'ordre sur  $\mathbb{N}$ . Elle n'est pas totale (par exemple  $2 \nmid 3$  et  $3 \nmid 2$ ).

**Preuve.** Si  $b \mid a$ , alors on dispose de  $c \in \mathbb{Z}$  tel que  $a = bc$ .

Supposons d'abord  $a > 0$ . Par la proposition 3.30, on sait que  $c$  est un élément de  $\mathbb{N}$ , c'est-à-dire  $c \geq 1$ . L'entier  $b$  étant positif, on a donc  $bc > b$  (propriété 3 de la proposition 3.31), c'est-à-dire  $a > b$ .

Supposons enfin  $a < 0$ . On se ramène au premier cas en remarquant que  $b$  divise l'entier positif  $-a$  (car  $-a = b \cdot (-c)$ ). Ainsi  $b \leq -a$ , c'est-à-dire  $-b \geq a$ .

Pour la seconde partie de l'énoncé, si maintenant  $a$  et  $b$  sont de même signe, et si  $a \mid b$  et  $b \mid a$ , alors on vient de démontrer que cela implique  $a \leq b$  et  $b \leq a$ , donc  $a = b$ .  $\square$

Le raisonnement par induction admet quelques variantes. En voici une première, permettant de démontrer des énoncés du type «  $\forall n \geq k, P(n)$  », où  $k$  est un entier non nécessairement égal à 1 (rappelons la proposition 3.38 qui nous dit que pour  $k = 1$ , on retrouve l'énoncé «  $\forall n \in \mathbb{N}, P(n)$  »).

**Notation :** Rappelons l'abus de notation «  $\forall n \geq k$  » qui signifie «  $\forall n \in \{a \in \mathbb{Z} \mid a \geq k\}$  ». À n'utiliser que lorsque le contexte est clair (dans un autre contexte, cela pourrait par exemple signifier «  $\forall n \in \{a \in \mathbb{R} \mid a > k\}$  »).

**Méthode de preuve 3.46.** Soit  $k$  un entier. Pour tout  $n \geq k$ , on considère une assertion  $P(n)$ . Alors «  $\forall n \geq k, P(n)$  » est équivalente à

$$P(k) \wedge \left( \forall n \geq k, P(n) \Rightarrow P(n+1) \right).$$

Ainsi, pour montrer «  $\forall n \geq k, P(n)$  », le raisonnement par induction consiste à

- (initialisation) montrer  $P(k)$  ;
- (étape d'induction) montrer que, pour un entier  $n \geq k$  quelconque, si  $P(n)$  est vraie (hypothèse d'induction), alors  $P(n+1)$  est vraie.

**Preuve.** Il s'agit en fait du raisonnement par induction classique avec un décalage d'indice. En posant, pour tout  $m \in \mathbb{N}$ ,  $Q(m) = P(m+k-1)$ , on se ramène au raisonnement par induction classique.  $\square$

**Exemple 3.47.** Dans l'exemple 3.34, on pouvait aussi montrer la propriété pour tout  $n \geq 0$ , de même pour l'exemple 3.35.

Les deux variantes du raisonnement par induction qui suivent sont nécessaires lorsque  $P(n)$  ne suffit pas pour impliquer  $P(n+1)$ .

**Méthode de preuve 3.48** (Raisonnement par double induction). Pour tout  $n \in \mathbb{N}$ , on considère une assertion  $P(n)$ . Alors «  $\forall n \in \mathbb{N}, P(n)$  » est équivalente à

$$\left( P(1) \wedge P(2) \right) \wedge \left( \forall n \geq 1, (P(n) \wedge P(n+1)) \Rightarrow P(n+2) \right).$$

Ainsi, pour montrer «  $\forall n \in \mathbb{N}, P(n)$  », le raisonnement par double induction consiste à

- (initialisation) montrer  $P(1)$  et  $P(2)$  ;
- (étape d'induction) montrer que, pour un entier  $n \in \mathbb{N}$  quelconque, si  $P(n)$  et  $P(n+1)$  sont vraies (hypothèse d'induction), alors  $P(n+2)$  est vraie.

**Preuve.** Il s'agit du raisonnement par induction classique avec  $Q(m) = P(m) \wedge P(m+1)$  pour tout  $m \in \mathbb{N}$ , en remarquant que les assertions

$$(P(m) \wedge P(m+1)) \Rightarrow (P(m+1) \wedge P(m+2))$$

$$\text{et } (P(m) \wedge P(m+1)) \Rightarrow P(m+2)$$

sont équivalentes.  $\square$

**Méthode de preuve 3.49** (Raisonnement par induction forte). Pour tout  $n \in \mathbb{N}$ , on considère une assertion  $P(n)$ . Alors «  $\forall n \in \mathbb{N}, P(n)$  » est équivalente à

$$P(1) \wedge \left( \forall n \in \mathbb{N}, (P(1) \wedge P(2) \wedge \dots \wedge P(n)) \Rightarrow P(n+1) \right).$$

Ainsi, pour montrer «  $\forall n \in \mathbb{N}, P(n)$  », le raisonnement par induction forte consiste à

- (initialisation) montrer  $P(1)$  ;

- (étape d'induction) montrer que, pour un entier  $n \in \mathbb{N}$  quelconque, si  $P(1), P(2), \dots, P(n)$  sont vraies (hypothèse d'induction), alors  $P(n+1)$  est vraie.

**Preuve.** Il s'agit du raisonnement par induction classique avec  $Q(m) = \mathcal{P}(1) \wedge \mathcal{P}(2) \wedge \dots \wedge \mathcal{P}(m)$  pour tout  $m \in \mathbb{N}$ , en remarquant les assertions

$$\left( \mathcal{P}(1) \wedge \mathcal{P}(2) \wedge \dots \wedge \mathcal{P}(m) \right) \Rightarrow \left( \mathcal{P}(2) \wedge \mathcal{P}(3) \wedge \dots \wedge \mathcal{P}(m+1) \right)$$

$$\text{et } \left( \mathcal{P}(1) \wedge \mathcal{P}(2) \wedge \dots \wedge \mathcal{P}(m) \right) \Rightarrow P(m+1)$$

sont équivalentes. □

Voici un exemple de raisonnement par double induction.

**Exemple 3.50.** On définit la suite de Fibonacci  $(f_n)_{n \in \mathbb{N}}$  de la manière suivante :

- $f_1 = f_2 = 1$  ;
- pour tout  $n \in \mathbb{N}$ ,  $f_{n+2} = f_{n+1} + f_n$ .

On pose

$$a = \frac{1 + \sqrt{5}}{2} \text{ et } b = \frac{1 - \sqrt{5}}{2}.$$

Montrons que pour tout  $n \in \mathbb{N}$ ,

$$f_n = \frac{1}{\sqrt{5}} (a^n - b^n).$$

Avant de le montrer, vérifier (exercice) que  $a$  et  $b$  vérifient

$$a^2 = a + 1 \text{ et } b^2 = b + 1.$$

Par double induction, montrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n) = \ll f_n = \frac{1}{\sqrt{5}} (a^n - b^n) \gg$ .

**Initialisation :** Montrons  $P(1)$  et  $P(2)$ . À vérifier, exercice.

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et  $P(n+1)$ , et démontrons  $P(n+2)$ .

On sait que  $f_{n+2} = f_{n+1} + f_n$ , et l'hypothèse d'induction nous donne les expressions de  $f_n$  et  $f_{n+1}$ . On a ainsi

$$\begin{aligned} f_{n+2} &= \frac{1}{\sqrt{5}} (a^{n+1} - b^{n+1} + a^n - b^n) \\ &= \frac{1}{\sqrt{5}} (a^n(a+1) - b^n(b+1)) \\ &= \frac{1}{\sqrt{5}} (a^n \cdot a^2 - b^n \cdot b^2) \\ &= \frac{1}{\sqrt{5}} (a^{n+2} - b^{n+2}), \end{aligned}$$

d'où  $P(n+2)$ .

**Exercice 3.51.** Soit  $(f_n)_{n \in \mathbb{N}}$  la suite de Fibonacci définie dans l'exemple ci-dessus. Montrer que pour tout  $n \in \mathbb{N}$ ,  $f_n$  est bien défini et est un entier positif. Noter que cela ne saute pas

aux yeux que  $\frac{1}{5} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right)$  soit un entier.

Voici enfin un exemple de raisonnement par induction forte, où le raisonnement par double induction n'est pas suffisant.

**Exemple 3.52.** Un nombre premier est un entier positif  $p$  vérifiant :  $p \neq 1$ , et si  $a$  et  $b$  sont des entiers positifs tels que  $p = ab$ , alors  $p = a$  ou  $p = b$ . Autrement dit, les seuls diviseurs positifs de  $p$  sont 1 et lui-même.

Montrons que tout entier  $\geq 2$  s'écrit comme produit de nombres premiers. Par induction forte, montrons pour tout  $n \geq 2$  la propriété  $P(n)$  = «  $n$  s'écrit comme produit de nombres premiers ».

**Initialisation :** 2 est un nombre premier. En effet, si  $a \in \mathbb{N}$  est un diviseur de 2, alors  $a \leq 2$  (proposition 3.45). Ainsi  $a$  ne peut valoir que 1 ou 2, d'où le fait que 2 est premier. Ainsi 2 s'écrit comme un produit avec un seul facteur, lui-même. D'où  $P(2)$ .

**Étape d'induction :** Soit  $n \geq 2$ . Supposons  $P(1), \dots, P(n)$  et montrons  $P(n+1)$ . Si  $n+1$  est premier, alors c'est gagné (comme pour l'étape d'initialisation). Sinon, il existe par définition un entier positif  $a$ , différent de 1 et  $n+1$ , qui divise  $n+1$ . Cela signifie qu'il existe  $b \in \mathbb{N}$  tel que  $n+1 = ab$ . Remarquons que  $b$  ne vaut ni 1 (sinon  $a = n+1$ ), ni  $n+1$  (sinon  $a = 1$ ), et c'est un diviseur de  $n+1$ . Donc  $a$  et  $b$  sont  $\leq n$  (proposition 3.45). Par  $P(a)$  et  $P(b)$ , on peut écrire  $a$  et  $b$  comme produits de nombre premiers. Le produit entre deux produits de nombres premiers est un produit de nombres premiers, donc on a démontré la propriété pour  $n+1$ .

D'où le résultat par induction forte.

Voici une dernière variante, assez particulière, qui s'applique quand on n'a qu'un nombre fini de propriétés à démontrer. On trouvera des exemples dans le chapitre précédent.

**Notation :** «  $\forall 1 \leq n \leq j$  » signifie «  $\forall n \in \{k \in \mathbb{Z} \mid 1 \leq k \leq j\}$  ». L'ensemble  $\{k \in \mathbb{Z} \mid 1 \leq k \leq j\}$  sera plutôt noté  $\{1, \dots, j\}$ .

**Méthode de preuve 3.53** (Raisonnement par induction finie). Soit  $j$  un entier positif. Pour tout entier  $n$  tel que  $1 \leq n \leq j$ , on considère une assertion  $P(n)$ . Alors «  $\forall 1 \leq n \leq j, P(n)$  » est équivalente à

$$P(1) \wedge \left( \forall 1 \leq n \leq j-1, P(n) \Rightarrow P(n+1) \right).$$

Ainsi, pour montrer «  $\forall 1 \leq n \leq j, P(n)$  », le raisonnement par induction finie consiste à

- (initialisation) montrer  $P(1)$  ;
- (étape d'induction) montrer que, pour un entier  $n$  quelconque dans  $\{1, \dots, j-1\}$ , si  $P(n)$  est vraie (hypothèse d'induction), alors  $P(n+1)$  est vraie.

Dans l'étape d'induction, il faut prendre  $n$  plus petit que  $j-1$ , sinon  $P(n+1)$  n'est pas défini.

**Preuve.** Il s'agit en fait du raisonnement par induction classique avec  $Q(m) = P(m)$  si  $1 \leq m \leq j$ ,  $Q(m) = \text{VRAI}$  si  $m \geq j+1$ . □

La proposition 3.56 ci-dessous se démontre par exemple avec un raisonnement par induction finie.

On a montré que certains ensembles infinis comme  $\mathbb{N}$  admettent un plus petit élément. Mais on ne s'est même pas intéressé au cas plus simple des sous-ensembles finis de  $\mathbb{N}$ , ou de manière générale des ensembles finis munis d'une relation d'ordre totale. Tout d'abord, définissons rigoureusement les ensembles finis.

**Définition 3.54.** On dit qu'un ensemble  $E$  est *fini* s'il est vide ou s'il existe  $n \in \mathbb{N}$  et une surjection  $\{1, \dots, n\} \rightarrow E$ . Dans le cas contraire, on dit que  $E$  est *infini*.

**Exemple 3.55.** Pour tout  $n \in \mathbb{N}$ , l'ensemble  $\{1, \dots, n\}$  est fini (la fonction identité sur  $\{1, \dots, n\}$  est surjective).

**Proposition 3.56.** Soit  $E$  un ensemble fini, non vide, muni d'une relation d'ordre totale qu'on note  $\leq$ . Alors  $E$  admet un plus petit élément et un plus grand élément.

**Preuve.** Soit  $n \in \mathbb{N}$  et  $f: \{1, \dots, n\} \rightarrow E$  une surjection.

Par induction finie, montrons pour tout  $1 \leq k \leq n$  la propriété  $P(k) = \llcorner$  l'ensemble  $\{f(1), \dots, f(k)\} \llcorner$ . La proposition sera alors une conséquence immédiate de la propriété  $P(n)$  puisque  $\{f(1), \dots, f(n)\} = E$ .

**Initialisation :**  $f(1)$  se majore et se minore lui-même, donc c'est le plus petit et le plus grand élément de  $\{f(1)\}$ .

**Étape d'induction :** Soit  $1 \leq k \leq n - 1$ . On suppose  $P(k)$  et on veut montrer  $P(k + 1)$ . Par  $P(k)$ , on sait que  $\{f(1), \dots, f(k)\}$  admet un plus grand élément, noté  $M$ . La relation d'ordre étant totale, on a  $f(k + 1) \leq M$  ou  $f(k + 1) \geq M$ . Si  $f(k + 1) \leq M$ , alors  $M$  est le plus grand élément de  $\{f(1), \dots, f(k), f(k + 1)\}$ . Si  $f(k + 1) \geq M$ , alors  $f(k + 1)$  est le plus grand élément de  $\{f(1), \dots, f(k), f(k + 1)\}$ . Dans tous les cas, on a montré que  $\{f(1), \dots, f(k), f(k + 1)\}$  admet un plus grand élément. On montre de la même manière que cet ensemble admet un plus petit élément. D'où  $P(k + 1)$ .  $\square$

Soit  $E$  un ensemble, et  $\leq$  une relation d'ordre sur  $E$ . On suppose que tout sous-ensemble non vide de  $E$  admet un plus petit élément et un plus grand élément. Montrer que  $E$  est un ensemble fini.

## 3.5 Problèmes

### 3.5.1 Problème 1

On cherche à montrer que les fonctions  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  vérifiant  $f(n + m) = f(n) + f(m)$  pour tout  $n, m \in \mathbb{Z}$ , sont exactement les  $n \in \mathbb{Z} \mapsto an \in \mathbb{Z}$  pour  $a \in \mathbb{Z}$ .

1. Soit  $a \in \mathbb{Z}$ . Montrer que la fonction  $f: n \in \mathbb{Z} \mapsto an \in \mathbb{Z}$  satisfait  $f(n + m) = f(n) + f(m)$  pour tout  $n, m \in \mathbb{Z}$ .

Soit  $f$  une fonction vérifiant  $f(n + m) = f(n) + f(m)$  pour tout  $n, m \in \mathbb{Z}$ .

2. Montrer que  $f(0) = 0$ .
3. Montrer que pour tout  $n \in \mathbb{Z}$ ,  $f(-n) = -f(n)$ .

4. Montrer que pour tout  $n \in \mathbb{N}$ ,  $f(n) = nf(1)$ .
5. Conclure

### 3.5.2 Problème 2

Un sous-monoïde de  $(\mathbb{Z}_{\geq 0}, +)$  est un sous-ensemble  $A \subset \mathbb{Z}_{\geq 0}$  vérifiant

- $0 \in A$ ;
- $\forall x, y \in A, x + y \in A$ .

Soient  $n \in \mathbb{N}$  et  $x_1, \dots, x_n \in \mathbb{Z}_{\geq 0}$ . On considère la relation d'ordre d'inclusion sur  $\mathcal{P}(\mathbb{Z}_{\geq 0})$ . Soit  $\mathcal{M}$  l'ensemble des sous-monoïdes de  $(\mathbb{Z}_{\geq 0}, +)$  dont  $x_1, \dots, x_n$  sont des éléments. Montrer que l'ensemble  $\{x_1k_1 + \dots + x_nk_n \mid k_1, \dots, k_n \in \mathbb{Z}_{\geq 0}\}$  est le plus petit élément de  $\mathcal{M}$ .

# Chapitre 4

## Séries finies

Ce chapitre aborde des outils fondamentaux de calcul. Comme nous venons d'introduire les entiers et que nous ne connaissons pas encore les nombres réels, nous ne travaillerons qu'avec des entiers. Cependant, la plupart des énoncés s'étendent de manière élémentaire au cas des nombres réels, nous le signalerons avec un

Ce sera encore valable dans  $\mathbb{R}$  ! [suivi des précisions nécessaires]

à la fin des énoncés concernés.

### 4.1 Préliminaires

**Fractions.** Pour l'instant, nous introduisons la notion de fraction dans un cas simple : si  $a$  et  $b$  sont des entiers, tels que  $b \mid a$  et  $b$  est non nul, alors  $\frac{a}{b}$  est défini comme étant l'unique entier  $c$  tel que  $a = bc$  (l'unicité vient du fait que  $b \neq 0$ ). La notation  $\frac{a}{b}$  n'est pour l'instant valable que lorsque  $b \mid a$ , nous élargirons sa définition plus tard.

**Exercice 4.1.** Avec la définition de fractions donnée ci-dessus, vérifier les règles de calcul suivantes. Pour tous  $a, b, c, d \in \mathbb{Z}$  tels que  $b$  et  $d$  sont non nuls,  $b \mid a$  et  $d \mid c$ , on a

1.  $\frac{a}{b} = 0 \iff a = 0$  ;
2.  $\frac{ad}{d} = a$  ;
3.  $bd$  divise  $ad + bc$ , et  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$  ;
4.  $bd$  divise  $ac$ , et  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$  ;
5. Si  $a \neq 0$ , alors  $\frac{a}{b}$  divise  $a$  et  $\frac{a}{\frac{a}{b}} = b$ .

**Suites.** Soient  $A$  et  $B$  des ensembles. Une *famille*  $(x_n)_{n \in A}$  d'éléments de  $B$ , indexée sur  $A$ , n'est autre que la fonction  $n \in A \mapsto x_n \in B$ .

Une *suite (infinie)*  $(x_n)_{n \in A}$  est une famille où  $A$  est de la forme  $\{n \in \mathbb{Z} \mid n \geq m\}$  pour un certain entier  $m$ , et  $B$  est un ensemble quelconque qu'on précisera.

On considérera souvent  $A = \mathbb{N}$  (entiers  $\geq 1$ ) ou  $A = \mathbb{Z}_{\geq 0}$  (entiers  $\geq 0$ ). Si  $A = \{n \in \mathbb{Z} \mid n \geq m\}$ , alors la famille pourra également être notée  $(x_n)_{n \geq m}$ , ou  $(x_n)_{n=m}^{\infty}$ , ou  $(x_m, x_{m+1}, x_{m+2}, \dots)$ . Si  $B$  vaut  $\mathbb{Z}$  (resp.  $\mathbb{N}$ , resp.  $\mathbb{R}$ ), on parlera de suite d'entiers (resp. d'entiers positifs, resp. de réels).

On parle de *suite finie* si  $A$  est de la forme  $\{n \in \mathbb{Z} \mid m \leq n \leq j\}$  pour certains entiers  $m$  et  $j$  tels que  $m \leq j$ . La famille pourra également être notée  $(x_n)_{m \leq n \leq j}$ , ou  $(x_n)_{n=m}^j$ , ou  $(x_m, \dots, x_j)$ .

Avec ces notations, on perd de vue le fait qu'une suite est une fonction, afin de donner l'idée d'une liste de termes. Quand on écrit  $(x_n)_{n \in \mathbb{N}}$ , la variable muette  $n$  peut être vue comme une variable temporelle. Dans le chapitre 7, on s'intéressera notamment au comportement de  $x_n$  au temps long, c'est-à-dire quand  $n$  est de plus en plus grand.

**Attention.** Comme nous l'avons souvent déjà dit, le «  $n$  » quand on écrit  $(x_n)_{n=m}^j$  ou  $(x_n)_{n=m}^\infty$  n'est pas une variable qu'on a déclarée. C'est une variable muette, simplement une notation pour exprimer le fait de parcourir l'ensemble des entiers entre  $m$  et  $j$ , ou l'ensemble des entiers plus grands ou égaux à  $m$ . On aurait pu écrire  $(x_i)_{i=m}^j$  ou  $(x_y)_{y=m}^j$  ou  $(x_\Psi)_{\Psi=m}^j$  (mais ne surtout pas utiliser des symboles de variables déjà déclarées, comme  $m$ ,  $j$ , voire la lettre  $x$  qui est utilisée pour les termes de la suite).

On peut définir une suite en donnant l'expression de chacun de ses termes.

**Exemple 4.2.** Soit  $(x_n)_{n=1}^\infty$  définie pour tout  $n \in \mathbb{N}$ , par  $x_n = n + 5$ . Alors  $x_1 = 6$ ,  $x_2 = 7$ ,  $x_3 = 8$ , etc.

Comme nous l'avons vu dans les exemples du précédent chapitre, il arrive que les suites  $(x_n)_{n=m}^\infty$  (resp. suites finies  $(x_n)_{n=m}^j$ ) soient définies *récurivement*, on dit aussi *par récurrence*. Sauf si on trouve une formule explicite vérifiée par les termes de la suite, on ne peut pas calculer ces termes directement. Pour calculer  $x_{m+3}$ , on a besoin de connaître  $x_m, x_{m+1}, x_{m+2}$ , mais calculer  $x_{m+2}$  demande de connaître  $x_m, x_{m+1}$ , et enfin  $x_{m+1}$  se calcule à partir de  $x_m$ . La définition ressemble à :

- définition de  $x_m$  ;
- pour tout  $n \geq m$  (resp. pour tout entier  $n$  vérifiant  $m \leq n \leq j-1$ ),  $x_{n+1}$  = quelque chose en fonction de  $x_m, x_{m+1}, \dots, x_n$ .

Le deuxième point sous-entend : supposons que  $x_m, \dots, x_n$  sont maintenant définis, alors  $x_{n+1}$  est construit de telle manière. La règle définissant  $x_{n+1}$  à partir de  $x_m, x_{m+1}, \dots, x_n$  est appelée une *relation de récurrence*.

**Remarque 4.3.** C'est le principe d'induction (voire induction forte) qui justifie qu'une suite définie récurivement est bien définie.

**Exemple 4.4.**

1. La suite de Fibonacci (cf. exemple 3.50 du chapitre précédent) est une suite définie récurivement. C'est même une suite d'entiers (exercice 3.51 du chapitre précédent).
2. On peut définir la suite d'entiers  $(x_n)_{n=1}^\infty$  définie par :
  - $x_1 = a$  ;
  - pour tout  $n \in \mathbb{N}$ ,  $x_{n+1}$  vaut  $\frac{x_n}{2}$  si  $x_n$  est pair,  $x_n + 1$  si  $x_n$  est impair.
 où  $a$  est un entier fixé.

**Exercice 4.5.** Considérons la seconde suite de l'exemple ci-dessus.

1. Supposons  $a \in \mathbb{N}$ . Montrer que  $(x_n)_{n \in \mathbb{N}}$  est une suite d'entiers positifs et qu'à partir d'un certain rang, les termes alternent entre la valeur 1 et la valeur 2, c'est-à-dire

qu'il existe  $m$  tel qu'à partir de cet indice, on a  $x_m = 1$ ,  $x_{m+1} = 2$ ,  $x_{m+2} = 1$ ,  $x_{m+3} = 2$ , etc.

2. Supposons  $a \leq 0$ . Montrer que  $(x_n)_{n \in \mathbb{N}}$  est une suite d'entiers négatifs ou nulles et qu'à partir d'un certain rang, les termes sont nuls, c'est-à-dire qu'il existe  $m$  tel que  $x_m = x_{m+1} = x_{m+2} = \dots = 0$ .

**Symboles somme et produit.** Étant donnée une suite finie  $(x_i)_{i=m}^j$  d'entiers, on définit

$$\sum_{i=m}^j x_i = x_m + x_{m+1} + \dots + x_j,$$

$$\prod_{i=m}^j x_i = x_m x_{m+1} \dots x_j.$$

Plus rigoureusement, on définit ces quantités de manière récursive<sup>1</sup> :

- $\sum_{i=m}^m x_i = x_m$  et  $\prod_{i=m}^m x_i = x_m$  ;
- pour tout entier  $n$  vérifiant  $m \leq n \leq j-1$ , on a

$$\sum_{i=m}^{n+1} x_i = x_{n+1} + \sum_{i=m}^n x_i$$

et

$$\prod_{i=m}^{n+1} x_i = x_{n+1} \cdot \left( \prod_{i=m}^n x_i \right).$$

Ce sera encore valable dans  $\mathbb{R}$  ! La définition est la même si les  $x_i$  sont plus généralement des réels.

Si  $j < m$ , on dit que  $\sum_{i=m}^j x_i$  est une *somme vide* (« vide » car l'indice muet  $i$  se balade dans l'ensemble vide des entiers  $\geq m$  et  $\leq j$ ), et on dit que  $\prod_{i=m}^j x_i$  est un *produit vide*.

Par convention, une somme vide vaut 0 et un produit vide vaut 1. C'est une convention qui permet d'étendre les relations de récurrence présentées ci-dessus à l'indice  $n = m - 1$ . Par exemple, la relation  $\sum_{i=m}^{n+1} x_i = x_{n+1} + \sum_{i=m}^n x_i$  reste vrai pour  $n = m - 1$ , car elle signifie simplement  $\sum_{i=m}^m x_i = x_m + 0$ .

**Factorielle.** Pour  $n \geq 0$ , on définit  $n!$  («  $n$  factorielle » ou « factorielle  $n$  ») par

$$n! = \prod_{i=1}^n i = 1 \cdot 2 \cdot \dots \cdot n.$$

Autrement dit, la factorielle se définit récursivement :

- $0! = 1$  ;
- pour tout  $n \in \mathbb{N}$ ,  $(n+1)! = (n+1) \cdot (n!)$ .

1. De même qu'un raisonnement (non rigoureux) incluant l'expression « et ainsi de suite » suggère un raisonnement par induction pour le rendre rigoureux, une expression avec « ... » se définit rigoureusement à l'aide d'une définition récursive. À un certain stade de compréhension, on peut se permettre une définition comme celle présentée ci-dessus (mais un raisonnement en « et ainsi de suite » sera toujours interdit).

**Puissance.** Pour deux entiers  $a$  et  $n$ , avec  $n \geq 0$ , on définit la *puissance*  $a^n = a \cdot a \cdot \dots \cdot a$  (avec  $n$  facteurs «  $a$  » dans le produit),  $n$  est l'*exposant*. Autrement dit :

- $a^0 = 1$  ;
- pour tout  $n \in \mathbb{N}$ ,  $a^{n+1} = a \cdot a^n$ .

Il s'ensuit que  $0^0 = 1$ . On peut démontrer les propriétés suivantes, pour tous entiers  $a$ ,  $b$ ,  $n$  et  $k$  tels que  $n \geq 0$  et  $k \geq 0$  :

1.  $(ab)^n = a^n \cdot b^n$  ;
2.  $a^n a^k = a^{n+k}$  ;
3.  $(a^n)^k = a^{nk}$ .

**Exercice 4.6.** Montrer les deux derniers points. Indication : fixer  $a$  et  $n$ , et montrer par induction que ces propriétés sont vraies pour tout  $k \geq 0$ .

Ce sera encore valable dans  $\mathbb{R}$  ! La définition et les propriétés sont les mêmes lorsque  $a$  est un réel et l'exposant est un entier positif ou nul.

Enfin, on a  $1^n = 1$  pour tout  $n \in \mathbb{N}$ . Le vérifier par induction, on ne sait jamais...

## 4.2 Premières propriétés des sommes

Voici quelques techniques nous permettant de calculer efficacement des sommes.

**Proposition 4.7** (Linéarité de la somme). Soit  $m$  et  $j$  des entiers tels que  $m \leq j$ , et soient  $(x_i)_{i=m}^j$  et  $(y_i)_{i=m}^j$  des suites finies d'entiers.

1.  $\sum_{i=m}^j x_i + \sum_{i=m}^j y_i = \sum_{i=m}^j (x_i + y_i)$ .
2. Pour tout  $a \in \mathbb{Z}$ ,  $a \cdot \sum_{i=m}^j x_i = \sum_{i=m}^j (ax_i)$ .

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$ , les  $y_i$  et  $a$  sont plus généralement des réels.

**Preuve.** Montrons la première propriété, la seconde est laissée en exercice.

Par induction finie, montrons pour tout  $n \in \{m, \dots, j\}$  la propriété  $P(n) = \ll \sum_{i=m}^n x_i + \sum_{i=m}^n y_i = \sum_{i=m}^n (x_i + y_i) \gg$ . La propriété au rang  $n = j$  donne ainsi le résultat.

**Initialisation :** La propriété  $P(m)$  est évidente puisqu'il s'agit de montrer  $x_m + y_m = x_m + y_m$ .

**Étape d'induction :** Soit  $n \in \{m, \dots, j-1\}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . La définition récursive de la somme, l'hypothèse de récurrence et la commutativité de

l'addition donnent

$$\begin{aligned}
 \sum_{i=1}^{n+1} (x_i + y_i) &= (x_{n+1} + y_{n+1}) + \sum_{i=1}^n (x_i + y_i) \\
 &= x_{n+1} + y_{n+1} + \sum_{i=1}^n x_i + \sum_{i=1}^n y_i \\
 &= x_{n+1} + \sum_{i=1}^n x_i + y_{n+1} + \sum_{i=1}^n y_i \\
 &= \sum_{i=1}^{n+1} x_i + \sum_{i=1}^{n+1} y_i.
 \end{aligned}$$

D'où  $P(n+1)$ . □

**Proposition 4.8** (Monotonie de la somme). *Soit  $m$  et  $j$  des entiers tels que  $m \leq j$ , et soient  $(x_i)_{i=m}^j$  et  $(y_i)_{i=m}^j$  des suites finies d'entiers. Si  $x_i \leq y_i$  pour tout  $m \leq i \leq j$ , alors*

$$\sum_{i=m}^j x_i \leq \sum_{i=m}^j y_i.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  et les  $y_i$  sont plus généralement des réels.

**Preuve.** Par induction finie (exercice). □

**Proposition 4.9** (Somme par paquet). *Soit  $m, j$  et  $k$  des entiers tels que  $m \leq k \leq j$ , et soit  $(x_i)_{i=m}^j$  une suite finie d'entiers. Alors*

$$\sum_{i=m}^j x_i = \sum_{i=m}^k x_i + \sum_{i=k+1}^j x_i.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  sont plus généralement des réels.

**Preuve.** Par induction finie, montrer  $\sum_{i=m}^n x_i = \sum_{i=m}^k x_i + \sum_{i=k+1}^n x_i$  pour tout entier  $n \in \{k, \dots, j\}$  (exercice). □

**Proposition 4.10** (Changement d'indice, ou changement de variable). *Soit  $m$  et  $j$  des entiers tels que  $m \leq j$ , et soit  $(x_i)_{i=m}^j$  une suite finie d'entiers. Pour tout entier  $r$ , on a*

$$\sum_{i=m}^j x_i = \sum_{i=m+r}^{j+r} x_{i-r}.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  sont plus généralement des réels.

**Preuve.** Par induction finie, montrer  $\sum_{i=m}^n x_i = \sum_{i=m+r}^{n+r} x_{i-r}$  pour tout entier  $n \in \{m, \dots, j\}$  (exercice).  $\square$

**Proposition 4.11** (Somme télescopique). *Soit  $m$  et  $j$  des entiers tels que  $m < j$ , et soit  $(x_i)_{i=m}^j$  une suite finie d'entiers. Alors*

$$\sum_{i=m}^{j-1} (x_{i+1} - x_i) = x_j - x_m.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  sont plus généralement des réels.

**Preuve.** Par induction finie, montrer  $\sum_{i=m}^{n-1} (x_{i+1} - x_i) = x_n - x_m$  pour tout entier  $n \in \{m, \dots, j\}$  (exercice).  $\square$

**Exercice 4.12.** Démontrer toutes les propositions de cette section.

Le changement d'indice et le télescopage peuvent facilement mener à des erreurs de calcul. Ne pas hésiter à écrire les premiers termes et les derniers termes au brouillon, pour voir si les indices sont corrects. Par exemple,

$$\begin{aligned} \sum_{i=m}^{j-1} (x_{i+1} - x_i) &= (x_{m+1} - x_m) + (x_{m+2} - x_{m+1}) + (x_{m+3} - x_{m+2}) \\ &\quad + \dots + (x_{j-2} - x_{j-3}) + (x_{j-1} - x_{j-2}) + (x_j - x_{j-1}) \\ &= (\cancel{x_{m+1}} - x_m) + (\cancel{x_{m+2}} - \cancel{x_{m+1}}) + (x_{m+3} - \cancel{x_{m+2}}) \\ &\quad + \dots + (\cancel{x_{j-2}} - x_{j-3}) + (\cancel{x_{j-1}} - \cancel{x_{j-2}}) + (x_j - \cancel{x_{j-1}}) \\ &= x_j - x_m. \end{aligned}$$

## 4.3 Exemples classiques de sommes

Voici maintenant des exemples de sommes que nous savons calculer.

**Proposition 4.13.** *Pour tout  $n \in \mathbb{N}$ ,*

- $\sum_{i=1}^n 1 = n$  ;
- (sommes d'entiers consécutifs)  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$  ;
- (sommes de carrés consécutifs)  $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$  ;

Par exemple, si  $a$  est un entier, alors  $\sum_{i=1}^n a = an$  (utiliser la linéarité de la somme). Ce sera aussi valable si  $a$  est un nombre réel.

Si  $m$  et  $j$  sont des entiers tels que  $m \leq j$ , alors un changement d'indice donne

$$\sum_{i=m}^j 1 = j - m + 1.$$

**Attention.** Le piège classique consiste à penser qu'il y a  $j - m$  entiers dans l'ensemble  $\{m, \dots, j\}$ . Or il y en a  $j - m + 1$ .

**Preuve.** On montre ces trois points par induction sur  $n$ . Écrivons-le pour la somme des entiers consécutifs (pour les autres sommes, exercice).

Par induction, montrons pour tout  $n \in \mathbb{N}$  la propriété  $P(n) = \ll \sum_{i=1}^n i = \frac{n(n+1)}{2} \gg$ .

**Initialisation :** D'une part,  $\sum_{i=1}^1 i = 1$ . D'autre part,  $\frac{1(1+1)}{2} = 1$ . D'où  $P(1)$ .

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . Alors on

a

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

D'où  $P(n+1)$ .

D'où le résultat par récurrence. □

**Exercice 4.14.** Démontrer ce qui a été laissé en exercice dans la preuve ci-dessus.

**Proposition 4.15.** Pour tous entiers  $m$  et  $j$  tels que  $m \leq j$ , pour tout entier  $x \neq 1$ , on

a

$$\sum_{i=m}^j x^i = \frac{x^m - x^{j+1}}{1 - x}.$$

En particulier, pour tout  $n \in \mathbb{N}$ , pour tout entier  $x \neq 1$ ,

$$\sum_{i=1}^n x^i = \frac{1 - x^{n+1}}{1 - x}.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est la même si  $x$  est plus généralement un réel différent de 1.

**Attention.** C'est faux si  $x = 1$ . En effet,  $\sum_{i=m}^j 1^i = \sum_{i=m}^j 1 = j - m + 1$ . C'est facile de se souvenir de cette hypothèse : si  $x = 1$ , le dénominateur nous indique qu'il y a un problème de division par 0 (cf. propriété 2 de la proposition 3.8 du chapitre précédent).

**Preuve.** Dans le calcul qui suit, la première égalité utilise la linéarité de la somme, la troisième applique un télescopage :

$$\begin{aligned}(1-x) \sum_{i=m}^j x^i &= \sum_{i=m}^j ((1-x)x^i) \\ &= \sum_{i=m}^j (x^i - x^{i+1}) \\ &= x^m - x^{j+1}.\end{aligned}$$

Ainsi,  $\sum_{i=m}^j x^i$  est l'entier  $c$  tel que  $(1-x)c = x^m - x^{j+1}$ , où  $x^m - x^{j+1}$  et  $1-x$  sont des entiers et  $1-x$  n'est pas nul (car  $x \neq 1$ ). Donc  $\sum_{i=m}^j x^i = \frac{x^m - x^{j+1}}{1-x}$  par définition de la fraction.  $\square$

**Exercice 4.16.** Soient  $N \in \mathbb{N}$  et  $x \in \mathbb{R}$ . Calculer  $\sum_{k=0}^N x^{8k+5}$ .

**Exercice 4.17.** Soient  $N \in \mathbb{N}$ . Calculer  $\sum_{k=1}^N \frac{1}{k(k+1)}$ .

Il reste une dernière identité à présenter : la formule du binôme. Nous la présentons dans la section 4.5.

## 4.4 Somme et produit sur un ensemble fini

**Proposition/définition 4.18.** Soit  $I$  un ensemble fini et  $(x_i)_{i \in I}$  une famille d'entiers. Si  $n$  est le nombre d'éléments de  $I$ , et si  $i_1, \dots, i_n$  sont les éléments deux à deux distincts de  $I$ , alors on définit

$$\begin{aligned}\sum_{i \in I} x_i &= \sum_{k=1}^n x_{i_k} \\ \text{et } \prod_{i \in I} x_i &= \prod_{k=1}^n x_{i_k}.\end{aligned}$$

Les définitions de  $\sum_{i \in I} x_i$  et de  $\prod_{i \in I} x_i$  ne dépendent pas du choix d'énumération  $i_1, \dots, i_n$  des éléments de  $I$ .

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  sont plus généralement des réels.

**Preuve.** Démontrons-le pour la somme (la preuve sera la même pour le produit). Par induction finie, montrons pour tout  $0 \leq \ell \leq n$  la propriété  $P(\ell) = \ll$  Pour tout sous-ensemble  $J \subset I$ , si  $J = \{i_1, \dots, i_\ell\} = \{j_1, \dots, j_\ell\}$  où  $i_1, \dots, i_\ell$  sont deux à deux distincts, de même pour  $j_1, \dots, j_\ell$ , alors  $\sum_{k=1}^\ell x_{i_k} = \sum_{k=1}^\ell x_{j_k} \gg$ . La propriété qu'on veut démontrer sera une conséquence de  $P(n)$ .

**Initialisation :**  $P(0)$  traite le cas de la somme vide, qui vaut 0. Donc  $P(0)$  est évidemment vraie.

**Étape d'induction :** Soit  $0 \leq \ell \leq n-1$ . Supposons  $P(\ell)$  et montrons  $P(\ell+1)$ .

Soit  $J \subset I$  que l'on écrit  $J = \{i_1, \dots, i_{\ell+1}\} = \{j_1, \dots, j_{\ell+1}\}$  avec  $i_1, \dots, i_{\ell+1}$  deux à deux distincts, de même pour  $j_1, \dots, j_{\ell+1}$ . Notons  $J' = \{i_1, \dots, i_\ell\}$  et  $K$  l'entier de  $\{1, \dots, \ell+1\}$  tel que  $i_{\ell+1} = j_K$ . On a donc  $J' = \{j_1, \dots, j_{K-1}, j_{K+1}, \dots, j_{\ell+1}\}$ , ce qu'on peut aussi écrire  $J' = \{j'_1, \dots, j'_\ell\}$  où  $j'_k = j_k$  si  $k \in \{1, \dots, K-1\}$ ,  $j'_k = j_{k+1}$  si  $k \in \{K, \dots, \ell\}$ . La propriété  $P(\ell)$  appliquée à  $J'$  nous permet d'affirmer que

$$\sum_{k=1}^{\ell} x_{i_k} = \sum_{k=1}^{\ell} x_{j'_k}$$

et on peut noter  $S$  la valeur commune. D'une part, la définition récursive de la somme donne

$$\sum_{k=1}^{\ell+1} x_{i_k} = x_{i_{\ell+1}} + \sum_{k=1}^{\ell} x_{i_k} = x_{i_{\ell+1}} + S.$$

D'autre part, on a

$$\begin{aligned} \sum_{k=1}^{\ell+1} x_{j_k} &= \sum_{k=1}^K x_{j_k} + \sum_{k=K+1}^{\ell+1} x_{j_k} \\ &= x_{j_K} + \sum_{k=1}^{K-1} x_{j_k} + \sum_{k=K+1}^{\ell+1} x_{j_k} \\ &= x_{j_K} + \sum_{k=1}^{K-1} x_{j'_k} + \sum_{k=K+1}^{\ell+1} x_{j'_{k-1}} \\ &= x_{j_K} + \sum_{k=1}^{K-1} x_{j'_k} + \sum_{k=K}^{\ell} x_{j'_k} \\ &= x_{j_K} + \sum_{k=1}^{\ell} x_{j'_k} \\ &= x_{i_{\ell+1}} + S, \end{aligned}$$

où on a utilisé dans l'ordre la sommation par paquet, la définition récursive de la somme, la définition des  $j'_k$ , un changement d'indice (au sens de la proposition 4.10) ainsi qu'une nouvelle sommation. Au total, on a  $\sum_{k=1}^{\ell+1} x_{i_k} = \sum_{k=1}^{\ell+1} x_{j_k}$ . D'où  $P(\ell+1)$ .  $\square$

Les propriétés de linéarité et de monotonie de la somme sont encore vérifiées dans ce contexte. Nous n'écrirons pas les énoncés, ils sont analogues aux propositions 4.7 et 4.8.

La proposition 4.10 est un cas particulier de l'énoncé qui suit (prendre  $J = \{m, \dots, k\}$ ,  $I = \{m+r, \dots, k+r\}$  et  $f: x \in I \mapsto x-r \in J$ ).

**Proposition 4.19** (Changement d'indice, ou changement de variable). *Soit  $f: I \rightarrow J$  une bijection entre deux ensembles finis  $I$  et  $J$ . Soit  $(x_j)_{j \in J}$  une famille d'entiers. Alors on a*

$$\sum_{j \in J} x_j = \sum_{i \in I} x_{f(i)}.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_j$  sont plus généralement des réels.

**Preuve.** Soit  $n$  le nombre d'éléments de  $I$  et  $i_1, \dots, i_n$  une énumération de ses éléments, c'est-à-dire que  $i_1, \dots, i_n$  sont deux à deux distincts et on a  $I = \{i_1, \dots, i_n\}$ . La fonction  $f$  étant injective, les éléments  $f(i_1), \dots, f(i_n)$  sont deux à deux distincts. Enfin, la fonction est surjective donc on a aussi  $J = \{f(i_1), \dots, f(i_n)\}$ . Ainsi  $f(i_1), \dots, f(i_n)$  est une énumération des éléments de  $J$ . On obtient ainsi le résultat en appliquant la définition de  $\sum_{j \in J} x_j$ .  $\square$

La proposition 4.9 est un cas particulier de l'énoncé qui suit (prendre  $I = \{m, \dots, j\}$ ,  $A = \{1, \dots, k\}$  et  $B = \{k+1, \dots, j\}$ ).

**Proposition 4.20** (Somme par paquet). *Soit  $I$  un ensemble fini et  $(x_i)_{i \in I}$  une famille d'entiers. Si  $A$  et  $B$  sont des sous-ensembles tels que  $I = A \sqcup B$ , alors on a*

$$\sum_{i \in I} x_i = \sum_{i \in A} x_i + \sum_{i \in B} x_i.$$

Ce sera encore valable dans  $\mathbb{R}$  ! La proposition est valable si les  $x_i$  sont plus généralement des réels.

**Preuve.** Il suffit d'énumérer les éléments de  $I$  en commençant par les éléments de  $A$  et en terminant avec les éléments de  $B$ . Soit donc  $a_1, \dots, a_K$  une énumération des éléments de  $A$ , et  $b_1, \dots, b_{K'}$  une énumération des éléments de  $B$ . On pose  $n = K + K'$ ,  $i_k = a_k$  si  $k \in \{1, \dots, K\}$ ,  $i_k = b_{k-K}$  si  $k \in \{K+1, \dots, n\}$ . Ainsi  $i_1, \dots, i_n$  est une énumération des éléments de  $I$ . La sommation par paquet (au sens de la proposition 4.9) donne enfin

$$\begin{aligned} \sum_{i \in I} x_i &= \sum_{k=1}^n x_{i_k} \\ &= \sum_{k=1}^K x_{i_k} + \sum_{k=K+1}^n x_{i_k} \\ &= \sum_{k=1}^K x_{i_k} + \sum_{k=1}^{K'} x_{i_{k+K}} \\ &= \sum_{k=1}^K x_{a_k} + \sum_{k=1}^{K'} x_{b_k} \\ &= \sum_{a \in A} x_a + \sum_{b \in B} x_b, \end{aligned}$$

comme voulu.  $\square$

**Exercice 4.21.** Soit  $N \in \mathbb{N}$  et  $S = \sum_{\substack{1 \leq k \leq N \\ k \text{ est impair}}} \frac{1}{k}$ . On pose pour tout  $n \in \mathbb{N}$ ,  $u_n = \sum_{k=1}^n \frac{1}{k}$ .

Exprimer  $S$  en fonction de certains termes de la suite  $(u_n)_{n \in \mathbb{N}}$ .

**Exercice 4.22.** Soit  $N \in \mathbb{N}$ . Calculer  $S = \sum_{\substack{0 \leq k \leq N \\ k \text{ est impair}}} k^2$ .

**Exercice 4.23.** Soit  $N \in \mathbb{N}$ . Calculer  $\prod_{\substack{1 \leq k \leq 2N \\ k \text{ pair}}} k$  en fonction de  $N!$ .

**Exercice 4.24.** Soit  $n \in \mathbb{N}$ . Notons  $D(n)$  l'ensemble des diviseurs de  $n$  et  $d(n)$  est le nombre de diviseurs de  $n$ . Montrer que

$$\prod_{m \in D(n)} m = n^{\frac{d(n)}{2}}.$$

Indication : On considérera l'application  $m \in D(n) \mapsto \frac{n}{m} \in D(n)$ .

## 4.5 Coefficients binomiaux et formule du binôme

**Proposition 4.25.** Si  $k$  et  $n$  sont des entiers vérifiant  $0 \leq k \leq n$ , alors  $k!(n-k)!$  divise  $n!$ .

**Preuve.** Par induction, montrons pour tout  $n \geq 0$  la propriété  $P(n) = \ll \forall 0 \leq k \leq n, k!(n-k)! \mid n! \gg$ .

**Initialisation :**  $P(0)$  est la propriété  $\ll \forall 0 \leq k \leq 0, k!(0-k)! \mid 0! \gg$ , c'est-à-dire  $\ll 0!0! \mid 0! \gg$ , ce qui est vrai.

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et démontrons  $P(n+1)$ . Soit  $k$  un entier vérifiant  $0 \leq k \leq n+1$ . Si  $k = 0$ , alors  $k!(n+1-k)! = (n+1)!$  donc  $k!(n+1-k)!$  divise  $(n+1)!$ . Si  $k = n+1$ , il se passe la même chose. Supposons maintenant  $1 \leq k \leq n$ . D'une part,  $k$  vérifie  $0 \leq k \leq n$  donc par  $P(n)$ , il existe un entier  $c$  tel que  $c \cdot k!(n-k)! = n!$ . D'autre part, on a  $0 \leq k-1 \leq n$  donc par  $P(n)$ , il existe un entier  $d$  tel que  $d \cdot (k-1)!(n-(k-1))! = n!$ . Ainsi, on a

$$\begin{aligned} (n+1)! &= n! \cdot (n+1) \\ &= n! \cdot k + n! \cdot (n+1-k) \\ &= d \cdot (k-1)!(n-(k-1))! \cdot k + c \cdot k!(n-k)! \cdot (n+1-k) \\ &= d \cdot k!(n+1-k)! + c \cdot k!(n+1-k)! \\ &= (d+c) \cdot k!(n+1-k)!. \end{aligned}$$

Donc  $k!(n+1-k)!$  divise  $(n+1)!$ . D'où  $P(n+1)$ . □

**Définition 4.26.** Si  $k$  et  $n$  sont des entiers vérifiant  $0 \leq k \leq n$ , alors on définit le *coefficient binomial*

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

C'est un entier (par la proposition précédente), appelé «  $k$  parmi  $n$  ».

Si  $k < 0$  ou  $k > n$ , alors  $\binom{n}{k} = 0$  par convention.

L'énoncé suivant donne une interprétation combinatoire des coefficients binomiaux. Ce cours n'abordera pas la théorie du cardinal, gardons seulement une approche intuitive : le cardinal d'un ensemble  $A$  est le nombre d'éléments dans  $A$ . Le cardinal peut être fini ou infini, il est nul

pour l'ensemble vide, il vaut 1 pour un singleton, 2 pour une paire.

**Proposition 4.27.**  $\binom{n}{k}$  est le nombre de sous-ensemble de cardinal  $k$  dans un ensemble de cardinal  $n$ .

**Preuve.** Considérons un ensemble de cardinal  $n$ . Sans perte de généralité, on considère l'ensemble  $\{1, \dots, n\}$  des entiers compris (au sens large) entre 1 et  $n$ . Pour fabriquer un ensemble de cardinal  $k$  :

1. on construit un  $k$ -uplet  $(x_1, \dots, x_k)$  d'éléments de  $\{1, \dots, n\}$  deux à deux distincts ;
2. on considère l'ensemble  $\{x_1, \dots, x_k\}$  (de cardinal  $k$  car les  $x_i$  sont deux à deux distincts).

Avec cette méthode, on construit tous les ensembles de cardinal  $k$ .

- Comptons le nombre de  $k$ -uplets que l'on peut construire à la première étape. Pour choisir un tel  $k$ -uplet, on doit d'abord choisir  $x_1 \in \{1, \dots, n\}$  ( $n$  choix), puis  $x_2 \in \{1, \dots, n\}$  distinct de  $x_1$  ( $n - 1$  choix), puis  $x_3 \in \{1, \dots, n\}$  distinct de  $x_1$  et  $x_2$  ( $n - 2$  choix), ..., et enfin  $x_k \in \{1, \dots, n\}$  distinct de  $x_1, \dots, x_{k-1}$  ( $n - (k - 1)$  choix)<sup>a</sup>. Ainsi il y a  $n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n-k)!}$   $k$ -uplets possibles.
- Dans la seconde étape, il y a des  $k$ -uplets qui peuvent donner le même ensemble. En effet, l'ordre des éléments importe lorsqu'on écrit  $(x_1, \dots, x_k)$ , pas quand on écrit  $\{x_1, \dots, x_k\}$ . Ainsi, si on fixe un sous-ensemble  $A$  de  $\{1, \dots, n\}$  de cardinal  $k$ , et qu'on note  $y_1, \dots, y_k$  ses  $k$  éléments (ils sont deux à deux distincts), alors l'ensemble des  $k$ -uplets qui donnent l'ensemble  $A$  dans la seconde étape sont les  $k$ -uplets  $(x_1, \dots, x_k)$  où les  $x_i$  décrivent l'ensemble des  $y_i$ , mais pas nécessairement dans le même ordre. Comptons le nombre de ces  $k$ -uplets qui donnent  $A$ . Il faut choisir  $x_1 \in A$  ( $k$  choix), puis  $x_2 \in A$  distinct de  $x_1$  ( $k - 1$  choix), puis  $x_3 \in A$  distinct de  $x_1$  et  $x_2$  ( $k - 2$  choix), ..., et enfin  $x_k \in A$  distinct de  $x_1, \dots, x_{k-1}$  (un seul choix). Donc il y a exactement  $k \cdot (k - 1) \cdot \dots \cdot 1 = k!$   $k$ -uplets qui donnent  $A$ .

Pour conclure, il y a donc  $k!$  fois moins de sous-ensembles de  $\{1, \dots, n\}$  de cardinal  $k$  qu'il n'y a de  $k$ -uplets d'éléments de  $\{1, \dots, n\}$  deux à deux distincts. Donc il y en a  $\frac{1}{k!} \frac{n!}{(n-k)!} = \binom{n}{k}$ .  $\square$

<sup>a</sup>. *Mea culpa*, c'est un raisonnement en « ... » (autrement dit en « et ainsi de suite »). Il faudrait raisonner par induction sur  $k$  pour rendre cela rigoureux, ce qu'on ne fait pas pour ne pas alourdir la preuve (exercice : le rédiger proprement).

### Exemple 4.28.

1. Pour tout  $n \geq 0$ ,  $\binom{n}{0} = \binom{n}{n} = 1$ .
2. Pour tout  $n \geq 1$ ,  $\binom{n}{1} = \binom{n}{n-1} = n$ .
3. Pour tout  $n \geq 2$ ,  $\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$ .

**Proposition 4.29.** Si  $k$  et  $n$  sont des entiers vérifiant  $0 \leq k \leq n$ , alors

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

**Preuve.** 
$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}. \quad \square$$

**Interprétation combinatoire de cette formule.** Construire un sous-ensemble  $E$  de cardinal  $k$  dans un ensemble  $A$  de cardinal  $n$ , c'est équivalent à construire son complémentaire  $A - E$ , de cardinal  $n - k$ .

**Proposition 4.30** (Formule de Pascal). *Si  $k$  et  $n$  sont des entiers vérifiant  $1 \leq k \leq n$ , alors*

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

**Preuve.** En écrivant  $(n+1)! = n! \cdot (n+1) = n! \cdot k + n! \cdot (n+1-k)$ , on obtient :

$$\begin{aligned} \binom{n+1}{k} &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \frac{n! \cdot k}{k!(n+1-k)!} + \frac{n! \cdot (n+1-k)}{k!(n+1-k)!} \\ &= \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\ &= \binom{n}{k-1} + \binom{n}{k}. \end{aligned}$$

□

**Interprétation combinatoire de la formule de Pascal.**  $\binom{n+1}{k}$  est le nombre de sous-ensembles de cardinal  $k$  dans un ensemble de cardinal  $n+1$ , disons dans  $\{1, \dots, n+1\}$  sans perte de généralité. Ou bien un tel sous-ensemble ne contient pas l'élément  $n+1$ , ses  $k$  éléments sont donc dans  $\{1, \dots, n\}$ , il y a donc  $\binom{n}{k}$  choix. Ou bien un tel sous-ensemble contient l'élément  $n+1$ , ses  $k-1$  autres éléments sont donc à choisir dans  $\{1, \dots, n\}$ , il y a  $\binom{n}{k-1}$  choix.

**Remarque 4.31.** La formule de Pascal est une méthode itérative de calcul de  $\binom{n}{k}$ . Je connais  $\binom{n}{k}$  à partir de  $\binom{n-1}{k}$  et  $\binom{n-1}{k-1}$ . Ces deux quantités se calculent ensuite respectivement à partir de  $\binom{n-2}{k}$  et  $\binom{n-2}{k-1}$ , et à partir de  $\binom{n-2}{k-1}$  et  $\binom{n-2}{k-2}$ , et ainsi de suite, jusqu'à obtenir des coefficients binomiaux de la forme  $\binom{a}{b}$  avec  $b = 0$  ou  $a = b$  (de tels coefficients binomiaux valent 1). Autrement dit, on utilise la formule de récurrence jusqu'à atteindre les bords du triangle de Pascal représenté ci-dessous.

| $n \backslash k$ | 0 | 1 | 2  | 3                                   | 4  | 5                | ... |
|------------------|---|---|----|-------------------------------------|----|------------------|-----|
| 0                | 1 |   |    |                                     |    |                  |     |
| 1                | 1 | 1 |    | $\binom{n-1}{k-1} + \binom{n-1}{k}$ |    |                  |     |
| 2                | 1 | 2 | 1  |                                     |    | $= \binom{n}{k}$ |     |
| 3                | 1 | 3 | 3  | 1                                   |    |                  |     |
| 4                | 1 | 4 | 6  | 4                                   | 1  |                  |     |
| 5                | 1 | 5 | 10 | 10                                  | 5  | 1                |     |
| 6                | 1 | 6 | 15 | 20                                  | 15 | 6                | 1   |

**Théorème 4.32** (Théorème du binôme). Si  $a, b \in \mathbb{Z}$  et  $n \in \mathbb{Z}_{\geq 0}$ , alors

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

Ce sera encore valable dans  $\mathbb{R}$  ! Le résultat est encore vrai même si  $a$  et  $b$  sont plus généralement des réels.

**Preuve.** Par induction, montrons pour tout  $n \geq 0$  la propriété  $P(n) = \ll (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \gg$ .

**Initialisation :** D'une part,  $(a + b)^0 = 1$ . D'autre part,

$$\sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1.$$

D'où  $P(0)$ .

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . On a

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

où la première égalité consiste à isoler les termes  $k = 0$  et  $k = n + 1$ , afin de pouvoir

utiliser la formule de Pascal lors de la deuxième égalité. D'une part,

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

où l'avant-dernière égalité utilise l'hypothèse d'induction. D'autre part, un changement d'indice et l'hypothèse d'induction donnent

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

Au total, on obtient

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

D'où  $P(n+1)$ . □

**Remarque 4.33.** Cette preuve par induction n'explique pas l'apparition des coefficients binomiaux. Voici une manière de comprendre, utilisant l'interprétation combinatoire de ces coefficients.

Le développement de  $(a+b)^n$ , c'est-à-dire de  $(a+b) \cdot (a+b) \cdot \dots \cdot (a+b)$  est une somme dont les termes sont de la forme  $\varepsilon_1 \cdot \dots \cdot \varepsilon_n$ , où  $\varepsilon_i$  est le  $a$  ou le  $b$  du  $i$ -ième facteur  $(a+b)$ . Chacun de ces termes est donc caractérisé par l'ensemble des  $i$  tels que  $\varepsilon_i = a$  (les autres seront des  $b$ ). Il y a donc exactement  $\binom{n}{k}$  termes  $\varepsilon_1 \cdot \dots \cdot \varepsilon_n$  dont l'ensemble des  $i$  tels que  $\varepsilon_i = a$  est de cardinal  $k$ , et chacun de ces termes vaut  $a^k b^{n-k}$ .

**Corollaire 4.34.** Pour tout  $n \in \mathbb{N}$ ,

1.  $\sum_{k=0}^n \binom{n}{k} = 2^n$  ;
2.  $\sum_{k=0}^n \binom{n}{k} (-1)^k = 0$ .

**Preuve.** Appliquer la formule à  $a = b = 1$ , puis à  $a = -1, b = 1$ .  $\square$

**Exercice 4.35.** Soit  $n \in \mathbb{N}$ . Calculer les sommes suivantes.

1.  $\sum_{k=0}^m \binom{n}{k}$  où  $m$  est le plus grand entier vérifiant  $2m \leq n$ .
2.  $\sum_{\substack{k \in \{0, \dots, n\} \\ k \text{ est pair}}} \binom{n}{k}$ .

**Remarque 4.36.** On peut trouver une interprétation combinatoire de  $\sum_{k=0}^n \binom{n}{k} = 2^n$ .

Étant donné un ensemble  $A$  de cardinal  $n$ , rappelons que  $\binom{n}{k}$  est le nombre d'éléments de  $\mathcal{P}(A)$  de cardinal  $k$ . Ainsi  $\sum_{k=0}^n \binom{n}{k}$  correspond au nombre d'éléments dans  $\mathcal{P}(A)$ . Ainsi, nous savons maintenant que  $\mathcal{P}(A)$  est de cardinal  $2^n$  ( $A$  admet  $2^n$  sous-ensembles).

On peut aussi l'obtenir si on compte différemment le nombre de sous-ensembles de  $A$ . En effet, pour construire un sous-ensemble de  $A$ , on peut parcourir les  $n$  éléments de  $A$  et décider pour chacun d'entre eux s'il appartient ou non au sous-ensemble. Il y a donc 2 choix par élément, d'où  $2^n$ . C'est en fait exactement l'idée de l'exercice 2.74.

## 4.6 Problèmes

### 4.6.1 Problème 1

Ce problème aborde la notion de cardinal d'un ensemble, c'est-à-dire le nombre d'éléments qui le constitue. On commence avec quelques résultats préliminaires permettant une définition rigoureuse du cardinal d'un ensemble, puis on calculera le cardinal d'ensembles classiques.

1. Soit  $m \geq 2$  un entier et  $k \in \{1, \dots, m\}$ . Montrer qu'il existe une bijection de  $\{1, \dots, m\} - \{k\}$  vers  $\{1, \dots, m-1\}$ .
2. Pour tout  $n \in \mathbb{N}$ , considérons la propriété  $P(n)$  = « pour tout  $m \in \mathbb{N}$ , s'il existe une injection de  $\{1, \dots, n\}$  vers  $\{1, \dots, m\}$ , alors  $n \leq m$  ». Par induction, montrer  $P(n)$  pour tout  $n \in \mathbb{N}$  (on utilisera la question précédente dans l'étape d'induction).
3. Soit  $A$  un ensemble. On suppose qu'il existe  $m, n \in \mathbb{N}$  tel que  $A$  est en bijection avec  $\{1, \dots, m\}$  et avec  $\{1, \dots, n\}$ . Montrer que  $m = n$ .
4. Pour tout  $n \in \mathbb{N}$ , pour tout sous-ensemble  $I$  de  $\{1, \dots, n\}$ , montrer qu'il existe  $m \leq n$  tel que  $I$  est en bijection avec  $\{1, \dots, m\}$ , et montrer  $m = n \iff I = \{1, \dots, n\}$ .
5. On rappelle qu'un ensemble  $A$  est fini s'il est vide ou s'il existe  $n \in \mathbb{N}$  et une surjection  $\{1, \dots, n\} \rightarrow A$ . Montrer qu'un ensemble  $A$  est fini et non vide si et seulement s'il existe  $n \in \mathbb{N}$  et une bijection entre  $\{1, \dots, n\}$  et  $A$ .

On définit alors le cardinal  $\#A$  d'un ensemble  $A$  de la manière suivante.

- Si  $A$  est fini, alors  $\#A = 0$  si  $A = \emptyset$ ,  $\#A = n \in \mathbb{N}$  si  $A$  est en bijection avec  $\{1, \dots, n\}$ .
- Si  $A$  est infini, alors  $\#A = \infty$ .

**Attention.**  $\infty$  n'est pas un entier, «  $\#A = \infty$  » est simplement une notation pour désigner une propriété.

6. Vérifier que  $\#A$  est bien défini lorsque  $A$  est fini.

7. Calculer le cardinal d'un singleton, le cardinal d'une paire, le cardinal de l'ensemble  $\{1, \dots, n\}$  pour  $n \in \mathbb{N}$ , le cardinal de  $\mathbb{N}$ .
8. Montrer que si  $A$  et  $B$  sont deux ensembles tels que  $A \subset B$  et  $\#A = \infty$ , alors  $\#B = \infty$ . Montrer que pour tout  $n \in \mathbb{N}$ , pour tout  $k \in \mathbb{Z}$ , il existe une bijection de  $\{1, \dots, n\}$  vers  $\{1+k, \dots, n+k\}$ .
9. En déduire que si  $A$  et  $B$  sont deux ensembles disjoints, alors  $\#(A \sqcup B) = \#A + \#B$  (avec la convention  $\infty + \infty = \infty$  et  $n + \infty = \infty$  pour tout  $n \in \mathbb{Z}_{\geq 0}$ ).
10. Soit  $k \in \mathbb{N}$  et  $A_1, \dots, A_k$  des ensembles formant une famille disjointe. Montrer que  $\#\bigsqcup_{i=1}^k A_i = \sum_{i=1}^k \#A_i$  (où on considère que la somme dans le membre de droite est infini si l'un des  $\#A_i$  est infini).
11. En déduire que si  $A$  et  $B$  sont des ensembles tels que  $A \subset B$ , alors  $\#(B - A) = \#B - \#A$ .
12. En déduire que si  $A$  et  $B$  sont des ensembles, alors  $\#(B - A) \leq \#B - \#A$ .
13. Si  $A$  et  $B$  sont des ensembles, calculer le cardinal de  $A \times B$  (on écrira judicieusement  $A \times B$  comme une union disjointe).
14. Si  $A$  et  $B$  sont des ensembles finis, calculer le cardinal de  $\mathcal{F}(A, B)$ . On procèdera par induction sur le cardinal de  $A$ , l'étape d'induction consistera à écrire judicieusement cet ensemble comme une union disjointe.
15. Quel est le cardinal de  $\mathcal{F}(A, B)$  lorsque  $A$  est infini ou  $B$  est infini?



# Chapitre 5

## Arithmétique modulaire

Le chapitre 3 a commencé à aborder les notions de diviseurs et de nombres premiers dans  $\mathbb{Z}$ . Le but est d'approfondir ces concepts.

### 5.1 Division euclidienne

**Théorème 5.1** (Division euclidienne). *Soit  $n \in \mathbb{N}$ . Pour tout  $m \in \mathbb{Z}$ , il existe un unique couple d'entiers  $(q, r) \in \mathbb{Z}^2$  tel que*

- $m = qn + r$  ;
- $0 \leq r \leq n - 1$ .

*L'entier  $q$  est appelé le quotient et  $r$  le reste de la division de  $m$  par  $n$ .*

**Preuve. Unicité :** Commençons par démontrer l'unicité. Soient  $q, q', r, r'$  des entiers vérifiant

- $m = qn + r = q'n + r'$  ;
- $0 \leq r \leq n - 1$  et  $0 \leq r' \leq n - 1$ .

La première hypothèse donne  $(q - q')n = r' - r$ , donc  $n$  divise  $r' - r$ . Si par l'absurde,  $r' - r$  n'est pas nul, alors la proposition 3.45 nous donne

$$r' - r \leq -n \text{ ou } r' - r \geq n.$$

Mais la seconde hypothèse nous donne

$$-(n - 1) \leq r' - r \leq n - 1,$$

on a donc une contradiction. Ainsi  $r' = r$ , ce qui donne  $qn = q'n$ , donc  $q = q'$  (car  $n \neq 0$ ).

**Existence :** Si on admet le résultat pour  $m \geq 0$ , alors on peut obtenir le résultat pour  $m < 0$ . En effet, si  $m < 0$ , alors  $-m > 0$  donc il existe des entiers  $q$  et  $r$  vérifiant  $-m = qn + r$  et  $0 \leq r \leq n - 1$ . Ainsi  $m = -qn - r$  avec  $-n + 1 \leq -r \leq 0$ . Si  $r = 0$ , alors on a bien  $0 \leq -r \leq n - 1$  et donc  $-q$  et  $-r$  sont les entiers qu'on cherchait pour  $m$ . Sinon  $r \neq 0$ , dans ce cas on écrit  $m = Qn + R$  avec  $Q = -q - 1$  et  $R = n - r$ , vérifiant  $1 \leq R < n$ , donc  $Q$  et  $R$  sont les entiers qu'on cherchait pour  $m$ . Il reste à montrer le résultat pour  $m \geq 0$ .

Par induction, montrons pour tout  $m \geq 0$  la propriété  $P(m) = \ll \text{il existe des entiers } q \text{ et } r \text{ tels que } m = qn + r \text{ et } 0 \leq r \leq n - 1 \gg$ .

**Initialisation :** En choisissant  $q = r = 0$ , on a bien  $0 = qn + r$  et  $0 \leq r \leq n - 1$ . D'où  $P(0)$ .

**Étape d'induction :** Soit  $m \geq 0$ . Supposons  $P(m)$  et montrons  $P(m + 1)$ . Par hypothèse, on dispose d'entiers  $q$  et  $r$  tels que  $m = qn + r$  et  $0 \leq r \leq n - 1$ . On a ainsi  $m + 1 = qn + r + 1$ . Si  $r \neq n - 1$ , alors  $1 \leq r + 1 \leq n - 1$ . Ainsi, avec  $Q = q$  et  $R = r + 1$ , on a  $m + 1 = Qn + R$  et  $0 \leq R \leq n - 1$ , donc  $Q$  et  $R$  sont les entiers qu'on cherchait pour  $m + 1$ . Sinon,  $r = n - 1$ , donc  $m + 1 = (q + 1)n$ . En posant  $Q = q + 1$  et  $R = 0$ , on obtient  $m + 1 = Qn + R$  et  $0 \leq R \leq n - 1$ , donc  $Q$  et  $R$  sont les entiers qu'on cherchait pour  $m + 1$ . D'où  $P(m + 1)$ .

D'où le résultat pour tout  $m \geq 0$ . □

### Exemple 5.2.

1. Pour  $m = 11$  et  $n = 3$ , on obtient  $q = 3$  et  $r = 2$ .
2. Pour  $m = -26$  et  $n = 5$ , on obtient  $q = -6$  et  $r = 4$ .

**Exercice 5.3.** Soit  $n \in \mathbb{N}$ .

1. Construire une bijection  $\mathbb{Z} \times \{0, \dots, n - 1\} \rightarrow \mathbb{Z}$ .
2. Construire une bijection  $\mathbb{N} \times \{0, \dots, n - 1\} \rightarrow \mathbb{N}$ .

**Corollaire 5.4.** *Un entier  $m \in \mathbb{Z}$  est impair si et seulement s'il existe un entier  $q$  tel que  $m = 2q + 1$ .*

**Preuve.** Supposons  $m$  impair. Il existe un unique entier  $q$  et un unique entier  $r$  tels que  $m = 2q + r$  et  $0 \leq r \leq 1$ . L'entier  $r$  ne peut être nul, sinon on aurait  $m = 2q$  donc  $m$  serait pair, ce qui est exclu. Donc  $r = 1$  et on obtient  $m = 2q + 1$ .

Réciproquement, supposons qu'il existe un entier  $q$  tel que  $m = 2q + 1$ , et montrons que  $m$  est impair. Par l'absurde, on va supposer que  $m$  est pair. Il existe donc un entier  $Q$  tel que  $m = 2Q$ . Alors les couples  $(q, 1)$  et  $(Q, 0)$  satisfont les hypothèses de la division euclidienne, donc l'unicité entraîne  $q = Q$  et  $1 = 0$ , c'est absurde. Donc  $m$  est impair. □

**Exercice 5.5.** Montrer que pour tout  $n \in \mathbb{Z}$ ,  $n$  est pair ou  $n + 1$  est pair.

**Exercice 5.6.** En utilisant la décomposition paire – impaire, construire une bijection entre  $\mathbb{N}$  et  $\mathbb{Z}$ .

## 5.2 Entiers modulo $n$

Nous rappelons que les notions de relation et de relation d'équivalence ont été introduites dans la section 2.4 du chapitre 2. Le but d'une relation d'équivalence est de classer les éléments d'un ensemble pour n'en retenir que l'information qui nous intéresse.

Dans le cas de l'ensemble  $\mathbb{Z}$ , classer les entiers selon le reste de leur division euclidienne par  $n$  est une information suffisante pour résoudre certains problèmes.

**Exemple 5.7.** Regardons l'équation  $x^2 = 5y + 3$ , pour  $x$  et  $y$  entiers. On remarque que 3 est le reste de la division de  $x^2$  par 5. Mais comme on le verra, le reste de la division d'un carré par 5 ne vaut jamais 3. Donc l'information sur le reste de la division par 5 est suffisante pour montrer que l'équation n'a pas de solution.

Définissons donc la relation d'équivalence qui permet de classer les entiers comme voulu.

**Définition 5.8.** Soit  $n \in \mathbb{N}$ . On définit une relation  $\equiv$  sur  $\mathbb{Z}$  par :

$$\forall x, y \in \mathbb{Z}, x \equiv y \iff n \mid (x - y).$$

Pour marquer la dépendance en l'entier  $n$ , on notera plus explicitement

$$x \equiv y \pmod{n},$$

cela se lit «  $x$  et  $y$  sont équivalents (ou congruents) modulo  $n$  » ou «  $x$  et  $y$  sont équivalents (ou congruents) mod  $n$  » pour faire court.

Tout entier  $a$  s'écrit  $a \cdot 1$ , autrement dit 1 est diviseur de tout entier. Ainsi, l'équivalence mod 1 n'a rien d'intéressant puisque tous les entiers sont reliés entre eux. L'équivalence mod  $n$  n'aura d'intérêt que pour  $n \geq 2$ .

**Exemple 5.9.**

1.  $x \equiv y \pmod{2}$  si et seulement si  $x - y$  est pair. Si c'est le cas, alors ou bien  $x$  et  $y$  sont pairs, ou bien  $x$  et  $y$  sont impairs.
2.  $23 \equiv 2 \pmod{7}$  car  $23 = 3 \times 7 + 2$ . Mais on a également  $23 \equiv 9 \pmod{7}$  car  $23 = 2 \times 7 + 9$ .
3. Étant donné un entier  $m$  et un entier positif  $n$ , on a  $m \equiv r \pmod{n}$  où  $r$  est le reste de la division euclidienne de  $m$  par  $n$ . En effet, on a  $m - r = qn$  où  $q$  est le quotient, donc  $n$  divise  $m - r$ .

**Proposition 5.10.** Pour tout  $n \in \mathbb{N}$ , l'équivalence mod  $n$  est une relation d'équivalence.

**Preuve.** Soit  $n \in \mathbb{N}$ . **Réflexivité :** Soit  $x \in \mathbb{Z}$ . Par la proposition 3.8,  $n$  est un diviseur de 0, c'est-à-dire de  $x - x$ . Donc  $x \equiv x \pmod{n}$ .

**Symétrie :** Soient  $x, y \in \mathbb{Z}$  tels que  $x \equiv y \pmod{n}$ . Alors  $n \mid (x - y)$ , donc  $n \mid (y - x)$  (proposition 3.9), donc  $y \equiv x \pmod{n}$ .

**Transitivité :** Soient  $x, y, z \in \mathbb{Z}$  tels que  $x \equiv y \pmod{n}$  et  $y \equiv z \pmod{n}$ . Alors  $n$  divise  $x - y$  et  $y - z$ . Par la proposition 3.9,  $n$  divise  $x - y + y - z$ , c'est-à-dire  $x - z$ , donc  $x \equiv z \pmod{n}$ .  $\square$

**Définition 5.11.** Soit  $n \in \mathbb{N}$ . L'ensemble  $\mathbb{Z}/\equiv$  des classes d'équivalence de «  $\equiv \pmod{n}$  » est plus communément noté  $\mathbb{Z}_n$  ou  $\mathbb{Z}/n\mathbb{Z}$ .

Par exemple,  $\mathbb{Z}_1 = \{\mathbb{Z}\}$ .

**Proposition 5.12.** Soit  $n \in \mathbb{N}$ . Il y a exactement  $n$  classes d'équivalence mod  $n$  :  $[0], [1], \dots, [n-1]$ . Autrement dit, l'ensemble  $\{0, 1, \dots, n-1\}$  est un système de représentants de la relation d'équivalence modulo  $n$ .

Ainsi  $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$  et l'ensemble est de cardinal  $n$ .

**Preuve.** Soit  $m$  un entier. L'existence d'une division euclidienne entraîne l'existence d'un entier  $r \in \{0, \dots, n-1\}$  tel que  $m \equiv r \pmod{n}$ , c'est-à-dire  $m \in [r]$ . On a donc montré que  $m$  appartient à au moins une des classes parmi  $[0], [1], \dots, [n-1]$ . De plus, si  $m$  appartient à  $[i]$  pour un certain entier  $i \in \{0, \dots, n-1\}$ , l'unicité de la division euclidienne caractérise l'entier  $i$  comme le reste de la division par  $n$ . Ainsi  $m$  n'appartient qu'à une seule des classes parmi  $[0], [1], \dots, [n-1]$ .  $\square$

En classant les entiers, il se pourrait qu'on perde toute la structure sur  $\mathbb{Z}$  avec ses opérations  $+$  et  $\cdot$ . La propriété suivante est cruciale pour la suite. Elle exprime le fait que l'addition et la multiplication sur  $\mathbb{Z}$  se comportent bien avec l'équivalence mod  $n$ , au point de permettre de définir naturellement des opérations sur  $\mathbb{Z}_n$ .

**Proposition 5.13.** Soit  $n \in \mathbb{N}$ . Soient  $a, a', b, b'$  des entiers tels que  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ . Alors

1.  $a + a' \equiv b + b' \pmod{n}$  ;
2.  $aa' \equiv bb' \pmod{n}$ .

**Preuve.** Soient  $c$  et  $c'$  des entiers tels que  $a - b = nc$  et  $a' - b' = nc'$ .

1. On a  $(a + a') - (b + b') = (a - b) + (a' - b') = (c + c')n$ , donc  $n$  divise  $(a + a') - (b + b')$ , donc  $a + a' \equiv b + b' \pmod{n}$ .
2. On a également  $aa' = (b + nc)(b' + nc') = bb' + (bc' + b'c + ncc')n$ , d'où  $aa' \equiv bb' \pmod{n}$ .  $\square$

**Proposition/définition 5.14.** On définit une addition et une multiplication sur  $\mathbb{Z}_n$ , encore notées  $+$  et  $\cdot$ , définies par :

$$\forall a, a' \in \mathbb{Z}, [a] + [a'] = [a + a'] \text{ et } [a] \cdot [a'] = [aa'].$$

Ces opérations sont bien définies.

**Preuve.** Démontrons que ces opérations sont bien définies.

**Remarque 5.15.** Il faut d'abord comprendre quel pourrait être le problème dans les définitions. Par exemple, la définition de l'addition dit que pour calculer l'addition  $c + c'$  entre deux classes  $c$  et  $c'$ , il suffit de prendre un représentant pour chacun, c'est-à-dire des entiers  $a$  et  $a'$  tels que  $c = [a]$  et  $c' = [a']$  et de suivre la règle de calcul. Ainsi  $c + c'$  vaut la classe de  $a + a'$ . Mais si au départ on choisit plutôt d'autres représentants  $b$  et  $b'$ , on obtient la classe de  $b + b'$ . Pourquoi le résultat serait-il le même ?

Soit  $a$  et  $a'$  deux entiers. Si  $b$  et  $b'$  sont deux entiers tels que  $[a] = [b]$  et  $[a'] = [b']$ ,

c'est-à-dire  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ , alors la proposition précédente affirme que  $a + a' \equiv b + b' \pmod{n}$  et  $aa' \equiv bb' \pmod{n}$ , c'est-à-dire  $[a + a'] = [b + b']$  et  $[aa'] = [bb']$ . Donc les définitions de  $+$  et  $\cdot$  ne dépendent pas du représentant qu'on considère dans chacune des classes.  $\square$

**Remarque 5.16.** Rappelons que l'on sait que les classes modulo  $n$  sont exactement  $[0], [1], \dots, [n-1]$ .

Ainsi par commodité, on écrira souvent les classes sous la forme  $[x]$  avec  $0 \leq x \leq n-1$ , autrement dit on choisit toujours un représentant entre 0 et  $n-1$ . Si  $x$  n'est pas entre 0 et  $n-1$ , alors on calcule le reste  $r$  de sa division par  $n$ , et on obtient  $[x] = [r]$ .

Pour le calcul, on pourra parfois préférer d'autres représentants. Par exemple, si  $x \equiv n-1 \pmod{n}$ , il peut être avantageux de choisir  $-1$  comme représentant plutôt que  $n-1$ . De même, si  $x \equiv n-2 \pmod{n}$ , il peut être avantageux de choisir  $-2$  comme représentant plutôt que  $n-2$ . Donc si c'est possible, on cherche le représentant le plus proche de 0 pour des calculs moins compliqués. Les exemples suivants rendront cela plus clair.

**Exemple 5.17.**

1. Modulo 4, on a  $[3] + [2] = [3 + 2] = [5] = [1]$ .
2. Modulo 5, on a  $[4] \cdot [3] = [4 \cdot 3] = [12] = [2]$ .
3. Modulo 13, on a  $[27] \cdot [38] = [27 \cdot 38] = \dots$  Ici, nous devons calculer  $27 \cdot 38$ . Mais nous pouvons éviter de le faire si on remarque que  $[27] = [1]$  et  $[38] = [-1]$ . Ainsi  $[27] \cdot [38] = [1] \cdot [-1] = [-1]$ , qu'on peut aussi écrire  $[12]$ .

Remarquons enfin que  $+$  et  $\cdot$  dans  $\mathbb{Z}_n$  satisfont des propriétés similaires à  $+$  et  $\cdot$  dans  $\mathbb{Z}$ , plus particulièrement les axiomes A.1, A.2, A.3 et A.4.

**Proposition 5.18.** Soient  $x, y$  et  $z$  des éléments de  $\mathbb{Z}_n$  (attention, ce ne sont pas des entiers, mais des classes).

1. (commutativité)  $x + y = y + x$  et  $xy = yx$ .
2. (associativité)  $(x + y) + z = x + (y + z)$  et  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .
3. (distributivité)  $x \cdot (y + z) = x \cdot y + x \cdot z$ .
4. (neutre additif, neutre multiplicatif)  $[0]$  est l'unique élément de  $\mathbb{Z}_n$  vérifiant : pour tout  $w \in \mathbb{Z}_n$ ,  $[0] + w = w$ .  $[1]$  est l'unique élément de  $\mathbb{Z}_n$  vérifiant pour tout  $w \in \mathbb{Z}_n$ ,  $[1] \cdot w = w$ .
5. (inverse additif)  $x$  admet un unique  $w \in \mathbb{Z}_n$  vérifiant  $x + w = [0]$ . Cet élément est noté  $-x$ . Si on écrit  $x = [a]$  avec  $a \in \mathbb{Z}$ , alors  $-[a] = [-a]$ .
6. (encore une propriété sur le neutre additif) S'il existe  $w \in \mathbb{Z}_n$  tel que  $x + w = w$ , alors  $x = [0]$ .

**Preuve.** Considérons des représentants  $a, b, c \in \mathbb{Z}$  de  $x, y$  et  $z$  respectivement, c'est-à-dire que  $x = [a]$ ,  $y = [b]$  et  $z = [c]$ .

1. On utilise la commutativité de  $+$  et  $\cdot$  dans  $\mathbb{Z}$ , pour obtenir :

$$x + y = [a] + [b] = [a + b] = [b + a] = [b] + [a] = y + x$$

et

$$x \cdot y = [a] \cdot [b] = [ab] = [ba] = [b] \cdot [a] = y \cdot x.$$

2. Comme pour la commutativité, l'associativité suit de l'associativité dans  $\mathbb{Z}$ .
3. Comme pour la commutativité, la distributivité suit de la distributivité dans  $\mathbb{Z}$ .
4. Étant donné  $w \in \mathbb{Z}_n$ , qu'on note  $[d]$  pour un certain entier  $d$ , on a  $[0] + w = [0] + [d] = [0 + d] = [d] = w$ . Si un élément  $v \in \mathbb{Z}_n$  est également un neutre additif, alors en prenant  $w = [0]$ , on obtient  $v = v + [0] = [0]$ . Cela prouve que  $[0]$  est l'unique neutre additif. Preuve similaire pour le neutre multiplicatif.
5. On montre facilement que  $[-a]$  est un inverse additif de  $[a]$ . L'unicité se montre comme dans  $\mathbb{Z}$ .
6. Il suffit d'ajouter l'inverse additif  $-w$  pour obtenir  $x = [0]$ .

□

**Exercice 5.19.** Pour chacune des questions suivantes, écrivez votre réponse sous la forme standard :  $[0], [1], \dots, [n-1]$ , si on se place dans  $\mathbb{Z}_n$ .

1. Calculer l'inverse additif de  $[3]$  dans  $\mathbb{Z}_7$ .
2. Calculer l'inverse additif de  $[3]$  dans  $\mathbb{Z}_6$ .
3. Calculer l'inverse additif de  $[3]$  dans  $\mathbb{Z}_{21}$ .
4. Existe-t-il  $[a] \in \mathbb{Z}_7$  tel que  $[a] \cdot [3] = [1]$  ?
5. Existe-t-il  $[a] \in \mathbb{Z}_{12}$  tel que  $[a] \cdot [3] = [1]$  ?
6. (Comportement différent de  $\mathbb{Z}$ ) Pour tout  $n \geq 2$ , pour tout  $[a], [b] \in \mathbb{Z}_n$ , est-il vrai que  $[a] \cdot [b] = [0] \Rightarrow [a] = [0]$  ou  $[b] = [0]$  ? Sinon, trouver un contre-exemple.

Pour  $[a] \in \mathbb{Z}_n$  et  $k \in \mathbb{Z}_{\geq 0}$ , on notera  $[a]^k$  le produit  $[a] \cdot \dots \cdot [a]$  ( $k$  fois). On remarque qu'on a  $[a]^k = [a^k]$  (on peut le montrer par induction).

**Exemple 5.20.** Déterminons le chiffre des unités de  $123456^{789}$ .

Comme le chiffre des unités est le reste de la division par 10, regardons modulo 10 :

$$[123456^{789}] = [123456]^{789} = [6]^{789}.$$

Il s'agit maintenant de comprendre les puissances de la classe de 6. En calculant les premières puissances :

$$[6]^1 = [6], [6]^2 = [36] = [6], [6]^3 = [6]^2 \cdot [6] = [6] \cdot [6] = [6];$$

on conjecture que toutes les puissances (sauf  $[6]^0$ ) valent  $[6]$ .

Démontrons-le par induction. **Initialisation** :  $[6]^1 = [6]$ . **Étape d'induction** : Soit  $n \in \mathbb{N}$ , supposons  $[6]^n = [6]$ . Alors  $[6]^{n+1} = [6]^n \cdot [6] = [6] \cdot [6] = [36] = [6]$ , d'où le résultat au rang  $n+1$ . D'où le résultat par induction.

Ainsi  $[6]^{789} = [6]$ . Le chiffre des unités de  $123456^{789}$  est donc 6.

**Exercice 5.21.** On reprend l'énoncé de l'exemple 3.35 : pour tout  $n \in \mathbb{N}$ ,  $11^n - 6$  est divisible par 5. On l'avait démontré par induction. Trouver une nouvelle preuve.

**Exercice 5.22.** Quel est le chiffre des unités de  $3^{2026}$  ?

**Exercice 5.23.** Montrer qu'un entier positif est divisible par 3 si et seulement si la somme des chiffres de son écriture décimale est divisible par 3.

Revenons sur l'équation mentionnée en début de section.

**Exemple 5.24.** Montrons qu'il n'existe pas d'entiers  $x$  et  $y$  satisfaisant  $x^2 = 5y + 3$ .

Par l'absurde, on suppose qu'il existe des entiers  $x$  et  $y$  satisfaisant  $x^2 = 5y + 3$ . Alors modulo 5, on obtient  $[x^2] = [3]$ , c'est-à-dire  $[x]^2 = [3]$ . Montrons que cela n'est pas possible qu'un carré  $\mathbb{Z}_5$  vale  $[3]$ . Testons donc sur les 5 éléments de  $\mathbb{Z}_5$  :

1.  $[0]^2 = [0] \neq [3]$  ;
2.  $[1]^2 = [1] \neq [3]$  ;
3.  $[2]^2 = [4] \neq [3]$  ;
4.  $[3]^2 = [9] = [4] \neq [3]$  ;
5.  $[4]^2 = [16] = [1] \neq [3]$ .

Donc il n'y a aucun carré valant  $[3]$  dans  $\mathbb{Z}_5$ . Ainsi l'équation n'a pas de solutions entières.

**Exercice 5.25.** Montrer qu'il n'existe pas d'entiers  $x$  et  $y$  tel que

$$x + 14x^2 + x^4 + 6y = 0 \text{ et } 24x + x^5 + 3y^2 = 1.$$

On raisonnera par l'absurde et on calculera modulo 3.

## 5.3 Nombres premiers, PGCD

**Définition 5.26.** Un entier  $p \geq 2$  est un *nombre premier* si ses seuls diviseurs positifs sont 1 et  $p$ , ou de manière équivalente si ses seuls diviseurs sont  $\pm 1$  et  $\pm p$ . Si un entier  $n$  s'écrit  $p_1 \dots p_k$ , où  $k \geq 1$  et pour tout  $1 \leq i \leq k$ ,  $p_i$  est premier, on parle de décomposition en facteurs premiers.

**Exemple 5.27.**

1. 2 est un nombre premier. En effet, si  $k$  est un diviseur positif de 2, alors on a  $1 \leq k \leq 2$ , donc  $k = 1$  ou  $k = 2$ .
2. 3 est un nombre premier. En effet, si  $k$  est un diviseur positif de 3, alors on a  $1 \leq k \leq 3$ , donc  $k = 1$  ou  $k = 2$  ou  $k = 3$ . Par l'absurde, si  $k = 2$ , alors on dispose de  $c \in \mathbb{N}$  tel que  $2c = 3$ . Si  $c = 1$ , alors  $2 = 3$ , ce n'est pas possible. Donc  $c \geq 2$ , donc  $2c \geq 4 > 3$ , c'est absurde. Donc  $k = 1$  ou  $k = 3$ .
3. La même méthode permet de montrer que 5, 7, 11, ..., sont premiers.
4.  $4 = 2 \times 2$  donc 2 divise 4, donc 4 n'est pas premier.

**Exercice 5.28.** Montrer que pour tout entier non nul, il existe un nombre fini de nombres premiers qui le divisent.

**Proposition 5.29.** *Tout entier  $n \geq 1$  admet une décomposition en facteurs premiers.*

**Preuve.** Nous l'avons démontré dans l'exemple 3.52. □

**Exemple 5.30.**

1.  $8 = 2 \cdot 2 \cdot 2$ .
2.  $60 = 2 \cdot 2 \cdot 3 \cdot 5$ .

**Proposition 5.31.** *Il existe une infinité de nombres premiers.*

**Preuve.** On sait déjà qu'il existe des nombres premiers  $(2, 3, 5, \dots)$ . Par l'absurde, supposons qu'ils sont en nombre fini, et notons les  $p_1, \dots, p_k$ . Posons

$$q = p_1 \dots p_k + 1.$$

Étant donné  $1 \leq i \leq k$ , le reste de la division euclidienne de  $q$  par  $p_i$  vaut 1, donc  $p_i \nmid q$  (par unicité du reste de la division euclidienne). Ainsi,  $q$  n'est divisible par aucun des  $p_1, \dots, p_k$ , donc par aucun nombre premier. Donc  $q$  n'admet pas de décomposition en facteurs premiers, cela contredit la proposition 5.29. □

**Proposition 5.32.** *Soit  $m$  et  $n$  des entiers, pas tous les deux nuls ( $m \neq 0$  ou  $n \neq 0$ ). L'ensemble*

$$\{am + bn \mid a, b \in \mathbb{Z}\} \cap \mathbb{N}$$

*est non vide, et on note  $\text{pgcd}(m, n)$  son plus petit élément (plus grand commun diviseur).*

**Exemple 5.33.**

- Si  $n > 0$ , alors  $\{bn \mid a, b \in \mathbb{Z}\} \cap \mathbb{N} = \{n, 2n, 3n, \dots\}$ . Ainsi  $\text{pgcd}(0, n) = \text{pgcd}(n, 0) = n$ .
- Prenons l'exemple  $m = 3$  et  $n = 2$ . On a  $1 = 1 \times 3 + (-1) \times 2$ , donc 1 est un élément de l'ensemble  $\{am + bn \mid a, b \in \mathbb{Z}\} \cap \mathbb{N}$ . C'est également un minorant de cet ensemble puisque 1 minore  $\mathbb{N}$ . Ainsi  $\text{pgcd}(3, 2) = 1$ .

**Preuve.** L'entier  $m^2 + n^2$  est un élément de cet ensemble. En effet, il s'écrit  $am + bn$  avec  $a = m$  et  $b = n$ . De plus,  $m^2$  et  $n^2$  sont positifs ou nuls, et au moins l'un des deux est non nul, donc  $m^2 + n^2$  est positif.

Ainsi l'ensemble  $\{am + bn \mid a, b \in \mathbb{Z}\} \cap \mathbb{N}$  est non vide. C'est également un sous-ensemble de  $\mathbb{N}$ , donc le principe du bon ordre (théorème 3.42) assure l'existence du plus petit élément, donc  $\text{pgcd}(m, n)$  est bien défini. □

**Remarque 5.34.**  $\text{pgcd}(m, n)$  est un entier positif. On ne le définit que si au moins un des deux entiers  $m$  et  $n$  est non nul.

L'énoncé suivant justifie le nom du pgcd.

**Proposition 5.35.** Soient  $m$  et  $n$  deux entiers, pas tous les deux nuls. Alors  $\text{pgcd}(m, n)$  est l'unique entier vérifiant les deux conditions :

1.  $\text{pgcd}(m, n)$  divise  $m$  et  $n$  ;
2. si  $c \in \mathbb{N}$  divise  $m$  et  $n$ , alors  $c$  divise  $\text{pgcd}(m, n)$ .

**Remarque 5.36.** La relation  $|$  étant une relation d'ordre sur  $\mathbb{N}$  (cf. l'exercice 3.12 et la proposition 3.45 du chapitre 3), on peut reformuler la proposition 5.35 de la manière suivante :  $\text{pgcd}(m, n)$  est le plus grand élément (pour la relation d'ordre  $|$ ) de l'ensemble  $\{c \in \mathbb{N} \mid c \mid m \text{ et } c \mid n\}$ .

Étant donné qu'un diviseur d'un entier est toujours plus petit (au sens de  $\leq$ ) que cet entier, on en déduit également la même propriété pour la relation d'ordre usuelle sur  $\mathbb{Z}$  :  $\text{pgcd}(m, n)$  est le plus grand élément (pour la relation d'ordre  $\leq$ ) de l'ensemble  $\{c \in \mathbb{N} \mid c \mid m \text{ et } c \mid n\}$ .

**Preuve.** Notons  $p = \text{pgcd}(m, n)$ . Par définition, on dispose d'entiers  $a$  et  $b$  tels que  $p = am + bn$ .

Montrons que  $p$  divise  $m$ . On dispose d'entiers  $q$  et  $r$  tels que  $m = qp + r$  et  $0 \leq r \leq p - 1$ . Supposons par l'absurde que  $r \neq 0$ . Comme

$$r = m - qp = (1 - qa)m + (-qb)n,$$

on obtient que  $r$  est un élément de  $\{am + bn \mid a, b \in \mathbb{Z}\} \cap \mathbb{N}$ . Par minimalité, on a donc  $r \geq p$ . Mais cela contredit  $r \leq p - 1$ . Donc  $r = 0$  et  $p$  divise  $m$ . De la même manière,  $p$  divise  $n$ .

La proposition 3.9 nous dit que si un entier  $c$  divise  $m$  et  $n$ , alors  $c$  divise  $am$  et  $bn$ , et donc divise  $am + bn$ , c'est-à-dire  $p$ .

Enfin, le fait que  $\text{pgcd}(m, n)$  est caractérisé par ces deux propriétés vient de l'unicité du plus grand élément (cf. remarque 5.36 qui reformule la proposition en terme de plus grand élément pour la relation  $|$  ou la relation  $\leq$ ).  $\square$

**Exercice 5.37.** Si  $a, b \in \mathbb{N}$  vérifient  $a \mid b$ , montrer que  $\text{pgcd}(a, b) = a$ .

Il existe aussi une méthode algorithmique pour calculer le pgcd : l'algorithme d'Euclide. C'est l'objet de l'exercice suivant.

**Exercice 5.38** (Algorithme d'Euclide). Soient  $m$  et  $n$  des entiers positifs.

- Si  $m \leq n$ , on définit  $m_1 = m$ ,  $n_1 = n$ . Sinon, on définit  $m_1 = n$  et  $n_1 = m$ . On note  $r_1$  le reste de la division de  $n_1$  par  $m_1$ .
- Soit  $k \in \mathbb{N}$ . Supposons que des entiers  $m_1, \dots, m_k$ ,  $n_1, \dots, n_k$  et  $r_1, \dots, r_k$  ont été définis, où pour tout  $1 \leq i \leq k$ ,  $m_i < n_i$  et  $r_i$  est le reste de la division de  $m_i$  par  $n_i$ .

- Si  $m_k \mid n_k$ , c'est-à-dire  $r_k = 0$ , alors l'algorithme s'arrête.
- Sinon,  $r_k \neq 0$  et on pose  $m_{k+1} = r_k$ ,  $n_{k+1} = m_k$  (on a  $m_{k+1} < n_{k+1}$  puisque  $m_{k+1}$  est le reste d'une division par  $n_{k+1}$ ). On note enfin  $r_{k+1}$  le reste de la division de  $n_{k+1}$  par  $m_{k+1}$ .

Nous allons montrer que l'algorithme s'arrête. De plus, si on note  $K$  l'entier tel que  $m_K \mid n_K$ , alors  $m_K = \text{pgcd}(m, n)$ .

1. Soient  $m$  et  $n$  des entiers, pas tous les deux nuls. On veut démontrer que pour tout  $k \in \mathbb{Z}$ , on a  $\text{pgcd}(m, n) = \text{pgcd}(m, n + km)$ .
  - (a) Soit  $k \in \mathbb{Z}$ . Démontrer l'égalité  $\{am + b(n + km) \mid a, b \in \mathbb{Z}\} = \{cm + dn \mid c, d \in \mathbb{Z}\}$ .
  - (b) Conclure.
2. En déduire que si  $m$  est non nul et si  $r$  est le reste de la division de  $n$  par  $m$ , alors  $\text{pgcd}(m, n) = \text{pgcd}(m, r)$ .

On considère maintenant  $m$  et  $n$  des entiers positifs non nuls, et on veut démontrer que l'algorithme d'Euclide appliquée à ces entiers s'arrêtent et donnent leur pgcd.

3. Supposons par l'absurde que l'algorithme ne s'arrête pas.
  - (a) Montrer que dans ce cas, l'algorithme fournit une suite  $(r_k)_{k \geq 1}$  d'entiers positifs ou nuls, qui est strictement décroissante : pour tout  $k \geq 1$ ,  $r_k > r_{k+1}$ .
  - (b) Justifier que l'ensemble  $\{r_k \mid k \in \mathbb{N}\}$  admet un plus petit élément.
  - (c) Obtenir une contradiction en utilisant ce plus petit élément.
4. Ainsi, l'algorithme s'arrête, et nous fournit des entiers  $m_1, \dots, m_K$ ,  $n_1, \dots, n_K$ ,  $r_1, \dots, r_K$ . On veut montrer que  $m_K$  est le pgcd de  $m$  et  $n$ .
  - (a) Montrer que pour tout  $1 \leq k \leq K - 1$ ,  $\text{pgcd}(m_k, n_k) = \text{pgcd}(m_{k+1}, n_{k+1})$ .
  - (b) Conclure.
5. En appliquant l'algorithme d'Euclide, déterminer  $\text{pgcd}(15, 21)$  et  $\text{pgcd}(135, 25)$ .

Le but est maintenant d'aboutir à l'unicité de la décomposition en facteurs premiers.

**Proposition 5.39.** *Soit  $m \in \mathbb{Z}$  et  $p$  un nombre premier.*

1. Si  $p \mid m$ , alors  $\text{pgcd}(m, p) = p$ .
2. Si  $p \nmid m$ , alors  $\text{pgcd}(m, p) = 1$ .

**Preuve.**

1. Si  $p$  divise  $m$ , alors  $p$  satisfait la caractérisation du pgcd :

- $p$  divise  $m$  et  $p$  divise  $p$ ;
- si un entier  $c \in \mathbb{N}$  divise  $m$  et  $p$ , alors il divise  $p$ .

Donc  $\text{pgcd}(m, p) = p$ .

2. Si  $p$  ne divise pas  $m$ , alors montrons que 1 satisfait la caractérisation du pgcd. Tout d'abord, 1 divise  $m$  et 1 divise  $p$ . Ensuite, considérons  $c \in \mathbb{N}$  qui divise  $m$  et  $p$  et montrons que  $c$  divise 1. Or l'entier  $p$  étant premier, le fait que  $c$  divise  $p$  entraîne que  $c = 1$  ou  $c = p$ . Mais  $c$  ne peut valoir  $p$  car  $c \mid m$  mais  $p \nmid m$ . Donc  $c = 1$  et ainsi  $c$  divise bien 1. D'où  $\text{pgcd}(m, p) = 1$ .

□

**Proposition 5.40.** Soient  $m$  et  $n$  des entiers, pas tous les deux nuls, et  $k \in \mathbb{N}$ . Alors

$$\text{pgcd}(km, kn) = k \cdot \text{pgcd}(m, n).$$

**Preuve.** Tout d'abord,  $k$  divise  $km$  et  $kn$ , donc  $k$  divise  $\text{pgcd}(km, kn)$ . On dispose alors de  $p \in \mathbb{N}$  tel que  $\text{pgcd}(km, kn) = kp$ . Montrons  $p = \text{pgcd}(m, n)$ . Pour cela, nous allons vérifier que  $p$  satisfait les propriétés suivantes :

- $p$  divise  $m$  et  $n$  ;
- si  $c \in \mathbb{N}$  divise  $m$  et  $n$ , alors  $c$  divise  $p$ .

On sait que  $\text{pgcd}(km, kn)$  divise  $km$ , donc il existe  $a \in \mathbb{N}$  tel que  $\text{pgcd}(km, kn) \cdot a = km$ , c'est-à-dire  $kpa = km$ . L'entier  $k$  est non nul, donc  $pa = m$ , donc  $p$  divise  $m$ . De la même manière,  $p$  divise  $n$ .

Soit  $c \in \mathbb{N}$  un entier positif divisant  $m$  et  $n$ . Alors  $kc$  divise  $km$  et  $kn$ , donc  $kc$  divise  $\text{pgcd}(km, kn)$ , c'est-à-dire que  $kc$  divise  $kp$ . Ainsi, par la même méthode, on en déduit que  $c$  divise  $p$ .

On a donc démontré que  $p$  satisfait la caractérisation de  $\text{pgcd}(m, n)$ , donc  $p = \text{pgcd}(m, n)$ . Ainsi,  $\text{pgcd}(km, kn) = kp = k \cdot \text{pgcd}(m, n)$ .  $\square$

**Proposition 5.41** (Lemme d'Euclide). Soient  $m, n \in \mathbb{N}$ , soit  $p$  un nombre premier. Si  $p$  divise  $mn$ , alors  $p$  divise  $m$  ou  $p$  divise  $n$ .

**Preuve.** Si  $p$  divise  $mn$ , supposons que  $p$  ne divise pas  $m$  et montrons que  $p$  divise  $n$ . La proposition 5.39 nous dit que  $\text{pgcd}(m, p) = 1$ . Ainsi, par la proposition 5.40, on a :

$$\text{pgcd}(mn, pn) = n \cdot \text{pgcd}(m, p) = n.$$

Or on sait par hypothèse que  $p \mid mn$ , et on sait également que  $p \mid pn$ . Par caractérisation du  $\text{pgcd}$ , on obtient que  $p$  divise  $\text{pgcd}(mn, pn)$ , c'est-à-dire que  $p$  divise  $n$ .  $\square$

**Corollaire 5.42.** Soit  $k \in \mathbb{N}$ , ainsi que  $m_1, \dots, m_k \in \mathbb{N}$ . Soit  $p$  un nombre premier. Si  $p \mid m_1 \dots m_k$ , alors il existe  $1 \leq i \leq k$  tel que  $p \mid m_i$ .

**Preuve.** Par induction, montrons pour tout  $k \in \mathbb{N}$  la propriété  $P(k) = \ll \text{pour tout } m_1, \dots, m_k \in \mathbb{N}, \text{ si } p \mid m_1 \dots m_k, \text{ alors il existe } 1 \leq i \leq k \text{ tel que } p \mid m_i \gg$ .

**Initialisation :** Soit  $m_1 \in \mathbb{N}$ . Si  $p \mid m_1$ , alors en posant  $i = 1$ , on a  $1 \leq i \leq 1$  et  $p \mid m_i$ . D'où  $P(1)$ .

**Étape d'induction :** Soit  $k \in \mathbb{N}$ . Supposons  $P(k)$  et montrons  $P(k+1)$ . Soient  $m_1, \dots, m_{k+1} \in \mathbb{N}$  tels que  $p \mid m_1 \dots m_{k+1}$ . En notant  $M = m_1 \dots m_k$  et  $N = m_{k+1}$ , on a alors  $p \mid MN$  donc  $p \mid M$  ou  $p \mid N$  d'après le lemme d'Euclide. Si  $p \mid m_{k+1}$ , alors on a le résultat voulu. Sinon, on a  $p \mid m_1 \dots m_k$ . La propriété  $P(k)$  appliquée à ces entiers  $m_1, \dots, m_k$  assure l'existence de  $1 \leq i \leq k$  tel que  $p \mid m_i$ , ce qu'on voulait. D'où  $P(k+1)$ .  $\square$

**Théorème 5.43.** Tout entier  $n \geq 1$  admet une unique décomposition en facteurs premiers : si  $n$  s'écrit  $p_1 \dots p_k$  et  $q_1 \dots q_\ell$  avec  $k, \ell \geq 0$  et des nombres premiers  $p_i$  et  $q_i$ , alors  $k = \ell$  et il existe une bijection  $f: \{1, \dots, k\} \rightarrow \{1, \dots, k\}$  tel que pour tout  $1 \leq i \leq k$ ,

$p_i = q_{f(i)}$  (autrement dit,  $p_i = q_i$  quitte à renuméroter).<sup>a</sup>

a. Par exemple,  $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2$ . Ici  $(2, 2, 3)$  et  $(2, 3, 2)$  sont les mêmes triplets quitte à réordonner les termes.

**Preuve.** L'existence d'une décomposition en facteurs premiers vient de la proposition 5.29. Démontrons maintenant l'unicité.

Par induction forte, montrons pour tout  $n \geq 1$  la propriété  $P(n) = \ll \text{si } n = p_1 \dots p_k = q_1 \dots q_\ell \text{ avec } k, \ell \geq 0 \text{ et des nombres premiers } p_i \text{ et } q_i, \text{ alors } k = \ell \text{ et } (p_1, \dots, p_k) = (q_1, \dots, q_\ell) \text{ quitte à changer la numérotation des } q_i \gg$ .

**Initialisation :** 1 n'est divisible par aucun nombre premier. Donc la seule décomposition en facteurs premiers de 1 est le produit vide, c'est-à-dire  $1 = p_1 \dots p_k$  avec  $k = 0$ . D'où  $P(1)$ .

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(1), \dots, P(n)$  et montrons  $P(n+1)$ . Soient  $k, \ell \geq 0$  et des nombres premiers  $p_1, \dots, p_k$  et  $q_1, \dots, q_\ell$  tels que  $n+1 = p_1 \dots p_k = q_1 \dots q_\ell$ . Un produit vide vaut toujours 1, mais  $n+1$  ne vaut pas 1, donc  $k$  et  $\ell$  sont  $\geq 1$ . Le nombre premier  $p_k$  divise  $q_1 \dots q_\ell$ , donc d'après le corollaire 5.42, il existe  $1 \leq j \leq \ell$  tel que  $p_k \mid q_j$ . Mais  $q_j$  étant un nombre premier,  $p_k = 1$  ou  $p_k = q_j$ , donc  $p_k = q_j$  (un nombre premier est  $\geq 2$  par définition). Quitte à changer la numérotation en intervertissant  $q_j$  et  $q_\ell$ , nous allons supposer sans perte de généralité que  $j = \ell$  (pour une écriture plus simple). Ainsi, on obtient  $p_1 \dots p_{k-1} = q_1 \dots q_{\ell-1}$  et on note  $m$  cette valeur commune. Comme  $mp_k = n+1$  avec  $p_k \geq 2$ , on a  $m < n+1$ . Ainsi, en appliquant  $P(m)$  à  $k-1, \ell-1, p_1, \dots, p_{k-1}$  et  $q_1, \dots, q_{\ell-1}$ , on obtient  $k-1 = \ell-1$ , c'est-à-dire  $k = \ell$ , ainsi qu'une bijection  $f: \{1, \dots, k-1\} \rightarrow \{1, \dots, k-1\}$  tel que  $p_i = q_{f(i)}$  pour tout  $1 \leq i \leq k-1$ , ce qui peut s'étendre à tout  $1 \leq i \leq k$  si on étend  $f$  en une bijection  $\{1, \dots, k\} \rightarrow \{1, \dots, k\}$  en posant  $f(k) = k$ . D'où  $P(n+1)$ .  $\square$

**Exercice 5.44.** Pour tout  $n \in \mathbb{N}$ , montrer qu'il existe un unique entier  $a \geq 0$  et un unique entier  $b \geq 0$  tels que  $n = 2^a(2b+1)$ . En déduire une bijection explicite de  $\mathbb{N}^2$  vers  $\mathbb{N}$  (cela donne une autre preuve du résultat de l'exercice 3.41).

**Définition 5.45.** Soit  $n \in \mathbb{N}$ .

- Pour tout nombre premier  $p$ , on définit la *valuation  $p$ -adique de  $n$*  comme étant l'entier  $\nu_p(n) = \max\{i \geq 0 \mid p^i \mid n\}$ .
- On définit  $\Pi(n)$  comme étant l'ensemble (fini) des nombres premiers qui divisent  $n$ , autrement dit  $\Pi(n) = \{p \text{ premier} \mid \nu_p(n) > 0\}$ .

**Proposition 5.46.** Soit  $n \in \mathbb{N}$ .

- Pour tout nombre premier  $p$ ,  $\nu_p(n)$  est un entier bien défini.
- La décomposition (unique) de  $n$  en facteurs premiers s'écrit :

$$n = \prod_{p \in \Pi(n)} p^{\nu_p(n)}.$$

**Exemple 5.47.**

1.  $24 = 2^3 \cdot 3$  donc  $\nu_2(24) = 3$ ,  $\nu_3(24) = 1$  et  $\nu_p(n) = 0$  pour les autres nombres premiers  $p$ .
2.  $125 = 5^3$  donc  $\nu_5(125) = 3$  et  $\nu_p(n) = 0$  pour les autres nombres premiers  $p$ .

**Preuve.** Voir l'exercice qui suit. □

**Exercice 5.48** (Autour de la valuation  $p$ -adique). On souhaite premièrement démontrer le théorème précédent, à savoir que pour tout  $n \in \mathbb{N}$ , l'entier  $\nu_p(n)$  est bien défini pour tout nombre premier  $p$ , et  $n = \prod_{p \in \Pi(n)} p^{\nu_p(n)}$ .

Soit  $n \in \mathbb{N}$ . Considérons sa décomposition unique en facteurs premiers. En regroupant les facteurs égaux, on obtient  $n = \prod_{p \in \Pi(n)} p^{\alpha_p(n)}$  où  $\alpha_p(n)$  est le nombre d'apparition de  $p$  en tant que facteur. Soit  $p$  un nombre premier.

1. Montrer que  $p^{\alpha_p(n)}$  divise  $n$ .
2. Soit  $i \in \mathbb{N}$  tel que  $p^i \mid n$ . Supposons par l'absurde que  $i > \alpha_p(n)$ .
  - (a) Montrer que  $p^{i-\alpha_p(n)}$  divise l'entier  $\frac{n}{p^{\alpha_p(n)}}$ .
  - (b) Obtenir une contradiction.
3. En déduire alors que  $\nu_p(n)$  est un entier bien défini, et une inégalité entre  $\alpha_p(n)$  et  $\nu_p(n)$ .
4. Déduire de la première question l'autre inégalité entre  $\alpha_p(n)$  et  $\nu_p(n)$ . Ainsi  $\alpha_p(n) = \nu_p(n)$ .

Voyons maintenant quelques propriétés de la valuation  $p$ -adique. Soit  $m, n \in \mathbb{N}$ .

5. Montrer que  $\nu_p(mn) = \nu_p(m) + \nu_p(n)$ .
6. Montrer l'équivalence suivante :  $m \mid n$  si et seulement si  $\nu_p(m) \leq \nu_p(n)$  pour tout nombre premier  $p$ . Dans ce cas, montrer que  $\nu_p(\frac{n}{m}) = \nu_p(n) - \nu_p(m)$ .
7. Montrer que  $\Pi(\text{pgcd}(m, n)) = \Pi(m) \cap \Pi(n)$  et que  $\nu_p(\text{pgcd}(m, n)) = \min(\nu_p(m), \nu_p(n))$ .
8. On dit que  $n$  est un *carré* s'il existe  $m \in \mathbb{N}$  tel que  $n = m^2$ . Montrer que  $n$  est un carré si et seulement si pour tout nombre premier  $p$ ,  $\nu_p(n)$  est pair.

**Définition 5.49.** Soient  $m$  et  $n$  des entiers, pas tous les deux nuls. On dit que  $m$  et  $n$  sont premiers entre eux si  $\text{pgcd}(m, n) = 1$ . Autrement dit, en utilisant la caractérisation du pgcd donné dans la proposition 5.35,  $m$  et  $n$  sont premiers entre eux si 1 est le seul entier positif qui divise  $m$  et  $n$ .

Le lemme d'Euclide peut se généraliser de la manière suivante.

**Proposition 5.50.** Soient  $a, b, c$  des entiers non nuls. On suppose que  $a$  et  $b$  sont premiers entre eux, et que  $a$  divise  $bc$ . Alors  $a$  divise  $c$ .

**Preuve.** L'entier  $a$  divise  $bc$  par hypothèse, il divise aussi  $ac$ . Ainsi  $a$  divise  $\text{pgcd}(bc, ac) = c \cdot \text{pgcd}(b, a) = c$ . □

Dans l'exercice qui suit, le théorème de Bézout est une caractérisation pour un couple d'entiers d'être premiers entre eux.

**Exercice 5.51** (Théorème de Bézout et application).

1. Soient  $m$  et  $n$  des entiers, pas tous les deux nuls. Démontrer le théorème de Bézout, à savoir que les deux assertions suivantes sont équivalentes :

- (a)  $m$  et  $n$  sont premiers entre eux ;
- (b) il existe des entiers  $a$  et  $b$  tels que  $am + bn = 1$ .

On utilisera la première définition du pgcd (comme plus petit élément d'un certain ensemble).

2. Une des applications du théorème de Bézout porte que l'existence d'un inverse multiplicatif pour un élément de  $\mathbb{Z}_n$ . Ainsi, on peut répondre sans calcul à deux questions de l'exercice 5.19 de la section précédente.

Soient  $n \geq 2$  un entier, soit  $x \in \mathbb{Z}$ . Montrer que les deux assertions suivantes sont équivalentes :

- (a)  $n$  et  $x$  sont premiers entre eux ;
- (b) il existe  $[a] \in \mathbb{Z}_n$  tel que  $[a] \cdot [x] = [1]$ .

On termine cette section avec le petit théorème de Fermat. Nous avons d'abord besoin d'un résultat préliminaire.

**Proposition 5.52.** *Soit  $p$  un nombre premier et  $k$  un entier tel que  $0 < k < p$ . Alors  $p$  divise  $\binom{p}{k}$ .*

**Preuve.** Par définition,  $\binom{p}{k}$  est l'entier positif  $c$  vérifiant  $c \cdot k! \cdot (p-k)! = p!$ . Or  $p!$  vaut  $p \cdot (p-1)!$  donc  $p$  divise  $c \cdot k! \cdot (p-k)!$ . Par le corollaire 5.42, on sait que  $p \mid c$  ou  $p \mid k!$  ou  $p \mid (p-k)!$ . Montrons que les deux derniers cas sont impossibles.

Par l'absurde,  $p \mid k!$ . Or  $k! = k \cdot (k-1) \cdot \dots \cdot 1$  donc le corollaire 5.42 nous dit qu'il existe  $1 \leq i \leq k$  tel que  $p \mid i$ . Ainsi  $p \leq i$  donc  $p \leq k$ . Cela contredit l'hypothèse  $k < p$ .

Par l'absurde,  $p \mid (p-k)!$ . Or  $(p-k)! = (p-k) \cdot (p-k-1) \cdot \dots \cdot 1$  donc le corollaire 5.42 nous dit qu'il existe  $1 \leq i \leq p-k$  tel que  $p \mid i$ . Ainsi  $p \leq i$  donc  $p \leq p-k$ . Cela contredit l'hypothèse  $k > 0$ .

Donc  $p$  divise  $c$ . □

**Corollaire 5.53.** *Soit  $p$  un nombre premier. Alors pour tous entiers  $a$  et  $b$ , on a*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

*Autrement dit, pour tout  $x, y \in \mathbb{Z}_p$ , on a*

$$(x+y)^p = x^p + y^p.$$

**Preuve.** Soient  $a, b \in \mathbb{Z}$ . Le théorème du binôme donne

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

D'après la proposition précédente,  $\binom{p}{k} \equiv 0 \pmod{p}$  dès que  $1 \leq k \leq p-1$ . Donc  $(a+b)^p \equiv a^p + b^p \pmod{p}$ . □

**Théorème 5.54** (Petit théorème de Fermat). *Si  $n \in \mathbb{Z}$  et si  $p$  est un nombre premier, alors*

$$n^p \equiv n \pmod{p}.$$

**Preuve.** Soit  $p$  un nombre premier.

Pour des raisons qui apparaîtront dans la preuve, on a besoin d'isoler le cas particulier où  $p$  est pair, c'est-à-dire  $p = 2$ . Or l'énoncé  $n^2 \equiv n \pmod{2}$  signifie que  $n^2$  et  $n$  ont même parité, ce qu'on a déjà démontré plus tôt dans ce cours. Le résultat est donc vrai pour  $p = 2$ .

Supposons maintenant que  $p$  est un nombre premier  $\geq 3$ , c'est-à-dire un nombre premier impair. Si le résultat est vrai pour tout  $n \geq 0$ , alors il est vrai pour tout  $n < 0$ . En effet, si  $n < 0$ , alors l'entier  $m = -n$  est  $\geq 0$ , donc  $m^p \equiv m \pmod{p}$ . Ainsi, modulo  $p$ , on a :

$$n^p \equiv (-m)^p \equiv (-1)^p m^p \equiv -m^p \equiv -m \equiv n,$$

où on a utilisé le fait que  $p$  est impair pour obtenir  $(-1)^p = -1$ .

Ainsi, il suffit de démontrer le résultat pour  $n \geq 0$ . Par induction, montrons pour tout  $n \geq 0$ , la propriété  $P(n) = \ll n^p \equiv n \pmod{p} \gg$ .

**Initialisation :** Puisque  $0^p = 0$ , la vérification de  $P(0)$  est immédiate.

**Étape d'induction :** Soit  $n \in \mathbb{N}$ . Supposons  $P(n)$  et montrons  $P(n+1)$ . D'après le corollaire précédent, on a  $(n+1)^p \equiv n^p + 1^p \pmod{p}$ . Or  $P(n)$  entraîne  $n^p \equiv n \pmod{p}$ , ce qui donne  $(n+1)^p \equiv n+1 \pmod{p}$ . D'où  $P(n+1)$ .  $\square$

**Exemple 5.55.** Existe-t-il des entiers  $x, y \in \mathbb{Z}$  vérifiant

$$y - (5x + y)^{50} = 1?$$

Nous allons montrer que cette équation n'a pas de solutions entières. Par l'absurde, supposons que  $(x, y)$  est un couple d'entiers solution de l'équation. Modulo 5, en appliquant le petit théorème de Fermat deux fois (5 est un nombre premier), on obtient

$$[(5x + y)^{50}] = [((5x + y)^{10})^5] = [(5x + y)^{10}] = [((5x + y)^2)^5] = [(5x + y)^2],$$

ce qui se simplifie en  $[5x + y]^2 = [y]^2$ . Donc on obtient  $[y] - [y]^2 - [1] = [0]$ . On aboutit à une contradiction une fois qu'on a remarqué qu'aucun élément  $c$  de  $\mathbb{Z}_5$  ne satisfait  $c - c^2 - [1] = [0]$  :

- $[0] - [0]^2 - [1] = -[1]$  ;
- $[1] - [1]^2 - [1] = -[1]$  ;
- $[2] - [2]^2 - [1] = -[3]$  ;
- $[3] - [3]^2 - [1] = -[7]$  ;
- $[4] - [4]^2 - [1] = -[13]$ .

Donc il n'existe pas de solutions entières.

**Exercice 5.56.** Soit  $p$  un nombre premier. Montrer que pour tout  $n \in \mathbb{Z}$ , l'entier  $3n^{p^2} - 5n^{p^3} + 2n$  est divisible par  $p$ .

**Corollaire 5.57.** Si  $n \in \mathbb{Z}$  et si  $p$  est un nombre premier qui ne divise pas  $n$ , alors

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

Remarquons que le résultat est faux lorsque  $p \mid n$ . En effet, on a alors  $n \equiv 0$ , donc  $n^{p-1} \equiv 0$ .

**Preuve.** Par le petit théorème de Fermat,  $n^p \equiv n \pmod{p}$ , c'est-à-dire  $p \mid (n^p - n)$ . Or  $n^p - n = (n^{p-1} - 1) \cdot n$  donc le lemme d'Euclide implique que  $p \mid (n^{p-1} - 1)$  ou  $p \mid n$ . Mais par hypothèse,  $p \nmid n$ . Donc  $p \mid n^{p-1} - 1$ .  $\square$

**Exercice 5.58.** Existe-t-il des entiers  $x$  et  $y$  tels que  $x^{12} + y^{12} = 5$  ?

## 5.4 Problèmes

### 5.4.1 Problème 1

On cherche les sous-ensembles  $A$  de  $\mathbb{Z}$  vérifiant les propriétés de stabilité suivantes :

- $0 \in A$  ;
- $\forall x, y \in A, x + y \in A$  ;
- $\forall x \in A, -x \in A$ .

Un tel sous-ensemble est appelé un *sous-groupe* de  $(\mathbb{Z}, +)$ .

Pour tout  $k \in \mathbb{Z}$ , on notera  $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$ . Par exemple,  $0\mathbb{Z} = \{0\}$ .

1. Soit  $k \in \mathbb{Z}$ . Montrer que  $k\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

On cherche maintenant à montrer que les  $k\mathbb{Z}$  sont les seuls sous-groupes de  $(\mathbb{Z}, +)$ . Soit  $A$  un sous-groupe de  $(\mathbb{Z}, +)$ .

2. Montrer que  $k = \min(A \cap \mathbb{N})$  est bien défini.
3. Montrer que  $k\mathbb{Z} \subset A$ .
4. Existe-t-il un élément de  $A$  compris entre 0 et  $k$  ? Existe-t-il un élément de  $A$  compris entre  $k$  et  $2k$  ?
5. Généraliser en montrant que tout élément de  $A$  est un multiple de  $k$  (on utilisera la division euclidienne par  $k$ ). Conclure.
6. Application : En déduire que si  $m$  et  $n$  sont des entiers, pas tous les deux nuls, alors il existe  $k \in \mathbb{N}$  tel que  $\{am + bn \mid a, b \in \mathbb{Z}\} = k\mathbb{Z}$ . Que vaut  $k$  par rapport à  $m$  et  $n$  ?

### 5.4.2 Problème 2

On souhaite démontrer la formule de Legendre.

**Théorème** (de Legendre). Pour tout  $n \in \mathbb{N}$ , pour tout nombre premier  $p$ , on a

$$\nu_p(n!) = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Il faut d'abord qu'on donne un sens à  $\sum_{k=0}^{\infty}$  et qu'on définisse  $\left\lfloor \frac{n}{p^k} \right\rfloor$ .

1. Soient  $a, b \in \mathbb{N}$ . Montrer que  $\max \{c \in \mathbb{N} \mid cb \leq a\}$  est bien définie. On le note  $\lfloor \frac{a}{b} \rfloor$ .<sup>1</sup>
2. Soit  $p$  un nombre premier. Montrer que pour tout  $n \in \mathbb{N}$ ,  $p^n \geq n+1$  (on utilisera l'inégalité de Bernoulli, cf. exercice 3.37).
3. Soit  $n \in \mathbb{N}$  et  $p$  un nombre premier. En déduire que pour tout  $k \geq n$ ,  $\lfloor \frac{n}{p^k} \rfloor = 0$ .

Fixons  $n \in \mathbb{N}$  et un nombre premier  $p$ . Grâce à la dernière question, on sait que les termes  $\lfloor \frac{n}{p^k} \rfloor = 0$  finisse par être nuls lorsque  $k$  est de plus en plus grand, donc la somme consiste à ajouter 0 à partir du rang  $n$ . On définira donc

$$\sum_{k=0}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=0}^{n-1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

4. Montrer que  $\nu_p(n!) = \sum_{j=1}^n \nu_p(j)$ . On utilisera ce qui est démontré dans l'exercice 5.48.
5. Montrer alors qu'on a

$$\nu_p(n!) = \sum_{k=1}^{n-1} (k \cdot \#\{1 \leq j \leq n \mid \nu_p(j) = k\}),$$

où  $\#A$  désigne le nombre d'éléments d'un ensemble  $A$  (cf. problème 4.6.1 pour plus de détail sur le nombre d'éléments d'un ensemble).

6. Soit  $k \in \mathbb{N}$ . Écrire l'ensemble  $\{1 \leq j \leq n \mid \nu_p(j) = k\}$  en fonction des ensembles de la forme  $\{1 \leq j \leq n \mid p^i \mid j\}$  pour  $i \in \mathbb{Z}_{\geq 0}$ .
7. Soit  $i \in \mathbb{Z}_{\geq 0}$ . Montrer que

$$\{1 \leq j \leq n \mid p^i \mid j\} = \left\{1, 2, \dots, \left\lfloor \frac{n}{p^i} \right\rfloor\right\}.$$

8. En déduire le nombre d'éléments de l'ensemble  $\{1 \leq j \leq n \mid \nu_p(j) = k\}$  pour tout  $k \in \mathbb{N}$ , puis terminer le travail.

### 5.4.3 Problème 3

Nous proposons une nouvelle preuve du petit théorème de Fermat. Le problème utilisera des résultats admis concernant la cardinalité (cf. problème 4.6.1 pour plus de détail).

Soit  $p$  un nombre premier. On pose  $\mathbb{Z}_p^\times = \mathbb{Z}_p - \{0\}$ .

1. Montrer que  $\mathbb{Z}_p^\times = \{[n] \mid n \in \mathbb{Z}, p \nmid n\}$ .
2. Montrer que pour tout  $x, y \in \mathbb{Z}_p^\times$ ,  $xy \in \mathbb{Z}_p^\times$ .
3. Montrer que pour tout  $x \in \mathbb{Z}_p^\times$ , il existe un unique  $z \in \mathbb{Z}_p^\times$  tel que  $xz = [1]$ , on le notera  $x^{-1}$ . On utilisera l'application du théorème de Bézout dans l'exercice 5.51.

Soit  $a \in \mathbb{Z}_p^\times$ . On note  $K = \min \{i \in \mathbb{N} \mid a^i = [1]\}$ .

4. Montrer que  $K$  est bien défini.
5. Soit  $A = \{[1], a, a^2, \dots, a^{K-1}\}$ . Montrer que la deuxième ainsi que la troisième question sont encore valables si on remplace  $\mathbb{Z}_p^\times$  par  $A$ .

---

1. Lorsqu'on parlera de nombres réels, on pourra définir  $\lfloor x \rfloor$  pour tout  $x \in \mathbb{R}$  comme étant le plus grand entier plus petit ou égal à  $x$ . Étant donné que nous ne savons pas encore ce que sont les nombres réels, encore moins ce qu'est une fraction  $\frac{a}{b}$  lorsque  $b \nmid a$ , on est obligé de proposer une définition alternative n'utilisant que ce qu'on sait faire avec  $\mathbb{Z}$ .

Important pour la suite :  $A$  admet  $K$  éléments, on notera  $\#A = K$ . On définit une relation  $\sim$  sur  $\mathbb{Z}_p^\times$  par : pour tout  $x, y \in \mathbb{Z}_p^\times$ ,  $x \sim y \iff x^{-1}y \in A$ .

6. Montrer que  $\sim$  est une relation d'équivalence sur  $\mathbb{Z}_p^\times$ .
7. Soit  $x \in \mathbb{Z}_p^\times$ . Montrer que la classe d'équivalence (pour  $\sim$ ) de  $x$  vaut  $\{x, xa, xa^2, \dots, xa^{K-1}\}$ , qu'on notera  $xA$ .
8. Soit  $x \in \mathbb{Z}_p^\times$ . Montrer que  $A$  et  $xA$  sont en bijection.

On admet que l'existence d'une bijection entre  $A$  et  $xA$  implique que  $xA$  admet également  $K$  éléments :  $\#(xA) = K$ . On admet également que si  $E$  est un ensemble et que  $\{E_1, \dots, E_i\}$  est une partition de  $E$ , alors le nombre d'éléments de  $E$  vaut la somme du nombre d'éléments des  $E_i$ , autrement dit  $\#E = \#E_1 + \dots + \#E_k$ .

9. En utilisant la partition en classes d'équivalence, montrer que  $K$  divise  $p - 1$ .<sup>2</sup>
10. En déduire que  $a^{p-1} = [1]$ .

---

2. Nous venons de démontrer le théorème de Lagrange, un résultat incontournable en théorie des groupes, que nous venons de voir dans un cas particulier. L'énoncé général, dont nous ne parlerons pas pour ne pas alourdir le propos, se démontre avec la même méthode.

# Chapitre 6

## L'ensemble des nombres réels

Nous allons maintenant introduire et étudier l'ensemble des nombres réels et l'ensemble des réels positifs, notés  $\mathbb{R}$  et  $\mathbb{R}_{>0}$ , munis d'opérations  $+$  et  $\cdot$ . Comme pour  $\mathbb{Z}$  et  $\mathbb{N}$ , nous partirons d'axiomes pour en déduire les grandes propriétés de cet ensemble. Nous ne montrerons pas qu'un tel ensemble existe, le lecteur curieux pourra s'intéresser à la construction par coupure de Dedekind, ou à la construction comme complété de  $\mathbb{Q}$  (l'ensemble des nombres rationnels).

On pourra munir  $\mathbb{R}$  d'un ordre  $\leq$  qui, contrairement à l'ordre usuelle sur  $\mathbb{Z}$ , ne vérifiera pas cette fois-ci le principe du bon ordre.

Enfin, bien qu'on sache depuis notre plus tendre enfance que  $\mathbb{Z}$  est un sous-ensemble de  $\mathbb{R}$  et  $\mathbb{N}$  un sous-ensemble de  $\mathbb{R}_{>0}$ , les axiomes de  $\mathbb{R}$  ne font mention ni de  $\mathbb{Z}$ , ni de  $\mathbb{N}$ . D'ailleurs, ces axiomes décrivent des opérations  $+$  et  $\cdot$  sur  $\mathbb{R}$  qui n'ont *a priori* rien à voir avec les opérations décrites par l'axiomatique de  $\mathbb{Z}$  et  $\mathbb{N}$ . Nous justifierons donc qu'il existe un sous-ensemble de  $\mathbb{R}$  que l'on peut identifier à  $\mathbb{Z}$ , avec des opérations  $+$  et  $\cdot$  qui sont les restrictions sur  $\mathbb{Z}$  des opérations entre réels. Le sous-ensemble  $\mathbb{N}$  de  $\mathbb{Z}$  sera un sous-ensemble de  $\mathbb{R}_{>0}$ .

### 6.1 Axiomatique de $\mathbb{R}$ et $\mathbb{R}_{>0}$

On suppose l'existence

- d'un ensemble  $\mathbb{R}$  dont les éléments sont appelés les nombres réels ;
- et d'un sous-ensemble  $\mathbb{R}_{>0} \subset \mathbb{R}$  dont les éléments sont appelés les nombres réels positifs,
- d'une addition  $+: \mathbb{R}^2 \rightarrow \mathbb{R}$  (l'évaluation en un couple  $(x, y) \in \mathbb{R}^2$  sera notée  $x + y$  plutôt que  $+(x, y)$ ) ;
- d'une multiplication  $\cdot: \mathbb{R}^2 \rightarrow \mathbb{R}$  (l'évaluation en un couple  $(x, y) \in \mathbb{R}^2$  sera notée  $x \cdot y$ , voire  $xy$ , plutôt que  $\cdot(x, y)$ ),

satisfaisant les axiomes qui suivent. Les axiomes C porteront sur  $\mathbb{R}$ , et les axiomes D concerneront plus particulièrement  $\mathbb{R}_{>0}$ .

**Axiome C.1** (Commutativité, associativité, distributivité). Pour tous réels  $x, y$  et  $z$ , on a

1.  $x + y = y + x$  ;
2.  $(x + y) + z = x + (y + z)$  ;
3.  $x \cdot (y + z) = x \cdot y + x \cdot z$  ;
4.  $x \cdot y = y \cdot x$  ;
5.  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

**Axiome C.2** (Élément neutre additif). Il existe un réel  $0$  tel que  $x + 0 = x$  pour tout  $x \in \mathbb{R}$ . Cet élément  $0$  est appelé un *élément neutre additif*, ou un *élément identité de l'addition*.

**Axiome C.3** (Élément neutre multiplicatif). Il existe un réel  $1$  tel que  $1 \neq 0$  et  $x \cdot 1 = x$  pour tout  $x \in \mathbb{R}$ . Cet élément  $1$  est appelé un *élément neutre multiplicatif*, ou un *élément identité de la multiplication*.

Ici, les éléments  $0$  et  $1$  n'ont rien à voir avec les entiers  $0$  et  $1$ . On pourra cependant les identifier une fois que nous aurons établi un lien entre  $\mathbb{Z}$  et  $\mathbb{R}$  (cf section 6.4).

**Axiome C.4** (Inverse additif). Pour tout  $x \in \mathbb{R}$ , il existe un réel, noté  $-x$  et appelé *l'inverse additif de  $x$* , tel que  $x + (-x) = 0$ .

**Attention.** L'élément  $-x$  est seulement défini par la propriété décrite par l'axiome, il n'est pas défini comme «  $x$  multiplié par  $-1$  » (et une telle définition nécessiterait d'abord de définir  $-1$ ). Les axiomes permettront cependant d'aboutir à l'égalité  $-x = (-1) \cdot x$ .

Jusqu'ici, les axiomes formulés sont analogues aux axiomes A.1, A.2, A.3 et A.4. Le prochain axiome est plus fort que l'analogue de l'axiome A.5 pour  $\mathbb{R}$ .

**Axiome C.5** (Inverse multiplicatif). Pour tout  $x \in \mathbb{R} - \{0\}$ , il existe un nombre réel, noté  $x^{-1}$ , tel que  $x \cdot x^{-1} = 1$ . L'élément  $x^{-1}$  est appelé un *inverse multiplicatif de  $x$* .

Justifions que l'axiome C.5 est plus fort que l'analogue de l'axiome A.5 où l'on remplace  $\mathbb{Z}$  par  $\mathbb{R}$ .

**Proposition 6.1.** Pour tout  $x, y, z \in \mathbb{R}$ , si  $xy = xz$  et  $x \neq 0$ , alors  $y = z$ .

**Preuve.** Le nombre réel  $x$  n'est pas nul, donc l'axiome C.5 affirme qu'il possède un inverse multiplicatif, c'est-à-dire un réel  $x^{-1}$  tel que  $x \cdot x^{-1} = 1$ . Par commutativité, on a  $x^{-1}x = 1$ . Ainsi l'égalité  $xy = xz$  entraîne  $x^{-1} \cdot xy = x^{-1} \cdot xz$ , c'est-à-dire  $y = z$ .  $\square$

Reprenons l'énumération des axiomes.

Le principe du bon ordre sur  $\mathbb{Z}$  implique que tout sous-ensemble majoré de  $\mathbb{Z}$  admet un plus grand élément. Pour qu'un énoncé similaire soit vraie dans  $\mathbb{R}$ , il faut affaiblir la notion de plus grand élément. On s'intéresse alors à la nouvelle notion (plus faible) de *plus petite borne supérieure*, elle sera définie plus tard. Cette affaiblissement est nécessaire car nous verrons que des ensembles majorés de  $\mathbb{R}$  n'admettent pas de plus grand élément.

**Axiome C.6** (Axiome de complétude). Tout sous-ensemble non vide de  $\mathbb{R}$  qui est borné supérieurement admet une plus petite borne supérieure.

Enfin, pour  $\mathbb{R}_{>0}$ , l'axiome suivant est l'analogue de l'axiome B.1.

**Axiome D.1.**

1. Si  $x, y \in \mathbb{R}_{>0}$ , alors  $x + y \in \mathbb{R}_{>0}$  ( $\mathbb{R}_{>0}$  est fermé sous l'addition);

2. Si  $x, y \in \mathbb{R}_{>0}$ , alors  $xy \in \mathbb{R}_{>0}$  ( $\mathbb{R}_{>0}$  est fermé sous la multiplication) ;
3.  $0 \notin \mathbb{R}_{>0}$  ;
4. Pour tout  $x \in \mathbb{R}$ , on a  $x \in \mathbb{R}_{>0}$  ou  $x = 0$  ou  $-x \in \mathbb{R}_{>0}$ .

**Attention.** Dans certaines références, 0 est un élément de  $\mathbb{R}_{>0}$ .

On dira qu'un réel est *néglatif* s'il n'appartient pas à  $\mathbb{R}_{>0}$  et ne vaut pas 0. Ainsi, un réel est ou bien positif, ou bien négatif, ou bien nul (nul signifiant « égal à 0 »).

**Remarque 6.2.** Il n'y a pas d'axiome analogue à l'axiome B.2 (l'axiome d'induction). Remarquons que c'est cet axiome qui permet de décrire la structure de  $\mathbb{Z}$  muni de sa relation d'ordre. Par exemple, grâce à cet axiome, on peut lister les éléments de  $\mathbb{N}$  dans l'ordre croissant :  $1 < 2 < 3 < 4 < \dots$  ; et entre deux éléments consécutifs, il n'y a rien. Comme on le verra avec  $\mathbb{R}$ , entre deux réels  $x$  et  $y$  tels que  $x < y$ , il existe toujours un autre réel  $z$  tel que  $x < z < y$ .

Remarquons que  $\mathbb{N} \subset \mathbb{Z}$  vérifient tous les axiomes de  $\mathbb{R}_{>0} \subset \mathbb{R}$ , sauf l'axiome C.5 qui est bien plus fort que l'axiome A.5. C'est donc finalement cet axiome qui permet d'obtenir une structure plus riche que la structure sur  $\mathbb{Z}$ .

Enfin, l'axiome C.6 est pertinent car il permet de différencier  $\mathbb{Q}$  et  $\mathbb{R}$  ( $\mathbb{Q}$  ne satisfait pas cet axiome). Dans l'ensemble  $\mathbb{Q}$ , il manque des nombres très importants qui apparaissent naturellement en mathématiques ( $\pi$  quand on étudie un cercle,  $\sqrt{2}$  quand on étudie la longueur de l'hypoténuse d'un triangle rectangle). Nous verrons dans la section 6.7 que c'est grâce à cet axiome de complétude qu'on peut définir le réel  $\sqrt{2}$ . L'axiome de complétude permet en quelque sorte de combler les trous qu'il y a dans l'ensemble  $\mathbb{Q}$ , et c'est d'ailleurs cette idée qu'on retrouve derrière les constructions classiques de  $\mathbb{R}$  à partir de  $\mathbb{Q}$  (pour les plus curieux : construction de  $\mathbb{R}$  comme complété de  $\mathbb{Q}$ , construction de  $\mathbb{R}$  par coupure de Dedekind).

## 6.2 Premières conséquences

Les propositions 3.2 et 3.3 sont encore valables si on remplace  $\mathbb{Z}$  par  $\mathbb{R}$ . En particulier, il y a unicité des neutres additif et multiplicatif, et de l'inverse additif d'un nombre réel. La définition de la soustraction dans  $\mathbb{R}$  est similaire, ce qui signifie que la proposition/définition 3.4 est encore valable, et les propriétés de la soustraction sont encore vraies (proposition 3.5).

La notion de divisibilité n'a aucun intérêt dans  $\mathbb{R}$ . En effet, pour tout  $x, y \in \mathbb{R}$  tel que  $x \neq 0$ , on a  $y = zx$  avec  $z = yx^{-1}$ , donc  $x \mid y$ .

Montrons quelques propriétés vérifiées par l'inverse multiplicatif.

**Proposition 6.3.** Soient  $x$  et  $y$  des réels non nuls.

1. Si  $z \in \mathbb{R}$  satisfait  $xz = 1$ , alors  $z = x^{-1}$ . Ainsi, il existe un unique inverse multiplicatif.
2. (Involution)  $(x^{-1})^{-1} = x$ .
3.  $(-x)^{-1} = -(x^{-1})$ .
4.  $(xy)^{-1} = y^{-1}x^{-1}$ .

**Preuve.**

1. Dans l'égalité  $xz = 1$ , on multiplie par  $x^{-1}$  et on obtient  $z = x^{-1}$ .
2. Par définition de  $x^{-1}$ , on a  $x^{-1}x = 1$ . Tout d'abord, cela implique que  $x^{-1}$  est non nul (sinon  $x^{-1}x = 0$ ), donc admet bien un inverse multiplicatif. Ensuite, cela implique que  $x$  est l'unique réel  $z$  vérifiant  $x^{-1}z = 1$ . Donc  $x$  est l'inverse multiplicatif de  $x^{-1}$ .
3. Tout d'abord,  $-x$  est non nul donc admet bien un inverse multiplicatif. L'identité  $X(-Y) = (-X)Y$  (valable pour tout réels  $X, Y \in \mathbb{R}$ ) permet d'obtenir  $-(x^{-1}) \cdot (-x) = x^{-1} \cdot x = 1$ . Donc  $-(x^{-1})$  est l'unique réel  $z$  tel que  $z \cdot (-x) = 1$ , donc c'est l'inverse multiplicatif de  $-x$ .
4.  $xy$  est non nul donc admet bien un inverse multiplicatif. On a  $y^{-1}x^{-1} \cdot xy = y^{-1}(x^{-1} \cdot x)y = y^{-1}y = 1$ . Donc  $y^{-1}x^{-1}$  est l'unique réel  $z$  tel que  $z \cdot xy = 1$ , donc c'est l'inverse multiplicatif de  $xy$ .

□

On définit la division avec les mêmes idées que pour la soustraction.

**Proposition/définition 6.4.** *Étant donnés des réels  $x$  et  $y$ , avec  $y$  non nul, il existe un unique réel  $z$  tel que  $yz = x$ . Il s'agit de  $xy^{-1}$ , et on le note  $\frac{x}{y}$  («  $x$  divisé par  $y$  », «  $x$  sur  $y$  »).*

**Attention.**  $\frac{x}{y}$  n'est pas défini si  $y = 0$ . En effet, si  $x \neq 0$ , alors on ne peut pas avoir une écriture de la forme  $yz = x$  (car  $yz = 0$ ). Et si  $x = 0$ , alors l'égalité  $yz = x$  est valable pour tout réel  $z$ , il n'y a donc pas d'unicité.

**Proposition 6.5.** *Soient  $x, y, z, w$  des réels,  $z$  et  $w$  non nuls.*

1.  $\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z}$ .
2.  $\frac{x}{z} + \frac{y}{w} = \frac{xw + yz}{zw}$ .
3.  $\frac{xw}{zw} = \frac{x}{z}$ .
4.  $\frac{-x}{z} = \frac{x}{-z} = -\frac{x}{z}$ .
5.  $x \frac{y}{z} = \frac{xy}{z}$ .
6.  $\frac{x}{\left(\frac{z}{w}\right)} = \frac{xw}{z}$ .
7.  $\frac{x}{z} = 0 \iff x = 0$ .

**Preuve.** Exercice.

□

**Exercice 6.6.** Démontrer la proposition ci-dessus, dont la preuve a été laissée en exercice.

## 6.3 Ordre sur les réels

Nous définissons un ordre sur  $\mathbb{R}$  en utilisant  $\mathbb{R}_{>0}$ , comme nous l'avions fait avec  $\mathbb{Z}$  et  $\mathbb{N}$ . Les propositions qui suivent se démontrent comme dans le chapitre 3, nous n'écrirons donc pas la preuve. Nous ajouterons cependant les propriétés reliant la relation d'ordre et les inverses multiplicatifs.

**Définition 6.7.** On définit la relation  $<$  sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, x < y \iff y - x \in \mathbb{R}_{>0},$$

et la relation  $\leq$  sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, x \leq y \iff x < y \text{ ou } x = y.$$

**Définition 6.8** (Intervalles). Pour  $x, y \in \mathbb{R}$ , on définit :

- $[x, y] = \{z \in \mathbb{R} \mid x \leq z \leq y\}$  ;
- $(x, y] = \{z \in \mathbb{R} \mid x < z \leq y\}$  ;
- $[x, y) = \{z \in \mathbb{R} \mid x \leq z < y\}$  ;
- $(x, y) = \{z \in \mathbb{R} \mid x < z < y\}$  ;
- $(-\infty, y] = \{z \in \mathbb{R} \mid z \leq y\}$  ;
- $(-\infty, y) = \{z \in \mathbb{R} \mid z < y\}$  ;
- $[x, \infty) = \{z \in \mathbb{R} \mid x \leq z\}$  ;
- $(x, \infty) = \{z \in \mathbb{R} \mid x < z\}$  ;
- $(-\infty, \infty) = \mathbb{R}$ .

**Attention.** Les symboles  $-\infty$  et  $\infty$  ne désignent pas des réels. Ce sont juste des notations afin de désigner certains intervalles.

Ne pas confondre l'intervalle  $(x, y)$  et le couple  $(x, y) \in \mathbb{R}^2$ . Si le contexte n'est pas clair, alors des précisions sont nécessaires.

**Proposition 6.9.**

1. Pour tout  $x \in \mathbb{R}$ , la disjonction «  $x \in \mathbb{R}_{>0}$  ou  $x = 0$  ou  $-x \in \mathbb{R}_{>0}$  » est une disjonction exclusive.
2. Pour tout  $x, y \in \mathbb{R}$ , l'assertion «  $x < y$  ou  $x = y$  ou  $y < x$  » est vraie, et c'est une disjonction exclusive.
3.  $\mathbb{R}_{>0} = (0, \infty)$  ;
4.  $\mathbb{R} - (\mathbb{R}_{>0} \cup \{0\}) = (-\infty, 0) = \{-x \mid x \in \mathbb{R}_{>0}\}$  (noté  $-\mathbb{R}_{>0}$ ) ;
5. La relation  $\leq$  est une relation d'ordre totale. La relation  $<$  est transitive.

**Notation.** On notera  $\mathbb{R}_{\geq 0} = [0, \infty) = \mathbb{R}_{>0} \cup \{0\}$ .

**Attention aux conventions.** Dans la littérature,  $\mathbb{R}_{>0}$  peut correspondre à notre ensemble  $\mathbb{R}_{\geq 0}$ .

Ainsi on a une décomposition  $\mathbb{R} = -\mathbb{R}_{>0} \sqcup \{0\} \sqcup \mathbb{R}_{>0}$  qui correspond à la décomposition « négatif – nul – positif ».

**Remarque 6.10.** Pour tout  $x, y \in \mathbb{R}$ , on a

$$\begin{aligned} [x, x] &= \{x\}, \\ (x, x) &= \emptyset, \\ x > y &\Rightarrow [x, y] = \emptyset, \\ x \geq y &\Rightarrow (x, y] = [x, y) = (x, y) = \emptyset. \end{aligned}$$

**Proposition 6.11.** Pour tout réel  $x$  non nul,  $x^2 \in \mathbb{R}_{>0}$ . Ainsi,  $1 \in \mathbb{R}_{>0}$  (car  $1 = 1 \cdot 1$ ).

**Remarque 6.12.** Ainsi le nombre réel 2 défini par  $2 = 1 + 1$  est aussi dans  $\mathbb{R}_{>0}$ , par fermeture sous addition.

On en déduit aussi que  $-1$  n'est pas dans  $\mathbb{R}_{>0}$ . En particulier, il n'existe pas de réel  $x$  tel que  $x \cdot x = -1$ .

**Corollaire 6.13.** Pour tout réel  $x$ , on a  $x + 1 > x > x - 1$ . Ainsi  $\mathbb{R}$  et  $\mathbb{R}_{>0}$  n'admettent pas de plus grand élément, et  $\mathbb{R}$  n'admet pas de plus petit élément.

Contrairement à  $\mathbb{N}$ , nous verrons que  $\mathbb{R}_{>0}$  n'admet pas de plus petit élément. En revanche, cet ensemble admet une plus grande borne inférieure : il s'agit de 0. Nous le verrons plus tard.

**Proposition 6.14.** Soient  $x, y, z$  et  $w$  des réels.

1. Si  $x \in \mathbb{R}_{>0}$ , alors  $xy \in \mathbb{R}_{>0} \iff y \in \mathbb{R}_{>0}$ .
2. Si  $x < y$ , alors  $x + z < y + z$ .
3. Si  $x < y$  et  $z \leq w$ , alors  $x + z < y + w$ .
4. Si  $z > 0$ , alors  $x < y \iff xz < yz$ .
5.  $x > y \iff -x < -y$ .
6. Si  $z < 0$ , alors  $x < y \iff xz > yz$ .
7. Si  $0 < x < y$  et  $0 < z \leq w$ , alors  $xz < yw$ .

On peut aussi placer des inégalités larges dans l'énoncés. Par exemple, on peut démontrer

- $x \leq y$  et  $z \leq w \Rightarrow x + z \leq y + w$  ;
- $z > 0 \Rightarrow (x \leq y \iff xz \leq yz)$  ;
- $x \geq y \iff -x \leq -y$  ;
- etc.

Parlons maintenant du comportement de la relation d'ordre vis-à-vis du passage à l'inverse multiplicatif. Ce sont des propriétés non abordées dans le cas de  $\mathbb{Z}$ , l'inverse multiplicatif n'existant pas dans ce cadre.

**Remarque 6.15.** Notons que si  $x, y, z$  sont des réels, avec  $z \neq 0$ , alors  $\frac{x}{z}$  et  $\frac{y}{z}$  sont tout simplement  $x$  et  $y$  qu'on a multipliés par le réel  $\frac{1}{z}$ . Donc les propriétés du type «  $x < y \iff \frac{x}{z} < \frac{y}{z}$  » ou «  $x < y \iff \frac{y}{z} < \frac{x}{z}$  » (selon les cas) se déduisent de la proposition précédente. Cela demande de connaître le signe de  $\frac{1}{z}$ , c'est le propos de l'énoncé suivant.

**Proposition 6.16.** Soient  $x, y \in \mathbb{R}$ .

1.  $x > 0 \iff \frac{1}{x} > 0$ .
2. Si  $0 < x < y$ , alors  $0 < \frac{1}{y} < \frac{1}{x}$ .

**Preuve.**

1. Supposons  $x > 0$ . Comme  $x > 0$  et  $x \cdot x^{-1} = 1 > 0$ , la propriété 1 de la proposition 6.14 donne  $x^{-1} > 0$ . L'implication directe est en fait valable pour tout  $x > 0$ . On l'applique maintenant à  $\frac{1}{x}$  au lieu de  $x$  et on obtient la réciproque (on utilise la propriété d'involution  $(x^{-1})^{-1} = x$ ).
2. Supposons  $0 < x < y$ . Par le premier point, on sait alors que les réels  $\frac{1}{x}$  et  $\frac{1}{y}$  sont positifs. On utilise en deux temps la propriété 4 de la proposition 6.14. Dans un premier temps, en multipliant par  $\frac{1}{x}$ , on obtient  $\frac{1}{x}x < \frac{1}{x}y$ , c'est-à-dire  $1 < \frac{1}{x}y$ . Dans un second temps, en multipliant par  $\frac{1}{y}$ , on obtient  $\frac{1}{y} < \frac{1}{x} \frac{1}{y}y$ , c'est-à-dire  $\frac{1}{y} < \frac{1}{x}$ .  $\square$

**Exemple 6.17.** Montrons que pour tout  $x \in \mathbb{R}$ , on a

$$x^4 < 2x^5 \iff x > \frac{1}{2}.$$

Soit  $x$  réel vérifiant  $x^4 < 2x^5$ . Si  $x = 0$ , alors on obtient  $0 < 0$ , c'est absurde. Ainsi  $x \neq 0$ , donc  $x^4 \neq 0$ , donc  $\frac{1}{x^4}$  est bien défini. De plus,  $x^4 = (x^2)^2 > 0$ , donc  $\frac{1}{x^4} > 0$ . Cela donne donc  $x^4 \frac{1}{x^4} < 2x^5 \frac{1}{x^4}$ , c'est-à-dire  $1 < 2x$ . Puis  $2 > 0$ , donc  $\frac{1}{2} > 0$ , donc on peut multiplier par  $\frac{1}{2}$  sans changer l'inégalité, et cela donne  $x > \frac{1}{2}$ .

Réciproquement, si  $x > \frac{1}{2}$ , alors comme  $x^4 > 0$ , cela donne  $x^4 \cdot x > x^4 \frac{1}{2}$ , c'est-à-dire  $x^5 > \frac{x^4}{2}$ .

**Exercice 6.18.** Soit  $x, y \in \mathbb{R}$ . Montrer les assertions suivantes.

1.  $xy \in \mathbb{R}_{>0} \iff x, y \in \mathbb{R}_{>0} \text{ ou } -x, -y \in \mathbb{R}_{>0}$ .
2.  $\frac{x}{y} \in \mathbb{R}_{>0} \iff x, y \in \mathbb{R}_{>0} \text{ ou } -x, -y \in \mathbb{R}_{>0}$ .
3.  $x^2 > 4 \iff x > 2 \text{ ou } x < -2$ .

**Exercice 6.19.** Déterminer l'ensemble  $\{x^{-1} \mid x > 0\}$ .

On en vient maintenant à la différence notable entre l'ordre sur  $\mathbb{R}$  et l'ordre sur  $\mathbb{Z}$ . L'énoncé suivant est à comparer avec la proposition 3.39.

**Proposition 6.20.** Pour tout  $x, y \in \mathbb{R}$  tels que  $x < y$ , il existe  $z \in (x, y)$ .

Ainsi, contrairement aux entiers, on ne peut pas parler de « réels consécutifs ».

**Preuve.** Soient  $x, y \in \mathbb{R}$  tels que  $x < y$ . Posons  $z = \frac{y+x}{2}$  et montrons que  $z$  convient. D'une part,

$$z - x = \frac{y + x - 2x}{2} = \frac{y - x}{2}$$

où  $y - x > 0$ , donc  $z - x > 0$ , donc  $z > x$ . D'autre part,

$$z - y = \frac{y + x - 2y}{2} = \frac{x - y}{2}$$

où  $x - y < 0$ , donc  $z - y < 0$ , donc  $z < y$ . □

## 6.4 $\mathbb{Z}$ comme sous-ensemble de $\mathbb{R}$

Dans les chapitres 3 et 6, nous n'étudions pas seulement des ensembles  $\mathbb{R}$  et  $\mathbb{Z}$ , nous les étudions munis d'opérations et d'une relation d'ordre. On peut faire l'analogie avec un château de sable : ce n'est qu'un tas de sable mais on s'y intéresse parce qu'on l'a structuré d'une certaine manière. Il en est de même pour  $\mathbb{R}$  et  $\mathbb{Z}$ , sans la structure donnée par les opérations et la relation d'ordre, nous n'avons rien à dire sur ces ensembles.

Les axiomes de  $\mathbb{R}$  ne font jamais mention de  $\mathbb{Z}$ , alors qu'on a très envie d'identifier le neutre additif  $0_{\mathbb{R}}$  de  $\mathbb{R}$  avec le neutre additif  $0_{\mathbb{Z}}$  de  $\mathbb{Z}$ , puis  $1_{\mathbb{R}}$  avec  $1_{\mathbb{Z}}$ , puis  $1_{\mathbb{R}} + 1_{\mathbb{R}}$  avec  $1_{\mathbb{Z}} + 1_{\mathbb{Z}}$ , etc. De manière générale, on aimerait transférer la structure de  $\mathbb{Z}$  dans la structure de  $\mathbb{R}$ . On cherche ainsi une fonction injective  $f: \mathbb{Z} \rightarrow \mathbb{R}$ , qui envoie  $0_{\mathbb{Z}}$  sur  $0_{\mathbb{R}}$ ,  $1_{\mathbb{Z}}$  sur  $1_{\mathbb{R}}$ , qui se comporte bien avec l'addition, avec le passage à l'inverse additif (donc avec la soustraction) et avec la multiplication. L'injectivité permet alors d'obtenir une bijection entre  $\mathbb{Z}$  et  $f(\mathbb{Z})$  (en corestreignant la fonction à son image) et donc d'identifier  $\mathbb{Z}$  à  $f(\mathbb{Z})$ .

On définit  $f: \mathbb{Z} \rightarrow \mathbb{R}$  par :

- (définition récursive sur  $\mathbb{Z}_{\geq 0}$ )  $f(0_{\mathbb{Z}}) = 0_{\mathbb{R}}$ , puis pour tout  $n \in \mathbb{Z}_{\geq 0}$ , si  $f(n)$  a été défini, alors  $f(n+1) = f(n) + 1_{\mathbb{R}}$  ;
- (définition sur  $-\mathbb{N}$  à partir de la définition sur  $\mathbb{N}$ ) pour tout  $n \in \mathbb{Z}_{\geq 0}$ ,  $f(-n) = -f(n)$ .

On montre ensuite que  $f$  transfère bien les structures, c'est-à-dire :

1.  $f(0_{\mathbb{Z}}) = 0_{\mathbb{R}}$  ;
2.  $f(1_{\mathbb{Z}}) = 1_{\mathbb{R}}$  ;
3.  $\forall a \in \mathbb{Z}, f(-a) = -f(a)$  ;
4.  $\forall a, b \in \mathbb{Z}, f(a+b) = f(a) + f(b)$  ;
5.  $\forall a, b \in \mathbb{Z}, f(ab) = f(a)f(b)$  ;
6.  $\forall a, b \in \mathbb{Z}, a < b \Rightarrow f(a) < f(b)$  ;
7.  $f$  est injective ;
8.  $f(\mathbb{N}) \subset \mathbb{R}_{>0}$ .

**Exercice 6.21.** Justifier les propriétés sur  $f$ . Indication : par exemple pour «  $f(a+b) = f(a) + f(b)$  », on peut fixer un entier  $a$ , montrer  $f(a+b) = f(a) + f(b)$  par induction sur  $b \in \mathbb{N}$ , puis montrer  $f(a-b) = f(a) + f(-b)$  par induction sur  $b \in \mathbb{N}$ .

Ainsi,  $f(\mathbb{Z})$  est un sous-ensemble de  $\mathbb{R}$  qui s'identifie à  $\mathbb{Z}$ . On peut vérifier que  $f(\mathbb{Z})$  est le plus petit sous-ensemble de  $\mathbb{R}$  contenant  $0_{\mathbb{R}}$  et  $1_{\mathbb{R}}$ , stable par addition et par passage à l'inverse additif. Cela veut dire que dans  $f(\mathbb{Z})$ , on trouve  $0_{\mathbb{R}}, 1_{\mathbb{R}}, 2_{\mathbb{R}} = 1_{\mathbb{R}} + 1_{\mathbb{R}}, 3_{\mathbb{R}} = 1_{\mathbb{R}} + 1_{\mathbb{R}} + 1_{\mathbb{R}}, \dots$ , on trouve  $-1_{\mathbb{R}}, -2_{\mathbb{R}}, -3_{\mathbb{R}}, \dots$ , tout ce qui nous fait penser à  $\mathbb{Z}$ .

**Définition 6.22.** Quitte à utiliser l'injection  $f$ , on considérera abusivement que le sous-ensemble  $f(\mathbb{Z})$  n'est autre que  $\mathbb{Z}$ . Ainsi

- l'élément 0 désigne à la fois le neutre additif dans  $\mathbb{R}$  et le neutre additif dans  $\mathbb{Z}$  ;
- l'élément 1 désigne à la fois le neutre multiplicatif dans  $\mathbb{R}$  et le neutre multiplicatif dans  $\mathbb{Z}$  ;
- la fonction  $+: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  (addition sur  $\mathbb{Z}$ ) est la restriction à  $\mathbb{Z}^2$  et corestriction à  $\mathbb{Z}$  de la fonction  $+: \mathbb{R}^2 \rightarrow \mathbb{R}$  (l'addition sur  $\mathbb{R}$ ) ;
- la fonction  $\cdot: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  (multiplication sur  $\mathbb{Z}$ ) est la restriction à  $\mathbb{Z}^2$  et corestriction à  $\mathbb{Z}$  de la fonction  $\cdot: \mathbb{R}^2 \rightarrow \mathbb{R}$  (multiplication sur  $\mathbb{R}$ ) ;
- pour tout  $x \in \mathbb{Z}$ ,  $-x$  désigne à la fois le neutre additif sur  $\mathbb{Z}$  et le neutre additif sur  $\mathbb{R}$  ;
- l'ordre sur  $\mathbb{Z}$  est la restriction à  $\mathbb{Z}$  de l'ordre sur  $\mathbb{R}$ .<sup>a</sup>

a. Rappelons qu'une relation sur un ensemble  $A$  est par définition un sous-ensemble de  $A \times A$ . La restriction à un sous-ensemble  $B$  consiste à intersecter la relation avec  $B \times B$ . Ainsi l'énoncé signifie que pour tout  $a, b \in \mathbb{Z}$ ,  $a \leq_{\mathbb{Z}} b \iff a \leq_{\mathbb{R}} b$ .

**Exercice 6.23.** Soit  $a$  un entier non nul, c'est en particulier un réel non nul une fois avoir identifié  $\mathbb{Z}$  comme un sous-ensemble de  $\mathbb{R}$ . À quelle condition sur  $a$  a-t-on  $\frac{1}{a} \in \mathbb{Z}$  ?

**Remarque 6.24** (Culturel, ne fait pas partie des connaissances exigibles du cours). Pourquoi ne considère-t-on pas dès le début que  $\mathbb{Z}$  est un sous-ensemble de  $\mathbb{R}$  ? La réponse à cette question réside dans la construction de  $\mathbb{R}$ . Il faut savoir qu'une fois que  $\mathbb{Z}$  est construit, on peut définir  $\mathbb{Q}$  à partir de  $\mathbb{Z}$ , puis  $\mathbb{R}$  à partir de  $\mathbb{Q}$ .

Or dès la construction de  $\mathbb{Q}$  à partir de  $\mathbb{Z}$ , il y a un problème : l'ensemble  $\mathbb{Q}$  n'a aucun élément entier. Nous prenons l'exemple de la construction présentée dans le problème 8.3.1 du chapitre 8, où  $\mathbb{Q}$  est défini comme un quotient de  $\mathbb{Z} \times \mathbb{N}$  pour une certaine relation d'équivalence. Ainsi, à l'origine, les éléments de  $\mathbb{Q}$  sont des sous-ensembles de  $\mathbb{Z} \times \mathbb{N}$  (car ce sont des classes d'équivalence), aucun élément ne peut être entier. C'est seulement après une identification naturelle qu'on peut considérer que  $\mathbb{Z}$  est un sous-ensemble de  $\mathbb{Q}$ .

Pour  $\mathbb{R}$ , la même chose se produit. Dans toutes les constructions classiques (par coupure de Dedekind, ou par complétion de  $\mathbb{Q}$ ), l'ensemble  $\mathbb{R}$  ne contient pas d'éléments rationnels. Ce n'est le cas qu'après une identification naturelle des nombres rationnels dans ce nouvel ensemble.

**Remarque 6.25** (Culturel, ne fait pas partie des connaissances exigibles du cours). Rechercher une fonction bijective qui se comporte bien avec la structure des ensembles est un thème commun à quasiment tous les domaines des mathématiques. Dans le jargon, une telle fonction est appelée un *isomorphisme*, et la notion d'isomorphisme dépend du type de structure sur les ensembles. Voici quelques exemples que vous pourriez croiser dans d'autres cours de mathématiques :

- Isomorphisme de groupes (resp. d'anneaux, resp. de corps, etc.) : lorsque les ensembles sont munis d'opérations vérifiant certaines conditions qui font de cet ensemble un *groupe* (resp. un *anneau*, resp. un *corps*, etc.), on ne fournira pas de définition ;
- Homéomorphisme : c'est un isomorphisme lorsque les ensembles sont munis d'une topologie, c'est-à-dire (informellement) d'une structure qui va donner une « forme » à

l'ensemble. Par exemple, on peut donner à  $\mathbb{R}$  la forme d'une droite, on peut donner à  $\mathbb{R}^2$  la forme d'un plan, donc ils n'ont pas la même forme, on ne peut pas transférer la forme de l'un vers la forme de l'autre sans perte d'information, ils ne sont donc pas homéomorphes.

- Une bijection est un exemple d'isomorphisme, c'est juste qu'on ne donne pas de structure aux ensembles, on les voit comme de simples paquets d'éléments et on cherche une correspondance exacte entre les éléments des deux ensembles.

Pourquoi cherche-t-on ce genre de fonctions ? En fait, on peut remarquer qu'il n'existe pas qu'un seul  $\mathbb{Z}$ , c'est-à-dire qu'il existe plusieurs ensembles (avec leurs opérations  $+$  et  $\cdot$  associés) qui vérifient les axiomes énoncés dans le chapitre 3. Par exemple,  $\mathbb{Z}$  et le sous-ensemble  $f(\mathbb{Z})$  dans  $\mathbb{R}$  vérifient ces axiomes, pourtant ce ne sont pas les mêmes ensembles *a priori*. En revanche, on peut montrer que deux ensembles vérifiant ces axiomes admettent toujours une bijection de l'un vers l'autre, vérifiant les mêmes propriétés que la fonction  $f$  construite ci-dessus. Ainsi, à identification près, on considère qu'il n'y a qu'un seul  $\mathbb{Z}$ , on ne cherche plus du tout à savoir de quel ensemble il s'agit exactement, on ne regarde plus que la structure.

De même, comme nous l'avons mentionné dans la précédente remarque, il existe plusieurs constructions possibles de l'ensemble  $\mathbb{R}$ . Mais chacune des constructions donnent des ensembles différents, pourquoi prétend-on qu'on a construit  $\mathbb{R}$  ? Et bien parce qu'on est capable de trouver une bijection entre ces ensembles, qui préservent les structures. Quand on dit qu'on a construit  $\mathbb{R}$ , on veut plutôt dire qu'on a reproduit la structure de  $\mathbb{R}$ , mais on déclare abusivement qu'il s'agit de  $\mathbb{R}$ .

## 6.5 Supremum et infimum

Il est maintenant temps d'exploiter l'axiome C.6, celui qui permet de distinguer  $\mathbb{R}$  de l'ensemble  $\mathbb{Q}$  des nombres rationnels. Avant de l'utiliser, définissons la notion de supremum qui figure dans son énoncé.

**Définition 6.26.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ , et soit  $B$  un sous-ensemble de  $A$ . On dit qu'un élément  $a \in A$  est un *supremum* (resp. *infimum*) de  $B$  dans  $A$ , aussi appelé *plus petite borne supérieure* (resp. *plus grande borne inférieure*), s'il satisfait les deux conditions suivantes :

- $a$  est un majorant (resp. minorant) de  $B$  dans  $A$  ;
- pour tout majorant (resp. minorant)  $a'$  de  $B$  dans  $A$ , on a  $a \leq a'$  (resp.  $a' \leq a$ ).

**Proposition 6.27.** *S'il existe, le supremum (resp. infimum) de  $B$  dans  $A$  est unique.*

**Preuve.** On le montre seulement pour le supremum, la preuve pour l'infimum étant similaire. Supposons que  $a, a' \in A$  sont des supremum de  $B$ . Par définition,  $a$  est un majorant de  $B$  et  $a'$  est plus petit ou égal à tout majorant de  $B$ , donc  $a' \leq a$ . Et par symétrie, on a  $a \leq a'$ . Donc  $a = a'$  par antisymétrie de  $\leq$ .  $\square$

**Remarque 6.28.** Si  $B$  admet un plus grand élément  $a$ , alors  $a$  est le supremum de  $B$ . En effet,  $a$  majore tout élément de  $B$ . Puis tout majorant majore tout élément de  $B$ , donc en

particulier majeure  $a$  (rappelons que le plus grand élément doit être dans  $B$ ). De même, si le supremum de  $B$  dans  $A$  existe et appartient à  $B$ , alors c'est le plus grand élément de  $B$ .

Le supremum peut donc se voir comme un affaiblissement de la notion de plus grand élément.

**Définition 6.29.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ , et soit  $B$  un sous-ensemble de  $A$ . S'il existe, le supremum (resp. infimum) de  $B$  dans  $A$  est noté  $\sup B$  (resp.  $\inf B$ ).

**Remarque 6.30.** Remarquons que les notations  $\sup B$  et  $\inf B$  ne reflètent pas la dépendance en  $A$ . Dans la suite, le contexte sera clair :  $A$  est l'ensemble  $\mathbb{R}$  muni de sa relation d'ordre  $\leq$  usuelle. Il n'y aura donc pas d'ambiguïté sur l'ensemble ambiant.

**Notation.** Si l'ensemble  $B$  se définit avec une paramétrisation de ses éléments, par exemple  $B = \{f(x) \mid x \in X\}$  ou  $B = \{b_i \mid i \in I\}$ , alors on pourra noter  $\sup_{x \in X} f(x)$  ou  $\sup_{i \in I} b_i$  au lieu de  $\sup B$ . Même chose pour  $\inf$ ,  $\max$  et  $\min$ .

**Exercice 6.31.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ . Soient  $B$  et  $C$  deux sous-ensembles de  $A$ . Supposons que  $B$  et  $C$  admettent des supremums dans  $A$ . Montrer les assertions.

1. Si  $B \subset C$ , alors  $\sup B \leq \sup C$ .
2.  $B \cap C$  est majoré par  $\min(\sup B, \sup C)$ .
3. Si  $B \cap C$  admet un supremum, a-t-on  $\sup(B \cap C) = \min(\sup B, \sup C)$  ?
4. Donner les énoncés analogues où  $\sup$  est remplacé par  $\inf$ , et « majoré » par « minoré ».

**Exercice 6.32.** Soit  $\leq$  une relation d'ordre sur un ensemble  $A$ , et soit  $B$  un sous-ensemble non vide de  $A$ . On suppose que  $B$  admet un supremum et un infimum et que  $\inf B = \sup B$ , on note  $a$  la valeur commune. Montrer que  $B = \{a\}$ .

**Exemple 6.33.**

1.  $\inf \mathbb{R}_{>0} = 0$ .

Démontrons-le. Par définition de cet ensemble, 0 est un minorant de  $\mathbb{R}_{>0}$ . Montrons que c'est le plus grand minorant. Soit  $x \in \mathbb{R}$  qui minore  $\mathbb{R}_{>0}$ , montrons que  $x \leq 0$ . Par l'absurde, on suppose  $x > 0$ . Par la proposition 6.20, on dispose d'un réel  $y$  vérifiant  $0 < y < x$ . L'inégalité  $0 < y$  nous dit que  $y$  est un élément de  $\mathbb{R}_{>0}$ , donc l'inégalité  $y < x$  contredit le fait que  $x$  minore  $\mathbb{R}_{>0}$ . Donc on a bien  $x \leq 0$ .

2.  $\mathbb{R}_{>0}$  n'admet pas de supremum.

Par l'absurde, si un réel  $x$  est le supremum de  $\mathbb{R}_{>0}$ , alors  $x$  est un majorant de  $\mathbb{R}_{>0}$ . La transitivité de  $\leq$  entraîne alors que  $x$  est un élément de  $\mathbb{R}_{>0}$ , donc c'est le plus grand élément de  $\mathbb{R}_{>0}$ . Cela contredit le corollaire 6.13.

3. Des preuves similaires permettent d'obtenir que  $\mathbb{R}_{\geq 0}$  n'admet pas de supremum et que  $\inf \mathbb{R}_{\geq 0} = 0$ .

4. Soit  $B = \{2 - \frac{3}{x} \mid x > 0\}$ .

- $\sup B = 2$ .

En effet, on sait déjà que 2 est un majorant de  $B$  (si  $x > 0$ , alors  $-\frac{3}{x} < 0$  donc  $2 - \frac{3}{x} < 2$ ). Par l'absurde, supposons qu'il existe un majorant de  $B$ , noté  $y$ , qui soit  $< 2$ . Cela signifie alors que pour tout  $x > 0$ , on a  $2 - \frac{3}{x} < y$ , c'est-à-dire  $x < \frac{3}{2-y}$  (ici, on a utilisé le fait que  $x$  et  $2 - y$  sont positifs). On vient donc d'obtenir que  $\frac{3}{2-y}$  majore  $\mathbb{R}_{>0}$ , c'est absurde. Ainsi 2 est le plus petit des majorants de  $B$ .

- $B$  n'admet pas d'infimum.

Par l'absurde, supposons que  $y \in \mathbb{R}$  soit un infimum de  $B$ . Alors pour tout  $x > 0$ , on a  $2 - \frac{3}{x} > y$ , c'est-à-dire  $2 - y > \frac{3}{x} > 0$ , c'est-à-dire  $x > \frac{3}{2-y}$ . Ainsi  $\frac{3}{2-y}$  est un minorant positif de  $\mathbb{R}_{>0}$ , c'est absurde.

**Exercice 6.34.** Soit  $x, y \in \mathbb{R}$  tels que  $x < y$ . Démontrer les assertions suivantes et déterminer dans chaque cas si l'infimum/supremum obtenu est le plus petit/grand élément.

1.  $(-\infty, y)$  et  $(-\infty, y]$  n'admettent pas d'infimum, et admettent  $y$  pour supremum.
2.  $(x, \infty)$  et  $[x, \infty)$  n'admettent pas de supremum, et admettent  $x$  pour infimum.
3.  $\mathbb{R}$  n'a ni d'infimum, ni de supremum.
4.  $[x, y]$ ,  $(x, y]$ ,  $[x, y)$  et  $(x, y)$  admettent  $x$  pour infimum,  $y$  pour supremum.

Voici maintenant une conséquence directe de l'axiome C.6.

**Théorème 6.35.** *Tout ensemble majoré (resp. minoré) admet un supremum (resp. infimum).*

**Preuve.** Le fait que tout ensemble majoré admette un supremum est directement dû à l'axiome C.6. Enfin, si  $B \subset \mathbb{R}$  est minoré, alors  $-B = \{-x \mid x \in B\}$  est majoré, donc le supremum de  $-B$  existe. Puis on montre que  $-\sup(-B)$  est l'infimum de  $B$ . (Vérifier chaque point de cette preuve, exercice)  $\square$

**Remarque 6.36.** Voici la différence cruciale entre  $\mathbb{Q}$  et  $\mathbb{R}$  :

- l'ensemble  $\{x \in \mathbb{Q} \mid x^2 < 2\}$  admet un supremum dans  $\mathbb{R}$ , il s'agit de  $\sqrt{2}$ ;
- mais l'ensemble  $\{x \in \mathbb{Q} \mid x^2 < 2\}$  n'admet pas de supremum dans  $\mathbb{Q}$  (cf. exemple 1.8 du chapitre 1).

Les justifications du premier point se trouveront dans la section 6.7, ainsi que le chapitre 8 (cf. corollaire 8.8).

**Exercice 6.37.** Soit  $A$  un sous-ensemble majoré de  $\mathbb{R}$ . Montrer que l'ensemble

$$B = \{5 - 2x \mid x \in A\}$$

est minoré, et calculer  $\inf B$  en fonction de  $\sup A$ .

L'axiome C.6, et donc le théorème 6.35, admet plusieurs conséquences spectaculaires. D'une part, il permet de montrer que  $\mathbb{Z}$  n'est pas borné, ce que nous allons voir dans la prochaine section. Un corollaire de cette affirmation est le fait que le réel  $\frac{1}{n}$ , avec  $n \in \mathbb{N}$ , est de plus en plus

petit si  $n$  est de plus en plus grand, un phénomène assez intuitif mais qu'il faudra démontrer. D'autre part, l'existence de supremum et d'infimum permet de construire des nombres qu'on ne peut trouver dans  $\mathbb{Q}$ , comme  $\sqrt{2}$ ,  $\pi$ , etc. (ce qui nous ramène à la remarque précédente). Nous construirons la racine carrée dans la section 6.7.

Terminons pas une caractérisation du supremum. Cela nous amène pour la première fois vers des définitions *epsilonques* dont nous devons prendre l'habitude pour le prochain chapitre.

**Proposition 6.38.** *Soit  $B$  un sous-ensemble majoré de  $\mathbb{R}$ , soit  $x$  un réel. Les deux assertions suivantes sont équivalentes :*

1.  $x = \sup B$  ;
2.  $x$  majore  $B$ , et pour tout  $\varepsilon > 0$ , il existe  $b \in B$  tel que  $b \in (x - \varepsilon, x]$ .

Intuitivement,  $\sup B$  est un réel qui majore  $B$  et qui est « collé » à  $B$ . Si on regarde une épaisseur  $(x - \varepsilon, x]$  en-dessous de  $x$ , arbitrairement petite, on trouve toujours un élément de  $B$ .

**Preuve.** Démontrons l'implication indirecte. Supposons que  $x$  satisfasse la seconde condition. C'est donc un majorant de  $B$  et il suffit de démontrer qu'il s'agit du plus petit des majorants. Soit  $y$  un majorant de  $B$ . Par l'absurde, on suppose  $y < x$ . La proposition 6.20 affirme qu'il existe  $\varepsilon \in (0, x - y)$ . Par hypothèse, il existe  $b \in B$  tel que  $b \in (x - \varepsilon, x]$ . Mais alors  $y < x - \varepsilon < b$ , ce qui contredit le fait que  $y$  majore  $B$ . Donc on a bien  $x \leq y$ . D'où  $x = \sup B$ .

Démontrons maintenant l'implication directe par contraposée. Si  $x$  ne majore pas  $B$ , alors ce n'est pas un supremum de  $B$  (par définition). Maintenant, supposons que  $x$  majore  $B$ , mais qu'on dispose de  $\varepsilon > 0$  tel que  $B \cap (x - \varepsilon, x] = \emptyset$ . Alors tout élément de  $(x - \varepsilon, x)$  (non vide par la proposition 6.20) majore  $B$  et est  $< x$ . Donc  $x$  n'est pas le plus petit des majorants. Dans tous les cas,  $x$  n'est pas le supremum de  $B$ .  $\square$

On a aussi l'énoncé analogue pour l'infimum.

**Proposition 6.39.** *Soit  $B$  un sous-ensemble minoré de  $\mathbb{R}$ , soit  $x$  un réel. Les deux assertions suivantes sont équivalentes :*

1.  $x = \inf B$  ;
2.  $x$  minore  $B$ , et pour tout  $\varepsilon > 0$ , il existe  $b \in B$  tel que  $b \in [x, x + \varepsilon)$ .

## 6.6 $\mathbb{Z}$ non borné dans $\mathbb{R}$

Rappelons qu'on considère abusivement  $\mathbb{Z}$  comme un sous-ensemble de  $\mathbb{R}$ , après identification. Nous allons montrer que  $\mathbb{Z}$  n'est pas borné dans  $\mathbb{R}$ . Autrement dit, pour tout réel  $x$ , on peut toujours trouver un entier plus petit ou plus grand.

**Proposition 6.40.**  *$\mathbb{N}$  n'est pas majoré dans  $\mathbb{R}$ .*

**Preuve.** Par l'absurde, supposons que  $\mathbb{N}$  est majoré. L'axiome C.6 affirme donc que  $\mathbb{N}$  admet une borne supérieure, notée  $x$ . Par la proposition 6.38, appliquée à  $\varepsilon = \frac{1}{2}$ , on dispose de  $n \in \mathbb{N}$  tel que  $x - \frac{1}{2} < n < x$ . L'inégalité  $x - \frac{1}{2}$  implique  $n + 1 > (x - \frac{1}{2}) + \frac{1}{2} =$

$x + \frac{1}{2} > x$ , ce qui contredit l'inégalité  $n < x$ . Donc  $\mathbb{N}$  n'est pas majoré.  $\square$

**Corollaire 6.41.**  $\mathbb{Z}$  n'est ni majoré, ni minoré dans  $\mathbb{R}$ .

**Preuve.** Si  $\mathbb{Z}$  était majoré dans  $\mathbb{R}$ , alors  $\mathbb{N}$  le serait aussi, ce qui contredit le résultat précédent. Si  $\mathbb{Z}$  était minoré dans  $\mathbb{R}$ , alors  $-\mathbb{N}$  le serait aussi, donc par passage à l'inverse additif,  $\mathbb{N}$  serait majoré dans  $\mathbb{R}$ , ce qui contredit le résultat précédent.  $\square$

**Exercice 6.42.** Soit  $x \in \mathbb{R}$ . Montrer qu'il existe un unique  $n \in \mathbb{Z}$  tel que  $n \leq x < n + 1$ . On définit alors  $\lfloor x \rfloor = n$  (partie entière de  $x$ ).

**Exercice 6.43.** On définit la relation  $\sim$  sur  $\mathbb{R}$  de la manière suivante :

$$\forall x, y \in \mathbb{R}, y - x \in \mathbb{Z}.$$

1. Montrer que  $\sim$  est une relation d'équivalence sur  $\mathbb{R}$ .
2. Soit  $x \in \mathbb{R}$ . Montrer que sa classe d'équivalence  $[x]$  vaut  $\{x + n \mid n \in \mathbb{Z}\}$  (cet ensemble est plus communément noté  $x + \mathbb{Z}$ ).
3. Montrer que  $[0, 1)$  est un système de représentant.
4. Montrer que les ensembles suivants sont en bijection :
  - $\mathbb{R} / \sim$  ;
  - $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$  ;
  - $[0, 1] / \mathcal{R}$ , où  $\mathcal{R}$  est la relation d'équivalence sur  $[0, 1]$  définie par  $\mathcal{R} = \{(0, 1), (1, 0)\} \cup \{(x, x) \mid 0 \leq x \leq 1\}$ .

Pour comprendre la relation d'équivalence  $\mathcal{R}$ , ainsi que le quotient  $[0, 1] / \mathcal{R}$ , il suffit de remarquer que  $\mathcal{R}$  consiste seulement à confondre 0 et 1 (les autres points ne sont reliés qu'à eux-mêmes). Visuellement, le segment  $[0, 1]$  est un bout de ficelle et le quotient  $[0, 1] / \mathcal{R}$  consiste alors à coller ses extrémités 0 et 1 pour obtenir un cercle.

L'énoncé suivant en est une conséquence remarquable. Il énonce que la quantité  $\frac{1}{n}$  peut être rendu arbitrairement petite à mesure que  $n \in \mathbb{N}$  est de plus en plus grand. Même si cela paraît évident, il aura tout de même fallu une description rigoureuse des ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$  et  $\mathbb{R}$  pour le démontrer.

**Corollaire 6.44.** Pour tout  $\varepsilon > 0$ , il existe  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ , on a  $\frac{1}{n} < \varepsilon$ .

**Preuve.** Soit  $\varepsilon > 0$ . D'après la proposition 6.40, le réel  $\frac{1}{\varepsilon}$  ne majore pas  $\mathbb{N}$ . Cela signifie qu'on dispose de  $N \in \mathbb{N}$  tel que  $\frac{1}{\varepsilon} < N$ , c'est-à-dire  $\frac{1}{N} < \varepsilon$ . Enfin, pour tout  $n \in \mathbb{N}$ , si  $n \geq N$ , alors  $\frac{1}{n} \leq \frac{1}{N}$ , donc  $\frac{1}{n} < \varepsilon$ .  $\square$

**Exercice 6.45.** Soit  $B = \{5 + \frac{3}{2n} \mid n \in \mathbb{N}\}$ . S'ils existent, déterminer l'infimum, le plus petit élément, le supremum et le plus grand élément de  $B$ , ou justifier qu'ils n'existent pas.

## 6.7 Racine carrée

Depuis le début du cours, nous parlons beaucoup de racine carrée d'un nombre positif. Nous allons montrer que l'axiome C.6 est très utile pour la définir proprement.

**Proposition/définition 6.46.** Soit  $a \in \mathbb{R}_{\geq 0}$ . L'ensemble

$$R_a = \{x \in \mathbb{R}_{\geq 0} \mid x^2 \leq a\}$$

est non vide et majoré. Sa borne supérieure est notée  $\sqrt{a}$ .

**Preuve.** L'ensemble  $R_a$  contient 0, donc il n'est pas vide. Montrons qu'il est majoré. Par la proposition 6.40, on dispose de  $n \in \mathbb{N}$  tel que  $n > a$ . L'entier  $n$  étant  $\geq 1$ , on a donc  $n^2 > a$ . Ainsi, si  $x > n$ , alors  $x^2 > n^2 > a$ , donc  $x \notin R_a$ . Donc  $n$  majore  $R_a$ .  $\square$

**Proposition 6.47.** Pour tout  $a \in \mathbb{R}_{\geq 0}$ , on a  $\sqrt{a} \geq 0$  et  $\sqrt{a^2} = a$ .

**Preuve.** La positivité de  $\sqrt{a}$  vient du fait que  $R_a$  est inclus dans  $\mathbb{R}_{\geq 0}$ . Montrons que  $\sqrt{a^2} = a$ .

Montrons  $\sqrt{a^2} \geq a$ . Soit  $\varepsilon > 0$ . Par définition du supremum,  $\sqrt{a} + \varepsilon$  n'est pas un élément de  $R_a$ . Ainsi, on a

$$a < (\sqrt{a} + \varepsilon)^2 = \sqrt{a^2} + \varepsilon(2\sqrt{a} + \varepsilon),$$

qu'on peut aussi écrire  $\varepsilon(2\sqrt{a} + \varepsilon) > a - \sqrt{a^2}$ . Supposons par l'absurde que  $\sqrt{a^2} < a$ . Le nombre  $\delta = a - \sqrt{a^2}$  est donc positif, et on a montré que pour tout  $\varepsilon > 0$ ,  $\varepsilon(2\sqrt{a} + \varepsilon) > \delta$ . On choisit maintenant un réel  $\varepsilon > 0$  plus petit que 1 et que  $\delta/(2\sqrt{a} + 1)$  et on obtient :

$$\delta < \varepsilon(2\sqrt{a} + \varepsilon) < \frac{\delta}{(2\sqrt{a} + 1)}(2\sqrt{a} + 1) = \delta,$$

donc  $\delta < \delta$ , c'est absurde. Donc  $\sqrt{a^2} \geq a$ .

Montrons  $\sqrt{a^2} \leq a$ . On a besoin d'isoler le cas  $\sqrt{a} = 0$ . Or on a montré que  $\sqrt{a^2} \geq a$ , donc  $a$  étant positif ou nul, ce cas implique que  $a = 0$ , donc on a bien l'égalité  $\sqrt{a^2} = a$ . Supposons maintenant  $\sqrt{a} > 0$ . Soit  $\varepsilon \in (0, \sqrt{a})$ , de sorte que  $\sqrt{a} - \varepsilon$  soit positif. Par la proposition 6.38, on dispose de  $x \in R_a$  tel que  $\sqrt{a} - \varepsilon < x$ . Comme tout est positif, on peut élever au carré tout en préservant l'inégalité, et en développant, on obtient :

$$\sqrt{a^2} - 2\varepsilon\sqrt{a} + \varepsilon^2 < x^2.$$

On sait que  $\varepsilon^2 > 0$ , et par définition de  $R_a$ , on sait que  $x^2 \leq a$ . On a donc

$$2\varepsilon\sqrt{a} > \sqrt{a^2} - a.$$

Supposons maintenant par l'absurde que  $\sqrt{a^2} > a$ , de sorte que  $\delta = \sqrt{a^2} - a$  soit positif. On choisit  $\varepsilon > 0$  plus petit que  $\sqrt{a}$  et  $\delta/(2\sqrt{a})$ , et on obtient

$$\delta > 2\varepsilon\sqrt{a} > \delta,$$

c'est absurde. Donc  $\sqrt{a^2} \leq a$ .

On a donc démontré  $\sqrt{a^2} = a$ .  $\square$

On a donc bien défini la racine carrée.

**Proposition 6.48.** Soit  $a \in \mathbb{R}_{\geq 0}$ . Les seuls réels  $x$  vérifiant  $x^2 = a$  sont  $\sqrt{a}$  et  $-\sqrt{a}$ . En particulier,  $\sqrt{a}$  est l'unique  $x \in \mathbb{R}_{\geq 0}$  tel que  $x^2 = a$ .

Notons qu'il y a deux solutions réelles à l'équation  $x^2 = a$  lorsque  $a > 0$ , et 0 est l'unique solution lorsque  $a = 0$ .

**Preuve.** Soit  $x \in \mathbb{R}$  satisfaisant  $x^2 = a$ . On a montré que  $\sqrt{a}^2 = a$ , donc on a  $x^2 = \sqrt{a}^2$ , autrement dit

$$(x - \sqrt{a})(x + \sqrt{a}) = 0.$$

On déduit le résultat du fait que l'un des deux facteurs est nul.  $\square$

**Exercice 6.49.** En utilisant l'unicité de la racine carrée dans  $\mathbb{R}_{\geq 0}$ , montrer les assertions suivantes.

1. Pour tout  $x \in \mathbb{R}$ , on a  $\sqrt{x^2} = |x|$ , c'est-à-dire  $x$  si  $x \geq 0$ ,  $-x$  si  $x < 0$  (on étudiera la valeur absolue dans le chapitre 7).
2. Pour tous  $x, y \in \mathbb{R}_{\geq 0}$ , on a  $\sqrt{xy} = \sqrt{x}\sqrt{y}$ .
3. Pour tous  $x \in \mathbb{R}_{\geq 0}$  et  $y \in \mathbb{R}_{> 0}$ , on a  $\sqrt{\frac{x}{y}} = \frac{\sqrt{x}}{\sqrt{y}}$ .

Mentionnons enfin le fait que la racine carrée ne peut être définie sur les réels négatifs, étant donné qu'un carré est toujours positif ou nul. Il est toutefois possible de réaliser cela, à condition de sortir de  $\mathbb{R}$ . En effet, l'ensemble  $\mathbb{C}$  des nombres complexes, contenant  $\mathbb{R}$ , admet des éléments dont le carré est un réel négatif. On aurait ainsi une racine carrée définie sur l'ensemble des entiers négatifs, mais à valeurs complexes.

## 6.8 Problèmes

### 6.8.1 Problème 1

Ce problème aborde une construction simple de l'ensemble  $\mathbb{C}$  des nombres complexes à partir de  $\mathbb{R}$ .

Avant de commencer la construction, expliquons brièvement ce qu'on veut obtenir. Un nombre complexe s'écrit de manière unique  $a + ib$  où  $i$  est un « nouveau nombre », non réel, vérifiant  $i^2 = -1$ . Les opérations  $+$  et  $\times$  s'étendent aisément dans  $\mathbb{C}$ , en utilisant la distributivité, l'associativité, etc. Par exemple, on veut faire ce genre de calcul :  $(a+ib)+(c+id) = (a+c)+i(b+d)$  qu'on notera tout simplement  $a+c+i(b+d)$ , ainsi que  $(a+ib)(c+id) = ac+i^2bd+i(ad+bc) = ac - bd + i(ad+bc)$ . Il reste à construire  $\mathbb{C}$  et de définir ces opérations. L'idée est simplement d'implémenter  $a + ib$  par un couple  $(a, b)$ .

On définit des opérations  $+$  et  $\cdot$  sur  $\mathbb{R}^2$  de la manière suivante : pour tout  $(a, b), (c, d) \in \mathbb{R}^2$ ,

$$(a, b) + (c, d) = (a + c, b + d)$$

$$\text{et } (a, b)(c, d) = (ac - bd, ad + bc).$$

1. Montrer que  $+$  et  $\cdot$  sont associatives et commutatives, et que la distributivité est vérifiée.
2. Calculer  $(0, 1)^2$ .

3. Montrer que  $(0, 0)$  est l'unique neutre additif, et que tout élément admet un unique inverse additif.
4. Montrer que  $(1, 0)$  est neutre pour la multiplication.

On cherche maintenant à montrer que  $(1, 0)$  est l'unique neutre pour la multiplication, en montrant en fait que tout élément différent de  $(0, 0)$  admet un inverse multiplicatif.

5. Soit  $a \in \mathbb{R}$ . Montrer que  $(a, 0)$  admet un unique inverse multiplicatif si et seulement si  $a \neq 0$ .
6. Soit  $a, b \in \mathbb{R}$ . Calculer  $(a, b)(a, -b)$ . En déduire que  $(a, b)$  admet un inverse multiplicatif si et seulement si  $(a, b) \neq (0, 0)$ . Dans ce cas, l'inverse multiplicatif est noté  $(a, b)^{-1}$ .

Le couple  $(a, -b)$  est appelé le *conjugué* de  $(a, b)$ , noté  $\overline{(a, b)}$ .

7. Pour tout  $(a, b), (c, d) \in \mathbb{R}^2$ , montrer que

$$\overline{(a, b) + (c, d)} = \overline{(a, b)} + \overline{(c, d)}$$

$$\text{et } \overline{(a, b)(c, d)} = \overline{(a, b)}\overline{(c, d)}.$$

8. Montrer que  $f: a \in \mathbb{R} \rightarrow (a, 0) \in \mathbb{R}^2$  est une fonction injective qui se comporte bien avec les opérations  $+$  et  $\cdot$ , comme dans la section 6.4 sauf qu'on demande en plus la propriété  $f(a^{-1}) = f(a)^{-1}$  pour tout  $a \neq 0$ .

Muni des opérations  $+$  et  $\cdot$ , l'ensemble  $\mathbb{R}^2$  est plutôt noté  $\mathbb{C}$ , ensemble des nombres complexes.<sup>1</sup> Un couple  $(a, b)$  sera écrit  $a + ib$ . On notera plus simplement  $ib$  lorsque  $a = 0$ ,  $a + i$  lorsque  $b = 1$ ,  $a$  lorsque  $b = 0$ , etc. Via l'identification par  $f$ , un nombre complexe  $a + ib$  est réel si et seulement si  $b = 0$ , on appelle  $a$  la *partie réelle* et  $b$  la *partie imaginaire*.

Il est bon de reprendre les questions de ce problème avec cette écriture  $a + ib$ , plus intuitive. Par exemple, si on a bien répondu à une des questions ci-dessus, on remarque que  $(a + ib)\overline{(a + ib)}$  est le réel  $a^2 + b^2$  (positif ou nul), il est d'ailleurs positif si et seulement si  $a + ib \neq 0$ . On remarque que derrière cette quantité  $a^2 + b^2$ , c'est l'identité  $(x + y)(x - y) = x^2 - y^2$  qui est utilisé, le nouveau nombre  $i$  permettant cette fois-ci de transformer le  $-$  en  $+$ .

**Remarque 6.50.** La valeur absolue sur  $\mathbb{R}$  (définie dans la section 7.1 du chapitre 7) s'étend à  $\mathbb{C}$  de la manière suivante :

$$|(a + ib)| = \sqrt{(a + ib)\overline{(a + ib)}} = \sqrt{a^2 + b^2}.$$

On vérifie qu'on retrouve la valeur absolue de  $a$  lorsque  $b = 0$ . Cette extension est appelée le *module*. La majorité des propriétés vérifiées par la valeur absolue sur  $\mathbb{R}$  (cf. section 7.1) sont également vérifiées par le module sur  $\mathbb{C}$  (inégalité triangulaire par exemple).

Le module permet notamment de définir une notion de distance entre nombre complexe. On remarque d'ailleurs que  $a^2 + b^2$  n'est autre que la distance dans le plan entre les points  $(0, 0)$  et  $(a, b)$ , par le théorème de Pythagore.

Enfin, de même qu'on définit la notion de limite des suites réelles à l'aide de la valeur absolue, on utilise le module lorsqu'on parle de suite complexe.

Les nombres complexes ont beaucoup d'applications. Par exemple, lorsqu'un problème est difficile à résoudre dans  $\mathbb{R}$ , il est parfois plus facile de le résoudre dans  $\mathbb{C}$ . On fait donc un détour par  $\mathbb{C}$  pour répondre au problème dans  $\mathbb{R}$ .

1. Ne pas croire que  $\mathbb{R}^2$  désigne toujours l'ensemble des complexes. Ici, il y a une structure particulière grâce aux opérations qu'on a défini, on note  $\mathbb{C}$  pour exprimer implicitement qu'on considère cette structure.

Une fois l'exponentielle complexe introduite, on peut passer des coordonnées cartésiennes  $a + ib$  aux coordonnées polaires, et voir ainsi la multiplication par un complexe comme une transformation du plan par rotation et dilatation. Cette vision géométrique est cruciale dans certains problèmes. Elle permet par exemple de calculer des sommes de termes réelles, telles que  $\sum_{k=0}^n \cos(kx)$ , qu'on ne pourrait calculer si on s'obstinait à rester dans  $\mathbb{R}$ .

Passer dans  $\mathbb{C}$  permet également de résoudre tout un tas d'équations, des équations différentielles par exemple. Mentionnons enfin le fait qu'on utilise beaucoup les nombres complexes en physique, aussi bien pour des résolutions simples d'équation que dans le formalisme de la mécanique quantique.

### 6.8.2 Problème 2

On cherche les sous-ensembles  $A$  de  $\mathbb{R}$  vérifiant les propriétés de stabilité suivantes :

- $0 \in A$  ;
- $\forall x, y \in A, x + y \in A$  ;
- $\forall x \in A, -x \in A$ .

Un tel sous-ensemble est appelé un *sous-groupe* de  $(\mathbb{R}, +)$ . Pour tout  $a \in \mathbb{R}$ , on notera  $a\mathbb{Z} = \{an \mid n \in \mathbb{Z}\}$ . Par exemple,  $0\mathbb{Z} = \{0\}$ . Enfin, on dit qu'un sous-ensemble  $A$  de  $\mathbb{R}$  est *dense* dans  $\mathbb{R}$  si pour tout  $x, y \in \mathbb{R}$  tels que  $x < y$ , l'ensemble  $A \cap (x, y)$  est non vide.

On cherche à montrer que les sous-groupes  $A$  de  $(\mathbb{R}, +)$  sont denses dans  $\mathbb{R}$  ou de la forme  $a\mathbb{Z}$  avec  $a \in \mathbb{R}$ , et chercher à caractériser chacune des situations en fonction de  $A$  (à l'aide d'une quantité  $m$  qu'on va introduire).

1. Soit  $a \in \mathbb{R}$ . Montrer que  $a\mathbb{Z}$  est une sous-groupe de  $(\mathbb{R}, +)$ . Montrer qu'il n'est pas dense dans  $\mathbb{R}$ .

On fixe un sous-groupe  $A$  de  $(\mathbb{R}, +)$ . On suppose qu'il ne vaut pas  $\{0\}$ , c'est-à-dire  $0\mathbb{Z}$ .

2. Montrer que  $m = \inf(A \cap \mathbb{R}_{>0})$  est bien défini.
3. On suppose  $m > 0$ . Montrer que  $A = a\mathbb{Z}$ 
  - (a) Montrer que  $m\mathbb{Z} \subset A$ .
  - (b) Existe-il un élément de  $A$  compris entre 0 et  $m$  ? Existe-t-il un élément de  $A$  compris entre  $m$  et  $2m$  ?
  - (c) Généraliser et obtenir  $A \subset m\mathbb{Z}$ .
4. On suppose  $m = 0$ . Montrons que  $A$  est dense dans  $\mathbb{R}$ .
  - (a) Montrer que pour tout  $\varepsilon > 0$ , il existe  $b \in (0, \varepsilon)$  tel que  $b\mathbb{Z} \subset A$ .
  - (b) Soient  $x, y \in \mathbb{R}$  tels que  $x < y$ . En appliquant la question précédente à  $\varepsilon = y - x$ , trouver un élément de  $A$  compris entre  $x$  et  $y$ .

On a donc montré que le sous-groupe en question est

- dense si  $m = 0$  ;
- égal à  $m\mathbb{Z}$  si  $m > 0$  ;
- égal à  $\{0\}$  si  $m$  n'est pas défini.

1. Soient  $x, y \in \mathbb{R}$ . Montrer que  $x\mathbb{Z} + y\mathbb{Z}$ , c'est-à-dire l'ensemble  $\{ax + by \mid a, b \in \mathbb{Z}\}$ , est dense si et seulement si  $(x, y) \neq (0, 0)$  et  $x/y \in \mathbb{Q}$ .

Par exemple,  $\mathbb{Z} + \sqrt{2}\mathbb{Z}$  et  $\mathbb{Z} + 2\pi\mathbb{Z}$  sont denses dans  $\mathbb{R}$ .

# Chapitre 7

## Suites réelles, limites

Un ensemble n'a rien d'intéressant si on le regarde comme un paquet d'éléments. Il faut ajouter de la structure. Par exemple, on n'a pas seulement regardé l'ensemble  $\mathbb{Z}$ , on l'a étudié lorsqu'il était muni d'opérations  $+$  et  $\cdot$  et d'une relation d'ordre  $\leq$ . On a fait de même pour  $\mathbb{R}$ , puis on a pu comparer la structure de  $\mathbb{Z}$  avec celle de  $\mathbb{R}$ , en montrant que la première pouvait se voir dans la dernière.

Nous étudions maintenant l'ensemble  $\mathbb{R}$  avec un point de vue topologique. La topologie (du grec, « étude du lieu ») consiste intuitivement à introduire la notion de proximité entre éléments d'un ensemble, c'est une structure en plus qui rend intéressante l'étude de l'ensemble. Par exemple, ce qui rend intéressante une carte routière, ce n'est pas l'ensemble des emplacements, mais la distance entre chaque emplacement et la manière d'aller de l'un vers l'autre.

Ce chapitre n'est pas un cours de topologie générale, ni une introduction de la topologie dans l'ensemble  $\mathbb{R}$ . Nous aborderons seulement les notions de distance et de convergence d'une suite réelle.

### 7.1 Valeur absolue, distance

**Définition 7.1.** On définit la valeur absolue comme étant la fonction

$$\begin{aligned} |\cdot|: \mathbb{R} &\rightarrow \mathbb{R}_{\geq 0} \\ x &\rightarrow \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases} \end{aligned}$$

On vérifiera que cette fonction est bien définie, c'est-à-dire que pour tout  $x \in \mathbb{R}$ , le réel  $|x|$  est bien dans  $\mathbb{R}_{\geq 0}$ .

**Proposition 7.2.** Soient  $x, y \in \mathbb{R}$  et  $\varepsilon \in \mathbb{R}_{>0}$ .

1.  $|x| = 0 \iff x = 0$ .
2.  $-|x| \leq x \leq |x|$ , et  $x$  vaut  $|x|$  ou  $-|x|$ .
3.  $|xy| = |x| \cdot |y|$ .
4.  $|x| = |y| \iff x = y$  ou  $x = -y$ .
5. Inégalité triangulaire :  $|x + y| \leq |x| + |y|$ .
6. Inégalité triangulaire inversée :  $||x| - |y|| \leq |x - y|$ .
7.  $|x| < \varepsilon \iff x \in (-\varepsilon, \varepsilon)$ .

8.  $|x| \leq \varepsilon \iff x \in [-\varepsilon, \varepsilon]$ .
9.  $|x - y| < \varepsilon \iff x \in (y - \varepsilon, y + \varepsilon) \iff y \in (x - \varepsilon, x + \varepsilon)$ .
10.  $|x - y| \leq \varepsilon \iff x \in [y - \varepsilon, y + \varepsilon] \iff y \in [x - \varepsilon, x + \varepsilon]$ .

**Exercice 7.3.**

1. Soient  $x \in \mathbb{R}$  et  $n \in \mathbb{N}$ . Montrer que  $|x^n| = |x|^n$ .
2. Soit  $n \in \mathbb{N}$  et  $x_1, \dots, x_n \in \mathbb{R}$ . Montrer que  $|\sum_{i=1}^n x_i| \leq \sum_{i=1}^n |x_i|$ .

**Preuve.**

1. Utiliser la définition de  $|x|$ .
2. Si  $x \geq 0$ , alors  $x = |x|$  et  $-|x| \leq 0 \leq x$ . Si  $x < 0$ , alors  $|x| = -x$ , c'est-à-dire  $x = -|x|$ , et  $|x| \geq 0 \geq x$ .
3. Si  $x, y \geq 0$ , alors  $xy \geq 0$ , donc  $|xy| = xy = |x| \cdot |y|$ . Si  $x \geq 0$  et  $y < 0$ , alors  $xy \leq 0$ , donc  $|xy| = -xy = x \cdot (-y) = x \cdot |y|$ . Si  $x < 0$  et  $y \geq 0$ , même méthode. Si  $x < 0$  et  $y < 0$ , alors  $xy > 0$ , donc  $|xy| = xy = (-x)(-y) = |x| \cdot |y|$ .
4. En utilisant la définition, on a  $|-y| = |y|$ . Donc si  $x = \pm y$ , alors on a bien  $|x| = |y|$ . Réciproquement, supposons  $|x| = |y|$ . En utilisant ce qu'on vient de montrer, on peut supposer sans perte de généralité que  $y \geq 0$  (quitte à remplacer  $y$  par  $-y$ ). Ainsi on a  $|x| = y$ . Si  $x \geq 0$ , cela donne  $x = y$ . Si  $x < 0$ , cela donne  $x = -y$ .
5. Si  $x + y \geq 0$ , alors  $|x + y| = x + y$ . D'après la propriété 2,  $x \leq |x|$  et  $y \leq |y|$ , d'où  $|x + y| \leq |x| + |y|$ . Si  $x + y < 0$ , alors  $|x + y| = -(x + y) = -x + (-y)$ . D'après la propriété 2,  $-|x| \leq x$  et  $-|y| \leq y$ , donc  $-x \leq |x|$  et  $-y \leq |y|$ , d'où le résultat.
6. Supposons  $|x| - |y| \geq 0$  (même raisonnement si  $|y| - |x| \geq 0$ ), de sorte que  $||x| - |y|| = |x| - |y|$ . L'inégalité triangulaire donne  $|x| = |(x - y) + y| \leq |x - y| + |y|$ , donc  $|x| - |y| \leq |x - y| + |y| - |y| = |x - y|$ , ce qu'on voulait.
7. Distinguer les cas  $x \geq 0$  et  $x < 0$  (exercice).
8. Même méthode (exercice).
9.  $|x - y| < \varepsilon \iff -\varepsilon < x - y < \varepsilon \iff y - \varepsilon < x < y + \varepsilon$ . Et on peut interchanger  $x$  et  $y$ , en utilisant  $|x - y| = |-(x - y)| = |y - x|$ .
10. Même méthode (exercice).

□

Comment exprimer le fait que deux réels  $x$  et  $y$  sont proches ? L'idée est de quantifier leur proximité grâce à la quantité  $|x - y|$ . Les deux dernières propriétés de la proposition précédente rendent ce choix clair. Si  $x$  et  $y$  sont proches à moins de  $\varepsilon$ , c'est-à-dire si  $|x - y| < \varepsilon$ , alors  $x$  est confiné dans l'intervalle de centre  $y$  et d'épaisseur  $\varepsilon$ , et inversement  $y$  est confiné dans l'intervalle de centre  $x$  et d'épaisseur  $\varepsilon$ .

Notons que la propriété 6 de la proposition ci-dessus implique que si  $|x - y| < \varepsilon$ , alors  $||x| - |y|| < \varepsilon$ , autrement dit  $x$  et  $y$  sont proches à moins de  $\varepsilon$ , alors leurs valeurs absolues le sont aussi (cela démontre la continuité de la valeur absolue).

**Proposition 7.4.** *La fonction  $(x, y) \in \mathbb{R} \mapsto |x - y|$  est une distance, c'est-à-dire qu'elle satisfait les trois conditions suivantes.*

1. *Séparation* : pour tout  $x, y \in \mathbb{R}$ ,

$$|x - y| = 0 \iff x = y.$$

2. *Symétrie* : pour tout  $x, y \in \mathbb{R}$ ,

$$|x - y| = |y - x|.$$

3. *Inégalité triangulaire* : pour tout  $x, y, z \in \mathbb{R}$ ,

$$|x - z| \leq |x - y| + |y - z|.$$

**Remarque 7.5.** Explication intuitive de chaque point :

1. Séparation : Le but étant de quantifier la proximité entre  $x$  et  $y$  avec la quantité  $|x - y|$ , on voit qu'il existe une valeur de  $|x - y|$  qui caractérise l'égalité  $x = y$  (le cas où la distance est minimale).
2. Symétrie : la distance de  $x$  à  $y$  et la distance de  $y$  à  $x$  sont les mêmes.
3. Inégalité triangulaire : C'est plus court d'aller directement de  $x$  à  $z$ , plutôt que d'aller de  $x$  à  $y$ , puis de  $y$  à  $z$ .

**Preuve.** La séparation vient de la propriété 1 de la proposition 7.2. La symétrie vient de la propriété 4. L'inégalité triangulaire vient de... l'inégalité triangulaire :

$$|x - z| = |(x - y) - (y - z)| \leq |x - y| + |y - z|.$$

□

**Exercice 7.6.** Soient  $x, y \in \mathbb{R}$  tels que  $x < y$ .

1. Déterminer les ensembles  $\{z \in \mathbb{R} \mid |y - z| \leq |x - z|\}$  et  $\{z \in \mathbb{R} \mid |y - z| < |x - z|\}$ .  
On définit les fonctions suivantes :

$$\begin{aligned} f: \mathbb{R} &\rightarrow \mathbb{R} \\ z &\mapsto \min(|y - z|, |z - x|) \end{aligned}$$

$$\begin{aligned} g: \mathbb{R} &\rightarrow \mathbb{R} \\ z &\mapsto \max(|y - z|, |z - x|) \end{aligned}$$

2. Montrer que l'ensemble  $E = \{f(z) \mid z \in \mathbb{R}\}$  admet un plus petit élément et déterminer les éléments  $z_0 \in \mathbb{R}$  tels que  $f(z_0) = \min E$ .
3. Tracer le graphe de  $f$ .
4. Montrer que l'ensemble  $F = \{g(z) \mid z \in \mathbb{R}\}$  admet un plus petit élément et déterminer les éléments  $z_0 \in \mathbb{R}$  tels que  $g(z_0) = \min F$ .
5. Tracer le graphe de  $g$ .

Terminons avec cette propriété cruciale.

**Proposition 7.7.** Soit  $x \in \mathbb{R}$ . Alors

$$x = 0 \iff \forall \varepsilon > 0, |x| < \varepsilon.$$

**Preuve.** L'implication directe est immédiate. Supposons maintenant qu'on a  $|x| < \varepsilon$  pour tout  $\varepsilon > 0$ . Si par l'absurde  $|x| > 0$ , alors on applique l'inégalité à  $\varepsilon = |x|$  et on a  $|x| < |x|$ , c'est absurde. Donc  $|x| \leq 0$ . Mais  $|x| \geq 0$  par définition, donc  $|x| = 0$ , donc  $x = 0$ .  $\square$

**Remarque 7.8.** La section 6.6 nous permet également d'obtenir

$$x = 0 \iff \forall n \in \mathbb{N}, |x| < \frac{1}{n}.$$

Ainsi, on a remplacé un quantificateur sur  $\mathbb{R}_{>0}$  en un quantificateur sur  $\mathbb{N}$ .

Dans beaucoup de domaines des mathématiques (par exemple la théorie de la mesure, la topologie), il est très souvent utile de se ramener à un quantificateur sur  $\mathbb{N}$ , ou sur tout autre ensemble en bijection avec  $\mathbb{Q}$ . Cette modification est à l'origine de beaucoup de résultats d'existence spectaculaire (par exemple, existence d'une fonction continue de  $\mathbb{R}$  dans  $\mathbb{R}$ , nulle part différentiable). La proposition 6.40 et le corollaire 6.44 du chapitre 6 sont donc des résultats indispensables.

## 7.2 Limites

Soient  $(u_n)_{n \in \mathbb{N}}$  une suite réelle et  $L$  un réel. On veut caractériser le fait que quand  $n$  grandit,  $u_n$  et  $L$  deviennent de plus en plus proches. Le cas extrême, à savoir  $u_n = L$  est équivalent à « pour tout  $\varepsilon > 0$ ,  $|u_n - L| < \varepsilon$  » d'après la proposition 7.7. Ainsi, dire que  $u_n$  et  $L$  sont de plus en plus proches, c'est en quelque sorte dire que  $|u_n - L| < \varepsilon$  pour « de plus en plus » de  $\varepsilon > 0$ . C'est exactement l'idée derrière la définition de la convergence d'une suite réelle.

**Définition 7.9.** Soient  $(u_n)_{n \in \mathbb{N}}$  une suite réelle et  $L$  un réel. On dit que  $(u_n)_{n \in \mathbb{N}}$  converge vers  $L$ , ou que  $L$  est la *limite* de  $(u_n)_{n \in \mathbb{N}}$ , si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - L| < \varepsilon.$$

Dans ce cas, on note  $\lim_{n \rightarrow \infty} u_n = L$ , ou  $u_n \xrightarrow[n \rightarrow \infty]{} L$ .

On dit que la suite *diverge* si elle ne converge vers aucun réel  $L$ , autrement dit si

$$\forall L \in \mathbb{R}, \exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \geq N, |u_n - L| \geq \varepsilon.$$

**Remarque 7.10.** Étant données des assertions  $P(n)$  pour tout  $n \in \mathbb{N}$ , l'assertion «  $\forall N \in \mathbb{N}, \exists n \geq N, P(n)$  » signifie qu'il existe une infinité d'entiers  $n \in \mathbb{N}$  tels que  $P(n)$ .

Ainsi,  $(u_n)_{n \in \mathbb{N}}$  ne converge pas vers  $L$  si pour toute épaisseur  $\varepsilon$ , on trouvera une infinité d'entiers  $n > 0$  tels que  $u_n$  est loin de  $L$  à plus de  $\varepsilon$ .

**Remarque 7.11.**

- La définition de la limite s'applique aussi aux suites indexées sur  $\{n \in \mathbb{Z} \mid n \geq K\}$ ,  $K \in \mathbb{R}$  quelconque. Il suffit simplement de remplacer  $\mathbb{N}$  par cet ensemble dans la définition.
- De plus, pour  $K \in \mathbb{R}$ , la convergence de  $(u_n)_{n \in \mathbb{N}}$  est équivalente à la convergence de  $(u_n)_{n=K}^\infty$ . La limite ne concerne que les grandes valeurs de  $n$  !  
Justifions-le. Notons  $(v_n)_{n=K}^\infty = (u_n)_{n=K}^\infty$  (pour insister sur le fait que  $v_n$  n'est pas défini pour les mêmes  $n$ ). Supposons que  $\lim_{n \rightarrow \infty} u_n = L$ . Soit  $\varepsilon > 0$ . On dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $|u_n - L| < \varepsilon$ . Ou bien  $K \geq 1$ , et donc  $v_n$  est bien défini pour  $n \geq N$ , ou bien  $K > 1$ , et donc  $v_n$  est bien défini pour tout  $n \geq \max(N, K)$ . Dans tous les cas, on pose  $M = \max(N, K)$  et on obtient  $|v_n - L| = |u_n - L| < \varepsilon$  pour tout  $n \geq M$ . D'où  $\lim_{n \rightarrow \infty} v_n = L$ . L'autre sens se démontre de la même manière.
- Supposons que pour un certain  $K \in \mathbb{N}$ , une suite  $(u_n)_{n \in \mathbb{N}}$  vérifie  $u_n = 0$  pour tout  $n < K$  et  $u_n \neq 0$  pour  $n \geq K$ , alors  $\frac{1}{u_n}$  n'est défini que pour  $n \geq K$ . Si on s'intéresse à la limite de la suite de terme général  $1/u_n$ , on sous-entendra alors qu'on parle de la suite  $(\frac{1}{u_n})_{n \geq K}$ .

**Proposition 7.12** (Unicité de la limite). *Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle, soient  $L, L' \in \mathbb{R}$ . Si  $(u_n)_{n \in \mathbb{N}}$  converge vers  $L$  et vers  $L'$ , alors  $L = L'$ . Ainsi l'écriture  $\lim_{n \rightarrow \infty} u_n = L$  est bien définie.*

**Preuve.** Montrons  $|L - L'| < \varepsilon$  pour tout  $\varepsilon > 0$ . On conclut ensuite grâce à la proposition 7.7.

Soit  $\varepsilon > 0$ . On applique la définition de la convergence à  $\varepsilon/2$ . On dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $|u_n - L| < \varepsilon/2$ ; on dispose de  $N' \in \mathbb{N}$  tel que pour tout  $n \geq N'$ ,  $|u_n - L'| < \varepsilon/2$ . Notons  $M = \max(N, N')$ . Ainsi pour tout  $n \geq M$ , on a  $|u_n - L| < \varepsilon/2$  et  $|u_n - L'| < \varepsilon/2$ . Donc pour un entier  $n \geq N$  fixé, on obtient grâce à l'inégalité triangulaire :

$$|L - L'| \leq |L - u_n| + |u_n - L'| < \varepsilon/2 + \varepsilon/2 = \varepsilon,$$

ce qu'on voulait. □

**Remarque 7.13.**

1. Concernant la preuve qu'on vient d'écrire, on n'a pas besoin de s'embêter à chercher le bon «  $\varepsilon$  » auquel il faut appliquer la définition (ici  $\varepsilon/2$ ) pour tomber exactement sur  $|L - L'| < \varepsilon$ . On aurait pu appliquer la définition à  $\varepsilon$  lui-même et obtenir  $|L - L'| < 2\varepsilon$ . Vu que  $\{2\varepsilon \mid \varepsilon > 0\}$  et  $\{\varepsilon \mid \varepsilon > 0\}$  sont les mêmes ensembles, c'est-à-dire  $\mathbb{R}_{>0}$  (le vérifier, exercice), on peut toujours conclure.
2. Au lieu d'introduire plusieurs «  $N$  » ( $N_1$  et  $N_2$  dans la preuve précédente) et de prendre le maximum de ces entiers, on peut en fait directement considérer un seul entier  $N$  en commun à toutes applications de la définition de la convergence (à condition de l'appliquer un nombre fini de fois). Cela rend la preuve moins lourde au niveau des notations

**Exemple 7.14.**

1. Soit  $L \in \mathbb{R}$  et pour tout  $n \in \mathbb{N}$ ,  $u_n = L$ . Alors la suite converge vers  $L$ . En effet, étant donné  $\varepsilon > 0$  et  $n \in \mathbb{N}$ , on a  $|u_n - L| = 0 < \varepsilon$ .
2. Pour tout  $n \in \mathbb{N}$ , posons  $u_n = (-1)^n$ . La suite ne converge pas. En effet, soit  $L \in \mathbb{R}$ , montrons que  $(u_n)_{n \in \mathbb{N}}$  ne converge pas vers  $L$ . Si  $L \geq 0$ , alors prenons  $\varepsilon = \frac{1}{2}$ . Dès que  $n$  est impaire, on a  $|u_n - L| = |-1 - L| = L + 1 \geq 1 \geq \varepsilon$ . Il existe une infinité d'entiers impaires donc la suite ne converge pas vers  $L$ . Si  $L \leq 0$ , alors on considère le même  $\varepsilon$  et on regarde sur les entiers pairs.

**Exercice 7.15.** Pour tout  $n \in \mathbb{N}$ , on pose  $u_n = 0$  si  $n$  est pair,  $u_n = n$  si  $n$  est impair. La suite  $(u_n)_{n \in \mathbb{N}}$  converge-t-elle vers 0 ?

**Proposition 7.16.** Posons  $u_n = \frac{1}{n}$  pour tout  $n \in \mathbb{N}$ . Alors la suite converge vers 0.

**Preuve.** C'est une conséquence immédiate de la proposition 6.44 (et aussi du fait que  $\frac{1}{n}$  est positif, donc plus grand que  $-\varepsilon$ ).  $\square$

**Exercice 7.17.** Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle telle que  $\{u_n \mid n \in \mathbb{N}\}$  est fini. Montrer que  $(u_n)_{n \in \mathbb{N}}$  converge si et seulement si elle est stationnaire (cela veut dire qu'il existe  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $u_n = u_N$ .)

**Définition 7.18.** On dit qu'une suite  $(u_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$  si

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

Dans ce cas, on note  $\lim_{n \rightarrow \infty} u_n = \infty$ ,<sup>a</sup> ou  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$ .

On dit qu'une suite  $(u_n)_{n \in \mathbb{N}}$  diverge vers  $-\infty$  si

$$\forall x \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \leq x.$$

Dans ce cas, on note  $\lim_{n \rightarrow \infty} u_n = -\infty$ ,<sup>b</sup> ou  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty$ .

a.  $\infty$  n'est pas un réel, «  $\lim_{n \rightarrow \infty} u_n = +\infty$  » n'est pas une égalité entre réels, c'est juste une notation pour désigner une propriété.

b.  $-\infty$  n'est pas un réel, «  $\lim_{n \rightarrow \infty} u_n = -\infty$  » n'est pas une égalité entre réels, c'est juste une notation pour désigner une propriété.

De même que pour la convergence, la divergence vers  $\pm\infty$  ne concerne que les grands indices, on peut enlever les premiers termes de la suite sans changer la notion.

**Remarque 7.19.** La divergence vers  $\infty$  signifie que si on fixe un seuil  $x$  (n'importe lequel, arbitrairement grand), alors à partir d'un certain rang, les termes de la suite sont au-delà de  $x$ .

En utilisant les idées de la section 6.6, on peut également réduire la définition à

$$\forall K \in \mathbb{Z}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \geq K.$$

Les mêmes remarques sont valables pour la divergence vers  $-\infty$ .

**Exercice 7.20.** Vérifier que la suite  $(n)_{n \in \mathbb{N}}$  diverge vers  $\infty$ , et que la suite  $(-n)_{n \in \mathbb{N}}$  diverge vers  $-\infty$ .

**Proposition 7.21.** Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle. Alors les trois assertions suivantes s'excluent<sup>a</sup> :

- $(u_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$  ;
- $(u_n)_{n \in \mathbb{N}}$  diverge vers  $-\infty$  ;
- $(u_n)_{n \in \mathbb{N}}$  converge.

a. Attention, il se peut qu'aucune de ces assertions ne soit satisfaite.

**Preuve.** Supposons que  $(u_n)_{n \in \mathbb{N}}$  converge et notons  $L$  sa limite. La définition appliquée à  $\varepsilon = 1$  indique qu'on dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ , on a  $|u_n - L| < 1$ . En particulier, pour de tels entiers  $n$ , on a  $u_n < L + 1$ . Ainsi les termes de la suite ne sont pas  $\geq L + 1$  à partir d'un certain rang, cela contredit la définition de la divergence vers  $\infty$ , pour  $x = L + 1$ . Donc la suite ne diverge pas vers  $\infty$ . On montre de la même manière que la suite ne diverge pas vers  $-\infty$ .

Supposons que la suite diverge vers  $\infty$  et montrons qu'elle ne diverge pas vers  $-\infty$ . (exercice)

De la même manière, si la suite diverge vers  $-\infty$ , alors elle ne diverge pas vers  $\infty$ .  $\square$

**Exercice 7.22.** Prouver ce qui a été laissé en exercice dans la preuve ci-dessus.

**Exercice 7.23.** Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle, soit  $L \in \mathbb{R}$ . Montrer les implications suivantes.

1.  $u_n \xrightarrow[n \rightarrow \infty]{} L \Rightarrow |u_n| \xrightarrow[n \rightarrow \infty]{} |L|$ .
2.  $|u_n| \xrightarrow[n \rightarrow \infty]{} 0 \Rightarrow u_n \xrightarrow[n \rightarrow \infty]{} 0$ . La réciproque du premier point est-elle également vraie pour  $L \neq 0$  ?
3.  $u_n \xrightarrow[n \rightarrow \infty]{} \infty \Rightarrow |u_n| \xrightarrow[n \rightarrow \infty]{} \infty$ .
4.  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty \Rightarrow |u_n| \xrightarrow[n \rightarrow \infty]{} \infty$ .

Indication pour la première implication : inégalité triangulaire inversée.

**Exercice 7.24** (Somme de Cesàro). Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle et pour tout  $n \in \mathbb{N}$ ,

$$v_n = \frac{u_1 + \dots + u_n}{n}.$$

On suppose que  $(u_n)_{n \in \mathbb{N}}$  converge vers  $L \in \mathbb{R}$  (resp. diverge vers  $\infty$ , resp. diverge vers  $-\infty$ ). Montrer qu'il en est de même pour  $(v_n)_{n \in \mathbb{N}}$ . La réciproque est-elle vraie ?

**Proposition 7.25.** Soient  $(u_n)_{n \in \mathbb{N}}$  et  $(v_n)_{n \in \mathbb{N}}$  des suites réelles, soient  $L, L'$  et  $a$  des réels.

1. Si  $u_n \xrightarrow[n \rightarrow \infty]{} L$ , alors  $au_n \xrightarrow[n \rightarrow \infty]{} aL$ .
2. Si  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$ , alors  $au_n \xrightarrow[n \rightarrow \infty]{} \infty$  si  $a > 0$ ,  $-\infty$  si  $a < 0$ ,  $0$  si  $a = 0$ ; et inversement si  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty$ .
3. Si  $u_n \xrightarrow[n \rightarrow \infty]{} L$  et  $v_n \xrightarrow[n \rightarrow \infty]{} L'$ , alors  $u_n + v_n \xrightarrow[n \rightarrow \infty]{} L + L'$  et  $u_n v_n \xrightarrow[n \rightarrow \infty]{} LL'$ .
4. Si  $u_n \xrightarrow[n \rightarrow \infty]{} L$  et  $L \neq 0$ , alors  $u_n \neq 0$  à partir d'un certain rang, et  $\frac{1}{u_n} \xrightarrow[n \rightarrow \infty]{} \frac{1}{L}$ .
5. Si  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$  et  $v_n \xrightarrow[n \rightarrow \infty]{} \infty$ , alors  $u_n + v_n \xrightarrow[n \rightarrow \infty]{} \infty$  et  $u_n v_n \xrightarrow[n \rightarrow \infty]{} \infty$ .
6. Si  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty$  et  $v_n \xrightarrow[n \rightarrow \infty]{} -\infty$ , alors  $u_n + v_n \xrightarrow[n \rightarrow \infty]{} -\infty$  et  $u_n v_n \xrightarrow[n \rightarrow \infty]{} \infty$ .
7. Si  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$  et  $v_n \xrightarrow[n \rightarrow \infty]{} -\infty$ , alors  $u_n v_n \xrightarrow[n \rightarrow \infty]{} -\infty$ .
8. Si  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$  et  $v_n \xrightarrow[n \rightarrow \infty]{} L$ ,  $L \neq 0$ , alors  $u_n v_n \xrightarrow[n \rightarrow \infty]{} \infty$  si  $L > 0$ ,  $-\infty$  si  $L < 0$ .
9. Si  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty$  et  $v_n \xrightarrow[n \rightarrow \infty]{} L$ ,  $L \neq 0$ , alors  $u_n v_n \xrightarrow[n \rightarrow \infty]{} -\infty$  si  $L > 0$ ,  $\infty$  si  $L < 0$ .
10. Si  $(u_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$  ou  $-\infty$ , alors  $u_n \neq 0$  à partir d'un certain rang, et  $(1/u_n)_{n \in \mathbb{N}}$  converge vers  $0$ .

### Preuve.

1. Facile si  $a = 0$ . Supposons maintenant  $a \neq 0$ . Soit  $\varepsilon > 0$ . On dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $|u_n - L| < \varepsilon$ . Ainsi, pour tout  $n \geq N$ , on a  $|au_n - La| = |a| \cdot |u_n - L| < |a|\varepsilon$ . Ceci démontre ce qu'on veut puisque  $\{|a|\varepsilon \mid \varepsilon > 0\}$  vaut exactement  $\mathbb{R}_{>0}$ .
2. Par exemple si  $a > 0$ , on utilise le fait que  $u_n \geq x/a \Rightarrow au_n \geq x$ .
3. Soit  $\varepsilon > 0$ . On dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $|u_n - L| < \varepsilon$  et  $|v_n - L'| < \varepsilon$ . Ainsi pour tout  $n \geq N$ , on a

$$|(u_n + v_n) - (L + L')| = |(u_n - L) + (v_n - L')| \leq |u_n - L| + |v_n - L'| \leq 2\varepsilon.$$

D'où  $u_n + v_n \xrightarrow[n \rightarrow \infty]{} L + L'$ .

Pour tout  $n \in \mathbb{N}$ , on a

$$|u_n v_n - LL'| = |u_n v_n - Lv_n + Lv_n - LL'| \leq |u_n - L| \cdot |v_n| + L|v_n - L'|.$$

Or pour tout  $n \geq N$ , on a  $|v_n| \leq |L'| + \varepsilon$ . Quitte à augmenter  $N$ , on suppose sans perte de généralité que pour tout  $n \geq N$ ,  $|u_n - L| \leq \varepsilon/(|L'| + \varepsilon)$ . Ainsi, pour tout  $n \geq N$ ,

$$|u_n v_n - LL'| \leq |u_n - L| \cdot |v_n| + L|v_n - L'| \leq \frac{\varepsilon}{|L'| + \varepsilon}(|L'| + \varepsilon) + L\varepsilon = (L + 1)\varepsilon.$$

Pour conclure, on remarque que  $\{(L + 1)\varepsilon \mid \varepsilon > 0\}$  et  $\mathbb{R}_{>0}$  sont les mêmes ensembles.

4. En appliquant la définition de la convergence à  $|L|/2$ , on dispose de  $N \in \mathbb{N}$ , tel que pour tout  $n \geq N$ ,  $|u_n - L| < |L|/2$ . Ainsi  $|u_n| > |L|/2 > 0$ , donc  $u_n \neq 0$  pour tout  $n \geq N$ . Pour tout  $n \geq N$ , on peut donc considérer  $1/u_n$ . On a ainsi

$$\left| \frac{1}{u_n} - \frac{1}{L} \right| = \frac{|L - u_n|}{|u_n| \cdot |L|}.$$

Considérons maintenant  $\varepsilon > 0$ . Quitte à augmenter  $N$ , on suppose qu'on a  $|u_n - L| < \varepsilon$  pour tout  $n \geq N$ . Ainsi, pour  $n \geq N$ ,

$$\left| \frac{1}{u_n} - \frac{1}{L} \right| = \frac{|L - u_n|}{|u_n| \cdot |L|} \leq \frac{\varepsilon}{\frac{|L|}{2} |L|} = \varepsilon \frac{2}{L^2}.$$

D'où  $\frac{1}{u_n} \xrightarrow[n \rightarrow \infty]{} \frac{1}{L}$ .

5. Exercice.
6. Exercice.
7. Exercice.
8. Exercice.
9. Exercice.
10. Considérons le cas où  $u_n \rightarrow \infty$ . L'autre cas est similaire. Soit  $\varepsilon > 0$ . On dispose de  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ ,  $u_n > \frac{1}{\varepsilon}$ . En particulier, pour ces entiers  $n$ , on a  $u_n > 0$ , donc  $\frac{1}{u_n}$  est bien défini. Ainsi pour  $n \geq N$ , on a  $0 < \frac{1}{u_n} < \varepsilon$ , donc  $-\varepsilon < \frac{1}{u_n} < \varepsilon$ . D'où le résultat. □

**Exercice 7.26.** Prouver ce qui a été laissé en exercice dans la preuve ci-dessus.

**Exercice 7.27.** Pour chacun des points de la liste qui suit, trouver des suites  $(u_n)_{n \in \mathbb{N}}$  et  $(v_n)_{n \in \mathbb{N}}$  telles que  $(u_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$ ,  $(v_n)_{n \in \mathbb{N}}$  diverge vers  $-\infty$ , et telles que :

1.  $(u_n + v_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$  ;
2. ou  $(u_n + v_n)_{n \in \mathbb{N}}$  diverge vers  $-\infty$  ;
3. ou  $(u_n + v_n)_{n \in \mathbb{N}}$  converge vers  $L$  (avec  $L \in \mathbb{R}$  fixé) ;
4. ou  $(u_n + v_n)_{n \in \mathbb{N}}$  diverge, mais ne diverge ni vers  $+\infty$ , ni vers  $-\infty$ .

**Proposition 7.28.** Soit  $k \in \mathbb{N}$ . Alors  $(n^k)_{n \in \mathbb{N}}$  diverge vers  $+\infty$  et  $(1/n^k)_{n \in \mathbb{N}}$  converge vers 0.

**Preuve.** Par induction sur  $k \in \mathbb{N}$ . À vérifier, exercice. □

**Exercice 7.29.** Démontrer la proposition ci-dessus

**Exemple 7.30.** Considérons pour tout  $n \in \mathbb{N}$ ,  $u_n = \frac{2n^2 + 4n + 10}{3n^2 + 1}$ . On veut savoir si la suite converge ou diverge.

Pour cela, on factorise au numérateur par la puissance de  $n$  de plus haut exposant (ici  $n^2$ ), et de même au dénominateur (ici  $n^2$ ). On obtient

$$u_n = \frac{2n^2 + 4n + 10}{3n^2 + 1} = \frac{n^2}{n^2} \frac{2 + \frac{4}{n} + \frac{10}{n^2}}{3 + \frac{1}{n^2}} = \frac{2 + \frac{4}{n} + \frac{10}{n^2}}{3 + \frac{1}{n^2}}.$$

Puis par opération sur les limites, on obtient que la suite converge vers  $2/3$ .

Cela fonctionne également quand le plus haut exposant n'est pas le même au numérateur et au dénominateur. Par exemple,

$$\frac{5n^2 + 4}{n^3 + 6n} = \frac{n^2}{n^3} \frac{5 + \frac{4}{n^2}}{1 + \frac{6}{n^2}} = \underbrace{\frac{1}{n}}_{\xrightarrow[n \rightarrow \infty]{} 0} \underbrace{\frac{5 + \frac{4}{n^2}}{1 + \frac{6}{n^2}}}_{\xrightarrow[n \rightarrow \infty]{} 5} \xrightarrow[n \rightarrow \infty]{} 0.$$

Autre exemple :

$$\frac{-n^4 + 1}{n + 1} = \frac{n^4}{n} \frac{-1 + \frac{1}{n^4}}{1 + \frac{1}{n}} = \underbrace{n^3}_{\xrightarrow[n \rightarrow \infty]{} \infty} \underbrace{\frac{-1 + \frac{1}{n^4}}{1 + \frac{1}{n}}}_{\xrightarrow[n \rightarrow \infty]{} -1} \xrightarrow[n \rightarrow \infty]{} -\infty.$$

**Proposition 7.31.** Soient  $(u_n)_{n \in \mathbb{N}}$ ,  $(v_n)_{n \in \mathbb{N}}$  et  $(w_n)_{n \in \mathbb{N}}$  des suites réelles, soit  $L$  un réel. On suppose qu'il existe  $N$  tel que pour tout  $n \geq N$ ,  $v_n \leq u_n \leq w_n$

1. Si  $v_n \xrightarrow[n \rightarrow \infty]{} L$  et  $w_n \xrightarrow[n \rightarrow \infty]{} L$ , alors  $u_n \xrightarrow[n \rightarrow \infty]{} L$ .
2. Si  $v_n \xrightarrow[n \rightarrow \infty]{} \infty$ , alors  $u_n \xrightarrow[n \rightarrow \infty]{} \infty$ .
3. Si  $w_n \xrightarrow[n \rightarrow \infty]{} -\infty$ , alors  $u_n \xrightarrow[n \rightarrow \infty]{} -\infty$ .

**Preuve.** On ne démontre que le premier point, les autres sont laissés en exercice.

Soit  $\varepsilon > 0$ . Quitte à augmenter  $N$ , on suppose que pour tout  $n \geq N$ ,  $|v_n - L| < \varepsilon$  et  $|w_n - L| < \varepsilon$ . En particulier, on a  $v_n > L - \varepsilon$  et  $w_n < L + \varepsilon$ . Ainsi pour tout  $n \geq N$ ,

$$L - \varepsilon < v_n < u_n < w_n < L + \varepsilon,$$

donc  $|u_n - L| < \varepsilon$ . □

**Proposition 7.32.** Soit  $q \in \mathbb{R}$ .

1. Si  $q > 1$ , alors  $(q^n)_{n \in \mathbb{N}}$  diverge vers  $\infty$ .
2. Si  $q \leq -1$ , alors  $(q^n)_{n \in \mathbb{N}}$  diverge, mais ni vers  $\infty$ , ni vers  $-\infty$ .
3. Si  $q = 1$ , alors  $(q^n)_{n \in \mathbb{N}}$  converge vers 1.
4. Si  $|q| < 1$ , alors  $(q^n)_{n \in \mathbb{N}}$  converge vers 0.

**Preuve.** Rappelons l'inégalité de Bernoulli qui fait l'objet de l'exercice 3.37 : pour tout  $x \geq -1$ , pour tout  $n \in \mathbb{N}$ ,

$$(1 + x)^n \geq 1 + nx.$$

Par changement de variable, on obtient que pour tout  $x \geq 0$ , pour tout  $n \in \mathbb{N}$ ,  $x^n \geq 1 + n(x - 1)$ . C'est cette forme qu'on utilisera pour la preuve.

1. Soit  $q > 1$ . Pour tout  $n \in \mathbb{N}$ , on a  $q^n \geq 1 + n(q - 1)$ . Le réel  $q - 1$  est positif, donc  $1 + n(q - 1) \xrightarrow[n \rightarrow \infty]{} \infty$ . Donc  $q^n \xrightarrow[n \rightarrow \infty]{} \infty$ .
2. Soit  $q \leq -1$ . Dans le cas  $q = -1$ , on a déjà vu que la suite associée diverge (elle oscille entre  $-1$  et  $1$ ). Supposons donc  $q < -1$ . On a  $|q| > 1$  donc le point précédent

montre que  $|q^n| \xrightarrow{n \rightarrow \infty} \infty$ . Ainsi  $(q^n)_{n \in \mathbb{N}}$  ne converge pas. De plus, elle ne diverge pas vers  $\infty$ , sinon on aurait  $q^n \geq 0$  à partir d'un certain rang (or  $q^n < 0$  pour  $n$  impair). De même, la suite ne diverge pas vers  $-\infty$ .

3. Si  $q = 1$ , alors on a la suite constante égale à 1, elle converge donc vers 1.

4. Si  $|q| < 1$ , alors  $\frac{1}{|q|} > 1$ , donc  $\left(\frac{1}{|q|}\right)^n \xrightarrow{n \rightarrow \infty} \infty$ . Ainsi

$$|q^n| = \frac{1}{\frac{1}{|q^n|}} = \frac{1}{\left(\frac{1}{|q|}\right)^n} \xrightarrow{n \rightarrow \infty} 0.$$

□

**Exercice 7.33.** Pour tout  $n \in \mathbb{N}$ , soit  $u_n = \frac{1}{n}$  si  $n$  est pair,  $u_n = \frac{3}{5^n}$  si  $n$  est impair. Étudier la convergence de la suite  $(u_n)_{n \in \mathbb{N}}$ .

**Définition 7.34.** Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle. On dit que la suite est...

- *majorée* s'il existe  $x \in \mathbb{R}$  tel que pour tout  $n \in \mathbb{N}$ ,  $u_n \leq x$  ;
- *minorée* s'il existe  $x \in \mathbb{R}$  tel que pour tout  $n \in \mathbb{N}$ ,  $u_n \geq x$  ;
- *bornée* si elle est majorée et minorée ;
- *croissante* si pour tout  $n \in \mathbb{N}$ , on a  $u_n \leq u_{n+1}$  ;
- *décroissante* si pour tout  $n \in \mathbb{N}$ , on a  $u_n \geq u_{n+1}$  ;
- *monotone* si elle est croissante ou décroissante.

**Attention.** La négation de «  $(u_n)_{n \in \mathbb{N}}$  est croissante » n'est pas «  $(u_n)_{n \in \mathbb{N}}$  est décroissante ».

**Proposition 7.35.** Toute suite convergente est bornée.

**Preuve.** Soit  $(u_n)_{n \in \mathbb{N}}$  convergente, notons  $L$  sa limite. Par définition, il existe  $N \in \mathbb{N}$  tel que pour tout  $n \geq N$ , on a  $|u_n - L| < 1$ . Ainsi pour tout  $n \geq N$ , on a

$$L - 1 < u_n < L + 1.$$

Ceci n'est pas vrai pour tout  $n \in \mathbb{N}$ . Mais les indices  $n$  pour lesquels on n'a *a priori* pas l'encadrement, à savoir  $1, 2, \dots, N - 1$ , sont en nombre fini. Ainsi,  $\max(u_1, \dots, u_{N-1}, L + 1)$  est bien défini et majore la suite. De même,  $\min(u_1, \dots, u_{N-1}, L - 1)$  est bien défini et minore la suite. □

**Exercice 7.36.** Une suite divergente vers  $\infty$  ou  $-\infty$  peut-elle être bornée ? Une suite bornée est-elle convergente ?

**Proposition 7.37.** Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle.

1. Si  $(u_n)_{n \in \mathbb{N}}$  est croissante et majorée, alors elle converge et pour tout  $n \in \mathbb{N}$ , on a  $u_n \leq \lim_{k \rightarrow \infty} u_k$ .
2. Si  $(u_n)_{n \in \mathbb{N}}$  est décroissante et minorée, alors elle converge et pour tout  $n \in \mathbb{N}$ , on a

$$u_n \geq \lim_{k \rightarrow \infty} u_k.$$

En particulier, toute suite monotone et bornée converge.

**Preuve.** On ne démontre que le premier point. Supposons donc que la suite  $(u_n)_{n \in \mathbb{N}}$  est croissante et majorée. Comme elle est majorée, l'ensemble  $\{u_n \mid n \in \mathbb{N}\}$  est majorée dans  $\mathbb{R}$ . L'axiome C.6 assure donc l'existence d'un supremum, qu'on note  $L$ . Montrons que  $(u_n)_{n \in \mathbb{N}}$  converge vers  $L$ . Soit  $\varepsilon > 0$ . D'après la proposition 6.38, il existe un élément de  $\{u_n \mid n \in \mathbb{N}\}$  qui appartient à  $(L - \varepsilon, L]$ . Autrement dit, il existe  $N \in \mathbb{N}$  tel que  $u_N \in (L - \varepsilon, L]$ . Par croissance de la suite, on a  $u_N \leq u_n$  pour tout  $n \geq N$ , et  $u_n \leq L$  par définition d'un supremum. Ainsi pour tout  $n \geq N$ , on a

$$L - \varepsilon < u_N \leq u_n \leq L,$$

donc  $|u_n - L| < \varepsilon$ . Donc la suite converge vers  $L$ .  $\square$

**Exemple 7.38.** Soit  $(a_n)_{n \in \mathbb{N}}$  une suite de réels **positifs ou nuls**. Montrons que si la suite  $(\sum_{k=1}^n a_k)_{n \in \mathbb{N}}$  est majorée, alors elle converge. Ainsi, on note  $\sum_{k=1}^{\infty} a_k = \lim_{n \rightarrow \infty} \sum_{k=1}^n a_k$ .

Posons  $u_n = \sum_{k=1}^n a_k$  pour tout  $n \in \mathbb{N}$ . La suite  $(u_n)_{n \in \mathbb{N}}$  est croissante car  $u_{n+1} - u_n = a_{n+1} \geq 0$ . Par hypothèse, elle est majorée. Ainsi, elle converge.

Par exemple, on peut appliquer cela à  $a_n = \frac{b_n}{2^n}$  où  $(b_n)_{n \in \mathbb{N}}$  est une suite bornée d'éléments de  $\mathbb{R}_{\geq 0}$ . En effet, si on note  $M$  un majorant de  $(b_n)_{n \in \mathbb{N}}$ , on a pour tout  $n \in \mathbb{N}$  :

$$\sum_{k=1}^n \frac{b_k}{2^k} \leq \sum_{k=1}^n \frac{M}{2^k} = M \frac{\frac{1}{2} - \frac{1}{2^{n+1}}}{1 - \frac{1}{2}} = M \left(1 - \frac{1}{2^n}\right) \leq M.$$

**Exercice 7.39.** Soit  $(x_n)_{n \in \mathbb{N}}$  une suite d'éléments de  $\{0, 1, \dots, 8, 9\}$ . Pour tout  $n \in \mathbb{N}$ , on définit  $u_n = 0.x_1 \dots x_n$  en écriture décimale.

Par exemple, si  $x_1 = 4$ ,  $x_2 = 0$ ,  $x_3 = 2$ ,  $x_4 = 8$ , ..., alors  $u_1 = 0.4$ ,  $u_2 = 0.40$ ,  $u_3 = 0.402$ ,  $u_4 = 0.4028$ , etc.

Montrer que  $(u_n)_{n \in \mathbb{N}}$  converge.

On termine avec une caractérisation séquentielle du supremum et de l'infimum.

**Proposition 7.40.** Soit  $A$  un sous-ensemble majoré de  $\mathbb{R}$ , soit  $x \in \mathbb{R}$ . Alors  $x = \sup A$  si et seulement si les deux conditions suivantes sont vérifiées :

- $x$  est un majorant de  $A$  ;
- il existe une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $A$  qui converge vers  $x$ .

Si  $A$  est minoré, alors  $x = \inf A$  si et seulement si les deux conditions suivantes sont vérifiées :

- $x$  est un minorant de  $A$  ;
- il existe une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $A$  qui converge vers  $x$ .

**Preuve.** Montrons-le pour le supremum, la preuve est similaire pour l'infimum. Supposons  $x = \sup A$ . Par définition, c'est un majorant de  $A$ . Pour tout  $n \in \mathbb{N}$ , on applique la proposition 6.38 à  $\varepsilon = 1/n$ , pour ainsi obtenir l'existence d'un élément  $u_n$  de  $A$  tel que  $u_n \in (x - 1/n, x]$ . On a donc pour tout  $n \in \mathbb{N}$ ,  $x - \frac{1}{n} \leq u_n \leq x$ . Or  $1/n \xrightarrow{n \rightarrow \infty} 0$  donc par encadrement, on obtient  $u_n \xrightarrow{n \rightarrow \infty} x$ .

Réciproquement, supposons que  $x$  est un majorant de  $A$  admettant une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $A$  qui converge vers  $x$ . On utilise encore la caractérisation proposée par la proposition 6.38. Soit  $\varepsilon > 0$ . On cherche  $a \in A$  tel que  $a \in (x - \varepsilon, x]$ . Or la convergence de la suite vers  $x$  implique l'existence de  $n \in \mathbb{N}$  tel que  $u_n \in (x - \varepsilon, x + \varepsilon)$ . Mais  $u_n \in A$  et  $x$  majore  $A$ , donc  $u_n \leq x$ . Ainsi  $u_n \in A$  et  $u_n \in (x - \varepsilon, x]$ , c'est donc l'élément de  $A$  qu'on cherchait.  $\square$

## 7.3 Problèmes

### 7.3.1 Problème 1

Dans ce problème, on fixe une suite réelle  $(u_n)_{n \in \mathbb{N}}$ . On la suppose bornée.

1. Pour tout  $n \in \mathbb{N}$ , posons  $v_n = \sup \{u_k \mid k \geq n\}$ . Montrer que  $v_n$  est bien défini.
2. Étudier la monotonie de  $(v_n)_{n \in \mathbb{N}}$ , montrer qu'elle converge et que  $\lim_{n \rightarrow \infty} v_n = \inf_{n \in \mathbb{N}} v_n$ .

On définit alors la *limite supérieure* de  $(u_n)_{n \in \mathbb{N}}$  comme étant cette limite,

$$\limsup_{n \rightarrow \infty} u_n = \lim_{n \rightarrow \infty} \sup \{u_k \mid k \geq n\} = \inf_{n \in \mathbb{N}} \sup \{u_k \mid k \geq n\}.$$

De même, on définit la *limite inférieure* :

$$\liminf_{n \rightarrow \infty} u_n = \lim_{n \rightarrow \infty} \inf \{u_k \mid k \geq n\} = \sup_{n \in \mathbb{N}} \inf \{u_k \mid k \geq n\}.$$

3. Calculer les limites supérieure et inférieure de la suite  $(u_n)_{n \in \mathbb{N}}$  dans chacun des cas :
  - (a) pour tout  $n \in \mathbb{N}$ ,  $u_n = (-1)^n$  ;
  - (b) pour tout  $n \in \mathbb{N}$ ,  $u_n = (-1)^n (1 + \frac{1}{n})$ .
4. Montrer que  $(u_n)_{n \in \mathbb{N}}$  converge si et seulement si  $\limsup_{n \rightarrow \infty} u_n = \liminf_{n \rightarrow \infty} u_n$ , et que dans ce cas on a  $\lim_{n \rightarrow \infty} u_n = \limsup_{n \rightarrow \infty} u_n = \liminf_{n \rightarrow \infty} u_n$ .

#### Définition.

- Une *extractrice* est une fonction  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante :

$$\forall n, m \in \mathbb{N}, n < m \Rightarrow \varphi(n) < \varphi(m).$$

- Une *sous-suite* de  $(u_n)_{n \in \mathbb{N}}$  est une suite de la forme  $(u_{\varphi(n)})_{n \in \mathbb{N}}$  où  $\varphi$  est une extractrice.
- On dit qu'un nombre réel  $L$  est une *valeur d'adhérence* de la suite  $(u_n)_{n \in \mathbb{N}}$  si  $L$  est la limite d'une sous-suite de  $(u_n)_{n \in \mathbb{N}}$ .

5. Déterminer les valeurs d'adhérence de  $((-1)^n)_{n \in \mathbb{N}}$ . Déterminer les valeurs d'adhérence d'une suite convergente.

6. Soit  $L \in \mathbb{R}$ . Montrer que  $L$  est une valeur d'adhérence de la suite  $(u_n)_{n \in \mathbb{N}}$  si et seulement si

$$\forall \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \geq N, |u_n - L| < \varepsilon.$$

On souhaite démontrer ce résultat classique.

**Théorème** (de Bolzano-Weierstrass). *Toute suite bornée admet une valeur d'adhérence.*

Pour le prouver, on va justement pouvoir expliciter des valeurs d'adhérence.

7. Montrer que  $\limsup_{n \rightarrow \infty} u_n$  et  $\liminf_{n \rightarrow \infty} u_n$  sont des valeurs d'adhérence de  $(u_n)_{n \in \mathbb{N}}$ . On a ainsi démontré le théorème de Bolzano-Weierstrass<sup>1</sup>.
8. Montrer que toute valeur d'adhérence de  $(u_n)_{n \in \mathbb{N}}$  appartient à  $[\liminf_{n \rightarrow \infty} u_n, \limsup_{n \rightarrow \infty} u_n]$ .
9. En déduire que  $(u_n)_{n \in \mathbb{N}}$  converge si et seulement si elle admet une unique valeur d'adhérence.<sup>2</sup>

La notion de valeur d'adhérence est une généralisation très pratique de la notion de limite, comme nous l'illustrons dans les applications suivantes.

10. **Application 1** : Soient  $(a_n)_{n \in \mathbb{N}}$  et  $(b_n)_{n \in \mathbb{N}}$  vérifiant

$$a_n^2 + b_n^2 \xrightarrow{n \rightarrow \infty} 2 \text{ et } a_n - b_n \xrightarrow{n \rightarrow \infty} 0.$$

Montrer que  $(a_n)_{n \in \mathbb{N}}$  et  $(b_n)_{n \in \mathbb{N}}$  convergent et déterminer leur limite (on montrera que les suites sont bornées et on étudiera leurs valeurs d'adhérence).<sup>3</sup>

11. **Application 2** : Soit  $(a_n)_{n \in \mathbb{N}}$  une suite réelle convergeant vers 0. Soit  $(u_n)_{n \in \mathbb{N}}$  vérifiant pour tout  $n \in \mathbb{N}$ ,  $u_{n+1} = \frac{1}{2}(1 + a_n)u_n + \frac{1}{2}$ . On veut montrer que  $(u_n)_{n \in \mathbb{N}}$  converge et déterminer sa limite.
- (a) Montrer que  $(u_n)_{n \in \mathbb{N}}$  est bornée et admet une valeur d'adhérence.
- (b) Soit  $L$  une valeur d'adhérence de  $(u_n)_{n \in \mathbb{N}}$ , et  $\varphi$  une extractrice telle que  $u_{\varphi(n)} \xrightarrow{n \rightarrow \infty} L$ . Montrer que  $u_{\varphi(n)-1} \xrightarrow{n \rightarrow \infty} 2L - 1$ .
- (c) Soit  $L_0$  une valeur d'adhérence  $(u_n)_{n \in \mathbb{N}}$ , et pour tout  $n \in \mathbb{N}$ ,  $L_n = 2L_{n-1} - 1$ . Montrer que pour tout  $n \in \mathbb{Z}_{\geq 0}$ ,  $L_n$  est une valeur d'adhérence et  $L_n = 1 + 2^n(L_0 - 1)$ .
- (d) En déduire que  $L_0 = 1$ . Conclure.
12. **Application 3** : Soit  $(u_n)_{n \in \mathbb{N}}$  une suite réelle. On suppose que  $(u_{2n})_{n \in \mathbb{N}}$ ,  $(u_{2n+1})_{n \in \mathbb{N}}$  et  $(u_{3n})_{n \in \mathbb{N}}$  convergent. Montrer que  $(u_n)_{n \in \mathbb{N}}$  converge.
13. **Application 3** : Soit  $x$  un nombre réel irrationnel et  $(p_n)_{n \in \mathbb{N}}$ ,  $(q_n)_{n \in \mathbb{N}}$  des suites d'entiers. On suppose que pour tout  $n \in \mathbb{N}$ ,  $q_n \in \mathbb{N}$ . Montrer que si  $\left(\frac{p_n}{q_n}\right)_{n \in \mathbb{N}}$  converge vers  $x$ , alors  $(q_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$ , et  $(p_n)_{n \in \mathbb{N}}$  diverge vers  $\infty$  si  $x > 0$ ,  $-\infty$  si  $x < 0$ .

1. Il existe plusieurs autres preuves classiques de ce théorème. Une preuve consiste à montrer qu'il existe une sous-suite monotone. Une autre utilise un procédé dichotomique.

2. Rappelons qu'on suppose depuis le début que la suite est bornée. Plus rien n'est vrai si on enlève cette hypothèse (pourquoi?).

3. Il est tentant de considérer la limite  $L$  de  $(a_n)_{n \in \mathbb{N}}$  et la limite  $L'$  de  $(b_n)_{n \in \mathbb{N}}$ , et d'en déduire des informations sur  $L$  et  $L'$ . Le problème est qu'on n'a pas démontré que la limite existe. En revanche, les valeurs d'adhérence existent toujours (pour des suites bornées). Ainsi, pour un problème de limite, on fait un détour vers un problème de valeur d'adhérence (notion plus faible), pour pouvoir éventuellement répondre au problème initiale (par exemple si on a démontré qu'il y a unicité de la valeur d'adhérence).

# Chapitre 8

## Nombres rationnels, nombres irrationnels

Dans ce cours, nous avons souvent mentionné l'ensemble  $\mathbb{Q} \subset \mathbb{R}$  des nombres rationnels, ainsi que l'ensemble  $\mathbb{R} - \mathbb{Q}$  des nombres irrationnels, c'est-à-dire les nombres réels qui ne sont pas rationnels. Ce chapitre est consacré à l'étude de ces ensembles.

### Remarque 8.1.

1. Contrairement à  $\mathbb{Z}$  et  $\mathbb{R}$ , nous ne présentons pas  $\mathbb{Q}$  comme un ensemble vérifiant certains axiomes. Nous présentons cet ensemble directement comme un sous-ensemble de  $\mathbb{R}$ .
2. Noter aussi que l'ensemble  $\mathbb{R}$  se construit traditionnellement à partir de l'ensemble des rationnels (et d'ailleurs l'ensemble des rationnels se construit à partir de l'ensemble des entiers, cf. problème 8.3.1). L'ensemble  $\mathbb{Q}$  devrait donc être défini indépendamment de  $\mathbb{R}$ , ce que nous ne ferons pas car les constructions sous-jacentes demandent beaucoup de détail techniques. Définissons directement  $\mathbb{Q}$  à partir de  $\mathbb{R}$ .

## 8.1 Nombres rationnels

**Définition 8.2.** Un nombre réel est dit *rationnel* s'il s'écrit  $\frac{a}{b}$  où  $a$  et  $b$  sont des entiers et  $b \neq 0$ . L'ensemble des nombres rationnels est noté  $\mathbb{Q}$ .

**Proposition 8.3.**  $\mathbb{Z} \subset \mathbb{Q}$ .

**Preuve.** Si  $n \in \mathbb{Z}$ , alors  $n = \frac{n}{1}$ . □

**Proposition 8.4.** L'ensemble  $\mathbb{Q}$  est fermé...

1. ...sous l'addition :  $\forall r, r' \in \mathbb{Q}, r + r' \in \mathbb{Q}$  ;
2. ...sous la multiplication :  $\forall r, r' \in \mathbb{Q}, rr' \in \mathbb{Q}$  ;
3. ...sous le passage à l'inverse additif :  $\forall r \in \mathbb{Q}, -r \in \mathbb{Q}$  ;
4. ...sous la soustraction :  $\forall r, r' \in \mathbb{Q}, r - r' \in \mathbb{Q}$  ;
5. ...**presque** sous le passage à l'inverse multiplicatif :  $\forall r \in \mathbb{Q}, r \neq 0 \Rightarrow r^{-1} \in \mathbb{Q}$ .

**Preuve.** Il suffit d'écrire les rationnels comme fractions d'entiers, d'appliquer les règles de calcul de fractions et d'utiliser ce qu'on sait sur l'addition et la multiplication entre entiers.

Donnons l'exemple de l'addition. Soient  $r, r' \in \mathbb{Q}$ , qu'on écrit  $r = \frac{a}{b}$  et  $r' = \frac{a'}{b'}$  avec  $a, a', b, b' \in \mathbb{Z}$ ,  $b \neq 0$ ,  $b' \neq 0$ . Alors on a

$$r + r' = \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}.$$

Le numérateur  $ab' + a'b$  est bien un entier, il en est de même pour le dénominateur  $bb'$ . Les entiers  $b$  et  $b'$  ne sont pas nuls, donc l'entier  $bb'$  non plus. Donc  $r + r'$  est bien un nombre rationnel.  $\square$

**Proposition 8.5.** *Tout nombre rationnel peut s'écrire sous la forme  $\frac{a}{b}$  où  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}$  sont premiers entre eux. Une telle écriture est unique pour les rationnels non nuls.*

**Preuve.** Soit  $\frac{a}{b}$  un nombre rationnel, avec  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Si  $b < 0$ , alors on écrit  $\frac{a}{b} = \frac{-a}{-b}$  et on a  $-b \in \mathbb{N}$ . Supposons donc sans perte de généralité que  $b \in \mathbb{N}$ . Si  $p$  désigne le pgcd de  $a$  et  $b$ , alors  $p \mid a$  et  $p \mid b$ . De plus,  $p \cdot \text{pgcd}(a/p, b/p) = \text{pgcd}(p(a/p), p(b/p)) = \text{pgcd}(a, b) = p$ , donc  $\text{pgcd}(a/p, b/p) = 1$ , autrement dit les entiers  $a/p$  et  $b/p$  sont premiers entre eux. En écrivant  $\frac{a}{b} = \frac{a/p}{b/p}$ , on s'est donc ramené au cas où le numérateur et le dénominateur sont premiers entre eux.<sup>a</sup>

Montrons l'unicité. Supposons donc  $\frac{a}{b} = \frac{c}{d}$  avec  $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{N}$ ,  $a$  et  $b$  premiers entre eux,  $c$  et  $d$  premiers entre eux,  $a$  et  $c$  non nuls. Alors on a  $ad = bc$ . Les entiers  $d$  et  $b$  sont premiers entre eux et  $d \mid bc$ , donc  $d \mid b$  d'après la proposition 5.50. Le même raisonnement permet d'obtenir  $b \mid d$ . Étant de même signe, on obtient ainsi  $b = d$  d'après la proposition 3.45. Par conséquent, on a également  $a = c$ .  $\square$

<sup>a</sup>. Attention aux raisonnements en « sans perte de généralité », par exemple lorsqu'on a supposé  $b \in \mathbb{N}$  quitte à mettre un signe au numérateur et au dénominateur. Il faut s'assurer que cette propriété a toujours lieu lors des transformations suivantes. Ici, tout va bien, car le nouveau dénominateur  $b/p$  est encore dans  $\mathbb{N}$ .

**Exercice 8.6.** Montrer que  $\mathbb{Q}$  et  $\mathbb{N}$  sont en bijection.

Le prochain résultat exprime le fait que  $\mathbb{Q}$  est « partout » dans  $\mathbb{R}$ , on dira plutôt que  $\mathbb{Q}$  est *dense* dans  $\mathbb{R}$ . La densité admet une définition générale dans le domaine de la topologie que nous ne donnerons pas, contentons-nous seulement de cet énoncé simple.

Remarquons que, bien que  $\mathbb{Q}$  soit « partout » dans  $\mathbb{R}$ , c'est quand même un ensemble plus petit que  $\mathbb{R}$ . En effet,  $\mathbb{Q}$  est en bijection avec  $\mathbb{N}$  mais  $\mathbb{N}$  ne se surjecte pas dans  $\mathbb{R}$  (cf. problème 2.5.3 du chapitre 2).

**Théorème 8.7** ( $\mathbb{Q}$  est dense dans  $\mathbb{R}$ ). *Pour tout  $x, y \in \mathbb{R}$ , avec  $x < y$ , il existe  $r \in \mathbb{Q}$  tel que  $x < r < y$ .*

**Preuve.** D'après le corollaire 6.44, il existe  $b \in \mathbb{N}$  tel que  $\frac{1}{b} < y - x$ . L'ensemble  $\{a \in \mathbb{Z} \mid y \leq \frac{a}{b}\}$  est non vide (sinon  $\mathbb{Z}$  est majoré par  $y$ ), minoré (par  $y$ ) et est un sous-ensemble de  $\mathbb{Z}$ . Par le principe du bon ordre, il admet un plus petit élément noté

$M$ . Montrons que  $x < \frac{M-1}{b} < y$ . Par minimalité de  $M$ , on a  $\frac{M-1}{b} < y$ . Si par l'absurde, on avait  $\frac{M-1}{b} \leq x$ , alors on obtiendrait

$$\frac{1}{b} = \frac{M}{b} - \frac{M-1}{b} \geq y - x.$$

C'est absurde. Donc on a bien  $x < \frac{M-1}{b} < y$ .  $\square$

Étant donné  $a \in \mathbb{R}_{\geq 0}$ , on avait défini dans la section 6.7 du chapitre 6 :

$$\sqrt{a} = \sup \{x \in \mathbb{R}_{\geq 0} \mid x^2 < a\}.$$

L'énoncé suivant, conséquence de la densité de  $\mathbb{Q}$  dans  $\mathbb{R}$ , permet de restreindre à  $\mathbb{Q}$  l'ensemble dont on considère le supremum. On note  $\mathbb{Q}_{\geq 0} = \{r \in \mathbb{Q} \mid r \geq 0\}$ .

**Corollaire 8.8.** *Soit  $a \in \mathbb{R}_{\geq 0}$ . Alors*

$$\sqrt{a} = \sup \{x \in \mathbb{R}_{\geq 0} \mid x^2 < a\} = \sup \{x \in \mathbb{Q}_{\geq 0} \mid x^2 < a\},$$

*où on considère le supremum dans l'ensemble ambiant  $\mathbb{R}$ .*

**Preuve.** Notons  $r = \sup \{x \in \mathbb{Q}_{\geq 0} \mid x^2 < a\}$ .

- Montrons  $\sqrt{a} \geq r$ . Le réel  $\sqrt{a}$  majore l'ensemble  $\{x \in \mathbb{R}_{\geq 0} \mid x^2 < a\}$ , donc *a fortiori* son sous-ensemble  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < a\}$ . Donc  $\sqrt{a} \geq r$ .
- Montrons  $\sqrt{a} \leq r$ . Pour cela, montrons que  $r$  majore l'ensemble  $\{x \in \mathbb{R}_{\geq 0} \mid x^2 < a\}$ . Soit  $x \geq 0$  tel que  $x^2 < a$ . Comme le carré de  $\sqrt{a}$  vaut exactement  $a$ , on a  $x \neq \sqrt{a}$ . Par densité de  $\mathbb{Q}$  dans  $\mathbb{R}$ , il existe un rationnel  $q$  tel que  $x < q < \sqrt{a}$ . En élevant au carré, cela donne  $q^2 < \sqrt{a}^2 = a$ , donc  $q$  appartient à  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < a\}$ . Ainsi  $r \geq q$  par définition de  $r$ , donc  $r > x$ . Donc  $r$  majore l'ensemble  $\{x \in \mathbb{R}_{\geq 0} \mid x^2 < a\}$ . Ainsi  $\sqrt{a} \leq r$ .  $\square$

On peut donc justifier les affirmations de la remarque 6.36.

- Si  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < 2\}$  avait un supremum dans  $\mathbb{Q}$ , noté  $q$ , alors ce serait également le supremum dans  $\mathbb{R}$ , c'est-à-dire  $q = \sqrt{2}$ . En effet,  $q$  est en particulier un réel qui majore l'ensemble  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < 2\}$ , donc on a  $\sqrt{2} \leq q$ . Si par l'absurde, on a  $\sqrt{2} < q$ , alors la densité de  $\mathbb{Q}$  fournit un rationnel  $q'$  tel que  $\sqrt{2} < q' < q$ , donc  $q'$  est un majorant de  $\{x \in \mathbb{R}_{\geq 0} \mid x^2 < 2\}$  donc de  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < 2\}$ , qui est plus petit que  $q$ , cela contredit la définition de  $q$  comme supremum dans  $\mathbb{Q}$ . Donc  $q = \sqrt{2}$ .
- Mais  $q$  est rationnel (c'est un supremum dans  $\mathbb{Q}$ ) et  $\sqrt{2}$  n'est pas rationnel (exemple 1.8 du chapitre 1). C'est absurde.

L'ensemble  $\{x \in \mathbb{Q}_{\geq 0} \mid x^2 < 2\}$  n'admet donc pas de supremum dans  $\mathbb{Q}$ , mais en admet un dans  $\mathbb{R}$ . Ainsi, si on reste dans  $\mathbb{Q}$ , il manque des nombres importants comme  $\sqrt{2}$ .

## 8.2 Nombres irrationnels

**Définition 8.9.** Un nombre réel est dit *irrationnel* s'il n'est pas rationnel.

Il n'y a pas de notation usuelle pour l'ensemble des irrationnels, on notera simplement  $\mathbb{R} - \mathbb{Q}$ .

**Remarque 8.10. Attention !** Contrairement à  $\mathbb{Q}$ , l'ensemble  $\mathbb{R} - \mathbb{Q}$  n'est ni stable par addition, ni stable par multiplication (considérer par exemple  $\sqrt{2} + (-\sqrt{2})$  et  $\sqrt{2} \cdot \sqrt{2}$ ). En revanche, l'ensemble est stable par passage à l'inverse additif. De plus, pour tout irrationnel  $x$  non nul,  $x^{-1}$  est également irrationnel.

Comme nous l'avions montré dans l'exemple 1.8, le réel  $\sqrt{2}$  est irrationnel. Nous pouvons en fait énoncer un phénomène plus général.

**Proposition 8.11.** Soit  $a, b \in \mathbb{N}$  premiers entre eux. Alors  $\sqrt{\frac{a}{b}}$  est rationnel si et seulement si  $a$  et  $b$  sont des carrés<sup>a</sup>.

a. Un entier  $n$  est un carré s'il existe un autre entier  $k$  tel que  $n = k^2$ .

C'est évidemment faux pour  $a = 0$ . Le réel  $\sqrt{\frac{0}{b}}$  est toujours rationnel même pour un entier  $b$  qui n'est pas un carré.

**Preuve.** S'il existe des entiers  $A$  et  $B$  tels que  $a = A^2$  et  $b = B^2$ , alors  $B \neq 0$  et

$$\sqrt{\frac{a}{b}} = \sqrt{\frac{A^2}{B^2}} = \frac{\sqrt{A^2}}{\sqrt{B^2}} = \frac{|A|}{|B|}.$$

Donc  $\frac{a}{b}$  est rationnel.

Supposons que  $\sqrt{\frac{a}{b}}$  est rationnel. On dispose donc d'entiers  $A$  et  $B$  tels que  $B \neq 0$ ,  $A$  et  $B$  sont premiers entre eux, et  $\sqrt{\frac{a}{b}} = \frac{A}{B}$ . En élevant au carré, on obtient  $\frac{a}{b} = \frac{A^2}{B^2}$ . Or  $A^2$  et  $B^2$  sont premiers entre eux. En effet, si  $p$  est nombre premier divisant  $A^2$  et  $B^2$ , alors le lemme d'Euclide (remarquer que  $A^2 = A \cdot A$  et  $B^2 = B \cdot B$ ) implique que  $p$  divise  $A$  et  $B$ , ce qui est exclu. Ainsi par unicité (proposition 8.5), on a  $a = A^2$  et  $b = B^2$ .  $\square$

**Exemple 8.12.** Montrons que  $\sqrt{2} + \sqrt{3}$  est irrationnel.

Par l'absurde, supposons que  $\sqrt{2} + \sqrt{3}$  est rationnel. Alors son carré est également rationnel. Or

$$(\sqrt{2} + \sqrt{3})^2 = \sqrt{2}^2 + 2\sqrt{2}\sqrt{3} + \sqrt{3}^2 = 5 + 2\sqrt{6}.$$

Ainsi  $\sqrt{6} = \frac{(\sqrt{2} + \sqrt{3})^2 - 5}{2}$ , donc par stabilité de  $\mathbb{Q}$  pour les opérations usuelles,  $\sqrt{6}$  est rationnel. Cela contredit la proposition précédente, vu que l'entier 6 n'est pas un carré.

Finissons avec la densité de  $\mathbb{R} - \mathbb{Q}$  dans  $\mathbb{R}$ .

**Théorème 8.13** ( $\mathbb{R} - \mathbb{Q}$  est dense dans  $\mathbb{R}$ ). Pour tout  $x, y \in \mathbb{R}$  tels que  $x < y$ , il existe  $z \in \mathbb{R} - \mathbb{Q}$  tel que  $x < z < y$ .

**Preuve.** Soient  $x, y \in \mathbb{R}$  tels que  $x < y$ . D'après la théorème 8.7, il existe un nombre rationnel  $r$  tel que  $\frac{x}{\sqrt{2}} < r < \frac{y}{\sqrt{2}}$ . Ainsi, on a  $x < r\sqrt{2} < y$ . Le réel  $z = r\sqrt{2}$  est bien irrationnel, sinon la stabilité de  $\mathbb{Q}$  pour les opérations usuelles impliquerait que  $\sqrt{2} = z/r$  est rationnel. D'où le résultat.  $\square$

**Exercice 8.14.** Soit  $\sim$  la relation sur  $\mathbb{R}$  définie par :

$$\forall x, y \in \mathbb{R}, x \sim y \iff y - x \in \mathbb{Q}.$$

1. Montrer que  $\sim$  est une relation d'équivalence de  $\mathbb{R}$ .
2. Soit  $x \in \mathbb{R}$ , montrer que sa classe d'équivalence  $[x]$  vaut  $\{x + r \mid r \in \mathbb{Q}\}$  (cette ensemble est plus communément noté  $x + \mathbb{Q}$ ). Que vaut la classe d'un nombre rationnel ?
3. Soit  $x \in \mathbb{R}$ . Montrer que  $[x]$  et  $\mathbb{Q}$  sont en bijection.
4. Soit  $x \in \mathbb{R}$ . Montrer que  $[x]$  est dense dans  $\mathbb{R}$  : pour tout  $a, b \in \mathbb{R}$  tels que  $a < b$ , il existe  $y \in [x]$  tel que  $a < y < b$ .

## 8.3 Problèmes

### 8.3.1 Problème 1

Ce problème aborde la construction de  $\mathbb{Q}$  à partir de  $\mathbb{Z}$ . On ne suppose pas les nombres réels construits, on ne verra donc pas  $\mathbb{Q}$  comme un sous-ensemble de  $\mathbb{R}$ .

Sur  $\mathbb{Z} \times \mathbb{N}$ , considérons la relation  $\sim$  définie par : pour tout  $(a, b), (a', b') \in \mathbb{Z} \times \mathbb{N}$ ,  $(a, b) \sim (a', b') \iff ab' = a'b$ .

1. Montrer que  $\sim$  est une relation d'équivalence.
2. Soient  $(a, b) \in \mathbb{Z} \times \mathbb{N}$ . Montrer qu'il existe  $(a', b') \in \mathbb{Z} \times \mathbb{N}$  tel que  $\text{pgcd}(a', b') = 1$  et  $(a, b) \sim (a', b')$ .
3. Soit  $(a, b) \in \mathbb{Z} \times \mathbb{N}$  tel que  $\text{pgcd}(a, b) = 1$ . Décrire la classe d'équivalence de  $(a, b)$ .

On définit des opérations  $+$  et  $\cdot$  sur  $\mathbb{Z} \times \mathbb{N} / \sim$  de la manière suivante : pour tout  $(a, b), (a', b') \in \mathbb{Z} \times \mathbb{N}$ ,

$$[(a, b)] + [(a', b')] = [(ab' + a'b, bb')],$$

$$[(a, b)] \cdot [(a', b')] = [(aa', bb')].$$

4. Montrer que ces opérations sont bien définies.
5. Montrer qu'il existe un unique neutre additif, qu'on notera  $0'$ , et que tout élément  $x$  de  $\mathbb{Z} \times \mathbb{N} / \sim$  admet un inverse additif, noté  $-x$ .
6. Montrer qu'il existe un unique neutre multiplicatif, qu'on notera  $1'$ , et que tout élément  $x$  de  $\mathbb{Z} \times \mathbb{N} / \sim$ , différent de  $0'$ , admet un inverse multiplicatif, noté  $x^{-1}$ .

On pourra également, si on veut, vérifier que ces opérations sont également associatives et commutatives, que la distributivité est vérifiée, etc., comme dans les axiomes de  $\mathbb{Z}$ .

On définit sur  $\mathbb{Z} \times \mathbb{N} / \sim$  une relation  $\leq$  définie par : pour tout  $(a, b), (a', b') \in \mathbb{Z} \times \mathbb{N}$ ,  $[(a, b)] \leq [(a', b')] \iff ab' \leq a'b$ .

7. Montrer que  $\leq$  est bien définie.
8. Montrer que  $\leq$  est une relation d'ordre totale sur  $\mathbb{Z} \times \mathbb{N} / \sim$ .

9. Montrer que pour tout  $(a, b), (a', b') \in \mathbb{Z} \times \mathbb{N}$ , si  $(a, b) \sim (a', b')$ , alors  $a$  et  $a'$  ont le même signe.

On dit qu'un élément de  $\mathbb{Z} \times \mathbb{N} / \sim$  est positif s'il admet un représentant  $(a, b)$  avec  $a > 0$ . On vient en fait de montrer qu'un élément est positif si tous ses représentants sont de la forme  $(a, b)$  avec  $a > 0$ .

10. Montrer que l'ensemble des éléments positifs de  $\mathbb{Z} \times \mathbb{N} / \sim$  vérifient les mêmes conditions que dans l'axiome B.1, à savoir la fermeture sous addition et multiplication, le fait que  $0'$  n'est pas positif, ainsi que le fait que pour tout  $x \in \mathbb{Z} \times \mathbb{N} / \sim$ ,  $x$  est nul ou positif, ou  $-x$  est positif.

11. Montrer que pour tout  $x, y \in \mathbb{Z} \times \mathbb{N} / \sim$ ,  $x \leq y \iff y - x$  est un élément positif

On note alors  $\mathbb{Q} = \mathbb{Z} \times \mathbb{N} / \sim$  et  $\mathbb{Q}_{>0}$  l'ensemble des éléments positifs. On écrira les classes  $\frac{a}{b}$  au lieu de  $[(a, b)]$ .<sup>1</sup>

12. Montrer que  $f: n \in \mathbb{Z} \mapsto \frac{n}{1} \in \mathbb{Q}$  est injective et vérifie  $f(0) = 0$ ,  $f(1) = 1'$  et  $f(\mathbb{N}) \subset \mathbb{Q}_{>0}$ .
13. Montrer que  $f$  est compatible avec les opérations  $+$  et  $\cdot$ , et avec  $\leq$ , comme dans la section 6.4 du chapitre 6.

On peut donc, après identification par  $f$ , considérer pas abus que  $\mathbb{Z}$  est un sous-ensemble de  $\mathbb{Q}$ . Ceci n'est pas vrai à l'origine, les éléments de  $\mathbb{Q}$  étant des classes pour une relation d'équivalence sur  $\mathbb{Z} \times \mathbb{N}$ , et non des entiers.

### 8.3.2 Problème 2

On veut étendre le résultat du problème 3.5.1 du chapitre 3.

On cherche à montrer que les fonctions  $f: \mathbb{Q} \rightarrow \mathbb{R}$  vérifiant  $f(x + y) = f(x) + f(y)$  pour tout  $x, y \in \mathbb{Q}$ , sont exactement les  $x \in \mathbb{Q} \mapsto ax \in \mathbb{R}$  pour  $a \in \mathbb{R}$ .

1. Soit  $a \in \mathbb{R}$ . Montrer que la fonction  $f: x \in \mathbb{Q} \mapsto ax \in \mathbb{R}$  satisfait  $f(x + y) = f(x) + f(y)$  pour tout  $x, y \in \mathbb{Q}$ .

Soit  $f: \mathbb{Q} \rightarrow \mathbb{R}$  une fonction vérifiant  $f(x + y) = f(x) + f(y)$  pour tout  $x, y \in \mathbb{Q}$ . Par la même méthode que dans le problème 3.5.1 du chapitre 3, on sait déjà qu'il existe  $a \in \mathbb{R}$  tel que pour tout  $n \in \mathbb{Z}$ ,  $f(n) = na$ .

2. Montrer que pour tout  $x \in \mathbb{Q}$ , pour tout  $k \in \mathbb{N}$ , on a  $f(kx) = kf(x)$ .
3. Montrer que pour tout  $n \in \mathbb{Z}$ , pour tout  $k \in \mathbb{N}$ , on a  $f(\frac{n}{k}) = \frac{1}{k}f(n)$ .
4. Conclure.

### 8.3.3 Problème 3

On considère l'ensemble  $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ , que l'on notera  $\mathbb{Q}[\sqrt{2}]$ .

1. Montrer que la proposition 8.4 est encore vraie si on remplace  $\mathbb{Q}$  par  $\mathbb{Q}[\sqrt{2}]$ .
2. Montrer que pour tout  $a, a', b, b' \in \mathbb{Q}$ , on a  $a + b\sqrt{2} = a' + b'\sqrt{2}$  si et seulement si  $a = a'$  et  $b = b'$ .
3. Montrer que l'inclusion  $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$  n'est pas une égalité.
4. Montrer que l'inclusion  $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$  n'est pas une égalité. On cherchera un nombre réel qui n'est pas dans  $\mathbb{Q}[\sqrt{2}]$ .

Pour répondre à la dernière question, on peut aussi montrer que  $\mathbb{Q}[\sqrt{2}]$  est en bijection avec  $\mathbb{N}$  en utilisant les exercices de ces notes de cours, ce qui permet de conclure car  $\mathbb{R}$  n'est pas en bijection avec  $\mathbb{N}$  (problème 2.5.3 du chapitre 2).

<sup>1</sup> Pour se convaincre qu'on a bien défini l'ensemble des rationnels comme on se l'imaginait, réécrire les définitions de  $+$  et  $\cdot$  avec l'écriture fractionnaire, revoir les questions d'après avec ce point de vue.