# Cours « Fondements mathématiques »

Le document suivant contient le matériel relevant du cours de l'unité *UE 111 : Fondements Mathématiques (Portail M-I et MP, Nancy)* (année 2021/22 ; version actuelle datant du 04 / 09 / 2021), ainsi que quelques remarques supplémentaires et des liens internet (en gris dans le texte). La version mise à jour de ce document, ainsi que les TD et d'autres documents, seront toujours accessible via Arche, https://arche.univ-lorraine.fr/course/view.php?id=49068. La progression peut différer d'un groupe d'enseignement EI à l'autre, et des commentaires spécifiques aux groupes peuvent également être disponibles sur Arche.

## Fondements mathématiques – Introduction au cours

Par « fondements mathématiques », on peut entendre

(1) d'un point de vue *historique*, les origines des maths dans l'histoire de l'humanité ;

(2) d'un point de vue *philosophique*, la description de la place et du rôle des mathématiques dans l'ensemble du savoir humain, et en particulier de comprendre ses relations spécifiques avec les *sciences naturelles* ;

(3) d'un point de vue *conceptuel, intérieur aux mathématiques*, décrire les structures et concepts les plus basiques et fondamentaux des mathématiques.

C'est le dernier aspect qui fera l'objet de ce cours. Mais il n'est pas isolé des deux autres. Commençons par en dire quelques mots.

### Fondements de maths – repères historiques.

Il faut remonter très loin dans l'histoire de l'humanité pour trouver les origines des mathématiques. Mais, non sans raison, on cite souvent les *mathématiques grecques anciennes* comme étant la véritable origine des mathématiques

que nous connaissons : surtout, aux "Eléments" d'Euclide on doit la *méthode rigoureuse, "axiomatique"* qu'on emploie encore aujourd'hui :

- formuler clairement les propriétés et hypothèses fondamentales que nous acceptons comme point de départ : les *axiomes*, et en déduire tout le reste par un *raisonnement logique* : les *preuves*.

Autrement dit, nous mettons toutes les cartes sur la table au début du jeu ; ensuite, tout se déroule selon des règles strictes et logiques. Euclide a appliqué cette méthode surtout dans deux domaines :

1. la *géométrie*,
2. les *nombres* (l'arithmétique).

Cependant, après l' « explosion des mathématiques » qui débuta au XVIIe siècle avec l'invention du *calcul infinitésimal*, par Newton et Leibniz, les mathématiciens se rendaient compte du fait que les fondements posés par Euclide étaient insuffisants : ces « fondements » ne permettaient pas de dire ce qu'est un « nombre réel », ou de développer une théorie rigoureuse du calcul « infinitésimal », ni même d'éclaircir vraiment les fondements de la géométrie dite « euclidienne » !

Le XIXe et le XXe siècle donnent la « solution » à ces problèmes et mènent ainsi à une nouvelle ouverture, mais aussi à de nouveaux problèmes :

1. *Georg Cantor* crée la *Théorie des ensembles* qui donne un fondement rigoureux de toutes les mathématiques,
2. *Augustin Cauchy* et *Richard Dedekind* proposent des définitions rigoureuses des nombres réels,
3. *David Hilbert* analyse et repose en 1899 dans son texte *Fondements de la géométrie* les axiomes de la géométrie euclidienne,
4. le groupe Bourbaki essaie au XXe siècle de rassembler en plusieurs tomes les Éléments de mathématique, comme sorte de réponse moderne à Euclide,
5. la *Théorie des catégories* s'apprête au XXe siècle à remplacer la théorie des ensembles comme fondement universel des maths...

De tout ces développements, pour les études de maths en Licence, sont les plus importants : l'*analyse*, comportant comme outil de base les *nombres réels*, et l'*algèbre linéaire*, qui est la version moderne de constructions de modèles de la géométrie, les *espaces vectoriels*. Les deux théories utilisent le langage de la théorie des ensembles.

### Fondements de maths – point de vue philosophique.

Les mathématiques se distinguent profondément des sciences naturelles par le fait que ses « objets » *ne se situent ni dans l'espace, ni dans le temps* : un nombre, ou un théorème sont « éternels », ils existent « toujours et partout ». Pourtant, les mathématiques s'appliquent dans la plupart des sciences naturelles, surtout en physique : dans son célèbre article *The unreasonable effectiveness of mathematics in the natural sciences* (lien) le physicien Eugene Wigner concède que c'est un grand mystère. Nous n'en dirons pas plus ici.

Il existe aussi quelques domaines scientifiques et philosophiques qui partagent ces traits caractéristiques avec les maths :

1. La *logique*, i.e., l'étude des règles formelles que doit respecter toute argumentation correcte. Elle s'applique aussi bien à l'extérieur des mathématiques –dans notre discours sur le « monde réel »–, qu'à l'intérieur des mathématiques, comme une sorte de « règlement interne de la maison des maths » ; on parle aussi de logique mathématique. Ce dernier aspect nous occupera dans ce cours. Soulignons, cependant, que le rôle de la logique « dans le monde réel » (par exemple, dans les sciences expérimentales) peut être très différent du role de la logique en maths.

2. L'*informatique* – le concept d'information est difficile à cerner ; comme les objets mathématiques, l'information n'est pas vraiment localisée dans l'espace et le temps. L'informatique théorique est parfois considérée comme un sous-domaine des maths. Souvent, on assimile le « digital » avec les « maths discrètes », opposé au « continu », « analogue ».

### Les concepts fondateurs mathématiques, et l'infini.

Comme dit ci-dessus, au début du XXe siècle, la théorie des ensembles a accédé au rôle de langage commun des fondements des maths. Une grande partie de ce cours sera consacrée à « apprendre ce langage ». Dans ce contexte, une distinction est d'importance capitale : il faut distinguer le *fini* de l'*infini*. Au niveau des *ensembles finis*, on n'a pas besoin d'une théorie très élaborée : une « théorie naïve » convient bien, voire mieux. Par contre, *la théorie des ensembles prend sa vraie forme et vraie puissance seulement quand elle parle des ensembles infinis*. Ces ensembles infinis posent le problème suivant : on ne peut pas les écrire, en un temps fini et sur un bout de papier (ou ordinateur) fini, sous forme d'une « liste complète » ou « fichier complet » ! Or, les « ensembles de nombres usuels »,

1. les nombres naturels (entiers naturels) $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$,
2. les entiers relatifs $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
3. les nombres rationnels $\mathbb{Q}$ (fractions $r = \frac{m}{n}$ avec $m, n$ des entiers relatifs et $n \neq 0$),
4. les nombres réels $\mathbb{R}$ (« tous les nombres de la droite réelle »),
5. les nombres complexes $\mathbb{C}$ (« tous les nombres du plan d'Argand »)

sont bien infinis, et là, une théorie « naïve » n'est plus possible - il faut préciser : que signifie le symbole « . . . »– par exemple, peut-on écrire $\mathbb{R} = \{0, e, \pi, \sqrt{2}, \ldots\}$ ? Comment peut-on savoir que de tels ensembles « existent vraiment » si l'on ne peut pas les écrire sous forme d'une liste explicite ? Le mathématicien Hermann Weyl a caractérisé les maths ainsi : *les mathématiques sont la science de l'infini* ; elles commencent vraiment dès qu'on fait face au problème de l'infini. – Voici une piste de lecture recommandée pour le lecteur qui souhaite poursuivre ces réflexions : *Le commencement de l'infini* par D. Deutsch.

# Table des matières

**Table des matières** **4**

**1 Ensembles et parties** **8**
1.1 Ensembles. . . . . 8
1.2 Parties d'un ensemble . . . . . 9
1.3 Formules remarquables . . . . . 12

**2 Opérations sur les ensembles** **14**
2.1 Opérations sur les parties d'un ensemble $M$ . . . . . 14
2.2 Produit cartésien . . . . . 17
2.3 Somme disjointe . . . . . 18

**3 Applications, fonctions** **20**
3.1 Définitions fondamentales . . . . . 20
3.2 Composée d'applications . . . . . 23
3.3 Permutations . . . . . 24
3.4 Image directe et image réciproque d'une partie . . . . . 25

**4 Relations** **28**
4.1 Relations et graphes . . . . . 28
4.2 Relations d'ordre . . . . . 29
4.3 Relations d'équivalence . . . . . 30

**5 Les nombres naturels $\mathbb{N}$** **34**
5.1 Les axiomes de Peano, et le principe de récurrence . . . . . 34
5.2 Addition et multiplication dans $\mathbb{N}$ . . . . . 36
5.3 La relation d'ordre sur $\mathbb{N}$ . . . . . 38

**6 Nombres** **39**
6.1 Construction de $\mathbb{Z}$ : idée . . . . . 39
6.2 Construction de $\mathbb{Q}$ : idée . . . . . 40
6.3 Calcul dans $\mathbb{Z}$ et $\mathbb{Q}$ . . . . . 41

**7 Théorie des ensembles** **43**
7.1 Équipotence ; ensembles dénombrables . . . . . 43
7.2 L'argument diagonal de Cantor . . . . . 44

7.3 Axiomes de la théorie des ensembles . . . . . 45

**8 Logique et maths** **46**
8.1 Propositions et valeurs de vérité . . . . . 46
8.2 Calcul des propositions . . . . . 46
8.3 Calcul des prédicats . . . . . 49
8.4 Théorèmes et preuves . . . . . 50

**A Sur la construction de $\mathbb{Z}$** **51**
A.1 Construction de l'ensemble $\mathbb{Z}$ . . . . . 51
A.2 L'addition dans $\mathbb{Z}$ . . . . . 51
A.3 Relation d'ordre sur $\mathbb{Z}$ . . . . . 52
A.4 Produit dans $\mathbb{Z}$ . . . . . 52

**B Sur la construction de $\mathbb{Q}$** **54**
B.1 Construction de l'ensemble $\mathbb{Q}$ . . . . . 54

# Première partie : les ensembles finis

Dans cette partie du cours, nous suivons une « approche naïve » des mathématiques : la notion d'*ensemble fini* fait abstraction de notre expérience de regrouper un nombre fini d'objets ; de les « mettre dans un sac » ; et de pouvoir comparer la « taille » de ces sacs selon le *nombre* d'unités (les *éléments*) qu'ils contiennent : un, deux, trois,... (ou aucun : le *sac vide*). En somme, nous suivons la démarche par laquelle nous commençons à compter et à raisonner sur des nombres dans l'enseignement primaire et secondaire. Nous ne cherchons donc pas (encore) à donner une définition exacte d'un *nombre fini* $n \in \mathbb{N}$, et encore moins de *l'ensemble de tous les nombres finis (naturels)* $\mathbb{N}$ (qui constitue un ensemble infini).

Néanmoins, dans ce cadre, on peut déjà démontrer quelques « théorèmes » : des énoncés mathématiques « non triviaux », qui demandent une *preuve*. Pour l'instant, par *preuve* nous entendons « justification » ou « explication », et il suffira de la rédiger en lange française usuelle, en respectant bien les règles d'une bonne rédaction en français. Cela veut dire, entre autres, qu'il faudra écrire des phrases grammaticalement correctes, avec une ponctuation correcte, et surtout, *qui ont un sens* : si vous utilisez des symboles, la phrase doit être compréhensible pour quelqu'un à qui vous la lisez à voix haute, mais qui ne voit pas la phrase écrite. Par ailleurs, ces règles de bon sens garderont leur pertinence pour toute votre carrière en maths, pendant et après les études !

Lié à cette remarque, vous pouvez déjà jeter un coup d'œil sur le dernier chapitre du cours, qui porte sur la *logique mathématique*, sorte de « grammaire » du discours mathématique, et dont la connaissance est indispensable pour toute rédaction plus avancée en mathématiques. Cependant, les questions de fondement de la logique sont tout aussi délicats que celles des ensembles infinis, car le *domaine de discours* de la logique est encore plus difficile à délimiter que celui de la théorie des ensembles.

*Chapitre* 1

# Ensembles et parties

## 1.1 Ensembles.

Voici comment Georg Cantor a défini sa notion d' « ensemble » :

**Définition 1.1.1.** Par *ensemble*, nous entendons toute collection d'objets de notre intuition ou de notre pensée, définis et distincts, ces objets étant appelés les *éléments* de l'ensemble.

Notations :

$\boxed{m \in M}$ signifie : $m$ *est un élément de l'ensemble* $M$ ($m$ appartient à $M$),

$\boxed{m \notin M}$ signifie : $m$ *n'est pas un élément de* $M$ (n'appartient pas à $M$).

**Définition 1.1.2.** Un *ensemble fini* est donné par une *liste finie* de ses éléments, écrite entre accolades :

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Si les éléments $a_1, \ldots, a_n$ sont *deux à deux distincts* (ce qui veut dire : $a_i \neq a_j$ lorsque $i \neq j$, pour $i, j = 1, \ldots, n$), alors on dit que $A$ est un *ensemble de cardinal fini* $n$, et on écrit

$$n = \mathrm{card}(A) = |A|.$$

**Exemple 1.1.3.** $M = \{2, 4, 6\}$ est un ensemble de cardinal 3, et 2 appartient à $M$, mais 1 n'appartient pas à $M$ : $1 \notin M$, et $2 \in M$.

**Notations et explications.** Ainsi un ensemble fini est donné par la « liste » de ses éléments. Deux ensembles sont les mêmes s'ils ont les mêmes éléments. L'ordre dans lequel on présente cette liste ne joue aucun rôle : par exemple, si $M = \{a_1, a_2, \ldots, a_n\}$, on aurait pu écrire aussi $M = \{a_n, a_{n-1}, \ldots, a_1\}$. Aussi est-il possible d'écrire un élément plusieurs fois sans changer l'ensemble : ainsi $\{a, a\} = \{a\}$, ou $\{a, b, a\} = \{a, b\} = \{b, a, a, a\}$. Quand on écrit $M = \{a, b\}$, il faut bien préciser si les lettres $a$ et $b$ désignent le même élément ($a = b$; cardinal 1), ou non ($a \neq b$; cardinal 2). Attention à la typographie et à l'écriture : si un élément est noté $a$, il faut utiliser dans toute la suite le même symbole (reconnaissable), et non le changer en (par exemple) $A, \alpha, \mathrm{a}, \mathbf{a}, \mathtt{a}, \mathfrak{a}$,...

**Exemple 1.1.4.** L'ensemble « standard » de cardinal $n$ sera noté

$$[[1, \dots, n]] := \{1, 2, \dots, n\}$$

(ou parfois juste $[[1, n]]$). Un ensemble de cardinal $2n + 1$ est, par exemple,

$$[[-n, n]] = \{-n, -n + 1, \dots, 0, \dots, n\}.$$

**Définition 1.1.5.** L'ensemble vide est l'ensemble (de cardinal $0$) qui ne contient aucun élément. Il est noté

$$\emptyset = \{\,\}.$$

## 1.2 Parties d'un ensemble

**Définition 1.2.1.** Soit $M$ un ensemble. Une *partie de $M$*, ou *sous-ensemble de $M$*, est un ensemble $A$ tel que tout élément de $A$ est un élément de $M$. On écrit alors $A \subset M$.

**Exemple 1.2.2.** Si $m \in M$, alors $\{m\} \subset M$ est une partie contenant un unique élément (on dit, un *singleton*).

**Description d'une partie.** Si $M$ est fini, il y a deux façons de décrire ses parties :

1. par une *liste explicite*. Par exemple, soit $M = \{1, 2, 3, 4, 5, 6, 7\}$, alors $A = \{2, 4, 6\}$ est une partie de $M$ ;
2. par une *propriété* : par exemple, l'ensemble $A$ ci-dessus est *l'ensemble des éléments de $M$ qui sont pairs*. On écrit :

$$A = \{x \in M \mid x \text{ est pair }\}.$$

De manière générale, soit $P(x)$ une certaine « propriété » que $x$ peut avoir ($P(x)$ vrai) ou non ($P(x)$ faux). La partie $B$ des éléments de $M$ vérifiant la propriété $P$ (i.e., pour lesquels $P(x)$ est vraie) s'écrit

$$\boxed{B = \{x \in M \mid P(x)\}},$$

et celle des éléments de $M$ pour lesquels $P(x)$ est fausse s'écrit

$$\boxed{C = \{x \in M \mid \neg P(x)\}}.$$

Le symbôle $\neg$ designe la *négation logique* (contraire logique). Dans ce contexte, on dit aussi que $P(x)$ est un prédicat (une proposition logique dépendant d'une *variable* $x$), et on utilise souvent les symboles

$\forall$ pour abréger : *quel que soit* ou *pour tout*,

$\exists$ pour abréger : *il existe*.

Par exemple, la partie $A$ du point 1. s'écrit aussi

$$A = \{k \in M \mid \quad \exists \ell \in \{1, 2, 3\} : k = 2\ell\}$$

Voir le dernier chapitre du cours pour les règles de bonne utilisation de ces *quantificateurs* (« calcul des prédicats »).

**Définition 1.2.3.** Pour une partie $A$ de $M$, on note $A^c$ ou $M \setminus A$ son *complémentaire*, l'ensemble des éléments de $M$ qui ne sont pas dans $A$ :

$$A^c = \{x \in M \mid x \notin A\}.$$

**Remarque 1.2.4.** D'après les règles de la logique, des deux cas l'un (et seulement un) : soit, $x \in A$, soit $x \in A^c$. Il s'ensuit que

$$\mathrm{card}(A) + \mathrm{card}(A^c) = \mathrm{card}(M).$$

Une propriété liée, qui semble évidente, est qu'aucune partie ne peut avoir plus d'éléments que l'ensemble $M$ qui la contient : si $A \subset M$, alors

$$\mathrm{card}(A) \leq \mathrm{card}(M).$$

**Remarque 1.2.5.** Deux ensembles sont *égaux* (notation : $A = B$), si, et seulement si, on a la *double inclusion* $A \subset B$ et $B \subset A$. Une inclusion $A \subset B$ est dite *stricte* s'il existe un élément $b \in B$ qui *n'est pas* un élément de $A$.

**Remarque 1.2.6.** L'*ensemble vide* fait partie de n'importe quel autre ensemble : $\emptyset \subset M$. Aussi, tout ensemble $A$ est une partie de lui-même : $A \subset A$.

**Exemple 1.2.7.** L'ensemble $M = \{1\}$ a deux parties : $\emptyset$ et $M$.

**Exemple 1.2.8.** Voici une liste de *toutes les parties* de l'ensemble $M = \{1, 2\}$ : il y en a $4$,

$$\emptyset,\ \{1\},\ \{2\},\ M.$$

**Exemple 1.2.9.** Voici une liste de *toutes les parties* de l'ensemble $M = \{1, 2, 3\}$ : il y en a $8$,

$$\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{2, 3\},\ \{1, 3\},\ M.$$

TD : faire la même chose pour $M = \{1, 2, 3, 4\}$.

**Définition 1.2.10.** Soit $M$ un ensemble (fini). On note :

$\mathcal{P}(M)$ l'ensemble de *toutes* les parties de $M$ (*ensemble des parties*),

$\mathcal{P}_k(M)$ l'ensemble de toutes les parties $A \subset M$ telles que $\mathrm{card}(A) = k$.

**Théorème 1.2.11.** *Soit $M$ un ensemble fini de cardinal $n$. Alors $M$ a exactement $2^n$ parties. Autrement dit, $\mathcal{P}(M)$ est un ensemble fini de cardinal $2^n$ :*

$$\boxed{\mathrm{card}(\mathcal{P}(M)) = 2^{\mathrm{card}(M)}}$$

*Démonstration.* La méthode principale de cette preuve (et de la suivante) est celle de *distinction de cas* : énumérer tous les cas possibles, en faisant attention qu'ils s'excluent mutuellement (ce qui permet de compter le nombre total des cas possibles). Si l'argument général vous parait abstrait, détaillez-le pour les cas $n = 2, 3, 4$ évoqués ci-dessus !

Soit $M = \{a_1, a_2, \ldots, a_n\}$, et $A \subset M$. Combien de possibilités de choisir $A$ y a-t-il ? Pour l'élément $a_1$ de $M$, il existe deux possibilités :

– soit, $a_1 \in A$,

– soit, $a_1 \notin A$ (autrement dit, $a_1 \in A^c$).

Ensuite, pour $a_2$ il y a de nouveau deux possibilités, et ainsi de suite, jusqu'à $a_n$ : cela donne $n$ choix (chacun binaire : deux issues possibles) à effectuer. Ces $n$ choix mènent à $2 \times \ldots \times 2$ ($n$ fois) issues possibles, soit $2^n$ issues. Graphiquement, on peut représenter la séquence des choix par un arbre : la première étage (choix concernant $a_1$) a deux branches, la deuxième (choix concernant $a_2$) a $2 \times 2 = 4$ branches (chacune des deux branches se ramifie en deux branches), la troisième a $2 \times 4 = 8$ branches, et ainsi de suite. □

**Définition 1.2.12.** Si $M$ est un ensemble de cardial $n$, on note $\binom{n}{k}$ le cardinal de l'ensemble $\mathcal{P}_k(M)$ ; autrement dit, c'est le nombre de parties de cardinal $k$ dans un ensemble de cardinal $n$ ; on appelle ce nombre « $k$ parmi $n$ ».

**Exemple 1.2.13.** Par l'exemple 1.2.9, $\binom{3}{1} = 3 = \binom{3}{2}$. Pour tout $n$, on a $\binom{n}{1} = n$ (il y a $n$ singletons).

**Théorème 1.2.14** ($k$ parmi $n$)**.**

1. *Si $k > n$, alors $\binom{n}{k} = 0$ ;*
2. *$\binom{n}{0} = 1$ et $\binom{n}{n} = 1$ ;*
3. *(« règle de Pascal ») si $k \in [[1, \ldots, n]]$,*

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

4. *(symétrie) pour tout $k \in [[0, \ldots, n]]$,*

$$\binom{n}{k} = \binom{n}{n-k}$$

*Démonstration.* 1. La formule traduit la remarque qu'aucune partie de $M$ ne peut avoir plus d'éléments que $M$ (remarque 1.2.4).

2. La seule partie de $M$ ayant autant d'éléments que $M$ est $M$ lui-même, et la seule partie ayant $0$ éléments est l'ensemble vide.

3. Soit $M = \{a_1, \ldots, a_{n+1}\}$ un ensemble de cardinal $n+1$ et $A \subset M$ une partie de cardinal $k$. Il y a donc $\binom{n+1}{k}$ possibilités de choisir $A$. D'autre part :

(a) soit, l'élément $a_{n+1}$ appartient à $A$. Dans ce cas on peut choisir les $k-1$ autres éléments librement dans $\{a_1, \ldots, a_n\}$ ; il y a donc $\binom{n}{k-1}$ possibilités dans ce cas ; ou bien,

(b) tous les éléments de $A$ appartiennent à $\{a_1, \ldots, a_n\}$ : cela fait $\binom{n}{k}$ possibilités.

Comme les cas (a) et (b) sont exhaustifs et s'excluent mutuellement, le nombre total de possibilités est la somme des deux, soit $\binom{n}{k} + \binom{n}{k-1}$ possibilités de choisir $A$. D'où l'égalité qui était à démontrer.

4. Choisir $k$ éléments parmi $n$ (on peut les « colorier en blanc ») revient exactement à choisir les $n-k$ éléments restants (on peut les « colorier en noir »). Autrement dit, choisir une partie $A$ de cardinal $k$ revient à choisir $A^c$ qui est de cardinal $n-k$. Le nombre de choix est donc le même. □

**Le triangle de Pascal.** La propriété 3 du théorème précédent permet de calculer les coefficients $\binom{n}{k}$ de proche en proche : on les retrouve pour $k = 0, \ldots, n$ dans la $(n+1)$-ième ligne du triangle de Pascal suivant. Par exemple, on y trouve que $\binom{5}{3} = 10$ :

$$\begin{array}{ccccccccccc} & & & & & & 1 & & & & \\ & & & & & 1 & & 1 & & & \\ & & & & 1 & & 2 & & 1 & & \\ & & & 1 & & 3 & & 3 & & 1 & \\ & & 1 & & 4 & & 6 & & 4 & & 1 \\ & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & \ldots \end{array}$$

Ce schéma a de nombreuses propriétés intéressantes – voir TD pour quelques-unes, liées à des

## 1.3 Formules remarquables

Tout le monde connaît la formule remarquable $(a+b)^2 = a^2 + 2ab + b^2$. Pour la prouver, on utilise les propriétés suivantes de la somme et du produit usuels (de nombres réels ou complexes) :

(1) distributivité : $a(b+c) = ab + ac$

(2) commutativité : $a + b = b + a$ et $ab = ba$ ,

(3) associativité : $(a+b)+c = a+(b+c)$ et $(ab)c = a(bc)$.

Dans le calcul suivant, pour chaque égalité, notez à la marge laquelle de ces propriétés est utilisée pour la justifier :

$$\begin{aligned} (a+b)^2 &= (a+b)(a+b) \\ &= a(a+b) + b(a+b) \\ &= aa + ab + ba + bb \\ &= a^2 + 2ab + b^2. \end{aligned}$$

Procédez de la même façon pour

$$\begin{aligned} (a+b)^3 &= (a+b)(a+b)(a+b) \\ &= a(a+b)(a+b) + b(a+b)(a+b) \\ &= a(aa + ab + ba + bb) + b(aa + ab + ba + bb) \\ &= aaa + aab + aba + baa + abb + bab + bba + bbb \\ &= a^3 + 3a^2b + 3b^2a + b^3. \end{aligned}$$

**Théorème 1.3.1** (Formule du binôme de Newton)**.** *Soit $a, b$ deux nombres réels ou complexes et $n$ un nombre naturel. Alors*

$$\boxed{(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{k}a^{n-k}b^k + \ldots + \binom{n}{n-1}ab^{n-1} + b^n}.$$

*Démonstration.* En utilisant la distributivité et l'associativité, on développe le produit $(a+b)^n = (a+b)\cdots(a+b)$. On obtient $2^n$ termes, chacun contenant un certain nombre $k$ de facteurs $b$, et les autres $n-k$ facteurs $a$. Plus précisément, pour chaque partie $A \subset [[1,n]]$ il y a un terme de la forme

$$c_1 \cdot c_2 \cdot \ldots \cdot c_n,$$

où $c_i = b$ si $i \in A$, et $c_i = a$ si $i \notin A$. Soit $\mathrm{card}(A) = k$. On utilisant la commutativité et l'associativité, l'ordre des facteurs n'a pas d'importance, et donc ce terme vaut $b^k a^{n-k}$. Il y a exactement $\binom{n}{k}$ de telles parties $A$, et donc autant termes de ce type ; ainsi ils contribuent $\binom{n}{k} b^k a^{n-k}$ au résultat final. On peut faire cela pour tout $k = 0, \ldots, n$, et la somme de tout ces termes vaut donc $(a+b)^n$. (Si vous avez des difficultés à suivre l'argument dans le cas de $n$ général, détaillez-le encore pour le cas $n = 4$.) □

**Le signe somme.** Si $a_1, \ldots, a_n$ sont des nombres réels ou complexes, on abrège

$$\boxed{\sum_{i=1}^{n} a_i := a_1 + a_2 + \ldots + a_n}.$$

L'index $i$ est « muet » : on peut utiliser n'importe quelle autre lettre, hormis $n$ qui est déjà pris. Avec cette convention, la formule du binôme de Newton s'écrit :

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

*Chapitre* 2

# Opérations sur les ensembles

Etant donné des parties $A, B, C, \ldots$ d'un ensemble $M$, on peut en fabriquer d'autres par les opérations *intersection*, *union*, *différence*, *complémentaire*. Ce opérations vérifient certaines règles que nous allons étudier ; en langage plus élaboré, on dit que l'ensemble des parties $\mathcal{P}(M)$, muni de ces opérations, forme ce qu'on appelle une *algèbre de Boole*. En théorie des probabilités, on appelle souvent *univers* l'ensemble $M$, et on le note $\Omega$.

Aussi, à partir de deux ensembles $M$ et $N$, on peut former un autre, leur *produit cartésien*, noté $M \times N$. Ou encore, on peut dire qu'à partir de deux univers $\Omega_1$ et $\Omega_2$ on fabrique un nouveau, $\Omega_1 \times \Omega_2$.

## 2.1 Opérations sur les parties d'un ensemble $M$

**Définition 2.1.1.** Soit $A$ et $B$ deux parties d'un ensemble $M$. Leur *intersection* $A \cap B$ est définie par

$$\boxed{A \cap B := \{x \in M \mid x \in A \text{ et } x \in B\}}.$$

Cela veut dire que $x \in A \cap B$ est vrai si, et seulement si, à la fois $x \in A$ et $x \in B$. On définit l'*union* $A \cup B$ par

$$\boxed{A \cup B := \{x \in M \mid x \in A \text{ ou } x \in B\}}.$$

Cela veut dire que $x \in A \cup B$ est vrai si, et seulement si, $x$ appartient à $A$, ou à $B$, *ou aux deux à la fois* (il s'agit du « ou logique » ; on parlera plus tard de la logique en général). Puis, la *différence ensembliste de $B$ et de $A$*, ou : *$B$ privé de $A$*, $B \setminus A$, est défini par

$$\boxed{B \setminus A := \{x \in M \mid x \in B \text{ et } x \notin A\}}.$$

Ainsi $x \in B \setminus A$ est vrai si, et seulement si, $x$ appartient à $B$, mais non à $A$. Rappelons que le *complémentaire de $A$ dans $M$* est l'ensemble des éléments qui n'appartiennent pas à $A$, i.e., $A^c = \{x \in M \mid x \notin A\} = M \setminus A$. La *différence symétrique* est définie par

$$A \Delta B := \{x \in M \mid x \in A \text{ ou bien } x \in B\},$$

où « ou bien » est le *ou exclusif* : $x \in A\Delta B$ si et seulement si $x$ appartient à $A \setminus B$, ou à $B \setminus A$ (mais non à $A$ et $B$ à la fois).

**Représentation logique.** On peut résumer ces définitions par la *table de vérité* suivante : un symbole $0$ dans la colonne marquée $x \in A$ veut dire que cette propriété est fausse (donc, $x \notin A$ est vraie), et un symbole $1$ qu'elle est vraie (donc, $x \in A$ est vraie), etc. Par exemple, $x \in A \cap B$ est vraie dans le seul cas où $x \in A$ et $x \in B$, et fausse dans les autres $3$ cas :

| $x \in A$ | $x \in B$ | $x \in A \cap B$ | $x \in A \cup B$ | $x \in B \setminus A$ | $x \in A\Delta B$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 |

Vous pouvez dresser la table de vérité pour $B \cap A^c$, et constater qu'elle coïncide avec celle de $B \setminus A$, d'où : $B \setminus A = B \cap A^c$. De la même manière, on constate que (cf. TD)

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

**Représentation graphique.** En négligeant des propriétés « géométriques » ou autres, on représente des ensembles souvent par des « diagrammes en patates » (*diagrammes de Venn*), en coloriant ou en hachurant la partie $A \cap B$, etc. Cette représentation est souvent utile pour « fixer les idées » (arguments heuristiques), mais ne constitue jamais une preuve mathématique !

**Théorème 2.1.2.** *Les opérations ensemblistes vérifient les propriétés suivantes :*

1. *associativité :* $(A \cap B) \cap C = A \cap (B \cap C)$,
   $(A \cup B) \cup C = A \cup (B \cup C)$,
   $(A\Delta B)\Delta C = A\Delta(B\Delta C)$,
2. *commutativité :* $A \cap B = B \cap A$, $A \cup B = B \cup A$, $A\Delta B = B\Delta A$,
3. *distributivité :* $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$,
   $(A \cup B) \cap C = (A \cap C) \cup (A \cap C)$,
4. *lois de complément :* $(A^c)^c = A$, $\quad A \cap A^c = \emptyset$, $\quad A \cup A^c = M$,
5. *lois de de Morgan :* $(A \cup B)^c = A^c \cap B^c$, $\quad (A \cap B)^c = A^c \cup B^c$.

*Démonstration.* Il est conseillé d'illustrer chacune des propriétés par un diagramme de Venn. Pour donner une preuve formelle, il faut utiliser les propriétés logiques : on distingue tous les cas possibles – s'il y a deux ensembles en jeu, il y a $4$ cas, s'il y en a trois, cela fait 8 cas. Par exemple, pour la première loi de de Morgan, dressons la « table de vérité » avec les 4 cas possibles :

| $x \in A$ | $x \in B$ | $x \in A \cup B$ | $x \in (A \cup B)^c$ | $x \in A^c$ | $x \in B^c$ | $x \in A^c \cap B^c$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 |

Les valeurs des colonnes 4 et 7 coïncident, ce qui prouve que les conditions décrivant ces ensembles sont les mêmes ; donc ces ensembles sont égaux. Les autres points sont démontrés de la même façon. □

(Exercice de TD) : Prouver certaines propriétés de $\Delta$. (On dira que $\mathcal{P}(M)$, muni de la loi $\Delta$, est un *groupe*, ayant $\emptyset$ comme *élément neutre*.)

**Définition 2.1.3.** On dit que $A$ et $B$ sont *disjointes* si elles n'ont aucun élément en commun : $A \cap B = \emptyset$.

Une *partition de* $M$ est la donnée de parties $A_1, \ldots, A_k$ de $M$ telles que

– les $A_i$ sont tous non-vides ;

– elles sont deux à deux disjointes ($\forall i \neq j : A_i \cap A_j = \emptyset$) ;

– leur réunion est $M$ : $A_1 \cup \ldots \cup A_k = M$.

**Théorème 2.1.4.** *Soit $M$ un ensemble fini et $A, B \subset M$.*

1. *Si $A$ et $B$ sont disjointes, alors* $\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B)$,
2. *Si $A_1, \ldots, A_k$ sont des parties de $M$, deux à deux disjointes, alors*

$$\operatorname{card}(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} \operatorname{card}(A_i).$$

   *Si $A_1, \ldots, A_n$ est une partition de $M$, alors* $\sum_{i=1}^{n} \operatorname{card}(A_i) = \operatorname{card}(M)$.
3. *En général,* $\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B)$,
   *et* $\operatorname{card}(A \Delta B) = \operatorname{card}(A) + \operatorname{card}(B) - 2\operatorname{card}(A \cap B)$.

*Démonstration.* 1. Si $A \cap B = \emptyset$, tout élément de $A \cup B$ appartient, soit à $A$, soit à $B$ (et non au deux en même temps). Ainsi le nombre d'éléments de $A \cup B$ est bien la somme des nombres d'éléments de $A$ et de $B$.

2. Tout élément de $E = A_1 \cup A_2 \cup \ldots \cup A_k$ appartient à un seul des ensembles $A_i$, $i = 1, \ldots, k$. Ainsi le nombre d'éléments de $E$ est bien la somme des nombres d'éléments de $A_1$, $A_2$, jusqu'à $A_k$.

3. Remarquons d'abord que

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

est une réunion disjointe ; donc d'après 1., $\operatorname{card} A = \operatorname{card}(A \setminus B) + \operatorname{card}(A \cap B)$. Ensuite, remarquons que

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

est une réunion disjointe ; d'où d'après 2.,

$$\begin{aligned} \operatorname{card}(A \cup B) &= (\operatorname{card}(A) - \operatorname{card}(A \cap B)) + \operatorname{card}(A \cap B) + (\operatorname{card}(B) - \operatorname{card}(A \cap B)) \\ &= \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B). \end{aligned}$$

La deuxième formule s'ensuit de la même manière. □

Exemple : les groupes de TD de la promo de L1 forment une partition de cette promo. L'effectif total est donc la somme des effectifs des groupes de TD.

Exercice (TD) : Donner une formule pour $\mathrm{card}(A \cup B \cup C)$.

**Le principe des tiroirs.** Soit $\{A_1, \ldots, A_k\}$ une partition de $M$, et $\mathrm{card}(M) = n$. (Penser aux ensembles $A_i$ comme des « casiers », ou des « tiroirs » ; chaque élément de $M$ est rangé dans un unique casier ; il y a $k$ casiers et $n$ objets.) Alors :

1. il ne peut pas y être plus de casiers que d'éléments (car aucun casier n'est vide) : il n'est pas possible que $k > n$ ;
2. si $k = n$, alors les $A_i$ sont tous des singletons (i.e., elles sont de cardinal $1$ : chaque casier contient un unique élément) ;
3. et si $k < n$, il existe au moins un index $i$ tel que $\mathrm{card}(A_i) > 1$ (s'il y a moins de casiers que d'objets, alors au moins un casier contient plus qu'un objet).

Ces énoncés semblent évidents, et à ce stade, nous ne cherchons pas à les « prouver ».

## 2.2 Produit cartésien

**Définition 2.2.1.** Soit $M_1$ et $M_2$ deux ensembles. Le *produit cartésien* $M_1 \times M_2$ est l'ensemble des *couples* $(x, y)$ avec $x \in M_1$ et $y \in M_2$. La règle de base opératoire concernant les couples est de savoir que

| deux couples $(x, y)$ et $(x', y')$ sont égaux si et seulement si : $x = x'$ et $y = y'$. |
|---|

Cela s'écrit aussi : $(x_1, x_2) = (x'_1, x'_2)$ ssi ($x_1 = x'_1$ et $x_2 = x'_2$).

Retenir : Contrairement aux ensembles $\{x, y\}$, pour les couples $(x, y)$ l'ordre est important : en général, $(x, y) \neq (y, x)$ (le seul cas où il y a égalité est $x = y$).

Dans le cas $M_1 = M_2 = M$, on note $M^2 = M \times M$.

Notation (convention) : surtout dans le cas où $M = \mathbb{R}$, on note souvent les couples (éléments $(x_1\ x_2) \in \mathbb{R}^2$) sous forme de *colonne* : $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

**Théorème 2.2.2.** *Si $M_1$ est de cardinal fini $n$ et $M_2$ de cardinal fini $m$, alors $M_1 \times M_2$ est de cardinal fini $n \cdot m$ :*

$$\mathrm{card}(M_1 \times M_2) = \mathrm{card}(M_1) \cdot \mathrm{card}(M_2).$$

*Démonstration.* Pour choisir un élément $(x, y) \in M_1 \times M_2$, on a *d'abord*, pour $x$, le choix entre les $n$ éléments $x_1, \ldots, x_n$ de $M_1$ ; ce choix fixé, on a *ensuite*, pour $y$, le choix entre les $m$ éléments $y_1, \ldots, y_m$ de $M_2$. On pourra représenter ces choix par un *arbre* : la première étage a $n$ branches ; chaque branche se ramifie en $m$ branches au deuxième étage ; cela fait donc $n \cdot m$ branches au total. □

*Représentation graphique.* En théorie des probabilités, on utilise parfois une représentation par des arbres ; par contre, dans ce cours, il sera plus approprié

de représenter $M_1 \times M_2$ par un schéma rectangulaire – une sorte de tableau à double entrée avec $n$ lignes et $m$ colonnes, et l'élément $(x, y)$ au croisement de la « colonne sur $x$ » avec la « ligne au niveau $y$ ».

**Exemple 2.2.3.** L'ensemble $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ s'appelle le *plan réel*. Un couple $(x, y) \in \mathbb{R}^2$ est un *point* de ce plan. Si $A$ et $B$ sont des parties finies de $\mathbb{R}$, l'ensemble des couples $(x, y)$ avec $x \in A$ et $y \in B$ représente la partie $A \times B$ du plan (cf. TD pour des exemples).

**Exemple 2.2.4.** La partie

$$\delta := \{(x, y) \in M \times M \mid x = y\} = \{(x, x) \mid x \in M\}$$

est représentée par la *diagonale* du schéma (carré, car ici $M_1 = M_2$).

**Définition 2.2.5.** Soit $M_1, \ldots, M_n$ des ensembles. Leur *produit cartésien*, noté

$$M_1 \times \ldots \times M_n, \text{ ou } \times_{i=1}^{n} M_i,$$

est l'ensemble des *$n$-uplets* $(x_1, \ldots, x_n)$ avec $\forall i = 1, \ldots, n : x_i \in M_i$. Par définition, deux $n$-uplets $(x_1, \ldots, x_n)$ et $(x'_1, \ldots, x'_n)$ sont égaux si et seulement si $\forall i = 1, \ldots, n : x_i = x'_i$. Dans le cas où tous les $M_i$ sont le même ensemble $M$, on note $M^n = M \times \ldots \times M$.

**Théorème 2.2.6.** *Les ensembles*

$$M_1 \times M_2 \times M_3 \qquad \textit{et} \qquad (M_1 \times M_2) \times M_3 \qquad \textit{et} \qquad M_1 \times (M_2 \times M_3)$$

*sont « les mêmes », c'est-à-dire, en théorie des ensembles, ils sont « indistinguables » : nous pouvons alors écrire*

$$M_1 \times (M_2 \times M_3) = M_1 \times M_2 \times M_3 = (M_1 \times M_2) \times M_3.$$

*Démonstration.* Les paires $((x, y), z)$ se comportent exactement comme les triplets : on a $((x, y), z) = ((x', y'), z')$ ssi [$(x, y) = (x', y')$ et $z = z'$], ssi [$x = x'$ et $y = y'$ et $z = z'$]. Idem pour $(x, (y, z))$. □

**Remarque 2.2.7.** L'égalité $(M_1 \times M_2) \times M_3 = M_1 \times (M_2 \times M_3)$ se traduit en disant que le produit cartésien est *associatif*. (En revanche, on prendra soin de distinguer $M_1 \times M_2$ et $M_2 \times M_1$.)

**Théorème 2.2.8.** *Si, pour $i = 1, \ldots, m$, l'ensemble $M_i$ est de cardinal fini $n_i$, alors*

$$\mathrm{card}(M_1 \times \ldots \times M_m) = n_1 \cdots n_m.$$

*En particulier, $M^m$ est de cardinal $(\mathrm{card}(M))^m$.*

*Démonstration.* Mêmes arguments que pour le théorème 2.2.2 (on pourra les représenter par un arbre à $n$ étages et $n_i$ branches au niveau $i$). □

## 2.3 Somme disjointe

Cette section est un complément, hors programme !

Il existe encore une autre opération pour fabriquer un ensemble à partir de deux « univers » $M_1$ et $M_2$ : leur *coproduit*, aussi appelé *somme disjointe* ou

*somme cartésienne*, noté $M_1 \sqcup M_2$ ou $M_1 \coprod M_2$. On peut le voir comme une réunion de $M_1$ et de $M_2$, mais après avoir rendu $M_1$ et $M_2$ disjoints. Si $M_1$ et $M_2$ sont des parties disjointes d'un ensemble $M$, alors c'est leur réunion usuelle $M_1 \cup M_2$ ; mais sinon, il faut d'abord remplacer $M_2$ par une copie $M_2'$ qui assure que les éléments de $M_2'$ sont différents de tous les éléments de $M_1$. Ceci est fait pour que la règle

$$\mathrm{card}(M_1 \sqcup M_2) = \mathrm{card}(M_1) + \mathrm{card}(M_2)$$

soit valable (et qui justifie le terme « somme »). Par exemple, si $M_1 = \{1\} = M_2$, on pourra écrire $M_2 = \{1'\}$, et $M_1 \sqcup M_1 = \{1, 1'\}$ est de cardinal 2.

De même, $\mathbb{R} \sqcup \mathbb{R}$ est une union « de deux copies disjointes de $\mathbb{R}$ ». Retenez donc qu'on peut faire une « copie » d'un ensemble (comme on fait une copie d'un fichier informatique), mais alors c'est un autre ensemble. (En anticipant le langage des fonctions, chapitre 3 : ces deux ensembles *sont alors en bijection l'un avec l'autre*.)

Comment justifier l'existence des constructions « produit direct » et « somme disjointe » ? Cela fait partie de la théorie des ensembles (cf. chapitre 7) – à ce stade de théorie « naive », nous ne cherchons pas à le justifier vraiment – il s'agit surtout de comprendre le sens et l'utilisation de ces constructions.

*Chapitre* 3

# Applications, fonctions

On peut dire sans exagérer que les *fonctions* et *applications* sont l'objet d'étude le plus important des maths : dans le théâtre des maths, la théorie des ensembles met en place la scène, mais la pièce de théâtre elle-même est jouée par les fonctions. Ce chapitre est le plus important du cours.

## 3.1 Définitions fondamentales

**Définition 3.1.1.** Une *application* entre deux ensembles $A$ et $B$, notée

$$\boxed{f : A \to B,\ a \mapsto f(a)}$$

est la donnée de trois choses :

1. d'un ensemble $A$, dit *ensemble de départ*, ou : *domaine*,
2. d'un ensemble $B$, dit *ensemble d'arrivée*, ou : *codomaine*,
3. d'une règle qui associé à tout élément $a \in A$ un élément dit *image de* $a$ *par* $f$ et noté $f(a) \in B$.

Le symbôle désignant la *variable* est « muet » : on peut utiliser n'importe quelle lettre – par exemple, $f : A \to B$, $x \mapsto f(x)$ est la même application que celle écrite ci-dessus. Souvent, on utilise aussi le mot *fonction*, en particulier si $B = \mathbb{R}$ (*fonction réelle*, $f : A \to \mathbb{R}$); et si $A = B$, on parle aussi d'une *transformation (de A)*, $f : A \to A$.

**Définition 3.1.2.** Soit $f : A \to B$ une application, et $b \in B$. Tout élément $a \in A$ tel que $b = f(a)$ est dit un *antécédent* de $b$.

Noter bien : chaque $a \in A$ a une unique image $f(a)$ dans $B$; mais chaque $b \in B$ peut avoir plusieurs, ou aucun, antécédent (cf. les exemples suivants).

Représentation. Si $A$ et $B$ sont des ensembles finis, on peut représenter une application $f : A \to B$ de plusieurs façons :

1. par un schéma reliant (par une flèche ou un traît) chaque élement $a \in A$ à son image $f(a) \in B$,
2. par la liste des images $f(a)$ quand $a$ parcourt $A$.

**Exemple 3.1.3.** Si $A = B = \{1, 2\}$, alors il existe $4$ applications $f : A \to A$ possibles, à savoir, $f_i$, $i = 1, 2, 3, 4$, données par le tableau suivant (Exercice : pour chacune des ses applications, dessiner le schéma (item 1.) correspondant !) :

| | $f_i(1)$ | $f_i(2)$ |
|---|---|---|
| $f_1$ | 1 | 1 |
| $f_2$ | 2 | 2 |
| $f_3$ | 1 | 2 |
| $f_4$ | 2 | 1 |

**Définition 3.1.4** (injectif, surjectif, bijectif)**.** Une application $f : A \to B$ est

1. *surjective* si tout élément $b \in B$ a (au moins) un antécédent :
$$\forall b \in B : \exists a \in A : b = f(a);$$
2. *injective* si tout élément de $B$ a *au plus* un antécédent :
$$\forall a, a' \in A : [\text{ si } a \neq a', \text{ alors } f(a) \neq f(a')];$$
3. *bijective* si elle est surjective et injective : tout $b \in B$ a *exactement un* antécédent. En utilisant le quantificateur $\exists!$ (« il existe un unique ») cela s'érit, $\forall b \in B : \exists! a \in A : b = f(a)$.

On peut reformuler ces conditions :

1. Définissons $\mathrm{im}(f) := \{y \in B \mid \exists x \in A : y = f(x)\}$, l'*image de* $f$ (l'ensemble de tous les images) ; alors $f$ est surjetive ssi $\mathrm{im}(f) = B$.
2. Par le principe logique de *contraposition* (qu'on verra en chapitre 9), la condition 2. équivaut à : $f$ est injective, ssi on a
$$\forall a, a' \in A : [\text{ si } f(a) = f(a'), \text{ alors } a = a'].$$

**Exemple 3.1.5.** Parmi les applications de l'exemple 3.1.3, $f_3$ et $f_4$ sont bijectives (vérifier !), et $f_1$ et $f_2$ ne sont ni injectives, ni surjectives (par exemple, $2$ n'a pas d'antécédent par $f_1$ ; en revanche, $1$ a deux antécédents par $f_1$). En fait, $f_1$ et $f_2$ sont *constantes* :

**Définition 3.1.6.** Une application $f : A \to B$ est dite *constante* s'il existe $c \in B$ tel que $f(x) = c$ pour tout $x \in A$ (i.e., tout $b \in B$ est antécédant de $c$).

**Exemple 3.1.7.** Il est très important de préciser domaine et codomaine d'une application. Considérons

$$\begin{aligned} f : \mathbb{R} \to \mathbb{R}, &\quad x \mapsto x^2 \\ g : \mathbb{R} \to \mathbb{R}^+, &\quad x \mapsto x^2 \\ h : \mathbb{R}^+ \to \mathbb{R}^+, &\quad x \mapsto x^2. \end{aligned}$$

L'application $f$ n'est ni injective (car $b = 1$ a deux antécédents : $a = 1$ et $a' = -1$) ni surjective (car $-2$ n'a pas d'antécédent). L'application $g$ est surjective (car tout nombre réel positif $r$ admet une racine carrée, et $\pm\sqrt{r}$ sont deux antécédents de $r$), mais non injective. L'application $h$ est bijective (l'unique antécédent de $r \in \mathbb{R}^+$ est sa racine carrée $\sqrt{r} \in \mathbb{R}^+$). On dira que l'application $u : \mathbb{R}^+ \to \mathbb{R}^+$, $r \mapsto \sqrt{r}$ est l'*application réciproque* ou *inverse* de $h$ :

**Définition 3.1.8.** Si $f : A \to B$ est bijective, on définit l'*application réciproque*

$$\boxed{f^{-1} : B \to A,\ b \mapsto f^{-1}(b)}$$

en associant à $b \in B$ son unique antécédent dans $A$, donc $f^{-1}(b) = a$ où $f(a) = b$. Il s'ensuit que $\boxed{f^{-1}(f(a)) = a}$ et $\boxed{f(f^{-1}(b)) = b}$.

Généralisant l'exemple 3.1.3, si $A$ et $B$ sont finis, on peut toujours énumérer toutes les applications possibles de $A$ vers $B$ :

**Définition 3.1.9.** Pour deux ensembles $A$ et $B$, nous notons

$$B^A,\ \text{ou} : \text{Fon}(A, B),$$

l'ensemble de toutes les applications $f : A \to B$.

**Théorème 3.1.10.** *Soit $A$ un ensemble fini de cardinal $n$ et $B$ de cardinal $m$. Alors il existe exactement $m^n = \text{card}(B)^{\text{card}(A)}$ applications $f : A \to B$. Autrement dit,*

$$\text{card}(B^A) = \text{card}(B)^{\text{card}(A)}.$$

*Démonstration.* Soit $A = \{a_1, \ldots, a_n\}$ et $B = \{b_1, \ldots, b_m\}$. Nous avons $m$ possibilités de choisir $f(a_1)$ dans $B$, puis encore $m$ possibilités de choisir $f(a_2)$, etc. On peut encore représenter ces choix par un arbre, cette fois-ci avec $n$ étages, et $m$ ramifications à chaque étage. Au total, cela fait $m \cdots m = m^n$ choix possibles. □

**Théorème 3.1.11.** *Soit $n = \text{card}(A)$ et $m = \text{card}(B)$.*

1. *Si $n \leq m$, alors il y a exactement*

$$m(m-1)\cdots(m-n+1)$$

*applications injectives $f : A \to B$ ;*

2. *si $n = m$, il y a exactement*

$$n! := n(n-1)\cdots 2 \cdot 1$$

*applications bijectives $f : A \to B$ ;*

3. *si $n > m$, alors il n'existe aucune application injective $f : A \to B$ ;*
4. *si $n < m$, alors il n'existe aucune application surjective $f : A \to B$.*

*Démonstration.* 1. Soit $A = \{a_1, \ldots, a_n\}$. Pour choisir $f : A \to B$ injective, nous avons d'abord $m$ possibilités pour définir $f(a_1)$, disons $f(a_1) = b$; une fois ce choix fixé, nous pouvons choisir f($a_2$) librement parmi les $m - 1$ éléments différents de $b$; ce choix fixé, il reste $m - 2$ possibilités pour choisir $f(a_3)$, et ainsi de suite – pour la dernière valeur $f(a_n)$ il reste $m - n + 1$ choix. Ensemble, cela donne un arbre de décision à $n$ étages, avec $m(m-1)\cdots(m-n+1)$ branches au niveau final. Noter que, si $n = m$, alors pour la dernière valeur $f(a_n)$, il y a $n - n + 1 = 1$ choix; autrement dit, il faut prendre le dernier élément de $B$ qui n'est pas encore atteint comme image, et après ce

dernier choix, tout élément de $B$ est pris comme image : dans ce cas, $f$ est donc surjective. Si $n = m$, toute application injective est donc automatiquement surjective, et donc bijective, et il y en a $n!$ de telles applications.

3. On constate que l'argument du point 1. échoue quand $n > m$, car à la fin il n'y a plus aucune possibilité pour fixer la dernière valeur $f(a_n)$. Logiquement, cet énoncé est étroitement lié au *principe des tiroirs* énoncé en fin de la section 2.1, et idem pour le point 4. Une preuve rigoureuse devrait se placer dans le contexte de la théorie des ensembles (chapitre 7). En attendant, on pourra prouver 3. dans le cas $n = 2, m = 1$, et 4. dans le cas $n = 1, m = 2$ (exercice). □

**Remarque 3.1.12.** Si $n > m$, il est plus difficile de compter les applications surjectives. Cf. TD 2 pour les cas (relativement faciles) $m = 2$ et $n = m + 1$.

## 3.2 Composée d'applications

**Définition 3.2.1.** Soient $f : A \to B$, $a \mapsto f(a)$ et $g : B \to C$, $b \mapsto g(b)$ deux applications. On définit une application $g \circ f$ (lire « $g$ rond $f$ » ou « $g$ après $f$ »), la *composée de $f$ et de $g$*

$$g \circ f : A \to C, \quad a \mapsto (g \circ f)(a) = g(f(a))$$

**Théorème 3.2.2.** *La composition d'applications est* associative *: si $f : A \to B$ et $g : B \to C$ et $h : C \to D$, alors* $\boxed{h \circ (g \circ f) = (h \circ g) \circ f}$.

*Démonstration.* Pour tout $a \in A$,

$(h \circ (g \circ f))(a) = h(g \circ f(a)) = h(g(f(a))) = ((h \circ g) \circ f)(a)$. □

**Exemple 3.2.3.** Si $A = B$ et $f, g : A \to A$, alors on peut composer : $g \circ f$ est encore une application $A \to A$. Par exemple, si $A = B = \{1, 2\}$, en utilisant les notations de l'exemple 3.1.3,

$$f_1 \circ f_4(1) = f_1(2) = 1,\ f_1 \circ f_4(2) = f_1(1) = 1, \text{ donc } f_1 \circ f_4 = f_1 ;$$
$$f_4 \circ f_1(1) = f_4(1) = 2,\ f_4 \circ f_1(2) = f_4(1) = 2, \text{ donc } f_4 \circ f_1 = f_2.$$

Conclusion : la composée **n'est pas commutative** – en général, $g \circ f$ est différent de $f \circ g$! Exercice (cf TD) : compléter la table (où en ligne $i$ figurent les composées $f_i \circ f_j$ avec $j = 1, 2, 3, 4$) :

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | | | | $f_1$ |
| $f_2$ | | | | |
| $f_3$ | | | | |
| $f_4$ | $f_2$ | | | |

On constatera que $f_3 \circ f_i = f_i = f_i \circ f_3$ pour tout $i = 1, 2, 3, 4$ :

**Définition 3.2.4.** Pour tout ensemble $M$, l'application

$$\mathrm{id}_M : M \to M, \quad x \mapsto x = \mathrm{id}_M(x)$$

s'appelle l'(application) identité de $M$.

**Proposition 3.2.5.** *Pour toute application $f : A \to B$, on a* $\boxed{f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f}$.

**Théorème 3.2.6.** *Pour une application $f : A \to B$, les propriétés suivantes sont équivalentes :*

*(1) $f$ est bijective ;*

*(2) il existe une application $g : B \to A$ telle que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$.*

*Dans ce cas, $g$ est égale à l'application réciproque $f^{-1}$ définie ci-dessus.*

*Démonstration.* Dire que (1) et (2) sont équivalentes signifie que (1) implique (2), et (2) implique (1).

Montrons que (1) implique (2). Si $f$ est bijective, nous avons défini ci-dessus l'application $f^{-1}$ vérifiant $f(f^{-1}(y)) = y$ et $f^{-1}(f(x)) = x$ pour tout $x \in A, y \in B$, d'où (2).

Montrons que (2) implique (1). Supposons donc que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. Montrons que $f$ est injective : si $f(a) = f(a')$, alors $g(f(a)) = g(f(a'))$, car $g$ est une application, et donc $a = a'$ car $g \circ f = \mathrm{id}$.

Montrons que $f$ est surjective : soit $b \in B$ ; posons $a := g(b)$, alors $f(a) = f(g(b)) = b$. Donc tout $b \in B$ admet un antécédent. Et donc $f$ est bijective. □

**Proposition 3.2.7.** *Si $h : B \to C$ et $f : A \to B$ sont bijectives, alors $h \circ f$ est bijective, et*

$$(h \circ f)^{-1} = f^{-1} \circ h^{-1}.$$

*Démonstration.* En effet : $(h \circ f) \circ (f^{-1} \circ h^{-1}) = h \circ (f \circ f^{-1}) \circ h^{-1} = h \circ \mathrm{id} \circ h^{-1} = \mathrm{id}_C$ et idem $(f^{-1} \circ h^{-1}) \circ (h \circ f) = \mathrm{id}_A$, donc d'après le théorème précédent, $h \circ f$ est bijective, et $f^{-1} \circ h^{-1}$ est son inverse. □

## 3.3 Permutations

**Définition 3.3.1.** Une *permutation* d'un ensemble $M$ est une application bijective $f : M \to M$. L'ensemble $\mathfrak{S}(M)$ des permutations de $M$ est appelé le *groupe symétrique de $M$*.

**Théorème 3.3.2.** *Les permutations d'un ensemble $M$ forment un* groupe $G := \mathfrak{S}(M)$, *avec la composée $\circ$ comme loi de groupe et $e = \mathrm{id}_M$ comme élément neutre.*

**Définition 3.3.3.** Un *groupe* est un ensemble $G$ muni d'une *loi de groupe* qui associe à un couple $(g, h)$ un troisième élément noté $g \cdot h$ (ou juste $gh$, ou $g * h$, ou encore autrement...), tel que :

– la loi est *associative* : $\forall f, g, h \in G : (f \cdot g) \cdot h = f \cdot (g \cdot h)$,

– il existe un *élément neutre* $e \in G$ tel que : $\forall g \in G : e \cdot g = g = g \cdot e$,

– chaque $g \in G$ admet un *élément inverse* $g^{-1}$ vérifiant $g \cdot g^{-1} = e = g^{-1} \cdot g$.

*Démonstration. (du théorème.)* Le propriétés (associativité, neutre et inverse) ont déjà été démontrées. □

**Notation.** On note $\mathfrak{S}_n$ le groupe des bijections de $M = [[1, n]]$.

Attention : quelle que soit la notation du produit d'un groupe, il n'est pas toujours *commutatif* : en géneral, $g \cdot h \neq h \cdot g$. La théorie des groupes, et en particulier des groupes de permutations $\mathfrak{S}_n$, est un objet important des études de maths en Licence. Voir TD pour une première approche.

**Exemple 3.3.4.** Rappelons que le cardinal de $\mathfrak{S}_n$ est $n!$. Si $n = 1$, la seule permutation est $f = \mathrm{id}$, donc $\mathfrak{S}_1 = \{e\}$ est le *groupe trivial*.

Si $n = 2$, on peut écrire $\mathfrak{S}_2 = \{e, f\}$ avec $e = \mathrm{id}$ et $f : 1 \mapsto 2, 2 \mapsto 1$ (« transposition »). Sa *table de groupe* est très simple, et ce groupe est encore commutatif :

| $\circ$ | $e$ | $f$ |
|---|---|---|
| $e$ | $e$ | $f$ |
| $f$ | $f$ | $e$ |

Si $n = 3$, on fera en TD une liste des $3! = 6$ permutations de $\{1, 2, 3\}$, et on calculera la *table de groupe* de $\mathfrak{S}_3$ (en schéma en $6$ lignes et $6$ colonnnes, avec les $36 = 6 \times 6$ produits possibles entre les $6$ éléments). Ce groupe *n'est pas commutatif* : vous trouvez, dans cette table de groupe, deux éléments $h$ et $g$ avec $h \circ g \neq g \circ h$.

Le groupe $\mathfrak{S}_4$ a $24$ éléments, et $\mathfrak{S}_5$ en a $120$. Ces groupes seront étudiés dans les cours d'algèbre de L2 et L3.

**Théorème 3.3.5.** *Pour tout $k = 0, \ldots, n$, le coefficient $\binom{n}{k}$ est donné par les formules*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

*Démonstration.* Choisir un ensemble $\{i_1, \ldots, i_k\}$ de cardinal $k$ dans $[[1, \ldots, n]]$ se fait en deux étapes :

– d'abord, choisir le $k$-uplet $(i_1, \ldots, i_k)$ (d'après le théorème 3.1.11, le nombre de tels choix est de $n(n-1)\cdots(n-k+1)$) ;

– puis, comme chacune des $k!$ permutations de $[[1, \ldots, k]]$ donne le même ensemble, il faut diviser cette quantité par $k!$ pour obtenir le nombre de parties de cardinal $k$ dans $[[1, \ldots, n]]$. □

**Exemple 3.3.6.** Loto (ancienne version) : choisir $6$ parmi $49$ chiffres donne $\binom{49}{6} = \frac{49\cdot48\cdot47\cdot46\cdot45\cdot44}{2\cdot3\cdot4\cdot5\cdot6} = 49 \cdot 2 \cdot 47 \cdot 46 \cdot 3 \cdot 22 = 13\,983\,816$ possibilités. (Attention : toujours simplifier nominateur et dénominateur avant d'utiliser votre calculette !)

## 3.4 Image directe et image réciproque d'une partie

Si $f : A \to B$ est une application, on peut non seulement parler de l'image $f(a)$ d'un seul élément $a$, mais aussi de l'ensemble $f(U)$ de toutes les images

$f(a)$ avec $a \in U$. Idem, si $W \subset B$, on peut parler de l'*ensemble de tous les antécédents des* $b \in W$, qu'on note $f^{-1}(W)$. Attention, cette notation peut causer des confusions : elle est définie que $f$ soit bijective ou non, et cela ne veut pas dire que l' « application $f^{-1}$ » existe ! Il faut donc être prudent et respecter scrupuleusement les définitions, pour ce qui concerne les notions de ce paragraphe.

**Définition 3.4.1.** Soit $f : A \to B$ une application et $U \subset A$ une partie. L'*image directe* $f(U)$ est la partie de $B$ définie par

$$f(U) := \{b \in B \mid \exists a \in U : b = f(a)\} = \{f(a) \mid a \in U\}.$$

L'image directe $f(A)$ est appelée l'*image de* $f$, notée aussi $\mathrm{im}(f)$.

Remarque : $f$ est surjective si et seulement si $\mathrm{im}(f) = B$.

TD : on a toujours $f(U \cup V) = f(U) \cup f(V)$, mais $f(U \cap V)$ est en général différent de $f(U) \cap f(V)$. Aussi, on a toujours $(g \circ f)(U) = g(f(U))$.

**Définition 3.4.2.** Soit $f : A \to B$ une application, et $W \subset B$ une partie. L'*image réciproque* $f^{-1}(W)$ est la partie de $A$

$$f^{-1}(W) := \{a \in A \mid f(a) \in W\}.$$

TD : on a toujours les propriétés

$f^{-1}(W \cup V) = f^{-1}(W) \cup f^{-1}(V)$, et

$f^{-1}(W \cap V) = f^{-1}(W) \cap f^{-1}(V)$, et

$(g \circ f)^{-1}(W) = f^{-1}(g^{-1}(W))$.

**Définition 3.4.3.** Si $W = \{b\}$ est un *singleton* (partie contenant un seul élément), alors on appelle $f^{-1}(\{b\})$ (= ensemble des antécédents de $b$) aussi la *$b$-fibre de $f$*.

Noter : $b$ appartient à $\mathrm{im}(f)$ si et seulement si la $b$-fibre de $f$ est non-vide.

Et $f$ est injective si et seulement si chaque fibre contient *au plus* un élément.

**Théorème 3.4.4.** *Soit $f : A \to B$ une application, et $A$ et $B$ des ensembles finis. Alors les ensembles $f^{-1}(b)$, lorsque $b$ parcourt $\mathrm{im}(f)$, forment une* partition *de $A$. Il s'ensuit que*

$$\mathrm{card}(A) = \sum_{b \in \mathrm{im}(f)} \mathrm{card}(f^{-1}(\{b\})).$$

*Démonstration.* Il faut vérifier les propriétés d'une partition (définition 2.1.3).

Les fibres sont deux à deux disjointes : soit $a \in f^{-1}(\{b\}) \cap f^{-1}(\{b'\})$ ; alors $b = f(a) = b'$, ainsi, si deux fibres ont une intersection non-vide, elles sont égales. La réunion des fibres est $A$, car si $a \in A$, alors $a$ appartient à la fibre $f^{-1}(\{f(a)\})$. Ainsi les fibres forment une partition. Si $A$ et $B$ sont finis, l'affirmation sur les cardinalités s'ensuit par la remarque suivant le théorème 2.1.4. □

**Corollaire 3.4.5.** *Soit $A$ et $B$ des ensembles finis et $f : A \to B$ une application.*

1. *Si $f$ est injective, alors* $\mathrm{card}(A) = \mathrm{card}(\mathrm{im}\, f) \leq \mathrm{card}(B)$.
2. *Si* $\mathrm{card}(A) > \mathrm{card}(B)$, *alors $f$ ne peut pas être injective.*
3. *Si $f$ est surjective, alors* $\mathrm{card}(A) = \sum_{b \in B} \mathrm{card}(f^{-1}(\{b\})) \geq \mathrm{card}(B)$.
4. *Si* $\mathrm{card}(A) < \mathrm{card}(B)$, *alors $f$ ne peut pas être surjective.*
5. *Supposons* $\mathrm{card}(A) = \mathrm{card}(B)$. *Alors $f$ est injective si, et seulement si, $f$ est surjective.*

*Démonstration.* 1. Dire que $f$ est injective signifie que $\mathrm{card}(f^{-1}(\{b\}) \leq 1$, pour tout $b \in B$. La somme décrivant $\mathrm{card}(A)$ dans le théorème précédent ne peut donc pas excéder $\mathrm{card}(B)$ (chaque terme est $\leq 1$).

2. Si $\mathrm{card}(A) > \mathrm{card}(B)$, alors au moins un terme dans la somme doit être strictement plus grand que $1$, et cela veut dire que $f$ n'est pas injective.

3. Dire que $f$ est surjective signifie que $\mathrm{card}(f^{-1}(\{b\}) \geq 1$, pour tout $b \in B$. La somme décrivant $\mathrm{card}(A)$ dans le théorème précédent vaut donc au moins $\mathrm{card}(B)$ (chaque terme est $\geq 1$).

4. Si $\mathrm{card}(A) < \mathrm{card}(B)$, alors il n'est pas possible que tous les termes de la somme sont $\geq 1$, et cela veut dire que $f$ n'est pas surjective.

5. Soit $\mathrm{card}(A) = \mathrm{card}(B)$. Si $f$ est injective, chaque terme dans la somme vaut au plus $1$; pour que la somme soit égale à $\mathrm{card}(A)$, il faut alors que chaque terme vaut $1$, et donc $f$ est surjective. Réciproquement, si $f$ est surjective, chaque terme dans la somme vaut au moins $1$ ; pour que la somme soit égale à $\mathrm{card}(A)$, il faut alors que chaque terme vaut $1$, et donc $f$ est bijective, donc injective. □

Remarque. Ces arguments donnent en fait une preuve du « principe des tiroirs ». On y reviendra au chapitre 7.

*Chapitre* 4

# Relations

Les *relations* généralisent les applications : toute application est une relation, mais la réciproque est fausse. Pour un couple $(x, y)$, on écrira $xRy$, ou $(x, y) \in R$, quand $(x, y)$ sont « en relation $R$ ». Il existe des relations de différents types dont, par exemple,

(a) les relations *fonctionnelles* (de type $y = f(x)$),

(b) les relations *d'ordre* (on les note souvent $x \leq y$ au lieu de $xRy$),

(c) les relations *d'équivalence* (on les note souvent $x \sim y$ au lieu de $xRy$).

Le but de ce chapitre n'est pas de développer une théorie systématique, mais que vous commenciez à vous familiariser surtout avec les relations de type (b) et (c) : elles sont absolument fondamentales pour toutes les mathématiques.

## 4.1 Relations et graphes

**Définition 4.1.1.** Une *relation* entre deux ensembles $M_1$ et $M_2$ est la donnée de trois choses :

1. d'un ensemble $M_1$, le *domaine*,
2. d'un ensemble $M_2$, le *codomaine*,
3. d'une « règle » $R$ qui détermine pour un couple $(x, y) \in M_1 \times M_2$ si « $x$ est en relation $R$ avec $y$ » ; on écrit alors $xRy$ ; autrement dit, $R$ est une partie

$$R \subset (M_1 \times M_2), \qquad R = \{(x, y) \in M_1 \times M_2 \mid xRy\}.$$

Toute partie de $M_1 \times M_2$ définit ainsi une relation $R$.

Si $M_1 = M_2 = M$, on parle aussi d'une relation « sur $M$ ».

**Exemple 4.1.2.** Si $f : M_1 \to M_2$ est une application, et $(x, y) \in M_1 \times M_2$, on pose $xRy$ si $y = f(x)$ ; autrement dit, $R = R_f$ est le *graphe de* $f$, la partie de $M_1 \times M_2$ définie par

$$R = R_f = \{(x, y) \in M_1 \times M_2 \mid y = f(x)\}.$$

Exemples concrets : si $M_1 = M_2 = \mathbb{R}$, le graphe $R_f$ est une partie du plan $\mathbb{R}^2$.

1. si $f(x) = e^x$, alors $R_f$ est (le graphe de) la *courbe exponentielle* ;
2. si $f(x) = x^2$, $R_f$ est une *parabole* ;
3. si $f(x) = x$, le graphe $R_f$ est la *diagonale* $x = y$ ;
4. si $f(x) = ax + b$, $R_f$ est une *droite*, de *coefficient directeur* $a$, et coupant l'axe des ordonnées au point $(0, b)$.

Noter bien : *toute droite qui n'est pas verticale* est graphe d'une fonction ; mais les droites verticales ne peuvent pas être réalisées de cette façon ! Ce sont des relations, mais qui ne sont pas *fonctionnelles* :

**Définition 4.1.3.** Une relation $R$ est dite une *relation fonctionnelle* s'il existe une application $f : M_1 \to M_2$ telle que $R = R_f$ est le graphe de $f$.

**Exemple 4.1.4.** Pour tout ensemble $M$, on a la *relation « égalité »* : $xRy$ ssi $x = y$, donc $R = \delta_M = \{(x, x) \mid x \in M\}$ est la *diagonale*. C'est une relation fonctionnelle : graphe de la fonction $\mathrm{id}_M$.

**Exemple 4.1.5.** Si $R = \emptyset$, aucun élément de $M_2$ n'est en relation $R$ avec un élément de $M_1$ (relation vide).

Si $R = M_1 \times M_2$, alors tout élément de $M_2$ est en relation $R$ avec tout élément de $M_1$ (relation totale). Ces deux relations ne sont pas fonctionnelles.

**Exemple 4.1.6.** Soit $M_1 = M_2 = \mathbb{R}$ ou $\mathbb{Z}$. Alors on pose $xRy$ ssi $x \leq y$ (« relation d'ordre »). Cette relation n'est pas fonctionelle.

**Types de relations.** Supposons $M_1 = M_2 = M$. Voici quelques propriétés qu'une relation peut avoir (ou pas) :

**Définition 4.1.7.** Une relation $R$ sur un ensemble $M$ est dite

(1) *symétrique* si elle vérifie, $\forall x, y \in M$ : $xRy$ si et seulement si $yRx$ ;

(2) *antisymétrique* si, pour tout $x, y \in M$ : si [ $xRy$ et $yRx$ ], alors $x = y$ ;

(3) *réflexive* si elle vérifie : pour tout $x \in M$, $xRx$ ;

(4) *transitive* si elle vérifie : pour tout $x, y, z \in M$, si $xRy$ et $yRz$, alors $xRz$.

## 4.2 Relations d'ordre

Ce sont des relations qui formalisent l'idée d'une relation $xRy$ signifiant que « $x$ est inférieur ou égal à $y$ » :

**Définition 4.2.1.** Une relation $R$ sur $M$ est dite *relation d'ordre (partielle)* si elle est

– *antisymétrique*,

– *réflexive*, et

– *transitive*.

Dans ce cas, on écrit souvent $x \leq y$ au lieu de $xRy$, et on écrit $a \geq b$ ssi $b \leq a$.

On parle d'une *relation d'ordre total* si, de plus :

– $\forall (x, y) \in M^2$ : $x \leq y$ ou $y \leq x$.

Les relations d'ordre sont parmi les structures mathématiques les plus basiques (voir les exemples suivants), mais en même temps, elles donnent lieu à un grand nombre de questions et de problèmes importants et parfois difficiles.

**Exemple 4.2.2.** Soit $M_1 = M_2 = M = \mathbb{N}$ ou $\mathbb{Z}$ ou $\mathbb{R}$, et

$$R = \{(i, j) \in M^2 \mid i \leq j\}$$

(inégalité au sens usuel). C'est une relation d'ordre totale (justifier !).

**Exemple 4.2.3.** Soit $A$ un ensemble et $M = \mathcal{P}(A)$ son ensemble de parties. Alors on pose :

$$bRc \qquad \text{ssi} \qquad b \subset c$$

définit une relation d'ordre sur $M$ (relation d'inclusion), qui n'est pas totale. Par exemple, si $A = \{1, 2, 3\}$, et $a = \{1, 2\}$ et $b = \{2, 3\}$, on n'a ni $a \leq b$ ni $b \leq a$.

**Définition 4.2.4.** Si $\leq$ est une relation d'ordre, on définit la relation $<$ par :

$a < b$ ssi ($a \leq b$, et $a \neq b$).

**Définition 4.2.5.** Si $\leq$ est une relation d'ordre, et $(a, b) \in M^2$, on définit les intervalles

$$[a, b] := \{x \in M \mid a \leq x \text{ et } x \leq b\}, \qquad ]a, b[:= \{x \in M \mid a < x \text{ et } x < b\}.$$

**Remarque 4.2.6.** Cette définition semble évidente, mais elle donne lieu à des questions profondes, qui sont importantes en analyse : par exemple, a priori, l'ensemble $I = \{x \in \mathbb{R} \mid x^2 < 2\}$ n'est pas défini comme un intervalle. Et pourtant, on aurait envie de dire que c'en est un, à savoir $]-\sqrt{2}, \sqrt{2}[$....

## 4.3 Relations d'équivalence

C'est un autre type de relation très important, $xRy$ formalisant l'idée que « $x$ et $y$ ont une certaine propriété en commun » :

**Définition 4.3.1.** Une relation $R$ sur $M$ est dite *relation d'équivalence* sur $M$ si elle est

1. *symétrique*,
2. *réflexive*,
3. *transitive*.

Dans ce cas, on utilise souvent la notation $x \sim y$ au lieu de $xRy$.

**Exemple 4.3.2.** Soit $M$ l'ensemble des étudiants de la promo L1. On définit une relation par : $aRb$ si les étudiants $a$ et $b$ sont dans la même classe (i.e., appartiennent au même groupe de TD). Elle est clairement symétrique, transitive et réflexive.

**Proposition 4.3.3.** *Soit $M = \sqcup_{i=1}^{n} A_i$ une partition de $M$. Alors la relation $R$ définie par :*

$$xRy \quad \textit{ssi} \quad \exists i = 1, \ldots, n : \; x \in A_i \textit{ et } y \in A_i$$

*est une relation d'équivalence sur $M$.*

*Démonstration.* Arguments identitiques à ceux de l'exemple 1 :

1. si $x$ est dans la même classe que $y$, alors $y$ est dans la même classe que $x$ ;
2. tout $x$ est dans la même classe que $x$ ;
3. si $x$ est dans la même classe que $y$, et $y$ dans la même que $z$, alors $x$ est dans la même que $z$.

□

**Théorème 4.3.4.** *Toute relation d'équivalence sur $M$ est donnée par la construction précédente : si $R$ est une relation d'équivalence, il existe une partition de $M$ donnant lieu à $R$ comme dans la proposition 1. Ainsi on peut dire : « partitions et relations d'équivalence sur $M$ sont la même chose ».*

*Démonstration.* Preuve (supposons que $M$ soit un ensemble fini ; mais tout reste valable aussi si $M$ est infini) :

**Définition 4.3.5.** Si $R$ est une relation d'équivalence sur $M$, on note, pour tout $x \in M$, par $[x] = \{y \in M \mid yRx\}$, la *classe d'équivalence* de $x$ (= l'ensemble des éléments qui sont en relation avec $x$).

La clé de la preuve est de montrer : *Soit $x, z \in M$. Alors des deux cas l'un :*

$$\boxed{\text{soit } [x] = [z],\ \text{ soit } [x] \cap [z] = \emptyset}. \qquad (!)$$

En effet, supposons $[x] \cap [z]$ non vide, i.e., il existe $y \in [x] \cap [z]$. Montrons que $[x] \subset [z]$. Soit $u \in [x]$, alors : $uRx, xRy, yRz$, donc $uRz$, donc $u \in [z]$, d'où : $[x] \subset [z]$. Par symétrie, on aura de même $[z] \subset [x]$, donc $[x] = [z]$. Ainsi, on a bien la disjonction de cas (!).

Ensuite, fixons dans chaque classe $[x]$ le choix d'un élément $i \in [x]$, qu'on appellera un *représentant* de la classe (de sorte que $[i] = [x]$ ; penser à $i$ comme une sorte de « délégué de classe »), et soit $I$ l'ensemble de tout ces représentants. Alors on a $M = \cup_{i \in I} A_i$ avec $A_i = [i]$ (réunion disjointe, la partition cherchée). □

**Exemple 4.3.6.** La relation égalité est ue relation d'équivalence. Ses classes d'équivalence sont les singletons (parties ayant un seul élément). C'est la partition « la plus fine possible ».

**Exemple 4.3.7.** La relation totale est une relation d'équivalence. Il n'y a qu'une seule classe : l'ensemble $M$ lui-même. C'est la partition « la plus grossière possible ».

**Exemple 4.3.8.** On peut partitionner les entiers en deux classes : les entiers *paires* (les doubles, $2\mathbb{Z}$) et les entiers *impaires* ($2\mathbb{Z} + 1$).

Idem pour les multiples de 3 : on a une partition en trois parties, $A_0 = 3\mathbb{Z}$, $A_1 = 3\mathbb{Z} + 1$, $A_2 = 3\mathbb{Z} + 2$ (cf. TD 4).

**Remarque 4.3.9.** Ces résultats restent valables au cas des ensembles infinis. On utilise alors souvent les relations d'équivalence pour *définir de nouveaux ensembles*, qu'on appelle « ensemble quotient ». Nous en parlerons plus tard.

# Seconde Partie du cours :
# Les ensembles infinis

La définition, due à Cantor, d'un ensemble quelconque (chapitre 1) ne suppose en aucune manière que l'ensemble $A$ soit fini. Or, si on ne peut pas écrire $A$ sous forme d'une « liste » ou d'un « fichier fini », la question se pose : *comment « définir » ou « décrire » un ensemble infini ?* Dans le cours, nous allons étudier ce problème pour les ensembles infinis « les plus élémentaires » : les ensembles $\mathbb{N}$ et $\mathbb{Z}$ des nombres naturels, respectivement entiers. Une fois ce problème résolu, dans le cours d'analyse on enchaînera pour définir les nombres réels, $\mathbb{R}$, et complexes, $\mathbb{C}$.

L'ensemble $\mathbb{N}$ est absolument fondamental pour toutes les mathématiques. Nous allons *poser comme axiome qu'un ensemble* $\mathbb{N}$ *avec certaines propriétés existe*. Ces propriétés peuvent être formulées de diverses manières – la plus courante est les *axiomes de Peano*. Cependant, Cantor, et ses successeurs (Zermelo, Frankel), ont cherché à jeter les bases à un niveau plus profond encore : il faudra non seulement énoncer les axiomes de $\mathbb{N}$ de façon très précise, mais aussi *toute la théorie des ensembles*. Entrer dans les détails dépasserait le cadre de ce cours ; mais nous expliquerons quelques grandes lignes.

Les ensembles infinis ont des propriétés surprenantes. Par exemple, il existe « autant de nombres naturels que de nombres naturels pairs » (à $n$ on fait correspondre $2n$), et pourtant, il devait y en avoir « moins ». (Pour la petite histoire : l'Hôtel de Hilbert.) D'autres propriétés sont franchement paradoxales : la plus célèbre est le paradoxe de Russell : soit $M$ l'ensemble dont les éléments sont tous les ensembles n'appartenant pas à eux-mêmes :

$$M = \{x \mid x \notin x\}.$$

Alors, est-ce que $M \in M$ ? si oui, par définition $M$ n'est pas dans $M$ ; donc c'est impossible. Mais alors si non, par définition on a $M \in M$ ; donc c'est impossible aussi. En fait, dans le cadre de la logique ce paradoxe est connu depuis l'antiquité : le paradoxe du menteur (Un homme dit : « Je mens maintenant. » Vrai ou faux ? Si vrai, c'est qu'il ne ment pas, donc l'affirmation est fausse. Donc c'est impossible. Alors l'affirmation est fausse : cela veut dire qu'il dit la vérité, i.e., il ment - impossible également.) Il ne faut pas voir en ces paradoxes un simple tour de passe-passe : ce sont de vrais problèmes qui apparaissent quand on manipule de façon trop imprudente des univers de discours *infinis*, qui offrent la possibilité d'*autoréférence* (une phrase fait référence à elle-même). En effet, on constate que les problèmes de la théorie des ensembles infinis et de la logique sont étroitement liés entre eux. Pour cette raison, nous allons évoquer dans cette partie du cours aussi quelques notions fondamentales de la *logique mathématique*.

*Chapitre* 5

# Les nombres naturels $\mathbb{N}$

Le mathématicien Leopold Kronecker a écrit, en 1891, *« les nombres naturels sont la création de Dieu, tout le reste est l'œuvre de l'homme »*. Qu'on soit croyant ou non, il faut fixer, quelque part, un point de départ, considéré comme accepté par tous, pour ce qui concerne les théories mathématiques. Ces fondements s'appellent, en mathématiques, les *axiomes*. Voici les axiomes dits *axiomes de Peano* qui caractérisent les nombres naturels

## 5.1 Les axiomes de Peano, et le principe de récurrence

**Définition 5.1.1.** Les *entiers naturels* sont la donnée d'un ensemble $\mathbb{N}$, d'un élément particulier noté $0 \in \mathbb{N}$, et d'une application $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto s(n)$ ; l'élément $s(n)$ s'appelle le *successeur de* $n$ ; et ces données vérifient les propriétés suivantes :

(P1) $0$ n'est pas un successeur : $s(n)$ est différent de $0$ pour tout $n \in \mathbb{N}$ ;

(P2) l'application $s$ est injective : si $s(n) = s(m)$ pour $n, m \in \mathbb{N}$, alors $n = m$ ;

(P3) soit $M \subset \mathbb{N}$ une partie qui contient $0$ et telle que, si $m \in M$, alors $s(m) \in M$ ; alors on a $M = \mathbb{N}$.

**Remarque 5.1.2.** L'application $s : \mathbb{N} \to \mathbb{N}$ est donc *injective (d'après (P2)) mais pas surjective (d'après (P1))*. Cela confirme que $\mathbb{N}$ *ne peut pas être un ensemble fini* car nous avons vu (« principe des tiroirs ») qu'une application injective $f : M \to M$ d'un ensemble fini $M$ dans lui-même est toujours surjective.

**Notation.** Nous utilisons les symboles usuels : $1 := s(0)$, $2 := s(1)$, $3 := s(2)$, $4 := s(3)$, et nous utilisons aussi la notation : $n + 1 := s(n)$.

L'axiome (P3) permet de justifier le *principe de preuve par récurrence* : supposons que nous conjecturons qu'une certaine proposition (énoncé mathématique) dépendant de $n$ soit vraie, quel que soit $n \in \mathbb{N}$. Pour la prouver, il suffit

– de la démontrer "à la main" pour $n = 0$ ;

– de vérifier que, si elle vraie pour un $n \in \mathbb{N}$, alors elle l'est aussi pour $s(n)$ :

**Théorème 5.1.3** (Principe de récurrence)**.** *Supposons donné, pour tout $n \in \mathbb{N}$, une proposition $P(n)$, telle que*

1. *(initialisation) : la proposition $P(0)$ est vraie ;*
2. *(hérédité) : pour tout $n \in \mathbb{N}$ : [si $P(n)$ est vraie, alors $P(s(n))$ est vraie aussi].*

*Alors $P(n)$ est vraie pour tout $n \in \mathbb{N}$.*

*Démonstration.* On considère l'ensemble $M := \{n \in \mathbb{N} \mid P(n) \text{ est vraie}\}$. D'après (1) et (2), $M$ vérifie les hypothèses de l'axiome (P3) ; donc, d'après cet axiome, on a $M = \mathbb{N}$. Donc $P(n)$ est vraie pour tout $n \in \mathbb{N}$. □

**Exemple 5.1.4.** Soit $P(n)$ la proposition : *pour tout nombre réel ou complexe $a$ tel que $a \neq 1$,*

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

Initialisation : $P(0)$ revient à $a^0 = \frac{1-a^1}{1-a}$ ; c'est évidemment vrai (car $a^0 = 1$).

Hérédité : supposons que $P(n)$ soit vraie pour un $n \in \mathbb{N}$ (hypothèse de récurrence).

Montrons que $P(s(n))$ est vraie : en effet

$$\begin{aligned}
\sum_{k=0}^{s(n)} a^k &= \sum_{k=0}^{n} a^k + a^{s(n)} \\
&= \frac{1 - a^{s(n)}}{1 - a} + a^{s(n)} \quad \text{(par hypothèse de récurrence)} \\
&= \frac{1 - a^{s(n)} + (1 - a)a^{s(n)}}{1 - a} \\
&= \frac{1 - a^{s(n)}a}{1 - a} = \frac{1 - a^{s(n)+1}}{1 - a} = \frac{1 - a^{s(s(n))}}{1 - a}
\end{aligned}$$

donc $P(s(n))$ est vraie. Par le principe de récurrence, $P(n)$ est donc vraie pour tout $n \in \mathbb{N}$.

Sous-entendue dans ce raisonnement est la *définition des puissances* : on définit $a^0 := 1$, puis $a^{s(n)} := a^n \cdot a$ ; ainsi la puissance $a^n$ est définie pour tout $n \in \mathbb{N}$ (par récurrence).

On écrira désormais plutôt $n + 1$ au lieu de $s(n)$ ; la formule précédente, si $a \neq 1$,

$$\boxed{\sum_{k=0}^{n} a^k = \frac{1 - a^{n+1}}{1 - a}}$$

s'appelle la *formule de la somme géométrique*. Voir TD pour d'autres exemples !

**Exemple 5.1.5.** *Tout entier naturel non-nul $x$ admet un prédécesseur, i.e., $\exists y \in \mathbb{N}$ : $x = s(y)$.*

En effet, soit $S = \{x \in \mathbb{N} | \, x = 0 \text{ ou } \exists y \in \mathbb{N} : x = s(y)\}$. Clairement, $0 \in S$ ; et si $n \in S$, alors $x = s(n) \in S$ (en prenant $y = n$), donc d'après (P3), on a $S = \mathbb{N}$.

**Remarque 5.1.6.** Si l'initialisation se fait au rang $1$ (ou $2$ ou...), et l'héridité est vérifiée pour tout $n$ sauf $0$ (sauf $0$ et $1$...), alors $P(n)$ est vrai pour tout $n$ à partir du rang $1$, etc.

**Remarque 5.1.7.** Comme tous les mathématiciens, nous supposons qu'*un système* $(\mathbb{N}, 0, s)$ *vérifiant les axiomes de Peano existe* – nous ne cherchons pas à *démontrer* ce fait. En revanche, on peut prouver que, si un tel ensemble existe, alors il est *unique*, dans un sens à préciser : il ne peut pas y être "deux espèces différentes" de nombres naturels.

## 5.2 Addition et multiplication dans $\mathbb{N}$

Nous avons défini $n+1 := s(n)$ et $2 = s(1) = 1+1$. On définit maintenant

$$n+2 := s(s(n)) = (n+1)+1.$$

Ainsi $n+(1+1) = (n+1)+1$ pour tout $n \in \mathbb{N}$. Par récurrence, nous définissons : soit $k \in \mathbb{N}$; on pose $k+0 := k$, et si $k+n$ pour un $n \in \mathbb{N}$ est déjà défini, on pose

$$k + s(n) := s(k+n).$$

Autrement dit, $k+(n+1) := (k+n)+1$. Par (P3), on a ainsi défini la *somme* $k+n$ pour tout $n \in \mathbb{N}$.

**Théorème 5.2.1** (associativité)**.** *Pour tous* $k, m, n \in \mathbb{N}$,

$$\boxed{k+(m+n) = (k+m)+n}.$$

*Démonstration.* par récurrence : soit $P(n)$ la proposition « pour tout $k$ et $m$ dans $\mathbb{N}$, l'égalité $k+(m+n) = (k+m)+n$ est vraie ».

$P(0)$ est vrai car $k+(m+0) = k+m = (k+m)+0$, pour tout $k$ et $m$. Par ailleurs, $P(1)$ est vraie comme vue ci-dessus.

Supposons que $P(n)$ est vraie. Alors, $\forall k, m \in \mathbb{N}$ :

$$\begin{aligned} k+(m+(n+1)) &= k+((m+n)+1) && \text{(par le cas } n=1 \text{ déjà prouvé)} \\ &= (k+(m+n))+1 && \text{(par le cas } n=1 \text{ déjà prouvé)} \\ &= ((k+m)+n)+1 && \text{(par hypothèse de récurrence)} \\ &= (k+m)+(n+1) && \text{(par le cas } n=1 \text{ déjà prouvé).} \end{aligned}$$

Donc $P(n+1)$ est vraie aussi.

Par le principe de récurrence, $P(n)$ est donc vraie pour tout $n \in \mathbb{N}$. □

**Théorème 5.2.2** (commutativité)**.** *Pour tous* $m, n \in \mathbb{N}$,

$$\boxed{n+m = m+n}.$$

*Démonstration.* Par exemple, $2+1 = (1+1)+1 = 1+(1+1) = 1+2$. Montrer d'abord par récurrence que $n+1 = 1+n$ pour tout $n \in \mathbb{N}$, puis par une autre récurrence que $k+n = n+k$ (cf. TD). □

Ensuite, nous définissons par récurrence le *produit*

$$0\cdot m = 0, \quad 1\cdot m = m, \quad 2\cdot m := m+m, \quad 3\cdot m := 2\cdot m+m, \quad 4\cdot m := 3\cdot m+m,$$

et si $n \cdot m$ est déjà défini, on pose

$$(n+1)\cdot m := n\cdot m + m.$$

Ainsi $n \cdot m$ est défini pour tout $(n, m) \in \mathbb{N}^2$. On écrit souvent $mn$ au lieu de $n \cdot m$.

**Théorème 5.2.3** (règles de calcul)**.** *Pour tous $k, m, n, p, q \in \mathbb{N}$,*

*(D) distributivité : $k(m+n) = km + kn$,*

*(A) associativité : $k(mn) = (km)n$*

*(C) commutativité : $mn = nm$,*

*(S) règle de simplification additive : $p + m = q + m \Rightarrow p = q$,*

*(S') règle de simplification multiplicative : si $m \neq 0$, alors : $pm = qm \Rightarrow p = q$.*

*Démonstration.* On utilise les mêmes principes que ci-dessus – cf. TD. □

Utilisant l'associativité, on peut omettre des parenthèses dans les sommes

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$$

avec $a_i \in \mathbb{N}$, et dans les produits

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdots a_n.$$

Plus généralement, si $I$ est un ensemble *fini* d'indices (quelconque : pas forcément d'entiers), et $a_i \in \mathbb{N}$ est donné pour tout $i \in I$, on peut définir les sommes, resp. produits, de tout ces éléments, car le résultat ne dépend ni de l'ordre ni de la façon de regrouper les termes ; on note ces sommes, resp. produits, par

$$\sum_{i\in I} a_i, \qquad \prod_{i\in I} a_i.$$

**Proposition 5.2.4.** *La seule solution de l'équation $p + q = 0$ dans $\mathbb{N}$ est $p = q = 0$.*

*Démonstration.* Il s'agit d'une *preuve par l'absurde* : supposons que $p + q = 0$ et $q \neq 0$. D'après l'exemple 5.1.5, $q$ admet alors un prédécesseur : $\exists m \in \mathbb{N}$, $q = s(m) = m+1$. Donc $0 = p+q = (p+m)+1$ admet un prédécesseur – mais ceci est en contradiction avec l'axiome (P1). Ainsi l'hypothèse que $p + q = 0$ avec $q \neq 0$ mène à une contradiction logique ; il faut donc qu'elle est fausse. □

Remarque : cf. TD pour une autre preuve célèbre qui procède par l'absurde – celle d'Euclide, prouvant qu'il existe une infinité de nombres premiers.

## 5.3 La relation d'ordre sur $\mathbb{N}$

**Définition 5.3.1.** Soit $(m, n) \in \mathbb{N}^2$. On écrira $m \leq n$ s'il existe $p \in \mathbb{N}$ tel que $n = m + p$.

**Lemme 5.3.2** (règles de calcul)**.** *La relation $\leq$ sur $\mathbb{N}$ vérifie :*

*(1)* $\forall n \in \mathbb{N} : 0 \leq n$,

*(2) si $p \leq q$ et $n \in \mathbb{N}$, alors $p + n \leq q + n$ et $np \leq nq$.*

*Démonstration.* (1) On écrit $n = 0 + n$.

(2) Soit $q = p + k$ avec $k \in \mathbb{N}$. Alors, d'après les règles de calcul (théorème 5.2.3), $q + n = p + k + n = (p + n) + k$, et $nq = n(p + k) = np + nk = np + \ell$ avec $\ell = nk \in \mathbb{N}$. □

**Théorème 5.3.3.** *La relation $\leq$ est une relation d'ordre total sur $\mathbb{N}$.*

*Démonstration.* Vérifions

- Réflexivité : $n \leq n$ clair (prendre $p = 0$)
- Transitivité : si $k \leq m$ et $m \leq n$, alors $m = k + p$, $n = m + q$, donc $n = (k + p) + q = k + (p + q)$, donc $k \leq n$.
- Antisymétrie : soit $m \leq n$ et $n \leq m$, donc $n = m + p$ et $m = n + q$, donc $n = (n + q) + p = n + (p + q)$. D'après la règle de simplification, il s'ensuit que $p + q = 0$. D'après la proposition 5.2.4, il s'ensuit que $p = q = 0$, donc $m = n$.
- Totalité : pour $n \in \mathbb{N}$, posons

$$S_n := \{m \in \mathbb{N} \mid m < n\} \cup \{n\} \cup \{m \in \mathbb{N} \mid n < m\}$$

et montrons par récurrence que $S_n = \mathbb{N}$. L'initialisation vient du fait que $0 \leq m$ pour tout $m \in \mathbb{N}$, et l'hérédité se démontre à l'aide de la règle de calcul $p < q \Rightarrow p + 1 < q + 1$.

Ainsi $\leq$ vérifie les 4 propriétés définissant une relation d'ordre total. □

**Proposition 5.3.4.** *Soit $A \subset \mathbb{N}$ une partie non-vide. Alors il existe un* plus petit élément dans $A$. *En une formule mathématique :* $\exists k \in A : \forall a \in A : k \leq a$.

*Démonstration.* Supposons que $A$ n'a pas de plus petit élément. Soit alors $P(n)$ l'affirmation : $\forall k = 0, \ldots, n : k \notin A$. Alors $P(0)$ est vraie (sinon, $0$ serait le plus petit élément de $A$). Supposons $P(n)$ es vraie ; alors $P(n + 1)$ est vraie aussi (car si $k \notin A$ pour $k = 0, \ldots, n$, alors $n + 1$ serait le plus petit élément). Par le principe de récurrence, $P(n)$ est vraie pour tout $n \in \mathbb{N}$. Donc $A$ est vide. Par contraposé, si $A$ est non vide, alors $A$ admet un plus petit élément. □

La propriété précédente se résume en disant que *la relation $\leq$ est un bon ordre sur $\mathbb{N}$*. Une fois ces règles de calcul (« bien connues ») posées, on peut procéder à des choses plus intéressantes : définir les nombres premiers, prouver que tout entier naturel se factorise de façon unique en nombres premiers, et étudier ces propriétés, i.e., faire de l'*arithmétique*. Ce sera l'objet d'une option de maths en S2. Cf. aussi TD.

*Chapitre 6*

# Nombres

Suivant la phrase de Kronecker, une fois posé les axiomes de $\mathbb{N}$, c'est « l'œuvre de l'homme » de construire les « ensembles des nombres usuels », de plus en plus grands :

1. les entiers relatifs $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
2. les nombres rationnels $\mathbb{Q}$ (fractions $r = \frac{m}{n}$ avec $m, n$ des entiers relatifs et $n \neq 0$),
3. les nombres réels $\mathbb{R}$ (« tous les nombres de la droite réelle »),
4. les nombres complexes $\mathbb{C}$ (« tous les nombres du plan d'Argand »)

En général, on entend par « nombres » en mathématiques un ensemble $\mathbb{K}$, dont les éléments sont appelés des nombres, muni d'opérations, *addition* $+$ et *multiplication* $\times$, ou $\cdot$, vérifiant certaines propriétés. Pour prouver que ces nombres « existent »,

– soit qu'on pose ces propriétés comme « axiomes » (approche axiomatique),

– soit qu'on base la théorie sur celle de $\mathbb{N}$ (approche par construction) :

en supposant que l'existence de $\mathbb{N}$ est acquise, on *construit les nombres* $\mathbb{K}$ *à partir de* $\mathbb{N}$, via certaines constructions venant de la théorie des ensembles (produit cartésien ; relations d'équivalence,...). Pour $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, c'est tout à fait possible – l'étape la plus difficile est de *construire* $\mathbb{R}$ *à partir de* $\mathbb{Q}$ (la construction des nombres réels est un sujet intéressant, qui n'est malheureusement pas au programme des études universitaires, car jugé trop long et technique – pour abréger, on introduit, au cours d'analyse 1 en S2, les nombres réels de façon axiomatique). En revanche, il n'est pas trop difficile de construire $\mathbb{Z}$ à partir de $\mathbb{N}$, puis $\mathbb{Q}$ à partir de $\mathbb{Z}$. Vous allez voir ces constructions aux cours d'algèbre de Licence ; elles ne font pas objet de ce cours, mais il est utile d'en avoir un aperçu dès maintenant.

## 6.1 Construction de $\mathbb{Z}$ : idée

Nous avons vu que l'équation $a + x = b$ n'admet pas toujours de solution dans $\mathbb{N}$ : elle en admet une si $a \leq b$, mais non si $b < a$. Or, on aimerait bien

pouvoir dire qu'il existe *toujours* une solution – pour cela, il faut agrandir l'ensemble $\mathbb{N}$ en l'ensemble $\mathbb{Z}$ des *entiers relatifs*. On notera alors cette solution (qui sera unique), $x = b - a$. Ainsi, si cet ensemble de nombres $\mathbb{Z}$ existe, on aura une application

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}, \quad (a, b) \mapsto b - a.$$

Cette application sera surjective (car on aura bien $m = m - 0 = f((0, m))$), mais non injective : pour $m \in \mathbb{Z}$, la *fibre* $f^{-1}(m)$ est l'ensemble $[m] := \{(a, b) \in \mathbb{N}^2 \mid b - a = m\}$. On pourra dire que le couple $(a, b) \in \mathbb{N}^2$ "représente" l'entier $m$ ; et deux couples $(a, b), (a', b')$ représentent le même entier si $a - b = a' - b'$, autrement dit, si $a + b' = a' + b$.

Dit encore autrement, la relation $R$ sur $M = \mathbb{N}^2$ définie par :

$$(a, b)R(a', b') \qquad \text{ssi} \qquad a + b' = a' + b$$

devait être une *relation d'équivalence*, et $\mathbb{Z}$ devait s'identifier à *l'ensemble des classes d'équivalence de cette relation*. Et en effet, ce programme permet de *construire $\mathbb{Z}$ via une relation d'équivalence $R$ sur $\mathbb{N}^2$* : voir TD, et Annexe 1 du cours pour quelques détails de plus. Par cette construction, on obtient un ensemble ayant les propriétés suivantes :

**Théorème 6.1.1.** *Les entiers relatifs $\mathbb{Z}$ forment un ensemble, muni d'un élément particulier noté $0$, et de deux opérations $+$ et $\cdot$ associant à deux nombres un troisième, vérifient les propriétés d'un* anneau commutatif, *i.e.,*

1. *addition et multiplication sont* associatives et commutatives,
2. *ces opérations sont* distributives *entre elles ;*
3. *$0$ est neutre pour l'addition : $\forall m \in \mathbb{Z}$, $0 + m = m$,*
4. *pour tout $(m, n) \in \mathbb{Z}^2$, l'équation $m + x = n$ admet une unique solution (qu'on note $x = n - m \in \mathbb{Z}$) ;*

*de plus cet anneau est* ordonné *: il existe une* relation d'ordre total $\leq$ *sur $\mathbb{Z}$, telle que*

1. *$\forall a, b, c \in \mathbb{Z}$ : $a \leq b \Rightarrow a + c \leq b + c$,*
2. *$\forall a, b, c \in \mathbb{Z}$ : ($a \leq b$ et $0 \leq c$) $\Rightarrow ac \leq bc$.*

*Finalement, on a une bijection "canonique" entre $\mathbb{Z}^+ = \{m \in \mathbb{Z} \mid 0 \leq m\}$ et $\mathbb{N}$.*

Toutes ces propriétés ensemble caractérisent $\mathbb{Z}$ de façon unique, et peuvent donc être utilisées pour définir $\mathbb{Z}$ "axiomatiquement".

## 6.2 Construction de $\mathbb{Q}$ : idée

Dans $\mathbb{Z}$, on ne peut pas toujours résoudre des équations du type $ax = b$ : une solution $x = \frac{b}{a}$ serait une *fraction d'entiers* ; si $a = 1$ ou $a = -1$, c'est un entier, mais pas dans les autres cas (et si $a = 0$ elle n'est pas définie, car $0x = 0$ pour tout $x$). On veut donc agrandir le domaine des nombres encore une fois, pour qu'on puisse diviser par tout nombre non-nul. Ce genre de « domaine de nombres » joue un rôle très important en maths :

**Définition 6.2.1.** Un *corps* est un ensemble $\mathbb{K}$, tel que pour tout $(a, b) \in \mathbb{K}^2$ soient définis

– la somme $a + b \in \mathbb{K}$,

– le produit $ab \in \mathbb{K}$,

– la différence $a - b \in \mathbb{K}$,

– si $b \neq 0$, le quotient $\frac{a}{b} \in \mathbb{K}$,

et tel que toutes les lois usuelles (associativité, commutativité, distributivité,...) du calcul littéral des 4 opérations soient vérifiées. Il existe un élément neutre $0$ pour l'addition, et un élément neutre $1$ pour la multiplication.

Les corps les plus importants sont $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ; mais il y en a beaucoup d'autres (cours d'algèbre de L2-L3....). On peut prouver que *si $\mathbb{Z}$ existe, alors $\mathbb{Q}$ existe aussi*, en construisant le corps $\mathbb{Q}$ selon la même méthode qu'au paragraphe précédent : si $\mathbb{Q}$ existe, alors on a une application (surjective)

$$f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}, \quad (a, b) \mapsto \frac{a}{b}.$$

On a $f((a, b)) = f((a', b'))$ ssi $\frac{a}{b} = \frac{a'}{b'}$, ssi $ab' = a'b$. Ceci définit une relation d'équivalence, et on pourra définir $\mathbb{Q}$ comme l'ensemble de classes d'équivalences. De plus, par les règles du calcul littéral

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc},$$

on saura comment il faut définir les 4 opérations sur de telles classes. Voir Annexe 2 pour plus de détails. Voici le résultat :

**Théorème 6.2.2.** *Les nombres rationnelles $\mathbb{Q}$ forment un corps qui est* ordonnée, *i.e., muni d'un ordre total $\leq$ tel que :*

1. *si $a \leq b$, alors pour tout $c \in \mathbb{Q}$, on a : $a + c \leq b + c$,*
2. *si $a \leq b$ et $c \geq 0$ dans $\mathbb{Q}$, alors $ac \leq bc$.*

*De plus, $\mathbb{Q}$ contient $\mathbb{Z}$ comme partie ; et tout élément de $\mathbb{Q}$ est de la forme $q = \frac{m}{n}$ avec $m \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.*

Là aussi, ces propriétés caractérisent $\mathbb{Q}$ de façon unique, et pourrait servir à le définir axiomatiquement.

## 6.3 Calcul dans $\mathbb{Z}$ et $\mathbb{Q}$

Tout ce qui relève des « règles du calcul littéral des 4 opérations » est valable dans tout corps (dont $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$). En particulier :

**Définition 6.3.1.** Dans tout corps ou anneau commutatif $\mathbb{K}$, *sommes et produits de plusieurs éléments* sont définis comme nous l'avons fait dans $\mathbb{N}$ ; et de même, les *signes somme* $\sum_{i \in I}$ et *signe produit* $\prod_{i \in I}$, pour tout ensemble fini d'indices, sont définies comme nous l'avons fait dans $\mathbb{N}$.

En revanche, il existe des propriétés qui sont spécifiques à $\mathbb{Q}$ : on a déjà vu une propriété, à savoir que $\mathbb{Q}$ est un corps *ordonné*.

**Théorème 6.3.2.** *Dans un corps ordonné, les carrés sont positifs :* $\forall a \in \mathbb{Q}$, $a^2 \geq 0$.

*Démonstration.* par disjonction de cas : soit, $a \geq 0$, alors $a^2 \geq 0$ par l'item 2 du théorème 1 précédent. Soit $a < 0$. Alors $0 < -a$ par l'item 1, et alors $0 < (-a) \cdot (-a)$ par l'item 2. Or $(-a)(-a) = a^2$ (calcul littéral), donc encore $a^2 \geq 0$. □

**Corollaire 6.3.3.** *Le corps* $\mathbb{C}$ *n'est pas un corps ordonné.*

*Démonstration.* Si $\mathbb{C}$ était ordonné, on aurait, d'une part, $-1 = i^2 > 0$ ; d'autre part, $-1 < 0$ : contradiction ! □

Bien sûr, $\mathbb{R}$ sera un corps ordonné, comme $\mathbb{Q}$. Alors, que distingue $\mathbb{R}$ de $\mathbb{Q}$ ?

**Théorème 6.3.4.** *Il n'existe aucun nombre* $c \in \mathbb{Q}$ *tel que* $c^2 = 2$.

*Démonstration.* cf. TD ! □

On "sait" qu'il existe $c = \sqrt{2}$ dans $\mathbb{R}$ ; ainsi on a trouvé une propriété qui distingue $\mathbb{Q}$ de $\mathbb{R}$. Cependant, $\mathbb{R}$ n'est pas le seul corps qui a cette propriété (cf. TD). On peut aller plus loin et dire que $\mathbb{R}$ *contient toutes les racines de tous les entiers positifs*. Mais là encore, il existe d'autres corps qui ont cette propriété (cours d'algèbre de L2-L3). Alors, quelle est "la" propriété qui distingue $\mathbb{R}$ de $\mathbb{Q}$ ? En fait, il s'agit d'une propriété d'analyse, et non d'algèbre, et elle sera précisée en cours d'analyse de S2 : le corps $\mathbb{R}$ est *un corps ordonné complet* ; le mot "complet" signifie que $\mathbb{R}$ réalise la droite numérique "continue", "sans trou" (tandis que $\mathbb{Q}$ n'est pas complet : au lieu où devait se trouver le nombre $\sqrt{2}$, il n'y a rien, il y a un "trou"). Pour bien comprendre cette propriété, il faudra mobiliser à peu près tous les fondements qu'on vient de poser dans ce cours... et alors cela permettra de définir de "nouveaux nombres", comme $e$ ou $\pi$, qui n'existent pas dans $\mathbb{Q}$, et qui sont définis par des propriétés d'analyse.

*Chapitre 7*

# Théorie des ensembles

Avec la définition de $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ nous sommes entrés dans le « royaume des ensemble infinis ». C'est le moment d'évoquer quelques questions de fondements des maths : la *théorie des ensembes* est précisément la « théorie mathématique de l'infini ». La découverte révolutionnaire de Cantor était qu'il existent *plusieurs infinis*, et qu'il est possible d'en dire des choses précises en langage mathématique.

## 7.1 Équipotence ; ensembles dénombrables

Pour comparer la « taille » de deux ensembles, on définit :

**Définition 7.1.1.** Deux ensembles $A$ et $B$ sont dits *équipotents*, ou : *de même cardinalité*, s'il existe une application bijective $f : A \to B$. On écrit alors $\mathrm{card}(A) = \mathrm{card}(B)$.

**Remarque 7.1.2.** Nous avons les propriétés d'une relation d'équivalence (réflexif, symétrique, transitif) :

— $\mathrm{card}(A) = \mathrm{card}(A)$ (prendre $f = \mathrm{id}_A$),
— $\mathrm{card}(A) = \mathrm{card}(B)$ ssi $\mathrm{card}(B) = \mathrm{card}(A)$ (prendre $f^{-1} : B \to A$),
— si $\mathrm{card}(A) = \mathrm{card}(B)$ et $\mathrm{card}(B) = \mathrm{card}(C)$, alors $\mathrm{card}(A) = \mathrm{card}(C)$ (prendre $h = g \circ f$).

**Définition 7.1.3.** Un ensemble $A$ est fini, de cardinal $n \in \mathbb{N}$ si $A$ est équipotent à $\{1, \ldots, n\}$. Un ensemble $A$ est dit dénombrable s'il est équipotent à $\mathbb{N}$.

**Exemple 7.1.4. (cf TD).**

1. L'ensemble $2\mathbb{N}$ des nombres naturels *pairs* est dénombrable : montrer que $f : \mathbb{N} \to 2\mathbb{N}$, $n \mapsto 2n$ est bijective (TD). Ainsi $2\mathbb{N}$ est une partie strictement incluse dans $\mathbb{N}$, qui pourtant a le même cardinal que $\mathbb{N}$.
2. L'ensemble $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ est dénombrable : l'application $S : \mathbb{N} \to \mathbb{N}^*$, $n \mapsto S(n) = n + 1$ est bijective.
3. L'ensemble $A = \{n^2 \mid n \in \mathbb{N}\}$ est dénombrable : montrer que l'application $f : \mathbb{N} \to A$, $n \mapsto n^2$ est bijective.
4. $\mathbb{Z}$ est dénombrable. (Construire une bijection $f : \mathbb{N} \to \mathbb{Z}$, cf. TD.)

5. Les ensembles $A = \{1, 2\}$ et $B = \{1, 2, 3\}$ ne sont pas équipotents. (Il n'existe pas de bijection entre $A$ et $B$, cf. corollaire 3.4.5. : plus généralement, d'après le corollaire 3.4.5, un ensemble *fini* $M$ n'est jamais équipotent à une partie $A \subset M$, $A \neq M$.

Comparez les exemples 1. et 5. : un ensemble fini $M$ n'est jamais équipotent à une partie stricte $A \subset M$ (i.e., $A \neq M$), tandis que pour un ensemble *infini*, ceci est possible. En fait, cette propriété permet de distinguer les ensembles infinis des ensembles finis ! En imaginant un « hôtel avec un nombre dénombrable de chambres », David Hilbert à illustré cette propriété paradoxale (cf. TD).

**Définition 7.1.5.** On écrit $\mathrm{card}(A) \leq \mathrm{card}(B)$ s'il existe une application *injective* $f : A \to B$.

Pour justifier cette notation, il faudrait vérifier les 3 propriétés (a) transitive, (b) réflexive, (c) antisymétrique. La vérification de (a) et (b) est facile (vu en TD : la composée d'applications injectives est injective ; $\mathrm{id}$ est injective), et celle de (c) beaucoup plus difficile (dans le cas de cardinalité infinie ; dans le cas de cardinalité finie c'est un exercice facile) :

**Théorème 7.1.6** (de Cantor-Bernstein)**.** *Si* $\mathrm{card}(A) \leq \mathrm{card}(B)$ *et* $\mathrm{card}(B) \leq \mathrm{card}(A)$*, alors* $\mathrm{card}(A) = \mathrm{card}(B)$*. Autrement dit, s'il existe* $f : A \to B$*, et* $g : B \to A$*, les deux injectives, alors il existe aussi* $h : A \to B$*, bijective.*

## 7.2 L'argument diagonal de Cantor

Nous avons vu que l'ensemble $\mathbb{N}$ est infini. Existe-t-il d'autres ensembles infinis – à part ceux qui sont dénombrables, comme $\mathbb{Z}$, etc. ? Autrement dit, *existe-t-il des ensembles $A$ « de cardinal strictement plus grand que celui de $\mathbb{N}$ », dans le sens que $A$ n'est pas fini et* $\mathrm{card}(A) \neq \mathrm{card}(\mathbb{N})$ *?* La réponse, due à Cantor, est « oui » : par exemple, $A = \mathbb{R}$ est d'un infini plus grand que celui de $\mathbb{N}$.

Mais avant de penser à $\mathbb{R}$, on pourrait penser que l'ensemble $\mathbb{N} \times \mathbb{N}$ est déjà « bien plus grand que $\mathbb{N}$ ». En fait, cette impression trompe :

**Théorème 7.2.1.** *L'ensemble* $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ *est dénombrable.*

*Démonstration.* Voici deux preuves différentes :

1. Comme tout nombre naturel (non-nul) s'écrit $n = 2^k(2m + 1)$ avec $(k, m) \in \mathbb{N}^2$ (en faisant sortir la plus grande puissance de 2 qui divise $n$), on a une application surjective

$$\mathbb{N}^2 \to \mathbb{N}^*, \quad (k, m) \mapsto 2^k(2m + 1).$$

Elle est aussi injective (car $2^k(2m + 1) = 2k'(2m' + 1)$ implique $k = k'$ par unicité de la décomposition en facteurs premiers, et donc aussi $m = m'$), donc c'est une bijection. Comme $\mathbb{N}^*$ est dénombrable, $\mathbb{N}^2$ l'est donc aussi.

2. (TD) Montrer que l'application $f : \mathbb{N}^2 \to \mathbb{N}$ définie par

$$f((x, y)) = \frac{(x + y + 1)(x + y)}{2} + y$$

est bijective. Faire une figure : noter à coté de chaque couple $(x, y) \in \mathbb{N}^2$ dans le plan son « numéro » $f((x, y))$. □

**Remarque 7.2.2.** De manière analogue, on montre : *Les nombres rationnels* $\mathbb{Q}$ *sont dénombrables.* En effet, numéroter les couples $(a, b)$, et numéroter les fractions $\frac{a}{b}$ avec $a \in \mathbb{Z}, b \in \mathbb{Z}^*$, est presque la même tâche.

Alors, jusque-là nous n'avons pas trouvé d'ensemble qui soit de cardinal plus grand que $\mathbb{N}$. Y en-a-til ? La réponse est « oui », et la méthode pour le démontrer est le célèbre *argument de la diagonale de Cantor* :

**Théorème 7.2.3.** *L'ensemble* $\mathcal{P}(\mathbb{N})$ *de toutes les parties de* $\mathbb{N}$ *n'est pas dénombrable.*

*Démonstration.* Il s'agit d'une *preuve par l'absurde* : supposons que $\mathcal{P}(\mathbb{N})$ soit dénombrable – i.e., qu'il existe une bijection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Autrement dit, on peut faire une liste $A_1 = f(1)$, $A_2 = f(2), \ldots$ de *toutes* les parties de $\mathbb{N}$. Pour montrer que ceci est absurde, Cantor considère la partie

$$M := \{m \in \mathbb{N} \mid m \notin A_m\} \subset \mathbb{N},$$

et il montre que $M \neq A_n$, quel que soit $n$. Sinon, il existerait $n \in \mathbb{N}$ tel que $M = A_n$. Alors forcément on serait dans l'un des deux cas suivants : (a) soit $n \in A_n$, (b) soit $n \notin A_n$. Or, au cas (a), par définition de $M$, il s'ensuit que $n \notin A_n$, donc c'est impossible. Mais au cas (b), toujours par définition de $M$, il s'ensuit que $n \in M$, donc $n \in A_n$, donc c'est également impossible. Ainsi l'hypothèse que $f$ soit surjective est absurde, et Cantor conclut qu'il ne peut pas y être de surjection $\mathbb{N} \to \mathcal{P}(\mathbb{N})$, et donc pas de bijection non plus. Pour que la théorie soit non-contradictoire, il faut donc que $\mathcal{P}(\mathbb{N})$ soit non-dénombrable. □

Ainsi, $M = \mathcal{P}(\mathbb{N})$ vérifie bien $\mathrm{card}(M) > \mathrm{card}(\mathbb{N})$, et de plus

$$(\infty) \qquad \mathrm{card}(\mathbb{N}) < \mathrm{card}(\mathcal{P}(\mathbb{N})) < \mathrm{card}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \ldots$$

Il existe une chaine infinie de cardinaux infinis toujours plus grands ! Cette découverte marqua le véritable début de la théorie des ensembles. Ensuite, Cantor appliqua le même genre de raisonnement pour montrer (cf. https://fr.wikipedia.org/wiki/Argument_de_la_diagonale_de_Cantor) :

**Théorème 7.2.4.** *L'ensemble* $\mathbb{R}$ *des nombres réels n'est pas dénombrable.*

*Problème (dit « du continu »)* : où se trouve le cardinal $\mathbb{R}$ dans la chaine $(\infty)$ ?

Voici un livre qui donne une très bonne introduction à cet univers :

Patrick Dehornoy, *La théorie des ensembles*, Calvage et Mounet, Paris 2017.

## 7.3 Axiomes de la théorie des ensembles

L'argument de la diagonale de Cantor ressemble dans une certaine mesure à celui du « paradoxe de Russell » connu en logique et dont on parlera au chapitre suivant. Et, en effet, il faut être très prudent en utilisant ce genre d'arguments. Pour pouvoir les utiliser correctement, les mathématiciens (dont Zermelo et Frankel dans la suite de Cantor) ont posé une *base axiomatique de la théorie des ensembles (axiomes ZF, ou ZFC)*. Il n'est pas question dans ce cours d'expliquer ces axiomes en détail. Pour plus d'information, cf. par exemple la page wikipedia, ou le livre de Dehornoy cité ci-dessus.

*Chapitre 8*

# Logique et maths

La logique est une branche de la philosophie qui traite de la cohérence de notre discours sur le monde en général, et la *logique mathématique* traite de notre discours concernant les maths en particulier. Ainsi la logique ne fait pas partie des maths, mais elle pose le cadre nécessaire pour commencer à les développer (cf. l'introduction du cours, p.2 et 3).

## 8.1 Propositions et valeurs de vérité

Les mathématiques ont pour objectif d'étudier des *objets mathématiques*, et de *prouver des théorèmes* portant sur ces objets, c'est-à-dire, d'établir la *vérité de certaines propositions* concernant ces objets. En mathématiques, nous appelons proposition un énoncé portant sur des objets mathématiques, et qui a un sens. Cela veut dire que, au moins théoriquement, il devra être possible d'attribuer exactement l'une des deux *valeurs de vérité*, vraie ou fausse, à cet énoncé. Pour une proposition $\alpha$, on notera sa valeur de vérité $v(\alpha) = 0$ si $\alpha$ est fausse et $v(\alpha) = 1$ si $\alpha$ est vraie.[1] Par exemple, « 3 est plus grand » n'est pas une proposition (la phrase est syntaxiquement incomplète : impossible de dire si elle est vraie ou fausse...), et « il pleut » non plus (même si la phrase est syntaxiquement correcte, elle peut être ni vraie ni fausse : par exemple, une goutte par $(km)^2$, c'est de la pluie ou pas ? On n'accepte pas ce genre de situation en maths : une proposition ne peut pas être moitié vraie, moitié fausse...) ; mais « $3^2 + 4^2 = 5^2$ » et « $4^2 + 5^2 = 6^2$ » sont bien des propositions (l'une vraie, l'autre fausse).

## 8.2 Calcul des propositions

Le calcul des propositions porte sur les *connecteurs logiques* : à partir de deux propositions $\alpha$ et $\beta$, on en définit d'autres. D'abord, « non $\alpha$ », notée $\neg\alpha$, la *négation logique de* $\alpha$, est fausse si $\alpha$ est vraie, et vraie si $\alpha$ est fausse : $v(\neg\alpha) = 1$ si $v(\alpha) = 0$, et réciproquement. Ensuite, on définit d'autres propositions

1. On pourrait utiliser deux autres symbôles, comme $v$ et $f$ ; mais le choix des symboles 1 et 0 est judicieux dans beaucoup de domaines, comme par exemple dans l'électronique numérique : 1 = courant passe, 0 = pas de courant, etc.

$\alpha \wedge \beta$ (*conjonction logique* : "$\alpha$ et $\beta$")

$\alpha \vee \beta$ (*disjonction logique* : "$\alpha$ ou $\beta$")

$\alpha \oplus \beta$ (*disjonction exclusive* : "$\alpha$ ou bien $\beta$")

$\alpha \Rightarrow \beta$ (*implication logique* : "$\alpha$ implique $\beta$", "si $\alpha$, alors $\beta$")

$\alpha \Leftrightarrow \beta$ (*équivalence logique* : "$\alpha$ est équivalent à $\beta$", "ssi"),

par la table de vérité suivante (qui, non par hasard, ressemble celle vue en chapitre 2 sur les opérations sur les ensembles) :

| $v(\alpha)$ | $v(\beta)$ | $v(\alpha \wedge \beta)$ | $v(\alpha \vee \beta)$ | $v(\alpha \oplus \beta)$ | $v(\alpha \Rightarrow \beta)$ | $v(\alpha \Leftrightarrow \beta)$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 |

Par exemple, la troisième colonne dit que $\alpha \wedge \beta$ est vraie si $\alpha$ et $\beta$ le sont, et faux dans les autres 3 cas. L'avant-dernière colonne dit que l'implication logique $\alpha \Rightarrow \beta$ est fausse si [$\alpha$ est vraie et $\beta$ est fausse], et elle est vraie dans les autres 3 cas. La dernière colonne dit que $\alpha$ et $\beta$ sont équivalentes si elles ont mêmes valeurs de verité. Il faut dire quelques mots au sujet de l'avant-dernière colonne :

**Théorème 8.2.1.** *Quelles que soient les propositions $\alpha$, $\beta$, les propositions suivantes ont même valeur de vérité et sont donc équivalentes : "$\alpha \Rightarrow \beta$" et "$\neg(\alpha \wedge \neg\beta)$".*

*Démonstration.* En utilisant la table, on constate que $\neg(\alpha \wedge \neg\beta)$ est fausse si $\alpha$ est vraie et $\beta$ est fausse, et vraie dans les autres 3 cas ; ainsi les valeurs de vérité sont les mêmes, ce qui siginifie que ces propositions sont logiquement équivalentes. □

*Commentaire.* Cette définition de l'implication logique $\Rightarrow$ peut paraître étrange : par exemple, la proposition

« si $1 = 0$, alors $4^2 + 5^2 = 6^2$ » est vraie (car $v(\alpha) = 0 = v(\beta)$),

toute comme l'est « si $1 = 0$, alors $3^2 + 4^2 = 5^2$ » (car $v(\alpha) = 0$, $v(\beta) = 1$). Mais on peut motiver cette définition en remarquant que la *seule* façon de retorquer une affirmation de type « $\alpha$ implique $\beta$ » est en montrant que $\alpha$ est vraie, mais $\beta$ est fausse. Noter que ceci n'est pas forcément l'interprétation qu'on donne au mot « si » dans la vie réelle, où on suppose le plus souvent qu'il doit y être un « lien de causalité » quand on dit « si $\alpha$ alors $\beta$ ». Or, la notion de « causalité » n'a de sens qu'en présence de celle du temps (la cause « précède » l'effet) ; elle a sa place dans les sciences naturelles, mais non en mathématiques. En effet, on peut douter que les règles du calcul propositionnel ci-dessus s'appliquent à la « logique quotidienne du monde réel » : pourquoi seulement deux valeurs de vérité, 0 et 1 ; comment décider si une proposition portant sur le « monde réel » est vraie ou fausse, etc. ? Les sciences expérimentales doivent tenir compte de cette situation complexe peu claire ; ainsi leurs

règles de déduction et de raisonnement sont souvent différentes de celles utilisées en maths.

A partir de la table, on peut prouver les *lois de la logique formelle* les plus importantes. Le modus ponens, ou *règle de détachement*, est la règle de base du raisonnement logique.

**Théorème 8.2.2** (modus ponens)**.** *Si $\alpha$ et vraie, et $\alpha \Rightarrow \beta$ est vraie, alors $\beta$ est vraie aussi.*

*Démonstration.* Soit $v(\alpha) = 1$ et $v(\alpha \Rightarrow \beta) = 1$. Ce cas de figure correspond uniquement à la deuxième ligne du tableau ; et alors le tableau nous donne que $v(\beta) = 1$. □

**Théorème 8.2.3.** *Quelle que soit la proposition $\alpha$, on a :*

$v(\alpha \vee \neg\alpha) = 1$ *(“$\alpha$ ou non $\alpha$” est toujours vrai : tertium non datur = tiers exclu),*

$v(\alpha \wedge \neg\alpha) = 0$ *(“$\alpha$ et non $\alpha$” est impossible : principe de non-contradiction).*

*Démonstration.* Si $v(\alpha) = 0$, alors $v(\neg\alpha) = 1$, et donc $v(\alpha \vee \neg\alpha) = 1$. Si $v(\alpha) = 1$, alors $v(\neg\alpha) = 0$, et donc $v(\alpha \vee \neg\alpha) = 1$. Dans tous les cas, $v(\alpha \vee \neg\alpha) = 1$. De la même façon, on prouve la deuxième affirmation. □

**Théorème 8.2.4.** *Quelles que soient les propositions $\alpha$, $\beta$, pour chaque item suivant, les propositions ont même valeur de vérité et sont donc équivalentes :*

*(1)* $\neg(\neg\alpha)$ *et* $\alpha$ *(double négation)*

*(2)* $\neg(\alpha \vee \beta)$ *et* $(\neg\alpha) \wedge (\neg\beta)$ *;*
$\neg(\alpha \wedge \beta)$ *et* $(\neg\alpha) \vee (\neg\beta)$ *(lois de de Morgan) ;*

*(3)* $\alpha \Rightarrow \beta$ *et* $(\neg\beta) \Rightarrow (\neg\alpha)$ *(contraposition)*

*(4)* $(\alpha \vee \beta) \vee \gamma$ *et* $\alpha \vee (\beta \vee \gamma)$ *(associativité) ; idem pour* $\wedge$ *;*
$\alpha \vee \beta$ *et* $\beta \vee \alpha$ *(commutativité) ; idem pour* $\wedge$ *;*

*(5)* $\alpha \vee (\beta \wedge \gamma)$ *et* $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ *(distributivité) ;*

*(6)* $\alpha \Leftrightarrow \beta$ *et* $\neg(\alpha \oplus \beta)$*, et* $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$ *(double implication)*

*Démonstration.* À titre d’exemple, voici la preuve de (3) : on dresse les tables de vérité de $\alpha \Rightarrow \beta$ et de $(\neg\beta) \Rightarrow (\neg\alpha)$

| $v(\alpha)$ | $v(\beta)$ | $v(\alpha \Rightarrow \beta)$ | $v(\neg\beta)$ | $v(\neg\alpha)$ | $v(\neg\beta \Rightarrow \neg\alpha)$ |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |

Les valeurs de vérité dans les colonnes 3 et 6 sont les mêmes, d’où l’équivalence des deux propriétés. Et voici la preuve de (6) : dans la colonne $(d)$, on

trouve les valeurs de vérité de $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, dans la colonne $(u)$, celles de $\neg(\alpha \oplus \beta)$, et dans la colonne $(e)$, celles de $\alpha \Leftrightarrow \beta$ :

| $v(\alpha)$ | $v(\beta)$ | $v(\alpha \Rightarrow \beta)$ | $v(\beta \Rightarrow \alpha)$ | $(d)$ | $v(\alpha \oplus \beta)$ | $(u)$ | $(e)$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |

Les valeurs dans les colonnes $(d), (u)$ et $(e)$ sont les mêmes, d'où (6). Pareil pour les autres autres – notez que ces preuves sont presque identiques à celles du théorème 2.1.2, Chap.2, où nous avons explicité le cas d'une des lois de de Morgan, qui correspond au point (2). □

**Exemple 8.2.5.** D'après (6), pour prouver une proposition du type $\alpha \Leftrightarrow \beta$, on procède souvent en démontrant séparement la direction $\beta \Rightarrow \alpha$ (on dit souvent : $\alpha$ est « condition nécessaire » pour $\beta$), puis $\alpha \Rightarrow \beta$ (on dit : $\alpha$ est « condition suffisante » pour $\beta$).

## 8.3 Calcul des prédicats

Un *prédicat* $P(x)$ est une proposition $P$ qui dépend d'une « variable » $x$ : pour quelques $x$, la proposition $P(x)$ peut être vraie, et pour d'autres $x$, elle peut être fausse. Considérons par exemple $P(x) : x^2 \geq x$. Dans le contexte d'une formule mathématique, la variable $x$ appartient toujours à un ensemble, qu'il convient de préciser. Par exemple, dans $P(x) : x^2 \geq x$, si on prend $x \in \mathbb{Z}$, la proposition $P(x)$ est toujours vraie (on écrit : « $\forall x \in \mathbb{Z} : P(x)$ est vraie », ou juste : « $\forall x \in \mathbb{Z} : P(x)$ »), mais si on prend $x \in \mathbb{R}$, elle est vraie pour quelques $x$, et fausse pour d'autres (pouvez-vous dire pour lesquels ?).

En *calcul des prédicats*, ou : *logique de premier ordre*, on étudie les règles d'opération sur ces expressions. Ainsi, en mathématiques, la logique de premier ordre est une combinaison de la théorie des ensembles avec le calcul des propositions. Par exemple, la loi de de Morgan se généralise par la « règle de négation » suivante : la négation de [ $P(x)$ est vraie pour tout $x$ ] est [ il existe un $x$ pour lequel $P(x)$ est fausse ] :

$\neg(\forall x : P(x))$ équivaut à $\exists x : \neg P(x)$

De façon analogue,

$\neg(\exists x : P(x))$ équivaut à $\forall x : \neg P(x)$

Et l'associativité de $\wedge$ et de $\vee$ se traduit par des règles :

$\forall x : (P(x) \wedge Q(x))$ équivaut à $(\forall x : P(x)) \wedge (\forall x : Q(x))$,

$\exists x : (P(x) \vee Q(x))$ équivaut à $(\exists x : P(x)) \vee (\exists x : Q(x))$.

## 8.4 Théorèmes et preuves

Un *théorème* est une affirmation (mathématique ou logique) qui peut être démontrée, c'est-à-dire une assertion qui peut être établie comme vraie au travers d'un raisonnement logique. Un théorème peut être *démontré* de plusieurs façons – par exemple,

– par disjonction de cas,

– par contre-exemple,

– par récurrence,

– par analyse-synthèse,

– par l'absurde.

Il n'y a pas de « méthode générale » : c'est pendant les études de maths qu'on apprend quand et comment on applique ces types de raisonnement – vous en avez déjà vu quelques-uns. Souvent, en cherchant une preuve, on commence par « analyser » la situation (étude de cas particuiers, d'exemples numériques, faire des diagrammes et des figures...) ; la structure logique de la preuve en ressort lentement ; une fois qu'on a compris cette structure, la rédaction de la preuve « part à l'inverse » (i.e., le point de départ de la rédaction sont des principes généraux, et non l'analyse de cas particuliers).

Quant à la structure de l'énoncé du théorème, on distingue :

– les hypothèses, et

– la conclusion.

La forme générale d'un théorème est donc

*si $\alpha$ [hypothèses], alors $\beta$ [conclusion]* , ou :

*Supposons $\alpha$ [hypothèses]. Alors $\beta$ [conclusion].*

Normalement, il faudrait lister toutes les hypothèses pour préciser exactement le point de départ. Dans la pratique, on ne le fait pas toujours ; mais il est important de pouvoir le faire, si besoin est !

Conclusion. Il n'y a pas de « voie royale » pour apprendre à faire des preuves mathématiques – on ne l'apprend qu'en le faisant !

*Annexe* $A$

# Sur la construction de $\mathbb{Z}$

## A.1 Construction de l'ensemble $\mathbb{Z}$

**Lemme A.1.1.** *Nous définissons une relation $R$ sur $M = \mathbb{N}^2$ par :*

$$(a, b)R(a', b') \qquad \textit{ssi} \qquad a + b' = a' + b.$$

*Alors $R$ est une relation d'équivalence.*

Preuve : vérification directe des 3 propriétés (cf. TD)

**Définition A.1.2.** Rappelons la définition de la classe d'équivalence $[x] = \{y \in M \mid xRy\}$, pour tout $x \in M$. Alors on définit $\mathbb{Z}$ comme étant l'ensemble des classes d'équivalence de la relation $R$ définie dans le lemme 1 :

$$\mathbb{Z} = \{[(a, b)] \mid (a, b) \in \mathbb{N}^2\}.$$

D'après la définition, $\mathbb{Z}$ est une certaine partie de $\mathcal{P}(M)$, et on a $[(a, b)] = [(a', b')]$ ssi $a + b' = a' + b$.

**Définition A.1.3.** L'application canonique de $\mathbb{N}^2$ dans $\mathbb{Z}$ est l'application

$$\pi : \mathbb{N}^2 \to \mathbb{Z}, \quad (a, b) \mapsto \pi(a, b) := [(a, b)].$$

On pose ces définitions pour n'importe quelle relation d'équivalence sur n'importe quel ensemble. Alors l'application canonique est *surjective*, car $(a, b)$ est un antécédent de $[(a, b)]$, et les fibres de $\pi$ sont précisément les classes d'équivalence (cf. §1).

## A.2 L'addition dans $\mathbb{Z}$

Expliquons comment additionner deux classes $[(a, b)]$ et $[(c, d)]$ :

**Lemme A.2.1.** *Soit $m = [(a, b)] = [(a', b')]$, $n = [(c, d)] = [(c', d')] \in \mathbb{Z}$. Alors*

$$[(a + c, b + d)] = [(a' + c', b' + d')],$$

*et ainsi l'addition $m + n := [(a + c, b + d)]$ est bien définie, i.e., elle ne dépend pas des représentants des classes $m$ et $n$ qu'on a choisi.*

*Démonstration.* $(a+c)+(b'+d') = (a+b')+(c+d') = (b+a')+(c'+d) = (b+d)+(a'+c')$ □

**Théorème A.2.2.** *L'addition dans $\mathbb{Z}$ a les propriétés suivantes :*

1. *elle est associative,*
2. *elle est commutative,*
3. *elle a un élément neutre $0 = [(0,0)]$,*
4. *l'équation $m + x = n$ admet une unique solution, pour tout $m, n \in \mathbb{Z}$. On la note $x = n - m$.*

*Démonstration.* 1., 2., 3. : direct ; 4. l'unique solution est $[(a,b)] - [(c,d)] = [(a+d, b+c)]$ □

Remarque : le théorème dit que $(\mathbb{Z}, +)$ est un *groupe commutatif*.

## A.3 Relation d'ordre sur $\mathbb{Z}$

**Lemme A.3.1.** *L'application*

$$\kappa : \mathbb{N} \to \mathbb{Z}, \quad n \mapsto [(n,0)]$$

*est injective, et elle vérifie $\kappa(a+b) = \kappa(a) + \kappa(b)$.*

**Définition A.3.2.** Si $n \in \mathbb{N}$, nous allons *identifier* l'entier $[(n,0)]$ avec $n$, et ainsi considérer $\mathbb{N}$ comme une partie de $\mathbb{Z}$. Alors, pour $(m,n) \in \mathbb{Z}^2$, on écrira

$$m \leq n \qquad \text{ssi} \qquad n - m \in \mathbb{N}.$$

**Théorème A.3.3.** *La définition précédente définie une relation d'ordre total sur $\mathbb{Z}$, qui coincide avec celle de $\mathbb{N}$ sur la partie $\mathbb{N} \subset \mathbb{Z}$.*

## A.4 Produit dans $\mathbb{Z}$

Le calcul littéral usuel donne

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

Motivé par cela, on pose :

**Lemme A.4.1.** *Soit $m = [(a,b)] = [(a',b')]$, $n = [(c,d)] = [(c',d')] \in \mathbb{Z}$. Alors*

$$[(ac+bd, ad+bc)] = [(a'c'+b'd', a'd'+b'c')],$$

*et ainsi le produit $m \cdot n := [(ac+bd, ad+bc)]$ est bien défini.*

**Théorème A.4.2.** *Addition et multiplication dans $\mathbb{Z}$ ont les propriétés suivantes :*

1. *$(\mathbb{Z}, +)$ est un groupe commutatif,*
2. *la multiplication est associative et commutative,*
3. *la multiplication a un élément neutre $1 = [(1,0)]$,*

4. *on a la loi de distributivité :* $(k+m)n = kn + mn$.

*Démonstration.* Vérification directe. □

**Définition A.4.3.** On résume les propriétés du théorème précédent en disant que $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

**Remarque A.4.4.** Nous venons de démontrer le "théorème" suivant : *Si* $\mathbb{N}$ *existe, alors* $\mathbb{Z}$ *existe aussi.* Il est important de connaitre ce fait ; mais dans la suite, nous allons "oublier" la construction de $\mathbb{Z}$ par classes d'équivalence : il faut retenir les *propriétés* de $\mathbb{Z}$, et non une construction particulière (il en existe d'autres !). Cependant, le principe général de la construction est très important en maths : souvent, on construit de nouveaux objets en utilisant des relations et classes d'équivalence – la construction des nombres rationnels $\mathbb{Q}$, et celle des nombres réels $\mathbb{R}$ en sont d'autres exemples.

Annexe $B$

# Sur la construction de $\mathbb{Q}$

## B.1 Construction de l'ensemble $\mathbb{Q}$

**Lemme B.1.1.** *Soit $M = Z \times (\mathbb{Z} \setminus \{0\})$. Alors la relation suivante est une relation d'équivalence sur $M$ :*

$$(a, b)R(a', b') \qquad ssi \qquad ab' = a'b.$$

**Définition B.1.2.** Soit $\mathbb{Q}$ l'ensemble des classes d'équivalence de la relation $R$ du lemme 1, et $\pi : M \to \mathbb{Q}$ l'application canonique.

**Théorème B.1.3.** *Pour $[(a, b)], [(c, d)] \in \mathbb{Q}$, les éléments suivants sont bien définis :*

$$\begin{aligned}
[(a, b)] + [(c, d)] &= [(ad + bc, bd)], \\
[(a, b)] - [(c, d)] &= [(ad - bc, bd)], \\
[(a, b)] \cdot [(c, d)] &= [(ac, bd)], \\
[(a, b)] : [(c, d)] &= [(ad, bc)] \qquad (\textit{ si } c \neq 0),
\end{aligned}$$

*et $\mathbb{Q}$ muni de ces 4 opérations est un corps. De plus, l'application*

$$f : \mathbb{Z} \to \mathbb{Q}, \quad m \mapsto [(m, 1)]$$

*est injective et vérifie $f(ab) = f(a)f(b)$ et $f(a + b) = f(a) + f(b)$. On pourra donc identifier $\mathbb{Z}$ avec la partie $\mathrm{im}(f) \subset \mathbb{Q}$, et la classe $[(a, b)]$ avec la fraction $a : b = \frac{a}{b}$.*

*Démonstration.* Les vérifications sont similaires à celles du l'annexe précédent, et nous n'allons pas les détailler ici (en cours d'algèbre de L2-L3 vous allez les revoir ; mot-clef : "corps des fractions"). Signalons juste que, pour montrer que les opérations sont bien définies, nous avons besoin d'une propriété particulière du produit dans $\mathbb{Z}$ : $\mathbb{Z}$ est *intègre* (cf. TD). De même, nous admettons la preuve du théorème suivant : □

**Théorème B.1.4.** *Le corps $\mathbb{Q}$ admet un ordre total $\leq$ tel que :*

1. *si $a, b \in \mathbb{Z}$, alors $a \leq b$ dans $\mathbb{Q}$ ssi $a \leq b$ dans $\mathbb{Z}$ ;*
2. *si $a \leq b$, alors pour tout $c \in \mathbb{Q}$, on a : $a + c \leq b + c$,*

3. *si* $a \leq b$ *et* $c \geq 0$ *dans* $\mathbb{Q}$*, alors* $ac \leq bc$*.*

*Pour résumer, on dit que* $(\mathbb{Q}, \leq)$ *est un* corps ordonné*.*

Pour plus d'informations, sur la construction des entiers et des nombres rationnels et des questions liées, voici quelques pistes de lecture :

https://fr.wikipedia.org/wiki/Nombre_rationnel,

https://fr.wikipedia.org/wiki/Nombre,

https://fr.wikipedia.org/wiki/Entier_naturel,

https://fr.wikipedia.org/wiki/Construction_du_nombre_chez_l%27enfant