ENSEMBLES, APPLICATIONS ET NUMÉRATION

Du fini à l'infini mathématique

MATHESIS
l'Univers Mathématique
1ère année, Semestre I, Cours n°2

Jean Barbet

Ensembles, Applications et Numération

Du Fini à l'Infini Mathématique

Jean Barbet

M A T H E S I S
l'Univers Mathématique
1ère année – Semestre I – Cours no 2

Avant-propos

Présentation de l'auteur

Je m'appelle Jean Barbet, je suis mathématicien indépendant et enseignant en ligne. Docteur en mathématiques, je me suis réorienté après des études en sciences de la vie. A cause de lacunes universitaires j'ai rencontré mes premières difficultés et mes premiers échecs en mathématiques. Pour réussir ma reconversion, j'ai du retravailler par moi-même dans les manuels de référence, choisir ce qui était essentiel, intégrer les connaissances et la pratique, et trouver un sens aux différentes disciplines mathématiques et un lien entre elles, parce que je n'avais pas le temps de refaire tout ce qui m'avait manqué.
J'ai suivi la même méthode pour achever mes études et c'est celle que j'utilise aujourd'hui pour apprendre et créer des mathématiques. La science mathématique possède un sens en elle-même et forme une unité, et ses différents domaines sont profondément liés. Prendre ceci en compte permet d'apprendre, d'assimiler et de comprendre de manière naturelle le noyau de la connaissance mathématique supérieure et tout ce travail m'a permis de compléter mon cursus universitaire jusqu'au Doctorat en mathématiques (obtenu en 2010).
Après plus de dix années d'expérience dans l'enseignement des mathématiques, du collège à l'université et à l'école d'ingénieurs, j'ai rassemblé les résultats de ma synthèse dans un corpus du niveau de la Licence universitaire : Mathesis, l'Univers Mathématique. Avec Mathesis, je veux donner la possibilité, à quiconque veut apprendre sérieusement des mathématiques, d'acquérir le noyau de ce qu'on appelle la mathématique supérieure, c'est-à-dire celle qu'on fait après le lycée et qui correspond à la science mathématique moderne, avec ses concepts et ses méthodes.

Mathesis - l'Univers Mathématique

Le corpus intègre l'essentiel de ce qu'on trouve dans une Licence de mathématiques à l'université, ainsi que des compléments substantiels. Il se divise en trois années, de deux semestres chacune. Il sera publié sous la forme de fascicules correspondant chacun à un cours. Chaque semestre aborde en cinq ou six cours l'ensemble des disciplines et les fascicules. J'ai voulu éviter les écueils habituels liés aux contraintes de l'organisation de l'enseignement supérieur : des cours séparés dans des domaines étanches (Algèbre, Analyse...) et exposant des notions abstraites déconnectées de l'intuition, des exercices techniques trop difficiles et dépourvus de sens.
Dans Mathesis, l'abstraction mathématique, inévitable, est construite pas-à-pas

à partir de l'intuition concrète, comme on apprend aux jeunes enfants au cours élémentaire. Il n'y a pas de domaine étanche, ni plusieurs séries de manuels pour chaque domaine, mais un cursus unique, qui revient cycliquement sur chaque sujet en insistant sur les liens qu'ils entretiennent. Rien n'empêche cependant de choisir un sujet et de ne lire que les fascicules qui s'y rapportent. La pratique, essentielle, est intégrée à la théorie, en ce que des exercices d'un niveau abordable mettent en œuvre directement, à chaque section, ce qui a été exposé dans le cours, et complètent l'apprentissage par l'application des connaissances générales à des situations particulières naturelles.
La **méthode de travail** que je vous conseille est la même pour tous les cours : chaque section correspond à une leçon, et l'étudiant(e) devrait la lire une fois tranquillement, en essayant de la comprendre ; la prise de notes personnelles est recommandée, mais pas indispensable : vous pouvez aussi annoter votre cours. Lorsqu'il y a des démonstrations, il/elle est invité(e) à les analyser et à les refaire, et lorsqu'il y a des exercices, à les chercher systématiquement. Avant de commencer chaque nouvelle section, il vous faudra relire la précédente pour vous remémorer le travail accompli et vous mettre en condition.
Mathesis vous propose un apprentissage sans échec : pour construire votre connaissance mathématique il n'est pas nécessaire d'apprendre par cœur le cours ni les démonstrations (il suffit de les analyser), et il n'est pas nécessaire de trouver la solution des exercices et des problèmes (il suffit de les chercher honnêtement). L'effort sérieux et régulier est cumulatif et suffit à l'assimilation : apprendre des mathématiques est à la portée de tous, même il s'agit d'une tâche exigeante, qui demande de la persévérance. Chaque section ou leçon demande entre trente minutes et une heure de travail par jour ; à cinq jours par semaine, chaque cours demande environ un mois. Si les leçons sont trop longues, n'hésitez pas à les fractionner : il vaut mieux travailler un peu tous les jours selon sa capacité, plutôt que s'épuiser et espacer les séances d'étude.

Présentation du cours

Cet ouvrage est le second volume de la série, il s'agit donc du $2^{\text{ème}}$ cours du semestre I de la $1^{\text{ère}}$ année. En quatre chapitres, il comporte 18 sections ou leçons et 24 figures. Il traite notamment des compléments essentiels de théorie naïve des ensembles, des notions d'application et de bijection qui permettent de définir le nombre d'éléments d'un ensemble, du dénombrement ou détermination du nombre d'éléments de certains ensembles finis, et de la notion d'infini mathématique et de ses caractérisations.
Dans le premier volume, "Entrer dans l'Univers Mathématique", nous avons évoqué l'univers des objets mathématiques, l'expression mathématique avec sa logique et sa symbolique, les ensembles naturels de nombres dont $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ et leurs propriétés fondamentales, les bases de la théorie naïve des ensembles et les principaux types de raisonnements mathématiques, que nous avons illustrés sur les ensembles naturels.
Dans ce deuxième volume nous allons approfondir notre connaissance de la théorie naïve des ensembles, étroitement liée à la théorie intuitive des nombres entiers naturels, notamment à travers la *numération*, c'est-à-dire pour nous ici l'attribution d'un nombre d'éléments à un ensemble fini. La numération est le pendant théorique

du “comptage” et de ses propriétés et il est donc naturel d'associer les deux sujets; ce sera l'occasion d'aborder le “dénombrement” des ensembles finis, c'est-à-dire la détermination du *nombre d'éléments* de certains de ces ensembles.
Puisque nous parlons d'ensembles finis, dont l'intuition sert de base à la numération, ce cours est aussi l'occasion d'aborder le concept d'ensemble *infini*, concept complémentaire et fondamental dans toute la mathématique, et qui peut se définir et se caractériser à partir des éléments de théorie naïve des ensembles que nous introduisons.
La notion qui permet de travailler avec le fini et l'infini sur le plan de la théorie des ensembles, est la notion d'*application*, qui est la formalisation de ce qu'on entend par “fonction” mathématique au sens large. Elle repose elle-même sur la notion mathématique de *relation*, qu'on introduit ici avec celle de *produit cartésien*, opération ensembliste fondamentale qui généralise la représentation du plan géométrique par des coordonnées. Nous aurons l'occasion d'introduire tous ces fondements et de les illustrer dans ce cours, qui culminera avec la *caractérisation des ensembles infinis*. Autrement dit, nous donnerons une expression de ce qu'est un ensemble infini, n'utilisant explicitement que le vocabulaire de la théorie des ensembles ! C'est déjà un accomplissement mathématique significatif et un jalon dans le cursus.
A partir des éléments de ce cours, nous aurons tout ce qu'il nous faut pour aborder de manière rigoureusement scientifique la théorie centrale de la science mathématique, à savoir l'arithmétique. Nous aurons en effet l'occasion d'introduire dans la section sur l'infini le contenu des axiomes dits “de Peano”, liés à la fonction successeur, et que nous reprendrons explicitement dans le volume suivant pour bâtir solidement l'arithmétique élémentaire.

Jean Barbet, 10 février 2021

Compléments sur la méthode de travail

Comprendre le cours L'intégration du cours ne nécessite pas d'apprendre par cœur. Par contre, une simple lecture est insuffisante. Lorsqu'un enseignant donne un cours en direct, il insiste sur certains points, donne des explications supplémentaires. Ces éléments ne sont pas disponibles dans le cours écrit, il est donc nécessaire que l'étudiant(e) y supplée, ce qui est à sa portée ; il (elle) doit faire ce qu'on appelle une lecture analytique. Dans un cours de mathématiques, on distingue plusieurs parties : outre les exercices et problèmes, nous avons des explications, des définitions, des propositions et des exemples.

Les explications sont le corps du texte mathématique : on introduit un nouveau sujet, on expose les propriétés d'un nouvel objet. Il faut lire ce texte en se posant la question : est-ce que je comprends ce que je lis ? Si ce n'est pas le cas, il faut s'arrêter et chercher les réponses : soit nous n'avons pas compris le texte lui-même, soit nous sommes mal assurés relativement à un point exposé dans une section précédente ; il nous faut alors y revenir pour clarifier notre pensée.

Les définitions introduisent de nouveaux objets ou de nouvelles notions, toujours à partir d'objets ou de notions introduits précédemment. Comme pour le corps du texte, il faut s'assurer de bien comprendre les définitions, les analyser en détail et revenir à des sections précédentes si nécessaire. Parfois, certains notions du lycée ou du collège sont utilisées de manière intuitive, sans être redéfinies immédiatement : l'étudiant(e) les retrouvera facilement par ses propres moyens.

Les propositions (appelées propositions, théorèmes, lemmes et corollaires) énoncent des propriétés essentielles des objets dont traite le cours, ceux qui précisément constituent la connaissance mathématique propre, celle qu'on met en évidence. Comme pour les définitions, il faut s'assurer de bien en comprendre les énoncés, mais à la différence des définitions il faut aussi en comprendre les démonstrations. Une démonstration est une argumentation mathématique, qui cherche à établir la véracité de la proposition énoncée. Il faut l'analyser, c'est-à-dire en identifier les différentes parties et leurs articulations logiques, et chercher à en comprendre chaque partie, et comment toutes les parties s'agencent pour établir le résultat annoncé. Une fois une démonstration comprise, il est bon de chercher à la reproduire soi-même.

Les exemples servent à illustrer les nouveaux concepts introduits par les définitions, ou bien les propriétés démontrées dans les propositions. Ces concepts et propriétés sont en effet la plupart du temps des généralités : il est donc important de comprendre comment ils se réalisent ou se manifestent dans des cas particuliers. Les exemples sont à bien comprendre également.

L'étudiant(e) qui veut faire des fiches devrait prendre en note surtout les définitions et les énoncés des propositions. Quelques exemples choisis parmi les plus suggestifs peuvent illustrer utilement ses notes. Enfin, il est bon, avant de commencer une nouvelle séance d'étude, de relire le cours étudié à la session précédente ou de relire ses notes, pour se remémorer les concepts et propriétés étudiés juste avant. Comme tout apprentissage, l'apprentissage mathématique est cumulatif.

Travailler les exercices Les exercices mathématiques consistent à mettre en œuvre ou appliquer le cours dans des situations particulières. Les problèmes sont des exercices d'un niveau supérieur qui consistent à résoudre une question ou une série de questions en faisant preuve de plus de créativité. Il n'est pas toujours possible de trouver la solution d'un exercice ou d'un problème à la première tentative ; on peut même échouer régulièrement. Aussi surprenant soit-il, l'important dans la recherche de la solution d'un exercice ou d'un problème n'est pas de trouver la solution, mais de la chercher honnêtement.
La résolution d'un exercice ou d'un problème consiste à développer une stratégie et à la mettre en œuvre. La première étape consiste à analyser l'exercice ou le problème : il faut s'assurer qu'on en comprend tous les termes, et qu'on comprend la question posée ; cette étape est essentielle et est une première mise en œuvre du cours. La seconde étape consiste à élaborer une stratégie : en fonction de la question posée, il faut identifier les idées qui nous viennent à l'esprit, souvent de manière désordonnée, et inventer une série d'étapes pour aboutir à la réponse ; souvent, il faut identifier comment les éléments du cours présents dans l'énoncé peuvent être utilisés pour atteindre l'objectif. La troisième étape consiste à mettre en œuvre la stratégie : il faut faire un ou des calcul(s), un ou des raisonnement(s), de manière rigoureuse. La seconde et la troisième étapes se font souvent simultanément ; il n'est en général possible d'analyser la démarche adoptée qu'après avoir effectué une tentative.
On a cherché l'exercice ou le problème honnêtement quand on est allé aussi loin qu'on le peut. Parfois, l'analyse de la question s'avère déjà difficile, et on n'a pas d'idée pour la résoudre. Parfois une stratégie nous vient à l'esprit, mais il nous manque l'adresse nécessaire pour aboutir, soit raisonner ou calculer efficacement ; ou alors, la stratégie est incomplète ou erronée. Parfois enfin, on arrive jusqu'au bout ; si c'est la situation la plus satisfaisante, ce n'est toutefois pas toujours le cas : la difficulté est inhérente à la mathématique, et à l'impossible nul n'est tenu. Lorsqu'on n'aboutit pas à la solution du problème, on peut (et on devrait) y revenir ultérieurement. Mais il est possible de chercher honnêtement la solution de chaque exercice, le minimum étant l'analyse de la question posée ; celle-ci est en principe toujours accessible, si bien qu'on n'échoue à l'exercice que lorsqu'on renonce à se poser la question.

Table des matières

Chapitre 1

Produits cartésiens, Relations et Applications

1.1 Couples d'objets

Dans cette première leçon, nous voulons définir rigoureusement la notion de "couple d'objets", grâce aux ressources de la théorie naïve des ensembles, pour pouvoir définir la notion de "produit cartésien". Nous donnerons une caractérisation de l'égalité de tels couples à partir de leurs éléments.

Définir les produits cartésiens

Nous allons introduire une nouvelle opération fondamentale sur les ensembles, d'une autre nature que l'intersection et l'union, celle de *produit cartésien* de deux ensembles, qui permettra d'aborder les notions de *relation* et de *fonction* (ou *application*). L'adjectif "cartésien" vient du nom du mathématicien et philosophe français René Descartes, qui a introduit les (axes de) coordonnées dans sa description dite "analytique" de la géométrie plane, ce qui est l'archétype de cette construction.
Cette notion de produit cartésien sous-tend également la description ensembliste des

René Descartes, mathématicien, physicien et philosophe français.

relations, fonctions et opérations mathématiques telles que

$$=, <, \leq, +, \times, \ln, \cos, \sin, \exp, \ldots.$$

Il est donc essentiel de l'assimiler proprement.
Par exemple, rappelons que pour deux entiers naturels a, b, on écrit $a \leq b$ quand a est inférieur (ou égal) à b; il s'agit (pour l'instant) d'un concept intuitif, que nous *représenterons*, et ainsi conceptualiserons, comme un certain ensemble, en utilisant un produit cartésien.
L'idée, simple, est de considérer la relation $\leq$ à travers sa "table", c'est-à-dire l'ensemble T de tous les "couples" (a, b) d'entiers naturels a, b tels que $a \leq b$.
Nous pourrions introduire cette notion de "couple" comme primitive : si a, b sont deux objets, le "couple" (a, b) est un objet "formé" des deux objets a et b, dans cet ordre. Cependant, ceci serait redondant, puisque cette notion de couple peut être définie en utilisant la théorie des ensembles que nous connaissons déjà, comme nous allons le voir.
Notons d'abord que la notion intuitive de "couple" devrait respecter les contraintes suivantes :
i) Nous voulons distinguer le couple (a, b) du couple (b, a), autrement dit nous voulons conserver une trace de l'ordre (par exemple, on a $0 \leq 1$, mais pas $1 \leq 0$, donc $(0, 1)$ est dans la table de $\leq$, tandis que $(1, 0)$ n'y est pas)
ii) Si (a, b) and (a', b') sont deux couples d'objets tels que $(a, b) = (a', b')$, nous voulons que $a = a'$ et $b = b'$.
En fait, la condition (i) est une conséquence de la condition (ii), puisque si $a \neq b$ et (ii) est valide, alors $(a, b) \neq (b, a)$.
Une idée des plus naturelles serait de considérer l'ensemble $\{a, b\}$ comme le couple (a, b). Cependant, les propriétés précédentes sont en défaut, puisqu'en général, on ne peut distinguer, dans les définitions par extension, les ensembles $\{a, b\}$ et $\{b, a\}$, qui sont toujours égaux par extensionnalité, puisqu'ils ont les mêmes éléments, a et b, que $a = b$ ou non !

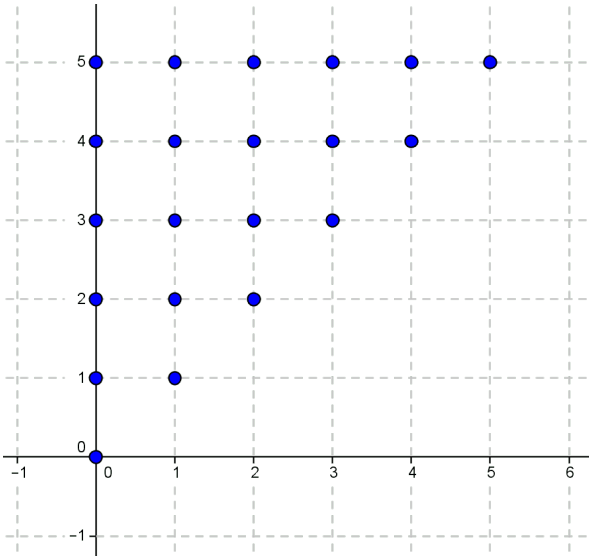

Figure 1.1: Une représentation graphique d'une partie de la table de la relation $\leq$ entre entiers naturels. On représente les couples (m, n) d'entiers naturels par des points du plan à coordonnées entières, et les points bleus sont ceux dont les coordonnées (m, n) ont la propriété $m \leq n$.

La notion ensembliste de couple d'objets

Heureusement, les ressources de la théorie des ensembles suffisent à conceptualiser rigoureusement cette notion, de la manière suivante.

Définition 1.1.1. Si a et b sont deux objets, le *couple* (a, b) (ou la *paire ordonnée* (a, b)) est l'ensemble $\{\{a\}, \{a, b\}\}$. L'objet a est la *première composante*, l'objet b est la *seconde composante*, du couple (a, b).

Remarque 1.1.2. Notons qu'on fait ici un usage intuitif essentiel du concept d'*objet*, qu'on a considéré comme concept primitif dans le premier cours.

Cette définition peut sembler abstraite ou formelle au premier abord, mais elle permet de capturer ingénieusement et précisément le concept d'un couple d'objets, du moins tel qu'il a été esquissé et tel qu'on a besoin d'en faire usage en mathématique. Par exemple, pour la première propriété, si $a \neq b$, alors le couple (a, b) est différent du couple (b, a) : en effet, on a $\{a\} \in (a, b) = \{\{a\}, \{a, b\}\}$, tandis que $\{a\} \notin (b, a) = \{\{b\}, \{a, b\}\}$! C'est bien sûr pour obtenir de telles propriétés qu'on définit ainsi le couple (a, b).
Notons que si $a = b$, alors le couple (a, a) est par définition l'ensemble $\{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\}$ (car $\{a, a\} = \{a\}$) $= \{\{a\}\}$. Cet ensemble ne contient qu'un élément, le singleton $\{a\}$.
En ce qui concerne la seconde propriété, nous l'énoncerons et la démontrerons ainsi :

Proposition 1.1.3. *Si deux couples d'objets (a, b) et (a', b') sont égaux (comme ensembles), alors $a = a'$ et $b = b'$.*

Démonstration. Nous distinguons deux cas : soit $a = b$, soit $a \neq b$. Si $a = b$, alors par définition et hypothèse, on a $\{\{a'\}, \{a', b'\}\} = (a', b') = (a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}\}$, et comme alors $\{a', b'\} \in (a, b)$, on obtient $\{a\} = \{a', b'\}$, car $\{a\}$ est le seul élément de (a, b), et donc $a = a' = b'$ par extensionnalité (deux ensembles égaux ont par définition les mêmes éléments, voir le premier cours).
Si maintenant $a \neq b$, notons d'abord que le couple (a, b) possède deux éléments distincts, $\{a\}$ et $\{a, b\}$. Comme $(a, b) = (a', b')$, on a $\{a'\} \in (a, b)$, et par ce qui précède soit $\{a'\} = \{a\}$, soit $\{a'\} = \{a, b\}$; comme $\{a, b\}$ a deux éléments par hypothèse (puisque $a \neq b$), la seconde possibilité est exclue, donc $\{a\} = \{a'\}$, et $a = a'$ par extensionnalité. Nous avons aussi $\{a', b'\} \in (a', b') = (a, b)$, donc soit $\{a', b'\} = \{a\}$, soit $\{a', b'\} = \{a, b\}$; si $\{a', b'\} = \{a\}$, alors $a = a' = b'$ et $(a, b) = (a', b') = (a', a')$ a un élément, $\{a'\}$, ce qui est exclu à nouveau; on obtient donc $\{a', b'\} = \{a, b\}$. Comme maintenant $b' \in \{a, b\}$, soit $b' = a$, soit $b' = b$; si $b' = a$, alors $a = a' = b'$ et à nouveau $(a, b) = (a', b')$ possède un seul élément, ce qui est impossible. Par conséquent, on a $b = b'$ et la démonstration est terminée. □

Remarque 1.1.4. i) Cette preuve est très détaillée, et nous supprimerons progressivement certains éléments évidents des arguments, pour ne pas surcharger le texte. L'étudiant(e) doit apprendre à interpréter les démonstrations en suppléant aux non-dits évidents.
ii) La démonstration utilise plusieurs raisonnements par cas et plusieurs raisonnements par l'absurde imbriqués. Il est normal d'éprouver de la difficulté à le suivre en entier la première fois. On apprend en faisant, et l'étude détaillée et la reproduction des preuves sont des étapes essentielles.
iii) Nous avons utilisé la signification intuitive des entiers naturels 1 et 2 dans le comptage des éléments de certains ensembles, ce qu'il n'est pas possible d'éviter, et illustre ce que nous voulions dire dans le premier cours lorsque nous affirmions que les entiers naturels sont des concepts primitifs en mathématique.

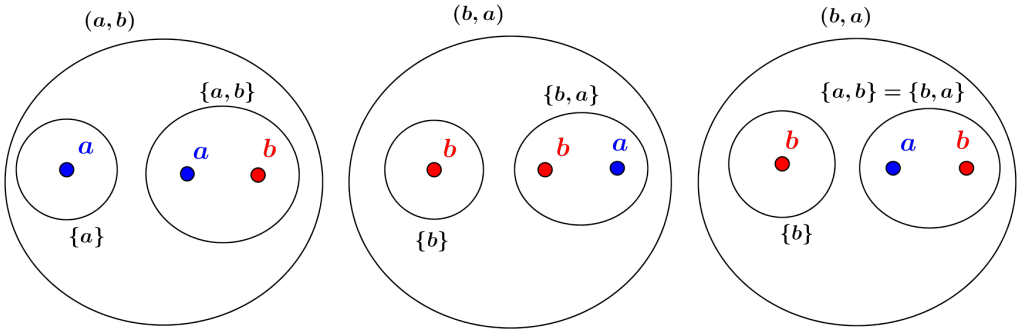

Figure 1.2: Représentation du couple (a, b), et du couple (b, a) de deux manières; l'ensemble $\{a, b\}$ et l'ensemble $\{b, a\}$ sont égaux, mais pas les couples (a, b) et (b, a).

Exercices de la section

Exercice 1.1.5. i) Soient $E = \{1, 3, 5, 7\}$ et $F = \{2, 4, 6, 8\}$. Ecrire tous les couples d'objets (a, b) qu'on peut former avec $a \in E$ et $b \in F$. Faire la même chose avec $a \in F$ et $b \in E$.

ii) Ecrire une preuve détaillée de la première propriété des couples d'objets (c'est-à-dire que si $a \neq b$, alors $(a, b) \neq (b, a)$), comme corollaire de la proposition.
iii) Si a, b, c sont trois objets, le *triplet* (a, b, c) est par définition le couple $((a, b), c)$. Lister tous les éléments de (a, b, c), qui sont des ensembles, puis les éléments de ses éléments.

1.2 Produits et relations

Produits cartésiens

Grâce à la définition conceptuelle d'un *couple* d'objet, donnée dans la section précédente, il est désormais possible de donner une définition purement ensembliste du produit (cartésien) de deux ensembles.

Définition 1.2.1. Si E et F sont deux ensembles, le *produit (cartésien) de E et F* est l'ensemble, noté $E \times F$, de tous les couples d'objets (a, b), où a est un élément de E et b un élément de F.

Remarque 1.2.2. Symboliquement, on pourrait écrire $E \times F = \{(x, y) : (x \in E) \wedge (y \in F)\}$. On préfère toutefois réserver ce genre de définition à des sous-ensembles d'un ensemble déjà donné, tandis que dans la notation présente on ne précise pas dans quel ensemble sont choisis les couples (x, y). On peut y remédier en notant que $\{a\}, \{a, b\} \in \mathscr{P}(E \cup F)$, d'où $(a, b) = \{\{a\}, \{a, b\}\} \in \mathscr{P}(\mathscr{P}(E \cup F))$! Une description symbolique plus appropriée du produit de E et F est donc $E \times F = \{(x, y) \in \mathscr{P}(\mathscr{P}(E \cup F)) : x \in E \ \& \ y \in F\}$.

Exemple 1.2.3. i) Si $E = F = \mathbb{N}$ est l'ensemble des entiers naturels, le produit $E \times F = \mathbb{N} \times \mathbb{N}$ est l'ensemble de tous les couples d'entiers naturels, c'est-à-dire des objets de la forme

$$(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3), (1, 2), (2, 1), (3, 0), \ldots.$$

ii) Soient $E = \mathbb{N} \times \mathbb{N}$ et $F = \mathbb{N}$, l'ensemble $E \times F = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ est l'ensemble de ce que nous appelons les *triplets* (m, n, p) d'entiers naturels (voir l'exercice 1.1.5). Un triplet est un couple $((m, n), p)$, où m, n et p sont des entiers naturels; c'est donc un couple formé de deux objets, le couple (m, n) et le nombre p.
iii) Si $E = F = \mathbb{R}$, le produit cartésien $E \times F = \mathbb{R} \times \mathbb{R}$ est aussi noté $\mathbb{R}^2$, et représente le *plan géométrique* avec ses *coordonnées cartésiennes*. Un élément de $\mathbb{R}^2$ est considéré comme un *point* ou un *vecteur*, selon le point de vue adopté. C'est donc un couple (a, b) de nombres réels et on dit que a et b sont les *coordonnées* de (a, b) (comme point ou comme vecteur); a est appelé *l'abscisse*, b est appelé *l'ordonnée*, du vecteur ou du point. En décrivant une addition et une multiplication sur $\mathbb{R}^2$, on définit l'ensemble $\mathbb{C}$ des nombres complexes, aussi appelé *plan complexe* : on note alors $a + ib$ le point $(a, b) \in \mathbb{R}^2$ (voir le premier cours).
iv) De même, si $E = \mathbb{R}^2$ et $F = \mathbb{R}$, le produit $E \times F$, noté $\mathbb{R}^3$, est l'ensemble des *triplets* (a, b, c) de nombres réels, qui représente l'espace tridimensionnel euclidien. Le nombre c est la *cote* du point ou vecteur considéré.

v) Dans le troisième cours, sur l'arithmétique élémentaire, nous donnerons une *construction* de l'ensemble $\mathbb{Z}$ à partir du produit $\mathbb{N}\times\mathbb{N}$, et une construction de l'ensemble $\mathbb{Q}$ à partir du produit $\mathbb{Z}\times\mathbb{N}^*$ (aussi possible à partir de $\mathbb{Z}\times\mathbb{Z}^*$).

Lorsque deux ensembles E et F sont égaux, on appelle parfois le produit $E\times F$ le *carré (cartésien)* de E, aussi noté E^2, par analogie avec le carré d'un nombre, produit de ce nombre par lui-même. En fait, nous prouverons plus tard que si E et F sont deux ensembles finis ayant respectivement m et n éléments, alors $E\times F$ possède $m.n = m\times n$ éléments, d'où une relation naturelle entre le produit d'ensembles finis et le produit des entiers naturels.
L'étudiant(e) doit maîtriser la notion de produit cartésien pour bien comprendre la suite du cours.

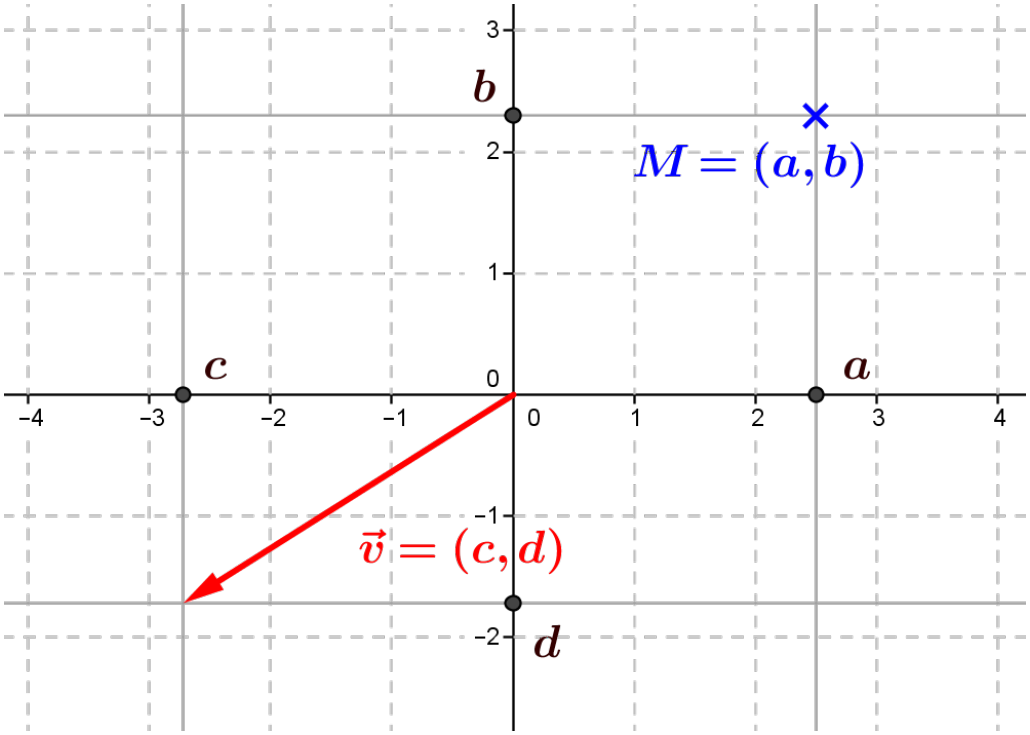

Figure 1.3: Le plan géométrique usuel, dit plan euclidien ou plan cartésien, représente le produit cartésien $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$. Les coordonnées de $M\in\mathbb{R}^2$, vu comme point, sont a et b, celles de $\vec{v}\in\mathbb{R}^2$, vu comme vecteur, sont c et d.

Relations

Rappelons que l'introduction des produits cartésiens a été motivée par la représentation de certaines relations et opérations mathématiques; il est maintenant possible de définir le concept général de relation en traduisant simplement l'idée de "table" d'une relation ou d'une opération, évoquée dans la leçon précédente.

Définition 1.2.4. Si E et F sont deux ensembles, une *relation entre E et F* ou *correspondance de E dans F* est par définition un sous-ensemble R du produit cartésien $E\times F$. E est appelé le *domaine* et F est appelé le *co-domaine* de la relation (ou correspondance) R.

Remarque 1.2.5. Le terme "relation" est en général appliqué lorsque $E = F$ (on parle alors de relation *binaire* sur E). Toutefois, la terminologie anglo-saxonne utilise plutôt l'anglais "relation"; nous avons donc jugé utile de conserver les deux termes, même si en français une relation désigne souvent simplement un sous-ensemble.

Exemple 1.2.6. i) Nous pouvons désormais considérer la relation $\leq$ sur un sous-ensemble quelconque E de $\mathbb{R}$, non (seulement) comme une relation "intuitive", mais aussi ou plutôt comme une relation entre E et E au sens présent, c'est-à-dire $\{(x, y) \in E \times E : x \leq y\}$. Bien sur, cela ne *définit* pas $\leq$, ce que nous ferons pour $E = \mathbb{N}$ dans le cours n° 3 ("Arithmétique élémentaire").
ii) De même, les relations intuitives $=$ et $<$ se représentent sur un sous-ensemble quelconque de $\mathbb{R}$ par des correspondances de $\mathbb{R}$ dans $\mathbb{R}$.
iii) L'addition $+$ des entiers naturels peut être conçue comme une correspondance de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$, soit un sous-ensemble de $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, à travers sa "table", c'est-à-dire l'ensemble $\{((m, n), p) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} : m + n = p\}$. C'est aussi le cas pour la multiplication, et on peut évidemment le faire aussi pour l'addition et la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$. L'addition et la multiplication des entiers naturels seront *définies* également dans le cours n° 3.
iv) Une autre relation, associée à la multiplication des entiers naturels (ou des entiers relatifs), est la *relation de divisibilité*, notée $|$, introduite au cours précédent : on dit qu'un entier naturel m *divise* un entier naturel n si il existe un entier naturel d tel que $n = m.d$, ce qu'on note $m|n$. En d'autres termes, cette relation de divisibilité entre $\mathbb{N}$ et $\mathbb{N}$ est conçue, et même ici *définie*, comme un sous-ensemble de $\mathbb{N} \times \mathbb{N}$, à savoir $\{(m, n) \in \mathbb{N} \times \mathbb{N} : \exists d \in \mathbb{N},\ n = m.d\}$.
v) Un exemple de relation est donné sur les sous-ensembles d'un ensemble donné E : si $X, Y \in \mathscr{P}(E)$ sont deux sous-ensembles de E, nous avons défini au premier cours l'inclusion $X \subseteq Y$ et nous pouvons cette fois-ci la considérer comme une correspondance R de $\mathscr{P}(E)$ dans lui-même au sens présent, à savoir comme $\{(X, Y) \in P(E)^2 : X \subseteq Y\}$, c'est-à-dire comme un ensemble et non plus seulement un concept de la théorie. Le fait de se restreindre aux parties d'un ensemble donné permet donc de considérer $\subseteq$ comme une véritable relation mathématique au sens strict. Il faut faire attention : la "méta-relation" d'inclusion $\subseteq$ n'est pas une relation au sens présent, car il n'y a pas d'"ensemble de tous les ensembles".
vi) Dans le même esprit, nous pouvons aussi considérer la relation d'appartenance R entre E et $P(E)$ comme $R = \{(x, Y) \in E \times \mathscr{P}(E) : x \in Y\}$, relation mathématique au sens strict. Ici aussi, la relation intuitive $\in$ en général est une méta-relation entre les objets et les ensembles mais n'est pas une relation au sens présent.

Le domaine E et le codomaine F d'une relation R font partie intégrante de la donnée de la relation. Pour cette raison, une relation est rigoureusement décrite par un *triplet* d'ensembles (E, F, R), où $R \subseteq E \times F$ est appelé le *graphe* (ou *champ*) de la relation. Par abus de langage, on dénote souvent le triplet par R, lorsque E et F sont clairement identifiés dans le contexte.

Exemple 1.2.7. i) La représentation de la relation intuitive $\leq$ entre $\mathbb{N}$ et $\mathbb{N}$ n'est pas la même relation que sa représentation comme correspondance de $\mathbb{N}^*$ dans lui-même. La première peut être décrite comme triplet par $(\mathbb{N}, \mathbb{N}, \leq)$, la seconde par $(\mathbb{N}^*, \mathbb{N}^*, \leq)$ (en conservant la même notation $\leq$ pour la relation intuitive et les deux

graphes (différents) !).
ii) La relation de divisibilité que nous avons définie est $(\mathbb{N}, \mathbb{N}, |)$. Considérant que 0 ne divise que lui-même et que tout nombre est diviseur de 0, on aurait pu la définir sans "perte d'information" comme la relation $(\mathbb{N}^*, \mathbb{N}^*, |)$.

Dans le cas particulier où $E = F$, nous avons déjà mentionné qu'une relation R entre E et E est appelée une *relation binaire sur* E. Si $S \subseteq E$ est un sous-ensemble de E, la *restriction de* R *à* S est la relation $(S, S, R|_S)$ où $R|_S = \{(x, y) \in S \times S : (x, y) \in R\} = R \cap (S \times S)$.

Exemple 1.2.8. i) Les relations $=$, $<$, $\leq$ sont des relations binaires sur $\mathbb{R}$, de même que leurs restrictions à tout sous-ensemble de $\mathbb{R}$ (et notamment à $\mathbb{Q}$, $\mathbb{Z}$ et $\mathbb{N}$).
ii) La relation de divisibilité $(\mathbb{N}, \mathbb{N}, |)$ est une relation binaire sur $\mathbb{N}$.
iii) La relation d'inclusion entre les sous-ensembles d'un ensemble donné E est une relation binaire sur $\mathscr{P}(E)$, mais la relation d'appartenance entre éléments de E et de $\mathscr{P}(E)$ ne l'est pas, puisque son domaine et son codomaine sont (toujours) distincts.

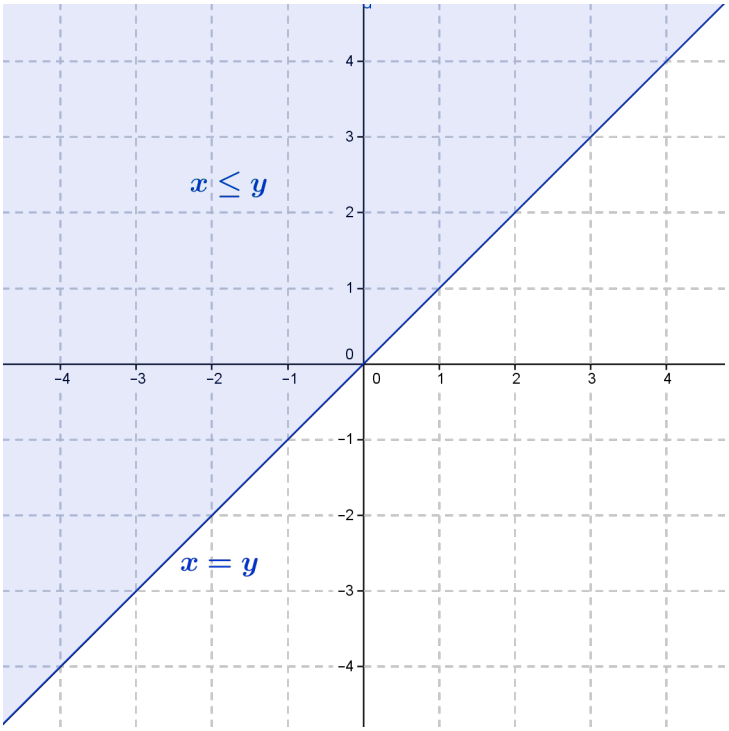

Figure 1.4: La relation binaire $\leq$ sur l'ensemble $\mathbb{R}$ peut se représenter comme l'ensemble des points $(x, y) \in \mathbb{R}^2$ tels que $x \leq y$ (zone bleue), tandis que la relation $=$ est représentée par l'ensemble des points $(x, y) \in \mathbb{R}^2$ tels que $x = y$ (bord inférieur de la zone bleue). La relation $<$ est alors représentée comme l'ensemble des points $(x, y) \in \mathbb{R}^2$ tels que $x < y$, soit les points de la zone bleue qui ne sont pas sur le bord.

Exercices de la section

Exercice 1.2.9. i) Si E est un ensemble, quels sont les éléments du produit $E \times \emptyset$? Quel est alors ce produit ?

ii) Donner une description du produit $\{a\} \times \{b\}$ par extension.
iii) Soit E un ensemble constitué de trois objets a, b, c et F un ensemble constitué de deux objets x, y. Décrire le produit $E \times F$ par extension (donner une liste de ses éléments).
iv) Définir deux ensembles d'objets non mathématiques différents E et F par intension (par une propriété), et décrire leur produit $E \times F$.
v) Donner une description ensembliste symbolique de la multiplication comme ensemble de triplets d'entiers naturels, c'est-à-dire sous forme d'une table (sous-ensemble de $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$).
vi) Décrire la représentation R de $\leq$ comme relation binaire sur $\mathbb{R}^*$, et montrer que (le graphe de) la représentation S de $\leq$ comme relation binaire sur $\mathbb{R}$ contient (au moins) un élément qui n'est pas dans R.
vii) Si R est une relation binaire sur un ensemble E et S est un sous-ensemble de E, démontrer que le champ de la restriction de R à S, soit l'ensemble $\{(x, y) \in S^2 : (x, y) \in R\}$, est l'ensemble $R \cap (S \times S)$.
viii) Si E et F sont deux ensembles et $S \subseteq E$ et $T \subseteq F$ deux sous-ensembles, respectivement de E et de F, démontrer que le produit $S \times T$ est un sous-ensemble de $E \times F$. En déduire que S^2 est un sous-ensemble de E^2.

1.3 Relations fonctionnelles et applications

La notion de relation mathématique n'est pas seulement utile pour décrire ou définir les relations telles que l'égalité $=$, les inégalités stricte $<$ et large $\leq$, la divisibilité $|$ et de nombreuses autres, mais aussi pour décrire les *fonctions* mathématiques, dont font partie les "opérations", notamment l'addition et la multiplication.
Nous en avons eu un aperçu à travers la représentation de la "table" de ces deux opérations : il faut concevoir les opérations comme des relations, ou des correspondances, le terme étant peut-être plus suggestif en ce qui concerne les fonctions.
Par exemple, à chaque entier naturel $n \in \mathbb{N}$ on peut "associer l'entier naturel suivant" $n+1$, appelé son *successeur*; il s'agit d'une notion intuitive, qui ne dépend pas *stricto sensu* de l'addition (la notation permet de fixer les idées) et nous pouvons considérer la relation binaire S sur $\mathbb{N}$ définie par $S = \{(m, n) \in \mathbb{N}^2 : n = m+1\}$. De cette manière, "l' opération" qui "transforme" un entier naturel n en l'entier naturel $n + 1$ est conçue comme une relation.
Dans cette section nous introduisons les raffinements de la notion de relation qui permettent de définir rigoureusement ce qu'est une "fonction" mathématique, et qu'on appelle une *application*, à partir des seules ressources de la théorie des ensembles. On peut donc, à nouveau, *réduire* la notion de fonction mathématique à celle d'ensemble, ce qui n'est pas évident au vu du caractère "dynamique" de l'intuition de cette notion, par contraste avec le caractère "statique" de l'idée d'ensemble.

Relations fonctionnelles

Le successeur est un cas bien particulier de relation binaire : pour tout entier naturel m, il existe *un unique* entier naturel n tel que $(m, n) \in S$, et cet entier est précisément $m + 1$. Ceci nous amène à introduire la définition suivante.

Définition 1.3.1. Si E et F sont deux ensembles, une relation R entre E et F est dite *fonctionnelle* si pour tout $x \in E$ il existe *au plus* un élément y de F tel que $(x, y) \in R$.

Exemple 1.3.2. i) Nous avons vu que la relation $S = \{(m, n) \in \mathbb{N}^2 : n = m+1\}$ est une relation fonctionnelle. On aurait pu définir une relation fonctionnelle analogue sur $\mathbb{Z}$.
ii) La table de l'addition des nombres réels, soit $A = \{((x, y), z) \in \mathbb{R}^2 \times \mathbb{R} : x+y = z\}$ est une relation fonctionnelle sur $\mathbb{R}^2 \times \mathbb{R}$: en effet, pour tous $x, y \in \mathbb{R}$, autrement dit pour tout couple $(x, y) \in \mathbb{R}^2$, il existe exactement un élément $z \in \mathbb{R}$ tel que $((x, y), z) \in A$, c'est précisément $z = x+y$. Il en est de même pour la multiplication des nombres complexes par exemple.
iii) Soit $R = \{(q, n) \in \mathbb{Q} \times \mathbb{N} : (n \leq q) \wedge (\forall m \in \mathbb{N},\ m \leq q \Rightarrow m \leq n)\}$. Il s'agit d'une correspondance de $\mathbb{Q}$ dans $\mathbb{N}$ et la clause un peu compliquée qui la définit signifie qu'un couple $(q, n) \in \mathbb{Q} \times \mathbb{N}$ est un élément de R si et seulement si n est "le plus grand entier naturel inférieur à q".
iv) Soit $R = \{(n, m) \in \mathbb{Z} \times \mathbb{N} : (m|n) \wedge (\forall d \in \mathbb{N},\ d|n \Rightarrow d \leq m)\}$. Si $(n, m) \in \mathbb{Z} \times \mathbb{N}$, on a $(n, m) \in R$ si et seulement si m est le "plus grand diviseur positif de n", soit n lui-même si $n \in \mathbb{N}$, sinon $-n$ si $n < 0$, dans tous les cas $|n|$ (voir le premier cours pour la définition de $|.|$, la valeur absolue) : R est une relation fonctionnelle.

L'exemple (iii), contrairement à tous les autres, illustre qu'on ne demande pas, pour qu'une relation R entre deux ensembles E et F soit fonctionnelle, que pour tout $x \in E$, il existe un élément $y \in F$ tel que $(x, y) \in R$: on demande seulement qu'il y en ait au plus un. En effet, dans cet exemple, si $q < 0$ aucun entier naturel n'est inférieur à q, donc il ne peut en exister de plus petit !

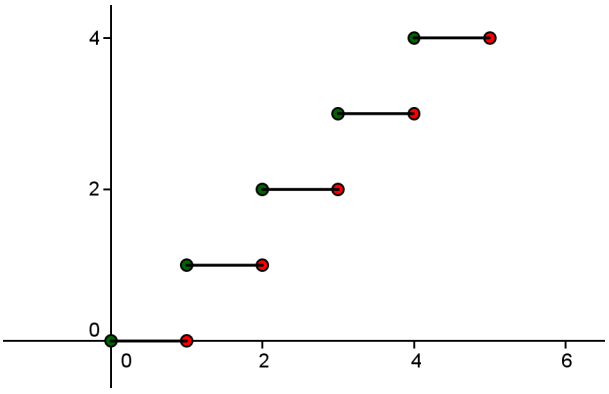

Figure 1.5: Pour les rationnels positifs q, le plus grand entier naturel n inférieur à q n'est autre que la partie entière de q (voir le premier cours). Les points indiqués en vert sont sur la représentation graphique, les points indiqués en rouge en sont exclus.

Applications

Nous allons désormais nous concentrer sur un cas particulier de relations fonctionnelles, celles pour lesquelles on demande l'existence d'un correspondant pour tout

élément du domaine, et qui permettent de capturer l'idée de "fonction mathématique" par le concept de relation.

Définition 1.3.3. Si R est une relation **fonctionnelle** entre deux ensembles E et F, on dit que (E, F, R) est une *application de E dans F* si pour tout $x \in E$, il existe (au moins, c'est-à-dire exactement) un élément y de F tel que $(x, y) \in R$. On note alors $R : E \to F$ une telle application.

Remarque 1.3.4. i) La "flèche" montre le caractère orienté de l'application car la fonctionnalité dépend du sens dans lequel on considère la relation.
ii) En effet, si (E, F, R) est une relation quelconque, la relation dite *opposée* à R est la relation qui consiste à intervertir les deux composantes, autrement dit la relation de F dans E de graphe $R^o = \{(y, x) \in F \times E : (x, y) \in R\}$. Lorsque R est une application, R^o n'en est pas toujours une.
iii) Par exemple, le graphe de relation opposée au successeur est $R = \{(n, m) \in \mathbb{N}^2 : n = m + 1\}$, et pour $n \in \mathbb{N}$, il n'existe pas toujours $m \in \mathbb{N}$ tel que $(n, m) \in R$, c'est-à-dire tel que $n = m + 1$, puisque ce n'est pas le cas pour $n = 0$.

La condition pour qu'une relation R entre E et F soit une application s'écrit symboliquement : $\forall x \in E, \exists! y \in F,\ (x, y) \in R$ (le quantificateur $\exists!$ signifiant "il existe un unique", abréviation commode).
En général, on utilise des minuscules $f, g, h \ldots$ ou des symboles particuliers pour dénoter les applications, et on choisit une autre lettre pour désigner leur graphe. Autrement dit, l'expression "soit $f : E \to F$ une application", signifie qu'on se donne une application (E, F, R) qu'on note f, considérée comme "fonction de E dans F". La relation fonctionnelle R est alors le *graphe* de l'application.
Dans la suite, lorsque nous considérerons une application $f : E \to F$ d'un ensemble E dans un ensemble F, pour tout $x \in E$ nous noterons $f(x)$ l'unique $y \in F$ tel que $(x, y) \in f$. Cette notation dynamique est standard et suggère qu'on réalise une "opération" (par exemple un calcul) sur l'objet x. En particulier, elle sera utile pour *définir* (c'est-à-dire décrire) des applications.
Enfin, lorsqu'on donne une expression explicite pour la définition d'une application, on utilise la flèche $\mapsto$. Ainsi, l'application "successeur" dont nous avons déjà parlé est l'application $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$.

Exemple 1.3.5. i) En prenant $E = F = \mathbb{N}$, on a une application $m : E \to F$ définie par $m(x) = 2.x$ pour tout $x \in E$, qui consiste à multiplier un nombre par 2. Ceci nous donne un autre exemple d'une *définition* d'une application par une expression qui n'est pas une clause; ici il s'agit du terme $2.m$. Ainsi, **si les clauses permettent de définir des ensembles, les *termes* permettent de définir des fonctions**. Si on choisit plutôt $F = 2\mathbb{N}$, l'application $m : E \to F$, $x \mapsto 2.x$ est toujours proprement définie, mais son co-domaine est différent de l'application précédente : ce sont donc, en toute rigueur, deux applications *différentes*.
ii) Puisque le successeur d'un entier naturel n'est jamais nul, on peut considérer l'application successeur comme application $s : \mathbb{N} \to \mathbb{N}^*$, où $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels non nuls.
iii) L'addition des nombres réels est l'application $+ : \mathbb{R}^2 \to \mathbb{R}$, $(x, y) \mapsto x + y$. C'est le triplet $(\mathbb{R}^2, \mathbb{R}, A)$, où $A = \{((x, y), z) \in \mathbb{R}^2 \times \mathbb{R} : x + y = z\}$.

iv) La multiplication des nombres complexes est l'application $\times : \mathbb{C}^2 \to \mathbb{C}$, $(z, w) \mapsto z.w$. C'est le triplet $(\mathbb{C}^2, \mathbb{C}, M)$, où $M = \{((z, w), u) \in \mathbb{C}^2 \times \mathbb{C} : z.w = u\}$.
v) Les fonctions valeur absolue ($|.| : \mathbb{R} \to \mathbb{R}$), cosinus ($\cos : \mathbb{R} \to \mathbb{R}$), sinus ($\sin : \mathbb{R} \to \mathbb{R}$), logarithme ($\ln : \mathbb{R}_+^* \to \mathbb{R}$) et exponentielle ($\exp : \mathbb{R} \to \mathbb{R}$), parmi de nombreuses autres "fonctions d'une variable réelle", sont des applications, que nous étudierons dans les cours d'analyse. Nous avons représenté une partie du graphe de ces fonctions sur la figure suivante.

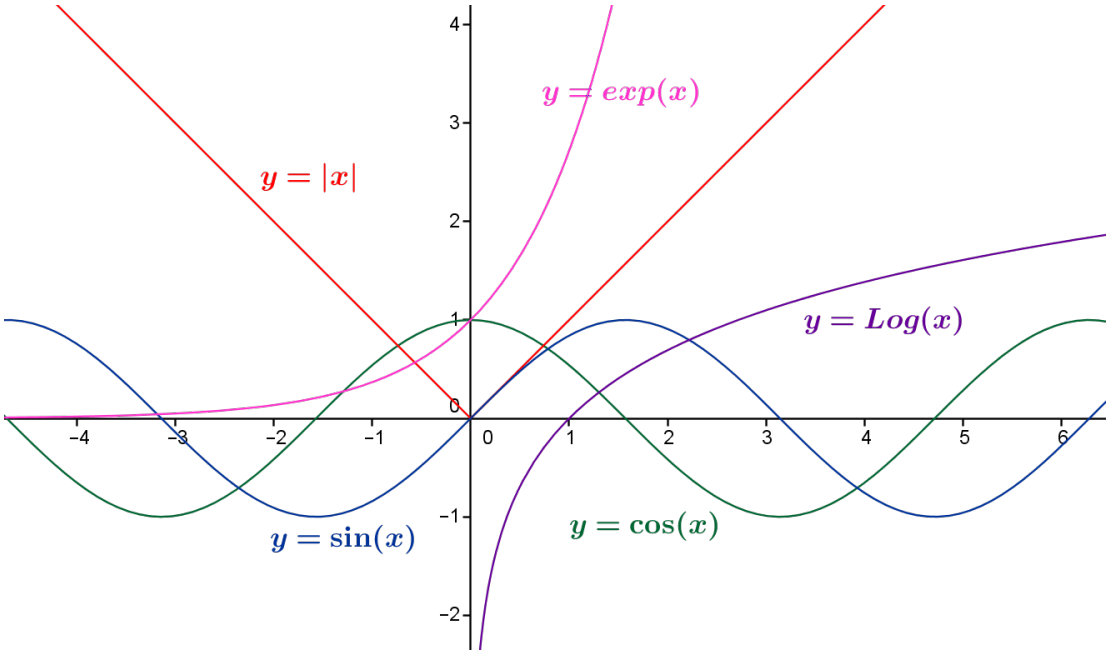

Figure 1.6: Représentation graphique d'une partie de certaines fonctions élémentaires de l'analyse réelle : le cosinus, le sinus, l'exponentielle, le logarithme népérien et la valeur absolue.

Insistons sur le fait que, *stricto sensu*, une application est un cas particulier de relation ou de correspondance (E, F, R), c'est-à-dire un ensemble (un triplet), dont les constituants E, F et R sont eux-mêmes des ensembles. On voit ici la puissance et la fécondité de la théorie des ensembles, car il n'était pas évident *a priori* que l'idée intuitivement "dynamique" de fonction (d'"opération") puisse être entièrement décrite grâce à l'idée intuitivement "statique" d'ensemble !
Notons également que nous avons dû utiliser intuitivement le nombre "deux" (il a bien fallu parler de "deux ensembles" !). Comme pour les autres définitions de théorie élémentaire des ensembles, on ne peut donc pas se passer de l'intuition des entiers naturels, ce qui confirme qu'il s'agit de notions "primitives" en mathématique.
Remarquons enfin que nous n'avons pas donné de *définition* de l'addition et de la multiplication dans les exemples : nous en avons une connaissance intuitive, et nous avons simplement cherché à en donner une traduction rigoureuse dans notre langage. **Dans le cours n° 3, nous définirons rigoureusement l'addition et la multiplication à partir de la seule fonction successeur** $s : \mathbb{N} \to \mathbb{N}$. Nous étendrons alors ces définitions, dans ce cours-là et les suivants, aux entiers relatifs,

aux rationnels, aux nombres réels, aux nombres complexes et aux quaternions en construisant ces différents ensembles.
Ainsi, nous aurons "construit" tous les ensembles fondamentaux évoqués lors du premier cours à partir de la seule fonction successeur et ses propriétés axiomatiques reposant sur l'intuition de la suite des nombres entiers naturels, et des ressources de la théorie naïve des ensembles.

L'application vide

De même qu'il existe un ensemble vide, il existe une application vide, c'est-à-dire dont le graphe est vide; toutefois, dans ce cas il existe plusieurs applications vides, qui ne dépendent en fait que du co-domaine, lequel peut varier.
En effet, si $f : E \to F$ est une application dont le graphe R est vide, alors comme pour tout $x \in E$ il doit exister $y \in F$ tel que $(x, y) \in R$, il faut nécessairement que E lui-même soit vide (sans quoi R ne peut être vide !).
Inversement, si $E = \emptyset$ alors le graphe R d'une application de E dans F ne peut être que l'ensemble vide, car c'est par définition un sous-ensemble de $E \times F = \emptyset \times F$, qui dans ce cas est vide (voir l'exercice 1.2.9(i)).
Or, puisque E ne possède aucun élément, par définition du sens des clauses (voir le premier cours) il est vrai que pour tout $x \in E$ il existe un unique $y \in F$ tel que $(x, y) \in R = E \times F$. Par conséquent, l'ensemble $\emptyset$ est bien le graphe d'une application de $E = \emptyset$ dans F, et il ne peut exister qu'une telle application.
Cependant, le choix de F est arbitraire et puisque le co-domaine est une donnée de l'application, il existe autant d'applications vides que d'ensembles F pris comme co-domaine.

Définition 1.3.6. La seule application de $\emptyset \to F$ est appelée *application vide (de co-domaine F)*. On pourra occasionnellement la noter, par abus, $\emptyset : \emptyset \to F$.

Exercices de la section

Exercice 1.3.7. o) Une relation étant un triplet (E, F, R), déterminer quels sont les éléments de ce triplet (pas ses composantes !).
i) Toute application est par définition une relation fonctionnelle. Montrer la "réciproque" suivante : si (E, F, R) est une relation fonctionnelle, il existe un sous-ensemble S de E tel que l'ensemble $R|_S = \{(x, y) \in S \times F : (x, y) \in R\}$ est le graphe d'une application de S dans F.
ii) Définir une application de $\mathbb{Z}$ dans $\mathbb{N}$ et la décrire rigoureusement.
iii) Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, avec $b > 0$, on rappelle qu'il existe d'uniques entiers relatifs q et r tels que $a = bq + r$ et $0 \leq r < b$ (division euclidienne de a par b, voir le premier cours). Le triplet $(\mathbb{Z} \times \mathbb{N}^*, \mathbb{N}, R)$, où R est l'ensemble des triplets $((a, b), r) \in (\mathbb{Z} \times \mathbb{N}^*) \times \mathbb{N}$ tels que r est le reste de la division euclidienne de a par b, est-il une relation fonctionnelle ? Est-ce une application ?

1.4 Opérations sur les relations et les applications

Restriction et co-restriction

Si E et F sont deux ensembles et R est une relation entre E et F, nous avons insisté sur le fait que *stricto sensu* la relation R est la donnée des trois ensembles E, F et R, soit du *triplet* (E, F, R), et nous avons donné des exemples où la "même" description d'une relation par son graphe donnait lieu à des relations différentes, lorsque le domaine ou le co-domaine étaient différents.
Il est important de bien comprendre ceci et de ne pas le considérer comme un formalisme stérile, ou comme du pédantisme. Il est en effet souvent nécessaire de définir de nouvelles relations ou de nouvelles applications en modifiant seulement le domaine ou le co-domaine, ce qu'on appelle *restriction* ou *co-restriction* d'une relation ou d'une application.
Nous l'avons déjà pratiqué sans le dire en définissant la "restriction" d'une relation (exercice 1.2.9(viii)), la "co-restriction" d'une application (exemple 1.3.5(ii)) et une application à partir d'une relation fonctionnelle (exercice 1.3.7(i)).
Ici, nous donnons des définitions rigoureuses qui ne devraient poser aucun problème à l'étudiant(e) qui a suivi attentivement le cours jusqu'ici.

Restriction d'une relation ou d'une application

Définition 1.4.1. Soit (E, F, R) une relation. Si $S \subseteq E$ est une partie de E, la *restriction de R à S* est la relation de S dans F décrite par le triplet $(S, F, R_{|S})$, autrement dit dont le graphe est le sous-ensemble $R_{|S} = \{(x, y) \in R : x \in S\}$ de $S \times F$.

Autrement dit, pour une relation R entre un ensemble E et un ensemble F, la restriction de R à un sous-ensemble S de E consiste précisément à "restreindre" la relation R aux seuls couples (x, y) pour lesquels x est un élément de S.
La restriction d'une relation a donc trait au *domaine* de cette relation.
Etant donné qu'une application est un cas particulier de relation, nous pouvons ici appliquer directement la notion de restriction à une application. Si $f : E \to F$ est une application, la *restriction* de f à un sous-ensemble S de E est tout simplement l'application notée $f_{|S} : S \to F$, et dont la description est $(S, F, R_{|S})$, si la description de f est (E, F, R).
La restriction d'une application est donc sa restriction comme relation.

Exemple 1.4.2. i) Si $|$ est la relation de divisibilité sur l'ensemble $\mathbb{Z} \times \mathbb{N}$, c'est-à-dire le triplet $(\mathbb{Z}, \mathbb{N}, R)$, où $R = \{(n, m) \in \mathbb{Z} \times \mathbb{N} : n|m\}$, alors la restriction de $|$ à $\mathbb{N} \subseteq \mathbb{Z}$ est la relation de divisibilité sur $\mathbb{N} \times \mathbb{N}$.
ii) Si $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est l'addition des nombres réels, alors comme le produit $\mathbb{N} \times \mathbb{N}$ est un sous-ensemble de $\mathbb{R} \times \mathbb{R}$, on peut définir la *restriction* de $+$ à $\mathbb{N} \times \mathbb{N}$, comme l'application $+_{|\mathbb{N}\times\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$, $(m, n) \mapsto m + n$. Comme opération, il s'agit bien de l'addition des entiers naturels mais attention : c'est une application *différente* de l'addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (on utilise la même notation par abus), car les co-domaines sont différents ! On peut bien sûr, dans cet exemple, remplacer $\mathbb{N}$ par $\mathbb{Z}$ ou $\mathbb{Q}$ par exemple.

Remarque 1.4.3. Nous avons parlé de relations binaires sur un ensemble E, comme relation de E dans E et en toute rigueur on devrait définir la restriction à S d'une telle relation comme la relation de graphe $\{(x, y) \in S \times E : (x, y) \in R\}$. Cependant, il arrive qu'on entende par "restriction" de R à S la relation binaire (S, S, R') sur S telle que $R' = \{(x, y) \in S \times S : (x, y) \in R\}$! Autrement dit, on fait aussi une restriction sur le co-domaine, qui est E lui-même. C'est dans ce sens où nous l'avons pris dans la section 1.2 sur les relations.
Cette confusion terminologique, regrettable, est en général levée par le contexte. Lorsqu'on considère des relations binaires sur des ensembles (et donc où le domaine et le co-domaine sont identiques), il est naturel d'appliquer la restriction aux deux.

Exemple 1.4.4. Si $\leq$ est la relation binaire d'ordre large sur $\mathbb{R}^2$, et si E est l'un des ensembles $\mathbb{N}, \mathbb{Z}$ ou $\mathbb{Q}$, alors on obtient par "restriction" de $\leq$ à E la relation binaire d'ordre large usuelle sur E.

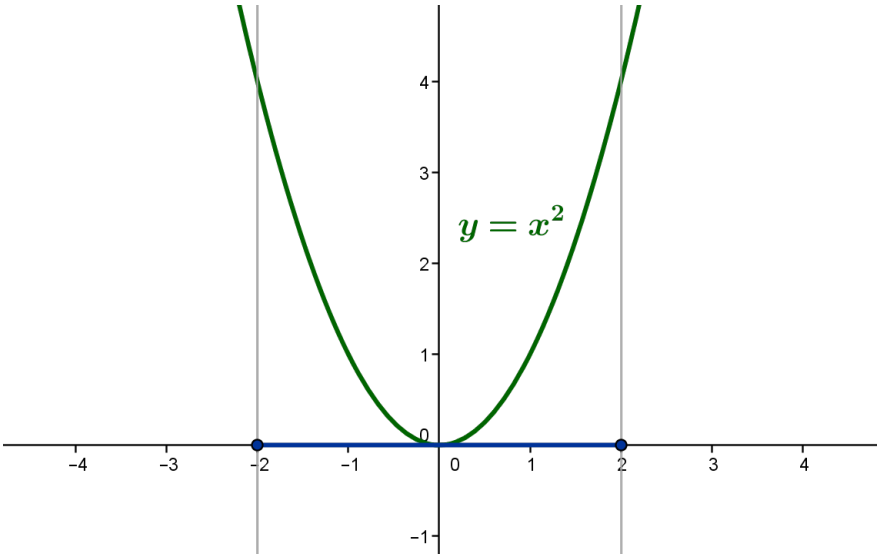

Figure 1.7: La fonction $y = x^2$ est représentée partiellement par la parabole en vert. Sa restriction au segment $[-2, 2] = \{x \in \mathbb{R} : -2 \leq x \leq 2\}$, représenté en bleu, est représentée par la portion de la courbe comprise entre les deux droites verticales (en gris).

Co-restriction d'une relation ou d'une application

Si la restriction consiste à rapporter une relation à un sous-ensemble de son domaine, la *co-restriction* consiste naturellement à rapporter une relation à un sous-ensemble de son co-domaine.

Définition 1.4.5. Soit (E, F, R) une relation. Si $T \subseteq F$ est une partie de F, la *co-restriction de R à T* est la relation $(E, T, R^{|T})$ entre E et T, dont le graphe est $R^{|T} = \{(x, y) \in R : y \in T\}$.

Autrement dit, pour une relation R entre deux ensembles E et F, la co-restriction de R à un sous-ensemble T de F consiste précisément à "restreindre" la relation R

aux seuls couples (x, y) pour lesquels y est un élément de T.
La co-restriction d'une relation a donc trait au *co-domaine* de cette relation.
Une application étant un cas particulier de relation, nous pouvons appliquer la définition de co-restriction à une application $f : E \to F$. Mais **attention** : si la co-restriction de f à un sous-ensemble T de F est bien définie comme relation, *ce n'est pas toujours une application*, car un élément de E n'a pas toujours un correspondant par f dans T !

Exemple 1.4.6. i) Si $|$ est la relation de divisibilité sur l'ensemble $\mathbb{N}\times\mathbb{Z}$, c'est-à-dire le triplet $(\mathbb{N}, \mathbb{Z}, R)$ où $R = \{(n, m) \in \mathbb{N} \times \mathbb{Z} : n|m\}$, alors la co-restriction de $|$ à $\mathbb{N} \subseteq \mathbb{Z}$ est la relation de divisibilité sur $\mathbb{N} \times \mathbb{N}$.
ii) Si $+_{|\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$ est l'addition des entiers naturels, considérée comme restriction de l'addition $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ des nombres réels (voir l'exemple du paragraphe précédent), alors la co-restriction de $+_{|\mathbb{N}}$ à $\mathbb{N} \subseteq \mathbb{R}$ est l'addition usuelle $+_{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ des entiers naturels. Dans ce cas, il s'agit bien d'une application.
iii) Si $s : \mathbb{N} \to \mathbb{N}, n \mapsto n + 1$ est l'application "successeur", que nous avons déjà rencontrée, le graphe R de la co-restriction $s^{|P}$ de s au sous-ensemble P de $\mathbb{N}$ des entiers naturels pairs est l'ensemble des couples (m, n) d'entiers naturels tels que $n = m+1$ et n est pair. Cette co-restriction n'est donc pas une application, puisque pour aucun entier naturel m pair il n'existe d'entier naturel n tel que $(m, n) \in R$: en effet, si m est pair, $n + 1$ est toujours impair !

Nous verrons dans la suite du cours comment il est possible de s'assurer que la co-restriction d'une application $f : E \to F$ est une application. Comme l'étudiant(e) l'aura peut-être deviné, cela revient à ce que le sous-ensemble T auquel on veut appliquer la co-restriction contienne *tous* les éléments de F de la forme $f(x)$, pour $x \in E$. Nous introduirons des définitions spécifiques pour préciser cette idée.

Exercices de la section

Exercice 1.4.7. i) On considère l'application $f : \mathbb{Z} \times \mathbb{N}^* \to \mathbb{Z} \times \mathbb{N}$ qui associe à un couple $(n, m) \in \mathbb{Z} \times \mathbb{N}^*$ le couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ où q est le quotient et r le reste de la division euclidienne de n par m (voir l'exercice 1.3.7(iii)). Décrire un sous-ensemble S de $\mathbb{N}$, le plus petit possible, tel que la co-restriction de f à $\mathbb{Z} \times S$ est encore une application.
ii) On note $g : \mathbb{N} \times \mathbb{N}^* \to \mathbb{N} \times \mathbb{N}$ l'application définie comme l'application f au (i). Comment obtenir g à partir de f par une ou des opérations sur f ? Si on pose la même question pour g que pour f, le sous-ensemble S de $\mathbb{N}$ trouvé au (i) convient-il ici ?
iii) Soit $f : \mathbb{R} \to \mathbb{R}$ la valeur absolue (voir le premier cours), c'est-à-dire $f(x) = |x|$ pour tout $x \in \mathbb{R}$, avec $|x| = x$ si $x \geq 0$, $|x| = -x$ si $x \leq 0$. On considère la restriction $g = f|_{\mathbb{Q}}$ de f à $\mathbb{Q} \subseteq \mathbb{R}$. Trouver un sous-ensemble S de $\mathbb{R}$, différent de $\mathbb{R}$ et ne contenant pas π, tel que la co-restriction de g à S est une application.
iv) Soit $f : E \to F$ une application. Montrer que pour tout sous-ensemble T de F, la co-restriction de f à T est une relation fonctionnelle.

1.5 Composition des applications

Avant d'aborder les concepts mathématiques fondamentaux qui permettent de déterminer ou de définir le "nombre d'éléments" d'un ensemble fini ou infini, nous introduisons la notion fondamentale de *composition des applications*, dont l'usage mathématique est ubiquitaire.
Il est possible de définir cette notion pour deux relations binaires en général, mais cela ne nous sera pas utile ici, aussi nous laisserons à l'étudiant(e) intéressé(e) le soin de le faire pour lui(elle)-même.
L'idée de la composition de deux applications est simple : si une fonction est un "procédé" qui produit un objet à partir d'un autre objet, et si on dispose de deux fonctions, on peut envisager appliquer les deux, l'une après l'autre : on devrait obtenir une nouvelle fonction, "composée" à partir des deux.
Les ressources de la théorie des ensembles permettent de le faire de manière rigoureuse.
Il faut bien sûr qu'il y ait une forme de "compatibilité" entre ces fonctions : la seconde doit pouvoir s'appliquer aux résultats de la première. Il s'agit d'une simple combinaison des notions de domaine, de co-domaine, et d'inclusion ensembliste :

Définition 1.5.1. Si E, F, G sont trois ensembles et $f : E \to F$ et $g : F \to G$ sont deux applications, alors *l'application composée de f par g* (on dit aussi *la composée de f par g*) est l'application noté $g \circ f : E \to G$ (lire "g rond f"), et définie par $g \circ f(x) = g(f(x))$ pour tout $x \in E$.

Discutons un peu la définition : pour pouvoir appliquer g au résultat de f, il faut que pour tout $x \in E$, $f(x)$ soit un élément du *domaine* de g : on s'en assure en demandant que le co-domaine de f et le domaine de g, ici F, soient identiques. Il suffirait de demander que le codomaine de f soit *inclus* dans le domaine de g, mais on peut toujours se ramener à la situation présente par une restriction de g, donc on se limite à cette description, qui est plus simple.
Pour décrire l'application composée $g \circ f$, il faudrait rigoureusement donner son domaine, son co-domaine et son graphe. Les deux premiers sont dans la définition : le domaine de $g \circ f$ est celui de f, soit E, le codomaine de $g \circ f$ est celui de g, soit G. Seul le graphe de $g \circ f$ n'a pas été explicité : d'après la définition, si R est le graphe de f et S est celui de g, alors le graphe de $g \circ f$ est $T = \{(x, z) \in E \times G : \exists y \in F,\ (x, y) \in R \ \&\ (y, z) \in S\}$ (nous utiliserons souvent le symbole & pour dénoter la conjonction des clauses mathématiques, notée aussi $\wedge$ dans le premier cours).
Cette définition conviendrait parfaitement pour composer des relations quelconques; en ce qui nous concerne ici, en toute rigueur il faudrait *démontrer* que la relation ainsi définie est une application, ce qui est implicite dans la définition, où l'on donne un *calcul* de $g \circ f(x)$. Faisons-les choses complètement :

Proposition 1.5.2. *Si $f : E \to F$ et $g : F \to G$ sont deux applications, alors le triplet (E, G, T) tel que décrit précédemment est une application et pour tous $x \in X$ et $z \in G$, on a $(x, z) \in T$ si et seulement si $z = g(f(x))$.*

Démonstration. Nous voulons démontrer que pour tout $x \in E$, il existe un unique $z \in G$ tel que $(x, z) \in T$ (définition 1.3.3). Soit donc $x \in E$: comme f est une application, il existe $y \in F$ tel que $f(x) = y$, c'est-à-dire tel que $(x, y) \in R$, le graphe

de f. Comme cette fois g est une application, il existe $z \in G$ tel que $z = g(y)$, c'est-à-dire $(y, z) \in S$, le graphe de g. Pour ce choix de z, il existe donc $y \in F$ tel que $(x, y) \in R$ et $(y, z) \in S$ donc par définition, on a $(x, z) \in T$. Nous devons montrer l'unicité de z avec cette propriété : supposons donc que $(x, z') \in T$ et montrons que $z = z'$. Par définition de T, il existe $y' \in F$ tel que $(x, y') \in R$ et $(y', z') \in S$; comme f est une application et $(x, y) \in R$, on a $y = y'$, donc $(y, z') \in S$; comme g est une application et $(y, z) \in S$, on a aussi $z = z'$, et l'unicité est démontrée, si bien que T est le graphe d'une application de E dans G. Or, pour tous $x \in E$ et $z \in G$, on a $(x, z) \in T$ si et seulement si il existe $y \in F$ tel que $y = f(x)$ et $z = g(y)$, si et seulement si $z = g(f(x))$. □

Exemple 1.5.3. i) Soit $f : \mathbb{R} \to \mathbb{R}_+$ l'application qui associe à un nombre réel x le nombre réel x^2, et soit $g : \mathbb{R}_+ \to \mathbb{R}$ l'application qui associe à un nombre réel y le nombre $\sqrt{y}$. L'application composée $g \circ f : \mathbb{R} \to \mathbb{R}$ associe à un nombre réel x le nombre $\sqrt{x^2}$, c'est-à-dire $|x|$.
ii) Soit $f : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ l'application qui associe à un entier naturel n le couple d'entiers relatifs $(2n, -3n)$ et soit $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ la multiplication des entiers relatifs. L'application $g \circ f : \mathbb{N} \to \mathbb{Z}$ associe à un entier naturel n l'entier relatif $(2n) \times (-3n) = -6n^2$.
iii) Si E est un ensemble et f et g sont deux applications de E dans E, alors $g \circ f$ et $f \circ g$ sont aussi deux applications de E dans lui-même : on peut toujours composer les applications d'un ensemble dans lui-même, dans n'importe quel ordre (mais on obtient en général deux fonctions différentes, voir les exercices).

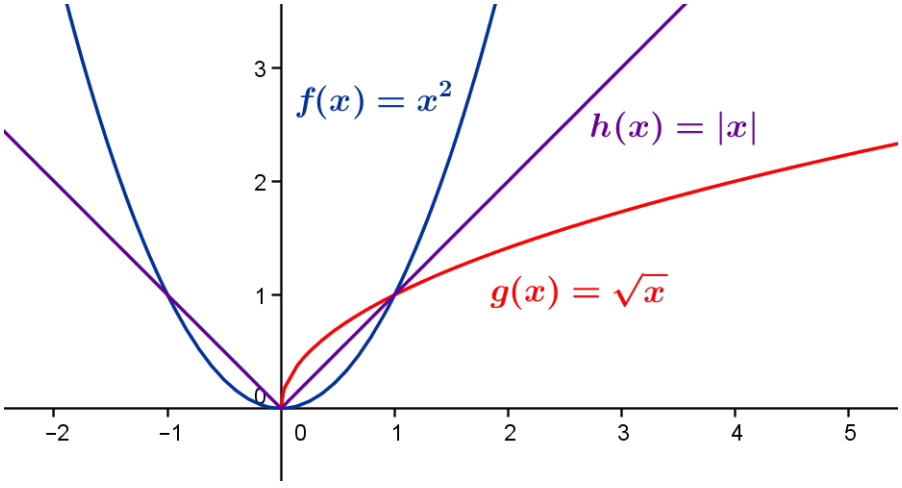

Figure 1.8: La fonction $h : x \in \mathbb{R} \mapsto |x| \in \mathbb{R}_+$ peut s'obtenir comme fonction composée $g \circ f$, à partir de la fonction $f : x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}_+$ et de la fonction $g : x \in \mathbb{R}_+ \mapsto \sqrt{x} \in \mathbb{R}_+$.

Exercices de la section

Exercice 1.5.4. Soient $f : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$ et $g : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n + 1$. Décrire les applications composées $f \circ g : \mathbb{Z} \to \mathbb{Z}$ et $g \circ f : \mathbb{Z} \to \mathbb{Z}$ sous la forme d'expressions

algébriques. Trouver $n \in \mathbb{Z}$ tel que $(f \circ g)(n) \neq (g \circ f)(n)$. Quelle conclusion en tirer sur la composition des applications ?

1.6 Image, antécédent et image réciproque

Dans la section précédente, nous avons abordé les notions de restriction, co-restriction et composition des relations et applications.
En ce qui concerne les applications, ces notions sont étroitement liées aux valeurs prises par les fonctions sur des sous-ensembles de leur domaine, et aux arguments des fonctions prenant leurs valeurs dans un sous-ensemble de leur co-domaine.
Dans cette section, nous allons préciser ces idées grâce aux concepts d'image et d'antécédent, qui nous fourniront un vocabulaire mathématique précis pour l'étude des fonctions en général, et en particulier pour aborder la théorie du "nombre d'éléments".

Image et antécédent d'un élément

On considère une application quelconque $f : E \to F$, de graphe R. On rappelle que pour tout $x \in E$, il existe un unique $y \in F$ tel que $(x, y) \in R$, et que c'est cet objet y qu'on note $f(x)$.

Définition 1.6.1. Si $x \in E$, on appelle *image de x par f* l'élément (unique) $y \in F$ tel que $(x, y) \in R$, soit tel que $y = f(x)$.

La notion "duale" consiste à associer à un élément y de F un élément x de E tel que $(x, y) \in R$, autrement dit tel que $f(x) = y$.
Ce n'est pas toujours possible, car pour certaines applications certains éléments ne sont pas "atteints" par l'application. Par exemple, la fonction successeur $s : \mathbb{N} \to \mathbb{N}$ ne prend comme valeurs que des entiers strictement positifs, si bien qu'il n'existe pas d'entier naturel n tel que $s(n) = 0$, autrement dit tel que $(n, 0)$ est dans le graphe du successeur.
D'un autre côté, dans certains cas *plusieurs* éléments de E peuvent répondre à la question, autrement dit avoir la *même* image par f. Par exemple, l'addition $+ : \mathbb{N}^2 \to \mathbb{N}$ a été décrite comme une application et si on se donne un nombre entier naturel $n > 1$, alors $0 + n = n$, donc $((0, n), n)$ est dans le graphe de l'addition, mais aussi $1 + (n - 1) = n$, donc $((1, n - 1), n)$ est aussi dans le graphe : les couples $(0, n)$ et $(1, n - 1)$, différents, ont la même image par l'application $+$.

Définition 1.6.2. Si $y \in F$, un *antécédent* de y par f, est un élément x de E tel que $f(x) = y$.

Exemple 1.6.3. i) L'image d'un entier naturel n par l'application successeur est $n + 1$.
ii) L'image du couple $(7/23, -6/5)$ de nombres rationnels par l'application $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ est $-103/115$.
iii) Un antécédent du nombre réel $2\sqrt{2}$ par la multiplication est le couple $(2, \sqrt{2})$. Un autre est $(\sqrt{2}, 2)$.

iv) Nous avons introduit au cours précédent la *valeur absolue d'un nombre réel* x, qui est le nombre réel non-négatif x si $x \geq 0$, $-x$, sinon, et noté $|x|$. Les antécédents d'un nombre réel $x \geq 0$ par la fonction valeur absolue sont x et $-x$ (avec $x = -x$ si $x = 0$).
v) Nous avons introduit dans le cours précédent la *partie entière* d'un nombre réel x, qui est l'entier relatif noté $E(x)$ ayant la propriété $E(x) \leq x < E(x) + 1$. Les antécédents d'un entier relatif n par la fonction partie entière sont donc tous les nombres réels x tels que $n \leq x < n + 1$, soit l'ensemble noté $[n, n + 1[$.

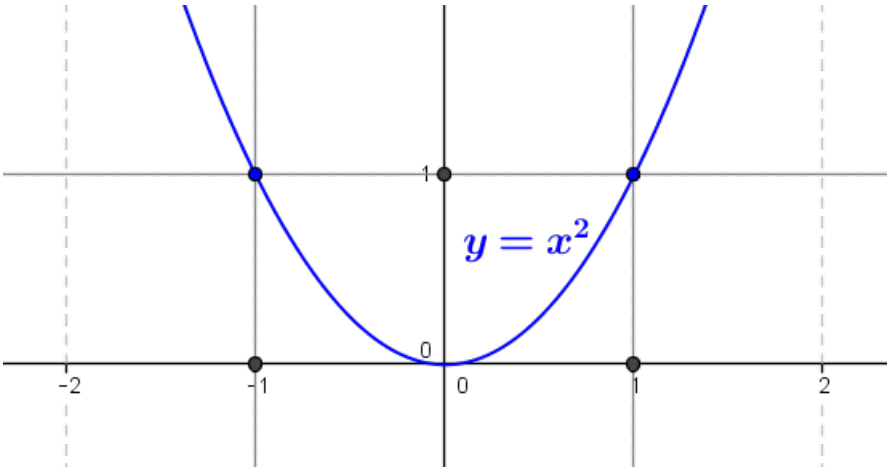

Figure 1.9: Le nombre réel 1 possède deux antécédents par la fonction $f : x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$, à savoir -1 et 1, puisque $(-1)^2 = 1^2 = 1$. En général, si $x \in \mathbb{R}_+^*$ (c'est-à-dire $x > 0$), x possède exactement deux antécédents par f, 0 ne possède qu'un antécédent, et aucun $x \in \mathbb{R}_-^*$ (c'est-à-dire $x < 0$) ne possède d'antécédent par f.

Image et image réciproque d'une partie

La notion d'image peut s'étendre aux sous-ensembles de E. Si $S \subseteq E$ est une partie de E, on considère souvent "l'ensemble des images des éléments de S", comme sous-ensemble de F.
Puisqu'un tel sous-ensemble est l'ensemble des éléments de F qui ont un antécédent dans S par f, on peut définir rigoureusement cette notion grâce à la notion d'antécédent et à la quantification existentielle :

Définition 1.6.4. L'*image de S par f*, notée $f(S)$, est l'ensemble des éléments y de F qui ont un antécédent dans S. Symboliquement, on l'écrit $f(S) = \{y \in F : \exists x \in S,\ y = f(x)\}$.
On appelle simplement *image de f* l'image de E par f, c'est-à-dire $f(E)$.

Remarque 1.6.5. Nous rejoignons ici la discussion sur la co-restriction des applications. Si $f : E \to F$ est une application et si $T \subseteq F$, alors la co-restriction de f à T est une application si et seulement si pour tout $x \in E$, l'image $f(x)$ de x est dans T, autrement dit si et seulement si $f(E) \subseteq T$.

Exemple 1.6.6. i) La valeur absolue est une application $|.| : \mathbb{R} \to \mathbb{R}$, et l'image de $\mathbb{R}$ par cette application est $\mathbb{R}_+$, puisque la valeur absolue de tout nombre réel est un réel non-négatif, et que tout nombre réel non-négatif x est tel que $|x| = x$.
ii) La partie entière se conçoit comme une application $E : \mathbb{R} \to \mathbb{R}$. L'image de E est l'ensemble $\mathbb{Z}$, puisque toute partie entière est un entier relatif, et tout entier relatif est sa propre partie entière ! L'image par E du sous-ensemble $\mathbb{R}_+$ des réels positifs est $\mathbb{N}$.
iii) Si $b \in \mathbb{N}$ est un entier > 0, à tout entier naturel a on peut associer le quotient et le reste de la division euclidienne de a par b (voir le premier cours). On définit ainsi deux applications $q_b : \mathbb{N} \to \mathbb{N}$, qui associe à $a \in \mathbb{N}$ le quotient de a par b, et $r_b : \mathbb{N} \to \mathbb{N}$, qui associe à a le reste de la division de a par b. Pour tout entier naturel $q \in \mathbb{N}$, le reste de la division euclidienne de qb par b est q, donc q est dans l'image de q_b, qui est donc $\mathbb{N}$ tout entier. En revanche, les restes de la division euclidienne ne peuvent prendre que les valeurs $0, \ldots, b-1$, et le reste de tout nombre compris entre 0 et $b-1$ par la division euclidienne par b est lui-même, donc l'image de r_b est l'ensemble $\{0, \ldots, b-1\}$.

La notion "duale" de l'image d'une partie est une sorte de généralisation aux sous-ensembles de la notion d'antécédent : si $T \subseteq F$ est une partie de F, cet ensemble des "éléments de E dont l'image est dans F" est défini de manière rigoureuse grâce à la notion d'image :

Définition 1.6.7. L'*image réciproque de T par f*, notée $f^{-1}(T)$, est l'ensemble des éléments x de E tels que $f(x) \in T$. Symboliquement, on l'écrit $f^{-1}(T) = \{x \in E : f(x) \in T\}$.

Remarque 1.6.8. i) Contrairement au cas de l'image, on n'utilise pas de quantification dans la définition de l'image réciproque. Il y a cependant une quantification universelle implicite qui apparaît si on utilise plutôt le graphe R de f, puisque $f^{-1}(T) = \{x \in E : \forall y \in F,\ (x, y) \in R \Rightarrow y \in T\}$. C'est bon exercice d'essayer de le démontrer.
ii) Il ne faut pas confondre la notion d'image réciproque avec celle d'image *duale*, qu'on rencontre notamment en logique mathématique et en théorie des catégories, et qui se formule avec une quantification universelle de manière analogue.

Notons bien le rapport entre les antécédents d'un élément $y \in F$ par f et l'image réciproque du singleton $\{y\}$, partie de F, par f : l'ensemble $f^{-1}(\{y\})$ est précisément *l'ensemble des antécédents de y par f* ! Il vaut ici aussi la peine de le démontrer.

Exemple 1.6.9. i) Soit $E : \mathbb{R} \to \mathbb{R}$ la fonction partie entière. L'image réciproque de $\mathbb{Z}$ est $\mathbb{R}$ tout entier (puisque la partie entière est toujours un entier relatif), et l'image réciproque $E^{-1}(\mathbb{N})$ de $\mathbb{N}$ est $\mathbb{R}_+$ (puisqu'un nombre réel qui a pour partie entière un entier naturel est positif).
ii) Soit $|.| : \mathbb{R} \to \mathbb{R}_+$ la fonction valeur absolue (on a changé ici le codomaine par co-restriction puisqu'il suffit de choisir $\mathbb{R}_+$). L'image réciproque de l'ensemble $[0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ par la valeur absolue est l'ensemble $[-1, 1] = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$.
iii) Soit $b \in \mathbb{N}$ non nul, et $r_b : \mathbb{N} \to \mathbb{N}$ la fonction "reste dans la division euclidienne par b". Par définition, un entier naturel a a pour reste 0 dans cette division,

autrement dit $r_b(a) = 0$, si et seulement si a est un multiple de b. Par conséquent, l'image réciproque $r_b^{-1}(\{0\})$ est l'ensemble des multiples de b dans $\mathbb{N}$, qu'on note $b\mathbb{N} = \{n \in \mathbb{N} : \exists k \in \mathbb{N},\ n = bk\}$.

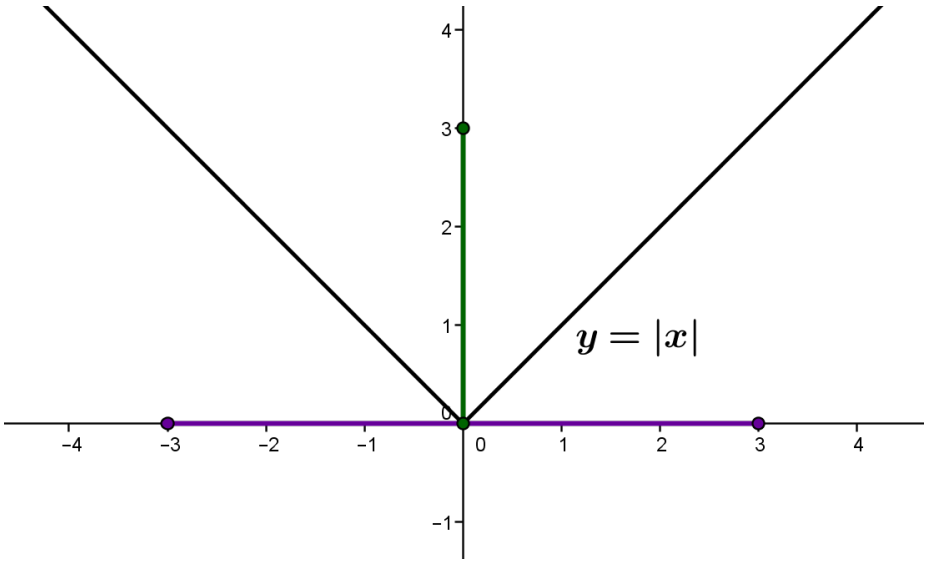

Figure 1.10: L'image réciproque du segment $[0, 3] = \{x \in \mathbb{R} : 0 \leq x \leq 3\}$ (en vert) par la fonction valeur absolue, est le segment $[-3, 3] = \{x \in \mathbb{R} : -3 \leq x \leq 3\}$ (en violet).

Exercices de la section

Exercice 1.6.10. i) Soit b un entier naturel strictement positif et soit $r_b : \mathbb{Z} \to \mathbb{N}$ (attention) l'application qui associe à tout entier relatif le reste de sa division euclidienne par b. Quelle est l'image de r_b ?
ii) Démontrer que l'image réciproque de l'ensemble $[0, 1]$ par la valeur absolue est $[-1, 1]$.
iii) Déterminer l'image de $\mathbb{Q}$ par la valeur absolue. Quelle est l'image de $\mathbb{Q} \cap [-1, 1]$?
iv) Soit $M : \mathbb{R} \to \mathbb{R}$ l'application qui associe à un nombre réel r le nombre $2 \times r$. Quelle est l'image de M ?
v) Déterminer l'image, par l'addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ des entiers naturels, du sous-ensemble $2\mathbb{N} \times 2\mathbb{N}$ des couples de nombres pairs. Déterminer l'image réciproque, par $+$, de l'ensemble des nombres pairs. Quels sont les antécédents de 0 par l'addition ?
vi) Déterminer l'image, par la multiplication $\times : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ des entiers relatifs, du sous-ensemble $3\mathbb{Z} \times 7\mathbb{Z}$ des couples d'entiers relatifs (n, m) où n est un multiple de 3 et m un multiple de 7. Déterminer l'image réciproque, par $\times$, de l'ensemble des nombres pairs. Quels sont les antécédents de 1 par la multiplication ?

1.7 Images directe et inverse et opérations ensemblistes élémentaires

L'image $f(S)$ d'une partie S d'un ensemble E par une application $f : E \to F$ est aussi appelée *image directe* de S par f, tandis que l'image réciproque $f^{-1}(T)$ d'une partie T de F par f est aussi appelée *image inverse* de T par f.
Il existe certaines relations entre l'image directe et l'image inverse, et les opérations ensemblistes élémentaires que sont le complément, l'intersection et la réunion. D'une manière générale, l'image inverse se "comporte mieux" que l'image directe par rapport à ces opérations, au sens où elle les "préserve" toutes, ce qui n'est pas le cas de l'image directe.
Plus précisément, on peut dire les choses suivantes :

Proposition 1.7.1. *Si $f : E \to F$ est une application, $S, S' \subseteq E$ et $T, T' \subseteq F$, alors on a les propriétés suivantes.*
Pour l'image directe :
i) si $S \subseteq S'$, alors $f(S) \subseteq f(S')$
ii) $f(S \cap S') \subseteq f(S) \cap f(S')$
iii) $f(S \cup S') = f(S) \cup f(S')$.
Pour l'image inverse :
iv) Si $T \subseteq T'$, alors $f^{-1}(T) \subseteq f^{-1}(T')$.
v) $f^{-1}(C_F(T)) = C_E(f^{-1}(T))$
vi) $f^{-1}(T \cap T') = f^{-1}(T) \cap f^{-1}(T')$
vii) $f^{-1}(T \cup T') = f^{-1}(T) \cup f^{-1}(T')$.

Nous allons démontrer cette proposition, étape-par-étape. C'est notre premier exemple d'une preuve un peu longue (et fastidieuse !) de ce genre de liste de propriétés. L'étudiant(e) est invité(e) à étudier attentivement et patiemment cette démonstration : il s'agit d'énoncés simples, mais il faut les démontrer de manière rigoureuse.

Démonstration. i) Supposons que $y \in f(S)$: par définition de l'image, il existe $x \in S$ tel que $y = f(x)$, et comme $S \subseteq S'$, on a $x \in S'$, si bien que $y = f(x) \in f(S')$, d'où $f(S) \subseteq f(S')$.
ii) Supposons que $y \in f(S \cap S')$: par définition de l'image, il existe $x \in S \cap S'$ tel que $y = f(x)$; en particulier, on a $x \in S$, d'où $y \in f(S)$ et $x \in S'$, d'où $y \in f(S')$, si bien que $y \in f(S) \cap f(S')$.
iii) Supposons que $y \in f(S \cup S')$, de sorte qu'il existe $x \in S \cup S'$ tel que $f(x) = y$ et distinguons deux cas, selon que $x \in S$ ou $x \in S'$. Si $x \in S$, alors $y = f(x) \in f(S) \subseteq f(S) \cup f(S')$ tandis que si $x \in S'$, alors $y = f(x) \in f(S') \subseteq f(S) \cup f(S')$ de la même manière. Dans les deux cas, on a $y \in f(S) \cup f(S')$, donc $f(S \cup S') \subseteq f(S) \cup f(S')$. Inversement, supposons que $y \in f(S) \cup f(S')$ et distinguons deux cas, selon que $y \in f(S)$ ou $y \in f(S')$; si $y \in f(S)$, il existe $x \in S$ tel que $y = f(x)$ et comme $S \subseteq S \cup S'$, on a $y \in f(S \cup S')$; l'autre cas se traite de la même manière et dans les deux cas on a $y \in f(S \cup S')$, si bien que $f(S) \cup f(S') \subseteq f(S \cup S')$, et puisque les deux inclusions sont vérifiées, on a $f(S \cup S') = f(S) \cup f(S')$.
iv) Voir les exercices.

v) Soit $x \in f^{-1}(C_F(T))$: par définition de f^{-1}, on a $f(x) \in C_F(T)$, donc $f(x) \notin T$. Alors, par définition de f^{-1}, x ne peut pas être dans $f^{-1}(T)$ (sinon on aurait $f(x) \in T$), si bien que $x \in C_E(f^{-1}(T))$, et on a $f^{-1}(C_F(T)) \subseteq C_F(f^{-1}(T))$. Dans l'autre sens, si $x \in C_E(f^{-1}(T))$, alors $x \notin f^{-1}(T)$, donc $f(x) \notin T$, autrement dit $f(x) \in C_F(T)$, donc $x \in f^{-1}(C_F(T))$, d'où $C_E(f^{-1}(T)) \subseteq f^{-1}(C_F(T))$, et comme on a les deux inclusions, les deux ensembles sont égaux.
vi) Raisonnons par équivalence : nous montrons que pour tout $x \in E$, on a $x \in f^{-1}(T \cap T')$ si et seulement $x \in f^{-1}(T) \cap f^{-1}(T')$, et alors ces deux clauses définissent le même sous-ensemble de E. Soit $x \in E$: on a $x \in f^{-1}(T \cap T')$ si et seulement si $f(x) \in T \cap T'$, si et seulement $f(x) \in T$ et $f(x) \in T'$, si et seulement si $x \in f^{-1}(T)$ et $f^{-1}(T')$, si et seulement si $x \in f^{-1}(T) \cap f^{-1}(T')$.
vii) Voir les exercices. □

Nous donnerons deux contre-exemples des propriétés prises en défaut (concernant l'intersection et le complément) pour l'image directe. Il sera profitable d'essayer de comprendre ces contre-exemples en détail.

Exemple 1.7.2. i) Si $f : \mathbb{R} \to \mathbb{R}$ est la fonction valeur absolue $x \mapsto |x|$, alors $f(\mathbb{R}_-) = f(\mathbb{R}_+) = \mathbb{R}_+$, d'où $f(\mathbb{R}_-) \cap f(\mathbb{R}_+) = \mathbb{R}_+$, tandis que $f(\mathbb{R}_- \cap \mathbb{R}_+) = f(\{0\}) = 0$. On n'a donc pas $f(S \cap S') = f(S) \cap f(S')$ pour $f : E \to F$ et $S, S' \subseteq E$ en général.
ii) Si $b > 0$ est un entier naturel et $g : \mathbb{Z} \to \mathbb{N}$ est l'application qui associe à un entier relatif n le reste de la division euclidienne de n par b, alors $g(C_{\mathbb{Z}}(\mathbb{N})) = \{0, \ldots, b-1\}$: en effet, par définition un tel reste est dans l'ensemble de droite, et si $k \in \{0, \ldots, b-1\}$, le reste de la division de $-b + k \in C_{\mathbb{Z}}(\mathbb{N})$ par b est k. Or, on a $C_{\mathbb{N}}(g(\mathbb{Z})) = \{n \in \mathbb{N} : n \geq b\}$, puisque aussi $g(\mathbb{Z}) = \{0, \ldots, b-1\}$. On n'a donc pas $f(C_E(S)) = C_F(f(S))$ pour $f : E \to F$ et $S \subseteq E$ en général, et ce contre-exemple montre qu'aucune de ces inclusions n'est vraie en général, puisqu'ici $g(C_{\mathbb{Z}}(\mathbb{N}))$ et $C_{\mathbb{N}}(g(\mathbb{Z}))$ sont non vides et disjoints.

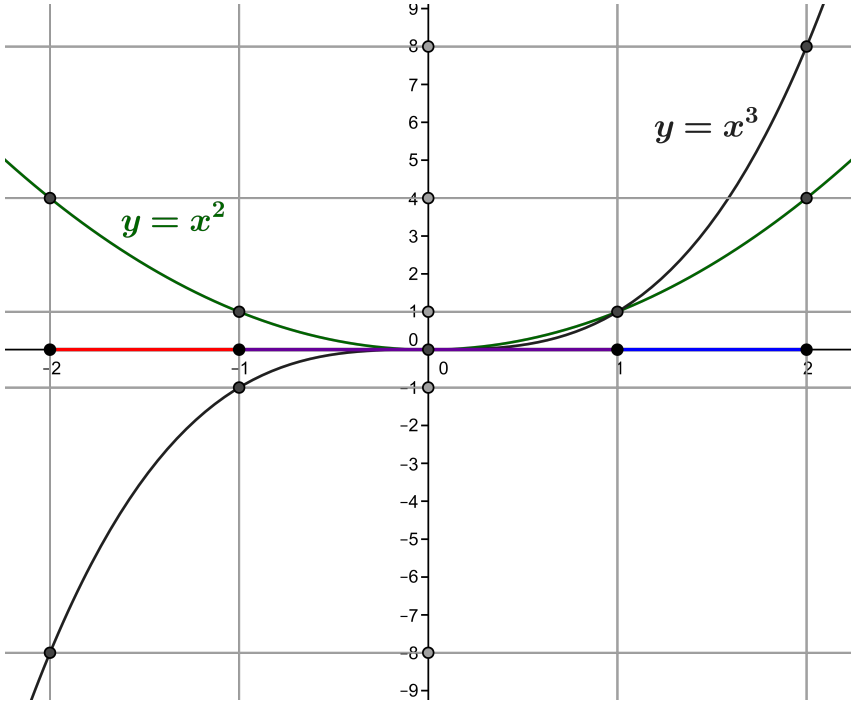

Figure 1.11: L'image de l'intervalle $[-1,1] = [-2,1] \cap [-1,2]$ par l'application $f(x) = x^3$ est l'intervalle $[-1,1] = [-8,1] \cap [-1,8] = f([-2,1]) \cap f([-1,2])$. En revanche, l'image de l'intervalle $[-1,1]$ par l'application $g(x) = x^2$ est l'intervalle $[0,1]$, qui n'est pas l'intersection des intervalles $[0,4] = f([-2,1])$ et $[0,4] = f([-1,2])$.

Exercices de la section

Exercice 1.7.3. i) Si $f : E \to F$ est une application et $T, T' \subseteq F$, montrer que si $T \subseteq T'$, alors $f^{-1}(T) \subseteq f^{-1}(T')$.
ii) En général, montrer que $f^{-1}(T \cup T') = f^{-1}(T) \cup f^{-1}(T')$.
iii) On considère l'application successeur $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$ et les sous-ensembles $\mathbb{N}^* = \{n \in \mathbb{N} : n \neq 0\}$ et $S = \{n \in \mathbb{N}^* : n > 1\}$. Quelle est l'image inverse de $\mathbb{N}^* \cap S$ par s ? De $\mathbb{N}^* \cup S$? Si P est l'ensemble des entiers naturels pairs, quelle est l'image de $C_{\mathbb{N}}(P)$ par s ? Quelle est l'image inverse de ce même ensemble par s ?
iv) Soit $f : E \to F$ une application quelconque. Montrer que si $S \subseteq E$ alors $S \subseteq f^{-1}(f(S))$. Montrer que si $T \subseteq F$, alors $f(f^{-1}(T)) \subseteq T$. **Plus difficile** : trouver des contre-exemples aux inclusions réciproques de ces deux inclusions.

Chapitre 2

Le Nombre d'Élements

Rappelons que si R est une relation entre deux ensembles E et F, la relation *inverse* ou *opposée* de R est la relation de F dans E, notée R^o, et dont le graphe est $\{(y,x) \in F \times E : (x,y) \in R\}$. Dans le cours de théorie naïve des ensembles, nous avons traité des relations fonctionnelles et des applications, et nous avons évoqué le caractère "orienté" d'une application : pour une application $f : E \to F$ de graphe R, on peut identifier, par définition, pour chaque x de E, un *unique* $y \in F$ tel que (x,y) est dans R. Cette propriété n'est pas toujours préservée par la relation opposée. Par exemple, la fonction successeur $s : \mathbb{N} \to \mathbb{N}$ est une application, et si $R = \{(m,n) \in \mathbb{N}^2 : n = m+1\}$ désigne son graphe, alors il n'existe pas d'entier naturel n tel que $(0,n) \in R^o$, autrement dit tel que $(n,0) \in R$: R^o ne définit donc pas une application. On a mis en défaut *l'existence* systématique d'un correspondant pour R^o.
Pour un contre-exemple ayant trait à la fonctionnalité, considérons l'addition $+ : \mathbb{R}^2 \to \mathbb{R}$ décrite comme application, de graphe $A = \{((m,n),p) \in (\mathbb{N}^2 \times \mathbb{N}) : m+n = p\}$. On a $0+3 = 3 = 1+2$, donc les deux triplets $((0,3),3)$ et $((1,2),3)$ sont éléments de A : comme nous l'avons déjà évoqué, un entier naturel donné peur avoir *plus d'un antécédent* pour l'addition, si bien que la relation opposée A^o sur $\mathbb{R} \times \mathbb{R}^2$ ne définit pas une application, puisqu'un élément donné de $\mathbb{R}$ peut avoir plusieurs correspondants par A^o. On a mis en défaut *l'unicité* systématique d'un correspondant par A^o.
Dans ce chapitre nous construisons progressivement la notion de *bijection* entre deux ensembles, qui permet de formaliser l'idée que deux ensembles puissent avoir le *même nombre d'éléments*, que ces ensembles soient finis ou non. Cette notion correspond précisément à l'idée d'une application dont la relation opposée est elle-même une application : on peut intuitivement **mettre en correspondance "un-à-un" les éléments d'un ensemble et d'un autre**. De même qu'il existe deux composantes dans l'idée d'application, celle de relation fonctionnelle (unicité d'un correspondant) et celle d'existence d'un correspondant, nous pouvons décomposer la notion de bijection en deux notions essentielles, celles d'*injection* ou *application injective*, et celle de *surjection* ou *application surjective*, qui s'interprètent également en termes de "nombre d'éléments".

2.1 Applications injectives

Nous considérons à nouveau l'application successeur $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$. Supposons que m, n sont deux entiers naturels tels que $s(m) = s(n)$: autrement dit, on a $m + 1 = n + 1$ et intuitivement, m est le plus grand entier naturel strictement inférieur à $s(m)$, et n le plus grand entier naturel strictement inférieur à $s(n)$, et comme ces derniers sont égaux, on a $m = n$. Une autre façon de le voir est d'utiliser la propriété dite de *simplifiabilité* de l'addition des entiers naturels : si m, n, p sont trois entiers naturels tels que $m + p = n + p$, alors $m = n$. Alors, si $s(m) = s(n)$, c'est que $m + 1 = n + 1$, donc $m = n$! Toutefois, nous ne définirons qu'ultérieurement l'addition à partir des propriétés de la fonction successeur, dans le cours sur l'ensemble $\mathbb{N}$ des entiers naturels. A moins donc d'admettre la simplifiabilité de $+$ comme un postulat, nous nous appuyons sur l'intuition de la fonction successeur. Ceci montre qu'un entier naturel n a toujours *au plus un antécédent* par la fonction s, même si par définition, 0 n'a pas d'antécédent. Cette propriété, qui est en quelque sorte la propriété "duale" de la fonctionnalité du graphe d'une application, nous mène à la définition suivante, qui formalise l'idée de *l'unicité systématique d'un antécédent* par une application.

Définition 2.1.1. Si E et F sont deux ensembles, une application $f : E \to F$ est dite *injective*, ou est appelée une *injection*, si pour tous $x, x' \in E$ tels que $f(x) = f(x')$, on a $x = x'$ (autrement dit, si deux éléments du domaine de f qui ont la même image sont égaux).

Cette définition est une reformulation rigoureuse de la propriété : "tout élément du co-domaine de f a au plus un antécédent par f", en disant que "si deux éléments du domaine de f ont la même image par f, alors ils sont égaux". Il est habituel en mathématique d'avoir à reformuler des notions ou des propriétés intuitives sous une forme moins intuitive ou moins directe, pour obtenir une expression rigoureuse, dépourvue d'ambiguïté, qui est susceptible d'une utilisation plus claire dans les descriptions et démonstrations mathématiques.
Le successeur est notre exemple fondamental d'application (ou fonction) injective, et nous en verrons de nombreux autres. Nous avons mentionné précédemment que les opérations $+$ et $\times$, sur $\mathbb{R}$ ou l'un quelconque des sous-ensembles $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$, ne sont pas injectives, puisque certains éléments du co-domaine possède plusieurs antécédents. Donnons un exemple non-mathématique instructif.

Exemple 2.1.2. Soient F l'ensemble des adultes français et $S : F \to \mathbb{N}$ l'application qui associe à un adulte $a \in S$ son numéro de sécurité sociale (autrement dit, le graphe de S est l'ensemble des couples (a, n), où n est le numéro de sécurité sociale de a). Toute personne possède un unique tel numéro, donc S est bien une application, et deux adultes différents ont des numéros de sécurité sociale différents, sinon ces numéros n'ont aucune utilité. Par contraposée, si deux personnes ont le même numéro de sécurité sociale, "ils sont la même personne". Autrement dit, l'application S est injective.

Remarque 2.1.3. Pour montrer qu'une application $f : E \to F$ est injective, on utilise souvent la contraposée de la définition : on montre que si $x, x' \in E$ et $x \neq x'$,

alors on a $f(x) \neq f(x')$. C'est ce que nous avons fait dans l'exemple précédent, mais il faut prendre garde que ce procédé s'appuie sur la logique classique naturelle et n'est pas transposable en logique intuitionniste.

Pour un exemple mathématique, tournons-vous vers les fonctions "puissance" :

Exemple 2.1.4. Si $n \in \mathbb{N}$, alors la fonction $f : x \in \mathbb{R} \mapsto x^n$ est injective si et seulement si n est impair. Nous démontrerons ce résultat dans le cours sur les fonctions d'une variable réelle.

Pour les fonctions de $\mathbb{R}$ dans $\mathbb{R}$, on peut "visualiser" l'injectivité en considérant la représentation graphique : une application $f : \mathbb{R} \to \mathbb{R}$ est injective si et seulement si à chaque ordonnée $y \in \mathbb{R}$ il correspond au plus un seul point du graphe de f d'ordonnée y (voir les exercices).

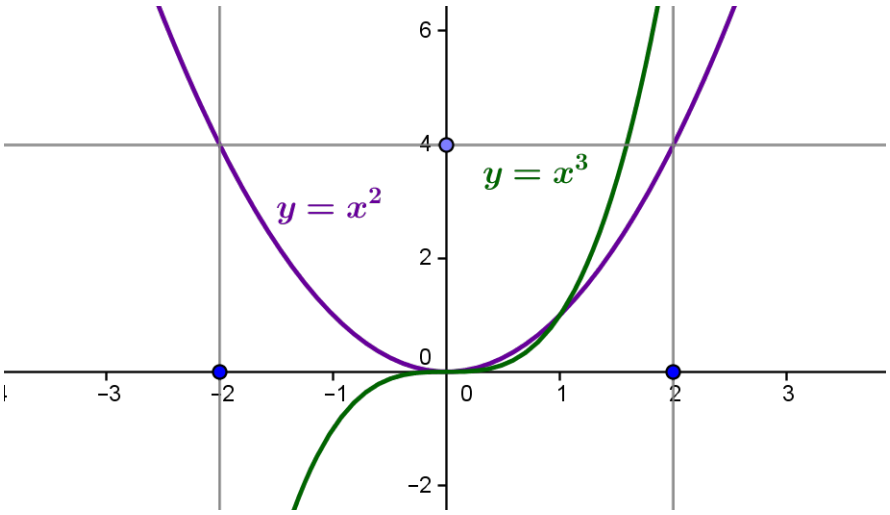

Figure 2.1: La fonction $f : x \in \mathbb{R} \mapsto x^3 \in \mathbb{R}$ est injective, tandis que la fonction $g : x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}^2$ n'est pas injective : par exemple, les deux nombres -2 et 2 ont la même image par g.

Le noyau d'une application

Si $f : E \to F$ est une application quelconque, il est possible de caractériser l'injectivité de f (c'est-à-dire de donner une condition équivalente à cette propriété) grâce à une certaine relation binaire sur E, appelée *noyau de* f.

Définition 2.1.5. Le *noyau de* f est l'ensemble N des couples $(x, y) \in E \times E$ tels que $f(x) = f(y)$.

Le noyau d'une application est l'exemple typique de ce que nous appellerons une *relation d'équivalence*. Il est évident que si $x \in E$, le couple (x, x) est un élément de N, car $f(x) = f(x)$. Ainsi, le noyau de f contient toujours l'ensemble des couples (x, x), pour $x \in E$, ce qu'on appelle la *diagonale* du produit $E \times E$, notée souvent Δ_E.
On peut alors caractériser les applications injectives grâce à cette diagonale, de la manière suivante :

Proposition 2.1.6. *Une application $f : E \to F$ est injective si et seulement si le noyau N de f est la diagonale Δ_E de E.*

Démonstration. Supposons que f est injective, et montrons que $N = \Delta_E$: comme $\Delta_E \subseteq N$, il suffit de montrer que $N \subseteq \Delta_E$. Soit donc $(x, y) \in N$: par définition, du noyau, on a $f(x) = f(y)$, et comme f est injective, on a $x = y$, si bien que $(x, y) = (x, x)$, donc $(x, y) \in \Delta_E$; on conclut que $N \subseteq \Delta_E$, d'où $N = \Delta_E$ par double inclusion. Réciproquement, supposons que $N = \Delta_E$ et montrons que f est injective : pour cela, soient $x, y \in E$ tels que $f(x) = f(y)$. Par définition du noyau, on a $(x, y) \in N$, et comme $N \subseteq \Delta_E$, on a $(x, y) \in \Delta_E$, soit $x = y$, si bien que f est injective. □

Exercices de la section

Exercice 2.1.7. i) Montrer qu'une application $f = (E, F, R)$ est injective si et seulement si la relation inverse de R est fonctionnelle.
ii) Montrer que l'application $m : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2.n$ est injective.
iii) La fonction valeur absolue $\mathbb{R} \to \mathbb{R}$ est-elle injective ?
iv) Si F est un ensemble, montrer que l'application vide $\emptyset \to F$ (c'est-à-dire à l'application dont le graphe est vide) est injective.
v) Si E est un ensemble, montrer que l'application $E \to E \times E$, $x \mapsto (x, x)$, est injective.
vi) Si $f : E \to F$ est une application, soit g la co-restriction de f à l'image de f. Si f est injective, montrer que g est injective.
vii) Montrer que la composition de deux applications injectives est injective.

2.2 Applications surjectives

Reprenons l'exemple de l'application "addition" $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, de graphe $A \subseteq \mathbb{R}^2 \times \mathbb{R}$. Pour tout nombre réel r, il existe un couple de nombres réels $(x, y) \in \mathbb{R}^2$ tel que $x + y = r$, par exemple le couple $(0, r)$. Comme nous l'avons déjà évoqué, il peut exister plusieurs antécédents différents pour r par l'addition (par exemple, $(r, 0)$ et $(1, r - 1)$ sont deux autres antécédents de r, puisque $r + 0 = r = 1 + (r - 1)$), ce qui montre que $+$ n'est pas injective. Cependant, cette propriété, "duale" de l'existence systématique d'un correspondant par une application, mène à la définition suivante, qui formalise l'idée de *l'existence systématique d'un antécédent* par une application.

Définition 2.2.1. Une application $f : E \to F$ est dite *surjective*, ou une *surjection*, si pour tout $y \in F$, il existe (au moins un) $x \in E$ tel que $f(x) = y$, autrement dit si tout élément y du co-domaine de f possède un antécédent par f.

Nous avons donné l'addition en exemple, il est évident que la multiplication des nombres réels (ou même complexes) est également surjective (voir les exercices). De même que le noyau d'une application est un ensemble particulier qui permet de caractériser les applications injectives, l'image d'une application (voir le cours de théorie naïve des ensembles) permet de caractériser les applications surjectives de manière simple.

Proposition 2.2.2. *Une application $f : E \to F$ est surjective si et seulement si l'image de f est F.*

Démonstration. Supposons que f soit surjective : si $y \in F$, il existe $x \in E$ tel que $f(x) = y$, si bien que $y \in Im(f)$, d'où $F = Im(f)$. Réciproquement si $F = Im(F)$, alors pour tout $y \in F$ on a $y \in Im(f)$ donc il existe $x \in E$ tel que $f(x) = y$, et f est surjective. □

Remarque 2.2.3. Le noyau et l'image d'une application ont des descriptions particulières en algèbre, ce que nous aurons l'occasion d'aborder dans les premiers cours d'algèbre, notamment à propos de la théorie des groupes et de la théorie des anneaux.

Mentionnons un cas très important d'application surjective. Si E et F sont deux ensembles *non vides*, on définit les *projections* $p : E \times F \to E$ (sur la première composante) et $q : E \times F \mapsto F$ (sur la seconde composante) par $p(x, y) = x$ et $q(x, y) = y$ pour tout $(x, y) \in E \times F$.
Notons que si E ou F est vide, alors $E \times F$ est vide, et on peut encore définir $p : E \times F \to E$ et $q : E \times F \to F$ comme les applications *vides* de co-domaines respectifs E et F, c'est-à-dire dont le graphe est l'ensemble vide (voir la section sur l'application vide dans le cours de théorie naïve des ensembles).

Proposition 2.2.4. *Si E et F ne sont pas vides, alors les projections $p : E \times F \to E$ et $q : E \times F \to F$ sont surjectives.*

Démonstration. La démonstration est proposée dans les exercices. □

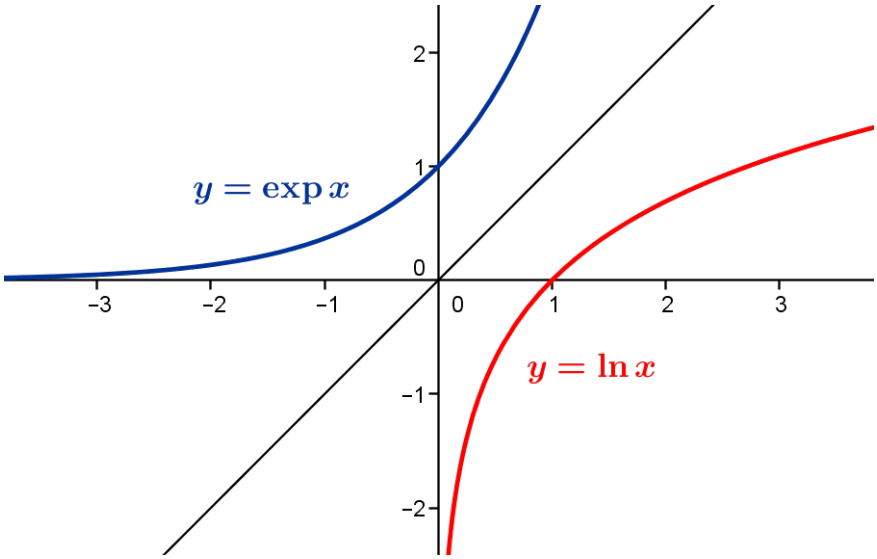

Figure 2.2: Les fonctions exponentielle $\exp : \mathbb{R} \to \mathbb{R}_+^*$ (en bleu) et logarithme (népérien) $\ln : \mathbb{R}_+^* \to \mathbb{R}$ (en rouge) sont réciproques, autrement dit pour $x \in \mathbb{R}$ on a $\ln \circ \exp(x) = x$, et pour $y \in \mathbb{R}_+^*$ on a $\exp \circ \ln(y) = y$. Elles sont donc toutes les deux surjectives.

Exercices de la section

Les exercices de cette leçon sont courts mais nombreux. Ces notions sont tellement importantes qu'il est nécessaire de s'y arrêter un peu.

Exercice 2.2.5. i) La fonction partie entière $E : \mathbb{R} \to \mathbb{Z}$ est-elle surjective ?
ii) Si F est un ensemble, à quelle condition l'application vide $\emptyset \to F$ est-elle surjective ?
iii) Si E est un ensemble, montrer que l'application $E \to E \times E$, $x \mapsto (x, x)$ n'est pas surjective. Quelle est son image ?
iv) Si E et F sont deux ensembles non vides, notons $p : E \times F \to E$, $(x, y) \mapsto x$ et $q : E \times F \to F$, $(x, y) \mapsto y$ les deux *projections* du produit $E \times F$. Montrer que p et q sont surjectives.
v) Montrer que la multiplication $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est surjective.
vi) Si $f : E \to F$ est une application, soit g la co-restriction de f à l'image de f. Expliquer pourquoi g est surjective.
vii) Montrer que la composition de deux applications surjectives est surjective.

2.3 Bijections et nombre d'éléments

Injections, surjections et le "nombre d'éléments"

Jusqu'ici nous n'avons pas discuté du "nombre d'éléments" d'un ensemble. Nous avons distingué au niveau intuitif entre les ensembles "finis" et les ensembles "infinis", et notre intuition est que le "nombre d'éléments" d'un ensemble fini est un entier naturel; cependant, le "nombre d'éléments" d'un ensemble infini, comme $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$, nous n'avons pas à ce stade d'indication sur ce qu'il serait.Pour le moment, considérons la notion d'injection $f : E \to F$ entre deux ensembles : tout élément de E "correspond" par f à un unique élément de F et deux éléments différents de E "correspondent" à deux éléments différents de F par f. On peut donc associer "un-à-un" tous les éléments de E avec certains éléments de F. Cependant, certains éléments de F peuvent bien n'avoir aucun antécédent par f; intuitivement, F *a plus d'éléments que* E lorsqu'il existe une injection f de E dans F. De manière duale, si $f : E \to F$ est une surjection, tout élément de F possède au moins un antécédent par f dans E, et deux éléments distincts de F ne peuvent pas avoir un antécédent commun, donc intuitivement E *a plus d'éléments que* F lorsqu'il existe une surjection de E sur F.
Il s'ensuit qu'on peut considérer que deux ensembles E et F "ont le même nombre d'éléments" lorsqu'il existe une injection de E dans F (F a "plus d'éléments" que E) et lorsqu'il existe une surjection de E sur F (E a "plus d'éléments" que F). On combine en fait les deux dans un seul concept, celui de *bijection*. Les exemples de l'addition et de la multiplication montrent qu'une surjection n'est pas nécessairement une injection; et l'exemple du successeur montre qu'une injection n'est pas nécessairement une surjection.

La notion de bijection

Quand nous combinons les deux notions, nous obtenons l'idée intuitive qui permet de déterminer quand deux ensembles ont "le même nombre d'éléments", et cette idée permet de définir à la fois ce qu'est un ensemble fini et ce qu'est son "nombre d'éléments", ainsi que ce qu'est un ensemble infini. La notion suivante exprime dans le langage de la théorie des ensembles l'idée simple qu'on peut mettre en correspondance "un-à-un" les éléments de deux ensembles, par le biais d'une application.

Définition 2.3.1. Une application $f : E \to F$ est dite *bijective*, ou une *bijection*, si elle est à la fois injective et surjective, en d'autres termes si pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$, symboliquement : $\forall y \in F,\ \exists! x \in E,\ f(x) = y$ (le symbole $\exists!$ signifie "il existe un unique").

Remarque 2.3.2. A travers une bijection, les éléments de deux ensembles sont mis en correspondance de manière unique (on dit aussi "bi-univoque"), de sorte que chaque élément d'un des deux ensembles est en relation avec exactement un élément de l'autre ensemble. De là provient l'idée que deux ensembles ont "le même nombre d'éléments" lorsqu'il existe une bijection de l'un sur l'autre, puisque leurs éléments sont "appariés". Il est remarquable qu'on n'ait pas pour cela à définir ce qu'est le nombre d'éléments d'un ensemble ! C'est en fait aussi une manière "détournée" de comparer la taille des ensembles infinis.

Vérifions que nous avons bien intégré les deux concepts d'injectivité et de surjectivité dans cette définition.

Proposition 2.3.3. *Une application $f : E \to F$ est bijective si et seulement si elle est à la fois injective et surjective.*

Démonstration. Supposons que f est bijective. En particulier, pour tout $y \in F$ il existe $x \in E$ tel que $f(x) = y$, donc f est surjective. De plus, si $x, x' \in E$ et $f(x) = f(x')$, posons $y = f(x)$: comme $f(x') = y = f(x)$ et f est bijective, il ne peut exister qu'un antécédent par f pour y, d'où $x = x'$, et f est injective. Inversement, supposons que f est à la fois injective et surjective, et soit $y \in F$: comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Supposons que $x' \in E$ ait cette propriété, c'est-à-dire que $f(x') = y$: comme f est injective, on a $x = x'$, donc il existe un unique $x \in E$ tel que $f(x) = y$, et ceci pour tout $y \in F$, si bien que f est bijective. □

Exemple 2.3.4. i) Nous avons déjà évoqué que l'application successeur $s : \mathbb{N} \to \mathbb{N}$ est injective, mais pas surjective. Sa co-restriction à son image, $s^{|\mathbb{N}^*} : \mathbb{N} \to \mathbb{N}^*$, est surjective : c'est donc une bijection. En général, la co-restriction de toute application injective à son image est une bijection.
ii) L'application $o : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto -n$, qui transforme un entier relatif en son opposé, est une bijection.

Rappelons que l'application dite *identique* d'un ensemble E dans lui-même est l'application notée $Id_E : E \to E$, qui associe à $x \in E$ le même élément $x \in E$. Il s'agit d'une bijection : en effet, pour tout $y \in E$, il existe un unique $x \in E$ tel

que $Id_E(x) = y$, à savoir y lui-même !
Lorsque $f : E \to F$ est une bijection entre deux ensembles, si pour chaque élément y de F on écrit $f^{-1}(y) = x$ pour l'unique élément x de E tel que $f(x) = y$, alors on définit une application en sens inverse, notée $f^{-1} : F \to E$.

Proposition 2.3.5. *Si E, F et G sont trois ensembles et $f : E \to F$, $g : F \to G$ sont deux bijections, alors :*
i) L'application $f^{-1} : F \to E$ est une aussi une bijection, et on a $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$. L'application f^{-1} est appelée bijection réciproque *de f.*
ii) L'application composée $g \circ f : E \to G$ est elle-même une bijection, de bijection réciproque $(g \circ f)^{-1} = f^{-1} \circ g^{-1} : G \to E$.

Démonstration. i) Soit $x \in E$: par définition d'une application, il existe un unique $y \in F$ tel que $y = f(x)$; par définition de f^{-1}, on a donc $f^{-1}(y) = x$, si bien qu'il existe un unique $y \in F$ tel que $f^{-1}(y) = x$, et f^{-1} est donc une bijection. La démonstration des égalités $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$ est laissée à l'étudiant(e).
ii) Soit $z \in G$: comme g est une bijection, il existe un unique $y \in F$ tel que $g(y) = z$; comme f est une bijection, il existe un unique $x \in E$ tel que $f(x) = y$. En particulier, on a $g \circ f(x) = z$, donc $g \circ f$ est surjective; si $x' \in E$ est tel que $g \circ f(x') = z$, alors $f(x) = f(x')$ puisque g est injective, et $x = x'$ puisque f est injective : $g \circ f$ est injective, c'est donc une bijection. Par définition, si $z \in G$ alors $(g \circ f)^{-1}(z)$ est l'unique $x \in E$ tel que $g \circ f(x) = z$; comme $g \circ f(f^{-1} \circ g^{-1}(z)) = g(f(f^{-1}(g^{-1}(z)))) = g(g^{-1}(z)) = z$ par (i), on en déduit que $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$, et puisque c'est vrai pour tout $z \in G$, que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Remarque 2.3.6. i) Il ne faut pas confondre la bijection réciproque f^{-1}, lorsqu'elle existe, avec l'image réciproque d'une partie, aussi notée f^{-1}. Cet abus de notation n'est pas gênant en pratique, car la bijection réciproque (qui n'existe pas toujours) s'applique à des éléments, et l'image réciproque (qui existe toujours) s'applique à des parties.
ii) Dans la fin de la démonstration de (ii), on démontre que deux applications sont égales en montrant qu'elles prennent la même valeur sur chaque élément de leur domaine. C'est la méthode générale qu'on emploie pour montrer l'égalité de deux applications, et c'est en fait une forme du principe d'extensionnalité (voir le cours de théorie naïve des ensembles).

Exemple 2.3.7. i) La bijection réciproque de la fonction $o : \mathbb{Q} \to \mathbb{Q}$, $q \mapsto -q$, est la fonction o elle-même.
ii) La restriction de la valeur absolue $|.| : \mathbb{R} \to \mathbb{R}_+$ à $\mathbb{R}_+$ est la fonction identique de $\mathbb{R}_+$, c'est donc une bijection. Mais la fonction valeur absolue n'est pas bijective, car elle n'est pas injective : par exemple $|-1| = 1 = |1|$, mais $-1 \neq 1$.
iii) La fonction $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$, est une bijection (nous le démontrerons lorsque nous aborderons les fonctions d'une variable réelle); sa bijection réciproque est la fonction *racine cubique* $\sqrt[3]{} : \mathbb{R} \to \mathbb{R}$. De même, l'application $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$, est une bijection, de bijection réciproque $h : \mathbb{R} \to \mathbb{R}$, $x \mapsto x - 1$. Il s'ensuit que l'application composée $g \circ f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 + 1$ est une bijection, de bijection réciproque $f^{-1} \circ g^{-1} : x \in \mathbb{R} \mapsto \sqrt[3]{x - 1}$.

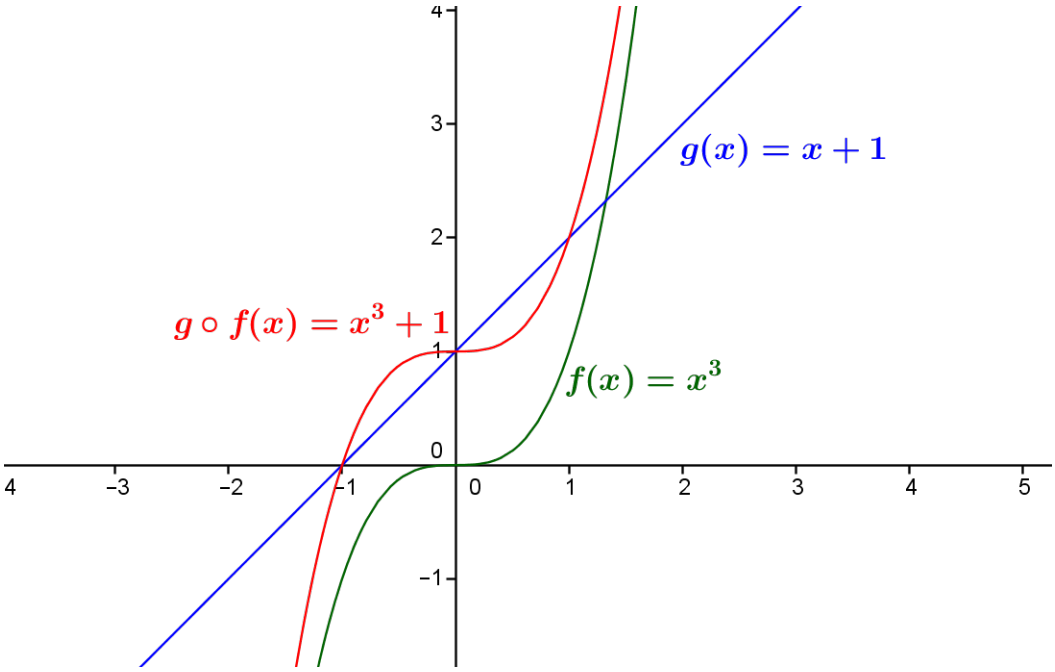

Figure 2.3: La fonction $x \mapsto x^3 + 1$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$, obtenue par composition des fonctions bijectives $f : x \mapsto x^3$ et $g : x \mapsto x + 1$, de $\mathbb{R}$ sur $\mathbb{R}$.

Équipotence

La notion de bijection, combinée avec l'intuition du "nombre d'éléments", se repense du point de vue des ensembles qu'on met en bijection :

Définition 2.3.8. Deux ensembles E et F sont dits *équipotents* (autrement dit E et F ont la même "puissance") si il existe une bijection de E sur F.

Remarque 2.3.9. o) Tout ensemble E est équipotent à lui-même, par l'application identique Id_E.
i) Si on peut mettre en évidence une bijection entre deux ensembles, il y a en général plusieurs bijections pour des ensembles contenant strictement plus d'un élément. Le choix de l'une d'entre elles n'a aucune importance par rapport à la question de l'équipotence. Autrement dit, peu importe comment on "apparie" les éléments des deux ensembles, si l'on ne s'intéresse qu'à leur "puissance".
ii) Si E et F sont équipotents, et si G est un troisième ensemble équipotent à F, alors E et F sont équipotents (voir les exercices).

A l'aide de ces quelques concepts nous pouvons déjà démontrer un théorème remarquable de Cantor, qui permet de comparer la "puissance" d'un ensemble et celle de l'ensemble de ses parties. Si E est un ensemble, notons qu'on a une application naturelle f qui associe à $x \in E$ le singleton $\{x\}$, élément de $\mathscr{P}(E)$; autrement dit, le graphe de f est l'ensemble des couples $(x, \{x\})$, pour $x \in E$. Si $y \in E$ et $f(x) = f(y)$, c'est que $\{x\} = \{y\}$ et par extensionnalité, on a nécessairement $x = y$, donc f est injective, et $\mathscr{P}(E)$ a "plus d'éléments" que E. En fait, il a "*strictement* plus d'éléments" :

Théorème 2.3.10 (Cantor)**.** *Pour tout ensemble E, il n'existe pas de surjection de E sur l'ensemble $\mathscr{P}(E)$ des sous-ensembles de E.*

Démonstration. Distinguons deux cas, selon que E est vide ou non. Si $E = \emptyset$, on a $\mathscr{P}(E) = \{\emptyset\}$; supposons par l'absurde qu'il existe une surjection $f : E \to \mathscr{P}(E)$: en particulier, comme $\emptyset \in \mathscr{P}(E)$ il existe $x \in E$ tel que $f(x) = \emptyset$, mais ceci contredit la vacuité de E. Par *reductio ad absurdum*, une telle surjection n'existe pas. Dans le second cas, c'est-à-dire si E n'est pas vide, supposons par l'absurde qu'il existe une surjection $f : E \to \mathscr{P}(E)$, et soit $A = \{x \in E : x \notin f(x)\}$, en d'autres termes A est l'ensemble des éléments de E qui ne sont pas éléments de leur image par f (ce qui a du sens puisque $f(x)$ est un sous-ensemble de E). Comme sous-ensemble de E, A est un élément de $\mathscr{P}(E)$, donc comme f est une surjection il existe $x \in E$ tel que $A = f(x)$. Supposons que $x \in A$: par définition de $A = f(x)$, on a $x \notin A$, ce qui est impossible, donc on a $x \notin A$. Cependant, par définition de A à nouveau, on a $x \in f(x) = A$, donc on a à la fois $x \in A$ et $x \notin A$, ce qui est impossible. Par *reductio ad absurdum*, il n'existe donc pas de surjection de E sur $\mathscr{P}(E)$, et les deux cas épuisant les possibilités, le théorème est démontré. □

Remarque 2.3.11. i) Cette démonstration est une variante du "paradoxe de Russell" : on ne peut pas parler d'un "ensemble de tous les ensembles".
ii) Puisqu'il n'existe pas de surjection de E sur $\mathscr{P}(E)$, en particulier il n'existe pas de bijection.

Ce théorème dit intuitivement que l'ensemble des parties d'un ensemble E donné a toujours strictement "plus d'éléments" que l'ensemble E.
Grâce à la notion de bijection, nous allons désormais pouvoir définir rigoureusement les notions d'ensemble *fini* et d'ensemble *infini*, et étudier quelques-unes de leurs propriétés.

Exercices de la section

Exercice 2.3.12. o) Montrer qu'une application $f : E \to F$ est bijective si et seulement si il existe une application $g : F \to E$ telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.
i) Montrer qu'une application $f : E \to F$ est bijective si et seulement si la relation opposée R^o du graphe R de f définit une application dans l'autre sens, c'est-à-dire de F dans E.
ii) Montrer que l'application $f : \mathbb{R}_+ \to \mathbb{R}_+$, $x \mapsto x^2$, est bijective. Quelle est la bijection réciproque de f ?
iii) Soient n et k deux entiers naturels, et soit $f : [[0, n]] \to [[k, k + n]]$, telle que $f(i) = i + k$ pour tout $i \in [[0, n]]$, où pour tous entiers naturels p et q, $[[p, q]] = \{m \in \mathbb{N} : p \leq m \leq q\}$. Démontrer que f est une bijection.
iv) Montrer que l'application $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto -2x$, est une bijection. Même question avec $h : \mathbb{R} \to \mathbb{R}$, $x \mapsto a.x + b$, où a est un nombre réel non nul quelconque et $b \in \mathbb{R}$: quelle est la bijection réciproque de h ?
v) Supposons que E, F et G sont trois ensembles et que E est équipotent à F, et F est équipotent à G. Montrer que E est équipotent à G. Indication : utiliser la composée de deux bijections.

2.4 Multiplets et produits finis d'ensembles

Cette section complète utilement les bases de théorie naïve des ensembles par la généralisation des couples, triplets... d'éléments d'un ensemble, et leur représentation comme des applications. Si a et b sont deux objets, le *couple* (a, b) a été défini dans le cours de théorie naïve des ensembles (Cycle I, cours n° 1), comme l'ensemble $\{\{a\}, \{a, b\}\}$, et si E et F sont deux ensembles, l'ensemble des couples (a, b), pour $a \in E$ et $b \in F$, est par définition le produit cartésien $E \times F$. La notion de triplet de trois objets a, b, c a été définie à partir de celle de couple : le *triplet* (a, b, c) est par définition le couple $((a, b), c)$ formé des objets (a, b) et c. De manière générale, on peut définir un *n-uplet* d'objets par récurrence sur $n \geq 1$, à condition de choisir ces objets dans un même ensemble E. Ceci revient à définir les *puissances cartésiennes* d'un ensemble E, par récurrence sur $n \geq 1$.

Définition 2.4.1. Si E est un ensemble et n un entier naturel non nul, on définit la *n-ième puissance (cartésienne)* de E, notée E^n, par récurrence sur n, en posant $E^1 := E$ et $E^{n+1} = E^n \times E$ pour tout $n \geq 1$.

Les éléments de E^n sont ainsi les "n-uplets" d'éléments de E : pour $n = 1$, on retrouve les éléments de E, pour $n = 2$, les couples d'éléments de E, et pour $n = 3$ les éléments de $E^3 = E^2 \times E$ sont les triplets $((a, b), c)$, où $a, b, c \in E$.
Cette description des n-uplets d'éléments d'un ensemble E devient vite illisible : pour $n = 4$, les éléments de E^4 sont les "quadruplets" (a, b, c, d) d'éléments de E, soit les couples $(((a, b), c), d)$ pour $((a, b), c) \in E^3$ et $d \in E$. Il est alors plus commode d'en donner une autre représentation, plus naturelle et conforme à l'idée intuitive qui consiste à les considérer comme des "listes" finie d'éléments, de longueur donnée.

Définition 2.4.2. Si E est un ensemble et $n \in \mathbb{N}^*$, un *n-uplet d'éléments de E* est une application $f : [[1, n]] \to E$.

Remarque 2.4.3. i) Pour $n = 1$, un 1-uplet est désormais une application de $[[1, 1]] = \{1\}$ dans E. Il devrait être évident que cet ensemble est naturellement en bijection avec E. Pour $n = 2$, un 2-uplet est une application $[[1, 2]] \to E$, qui spécifie bien une liste de 2 éléments, etc...
ii) On pourrait étendre la définition à $n = 0$, et alors E^0 serait l'ensemble des applications de $[[1, 0]] = \emptyset$ dans E, qui ne contient qu'un élément, puisque la seule application de $\emptyset$ dans E est l'application vide.

Lorsqu'on considère un n-uplet $f : [[1, n]] \to E$ d'un ensemble E, on note souvent les images des éléments de $[[1, n]]$ par f sous la forme f_i plutôt que $f(i)$. Ainsi l'image de f peut être décrite comme $Im(f) = \{f_1, f_2, \ldots, f_n\}$ et on note le n-uplet f lui-même comme $(f_1, \ldots, f_n)$, pour reprendre la notation des couples. On utilise aussi souvent pour f une notation qui suggère plutôt un élément, par exemple $a : [[1, n]] \to E$, ce qu'on écrit $(a_1, \ldots, a_n)$: l'ensemble E^n est donc $\{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in E\}$. Il faut bien noter ici que les éléments a_i ne sont pas nécessairement distincts : autrement dit, un multiplet $a : [[1, n]] \to E$ n'est pas une application injective en général. Pour décrire un ensemble E à n éléments, on utilise souvent cette notation, en omettant la description d'une fonction qui met en bijection les ensembles $[[1, n]]$ et

E. Dans ce cas, on écrit simplement $E = \{a_1, \ldots, a_n\}$ en introduisant implicitement une telle bijection $a : [[1, n]] \to E$ pour laquelle $a(i) = a_i$ pour $i = 1, \ldots, n$.
Cette définition alternative des multiplets d'éléments d'un ensemble est intéressante dans la mesure où elle remplace de manière "exacte" la définition donnée à partir des produits cartésiens : c'est ce que nous vérifions maintenant. La démonstration de la proposition suivante, un peu difficile, peut être omise en première lecture.

Proposition 2.4.4. *Pour tout ensemble E et pour tout entier naturel n non nul, il existe une bijection entre E^n et $E^{[[1,n]]}$.*

Démonstration. On distingue deux cas, selon que $E = \emptyset$ ou non. Si $E = \emptyset$, alors $E^{[[1,n]]}$ est vide, car il n'existe aucune application d'un ensemble non vide dans $\emptyset$; l'ensemble $E^1 = E$ est vide, et si on suppose par récurrence pour $n \geq 1$ que $E^n = \emptyset$, on a $E^{n+1} = E^n \times E = \emptyset$ également, si bien que $E^n = \emptyset$ pour tout $n \geq 1$ par récurrence, et $E^{[[1,n]]}$ et E^n sont en bijection pour tout $n \geq 1$ dans ce cas-là. Supposons désormais que $E \neq \emptyset$ et démontrons par récurrence que $n \geq 1$ qu'il existe une bijection entre E^n et $E^{[[1,n]]}$. Si $n = 1$, à $a \in E$ on associe l'application $f_a : \{1\} = [[1, 1]] \to E$, $1 \mapsto a$: on définit ainsi une application $\Phi : E^1 = E \to E^{\{1\}}$, $a \mapsto f_a$ et on vérifie facilement qu'il s'agit d'une bijection. Supposons la propriété établie au rang $n \geq 1$, c'est-à-dire qu'il existe une bijection $\Phi : E^n \cong E^{[[1,n]]}$ et montrons qu'il existe une bijection entre E^{n+1} et $E^{[[1,n+1]]}$. Par définition, on a $E^{n+1} = E^n \times E$, et si $(a, b) \in E^{n+1}$, on lui associe le $n+1$-uplet $f_{(a,b)} : [[1, n+1]] \to E$, défini de la manière suivante : par définition, $\Phi(a) \in E^{[[1,n]]}$ est un n-uplet $(\varphi(a)_1, \ldots, \varphi(a)_n)$ d'éléments de E, donc on pose $f_{(a,b)}(i) = \Phi(a)_i$ pour $i \in [[1, n]]$, et $f_{(a,b)}(n+1) = b$. On a ainsi défini une application $\Psi : E^{n+1} \to E^{[[1,n+1]]}$, $(a, b) \mapsto f_{(a,b)}$, et on vérifie qu'il s'agit d'une bijection. Supposons que $(a', b') \in E^{n+1}$, et que $\Psi_{(a,b)} = \Psi_{(a',b')}$: on a $f_{(a,b)} = f_{(a',b')}$, d'où $\Phi(a)_i = \Phi(a')_i$ pour $i = 1, \ldots, n$ et $b = b'$, si bien que $\Phi(a) = \Phi(a')$ et $b = b'$: comme Φ est injective, on en déduit que $(a, b) = (a', b')$, et Ψ est injective. Supposons que $(x_1, \ldots, x_{n+1}) \in E^{[[1,n+1]]}$: on a $(x_1, \ldots, x_n) \in E^{[[1,n]]}$ (restriction de x à $[[1, n]]$), et comme Φ est surjective, il existe $a \in E^n$ tel que $\Phi(a) = (x_1, \ldots, x_n)$; on alors $\Psi((a, x_{n+1})) = (x_1, \ldots, x_{n+1})$ par définition de Ψ, qui est donc surjective, et finalement bijective. Par récurrence, il existe une bijection de E^n sur $E^{[[1,n]]}$ pour tout $n \geq 1$. □

Par abus de notation, on écrit souvent E^n pour l'ensemble $E^{[[1,n]]}$, ou du moins on décrit les éléments de E^n comme des n-uplets de la forme $(a_1, \ldots, a_n)$, pour $a_1, \ldots, a_n \in E$. Cet abus se justifie par la proposition 2.4.4 et est fort utile dans toute la mathématique, notamment la théorie des espaces vectoriels.

Chapitre 3

Dénombrement des Ensembles Finis

Dans le chapitre précédent, nous avons appris à comparer le nombre d'éléments de deux ensembles sans avoir à les "compter", grâce aux notions d'injection, de surjection et de bijection. Dans ce chapitre, nous allons appliquer ces connaissances à la définition rigoureuse des ensembles finis, au dénombrement, c'est-à-dire au comptage "théorique" de certains d'entre eux, et plus largement à la combinatoire, c'est-à-dire à une théorie des ensembles finis.

3.1 Le nombre d'éléments d'un ensemble fini

Ensembles finis

Grâce à la notion de bijection, nous pouvons désormais définir rigoureusement ce qu'est un ensemble fini. Une fois n'est pas coutume, il suffit ici d'adopter la définition la plus intuitive qui soit : un ensemble est fini lorsqu'on peut en compter les éléments.

Définition 3.1.1. Un ensemble E est dit *fini* si il existe une bijection entre E et un sous-ensemble de $\mathbb{N}$ de la forme $[[1, n]] = \{m \in \mathbb{N} : 1 \leq m \leq n\}$. Un ensemble E est dit *infini* si il n'est pas fini.

Remarque 3.1.2. i) "Fini" et "infini" sont deux concepts "complémentaires" : si on a une définition de l'un, on a une définition de l'autre par la propriété opposée. La définition présente de l'infini peut paraître décevante.
ii) On pourrait définir autrement la notion d'ensemble infini et définir à partir de là la notion d'ensemble fini, mais cela serait assez maladroit. Nous donnerons dans le chapitre suivant deux caractérisations intéressantes des ensembles infinis, qui ne mentionnent pas explicitement les ensembles finis.
iii) La relation $\leq$ est pour l'instant entendue au sens intuitif, à moins de la définir à partir de l'addition grâce aux axiomes de Peano, que nous aborderons dans le cours d'arithmétique naturelle.
iv) Pour établir de nombreux résultats sur les ensembles finis, nous devrons utiliser le principe de récurrence (introduit dans le cours de logique mathématique naturelle).

Compter les ensembles finis

Il semble évident qu'un ensemble fini possède un nombre bien déterminé d'éléments, lequel est un entier naturel. Cela n'est toutefois pas immédiatement visible à partir de la définition : si E est un ensemble fini, il existe une bijection entre E et un ensemble de la forme $[[1, n]]$, mais rien ne garantit *a priori* qu'il n'existe pas une bijection entre E et un autre ensemble $[[1, m]]$ avec $m \neq n$! Il peut paraître étrange d'envisager une telle situation, mais gardons à l'esprit que nous théorisons rigoureusement la notion d'ensemble fini, et l'univocité du "nombre d'éléments" d'un tel ensemble ne fait pas partie explicitement de la définition. Nous devons le vérifier pour obtenir une définition sensée d'un ensemble fini, et du nombre d'éléments d'un tel ensemble. On se ramène pour commencer aux bijections entre ensembles de la forme $[[1, n]]$.

Lemme 3.1.3. *Si $f : [[1, n]] \hookrightarrow [[1, m]]$ est une injection, alors on a $n \leq m$.*

Démonstration. Eliminons le cas où $m = 0$: on a alors $[[1, m]] = \{x \in \mathbb{N} : 1 \leq m \leq 0\} = \emptyset$, puisqu'aucun entier supérieur à 1 n'est nul, si bien que $[[1, n]] = \emptyset$ également, donc $n = 0$, d'où $n \leq m$. Supposons désormais que $m > 0$ et raisonnons par récurrence sur n. Si $n = 0$, on a bien sûr $n \leq m$, et la propriété est vérifiée. Supposons que la propriété soit vérifiée pour l'entier n, et soit $f : [[1, n + 1]] \hookrightarrow [[1, m]]$ une application injective; nous distinguons deux cas. Si $f(n + 1) = m$, alors l'application $g : [[1, n]] \to [[1, m - 1]]$, $i \mapsto f(i)$ (et qui est la co-restriction à $[[1, m-1]]$ de la restriction de f à $[[1, n]]$) est injective, puisque f est injective, et par hypothèse de récurrence, on a $n \leq m - 1$, d'où $n+1 \leq m$, ce qui est la propriété au rang $n + 1$. Dans l'autre cas, c'est-à-dire si $f(n + 1) \neq m$, soit $g : [[1, m]] \to [[1, m]]$ l'application définie par $g(f(n + 1)) = m$, $g(m) = f(n + 1)$ et $g(i) = i$ pour tout $i \neq m, f(n+1)$ (g "échange" m et $n+1$); on vérifie facilement que g est injective (en fait, g est bijective), donc la fonction composée $g \circ f : [[1, n+1]] \hookrightarrow [[1, m]] \hookrightarrow [[1, m]]$ est injective, et $g \circ f(n+1) = m$ par définition de g. Par le premier cas, on en déduit cette fois encore que $n+1 \leq m$, ce qui est la propriété au rang $n+1$. Par le principe de récurrence, le lemme est démontré. □

Proposition 3.1.4. *Si E est un ensemble fini, il existe un unique entier naturel n tel qu'il existe une bijection entre E et $[[1, n]]$.*

Démonstration. Par définition, il existe un entier natural n et une bijection $f : E \to [[1, n]]$. Supposons que m soit un entier naturel avec cette propriété, c'est-à-dire qu'il existe une bijection $g : E \cong [[1, m]]$. L'application composée $g \circ f^{-1} : [[1, n]] \to [[1, m]]$ est une bijection par la proposition 2.3.5, et par le lemme 3.1.3 on a donc $n \leq m$. En considérant la bijection inverse $f \circ g^{-1} : [[1, m]] \to [[1, n]]$, pour la même raison on conclut que $m \leq n$, et finalement on a $n = m$, et n est unique. □

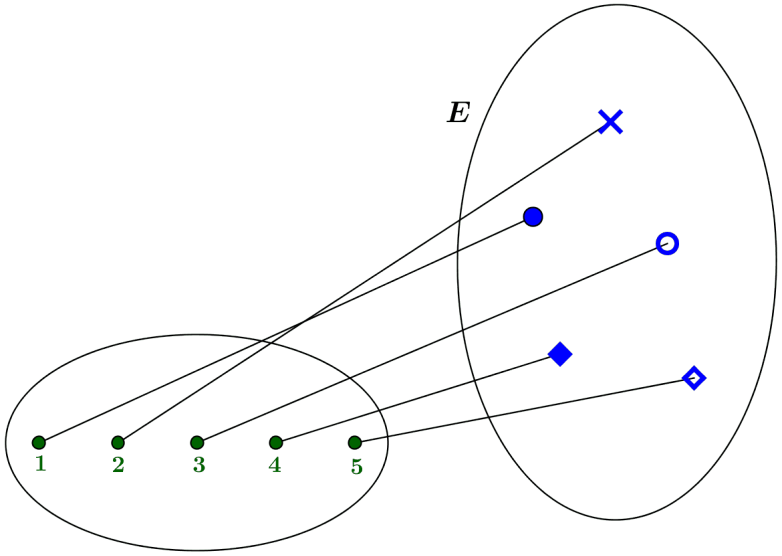

Figure 3.1: Dénombrer un ensemble E, c'est décrire *une* bijection entre E et un ensemble de la forme $[[1, n]]$; il existe en général plusieurs telles bijections. Ici, E possède 5 éléments.

Nous sommes désormais en mesure de *définir* proprement le nombre d'éléments d'un ensemble fini :

Définition 3.1.5. L'unique entier naturel n tel que l'ensemble fini E est en bijection avec l'ensemble $[[1, n]]$ s'appelle le *cardinal de* E ou *nombre d'éléments de* E. On note $|E|$ le cardinal de E.

Remarque 3.1.6. Rappelons que nous avons défini le concept d'équipotence ("avoir le même nombre d'éléments") *avant* d'avoir défini le nombre d'éléments d'un ensemble fini. En ce qui concerne les ensembles infinis, il n'est pas possible en théorie naïve des ensembles de définir leur cardinal ou nombre d'éléments, même si on peut dire quand deux tels ensembles ont le même nombre d'éléments. Pour compter le nombre d'éléments d'un ensemble infini, il faut des cardinaux infinis, qui doivent être introduits à l'intérieur d'un "univers ensembliste".

Proposition 3.1.7. *Si E est un ensemble fini à $n+1$ éléments, alors pour tout $x \in E$, l'ensemble $E - \{x\}$ est fini et possède n éléments.*

Démonstration. Par définition, il existe une bijection $f : E \cong [[1, n+1]]$; si $x \in E$, soit $F = E - \{x\}$, et soit $k = f(x)$. L'application $g : F \to [[1, n+1]] - \{k\}$, $y \in F \mapsto f(y)$, est évidemment une bijection (l'étudiant(e) est invité(e) à le vérifier), et il suffit par composition des bijections de démontrer maintenant la proposition pour $E = [[1, n+1]]$. En effet, si le résultat est démontrer pour ce type d'ensemble, alors F et $[[1, n+1]] - \{k\}$ ont alors le même nombre d'éléments, soit n. Soient donc $k \in E = [[1, n+1]]$ et $f : E - \{k\} \to [[1, n]]$ définie comme suit : on pose $f(i) = i$ si $i < k$ (si $k = 1$, ce cas n'existe pas) et $f(i) = i - 1$ si $k < i$. Montrons que f est injective : si $i, j \in E$ et $f(i) = f(j)$, soit $i, j < k$ et alors $i = f(i) = f(j) = j$, soit $i < k$ et $j > k$ et alors $i = f(i) = f(j) = j - 1 \geq k$, ce qui est impossible, soit

$i, j > k$ et alors $i - 1 = f(i) = f(j) = j - 1$, donc $i = j$: dans tous les cas, on a $i = j$, donc f est injective. Montrons que f est surjective : si $j \in [[1, n]]$, soit $j < k$ et alors $f(j) = j$, soit $j > k$ et alors $f(j + 1) = j$, donc f est surjective. On conclut que f est bijective, donc $[[1, n + 1]] - \{k\}$ possède n éléments, et la proposition est démontrée. □

A partir de là, on peut démontrer la finitude de la réunion de deux ensembles finis :

Corollaire 3.1.8. *La réunion de deux ensembles finis E et F est un ensemble fini.*

Démonstration. On raisonne par récurrence sur le cardinal m de $F - E$. Si $n = 0$, on a $F - E = \emptyset$, donc $E \cup F = E$, ensemble fini par hypothèse. Supposons que la propriété soit vérifiée au rang n et que $F - E$ possède $n + 1$ éléments : en particulier, il existe $x \in F - E$, si bien que $(F - \{x\}) - E = (F - E) - \{x\}$ est fini et possède n éléments par la proposition 3.1.7. Par hypothèse de récurrence, l'ensemble $(E \cup F) - \{x\} = E \cup (F - \{x\})$ est fini, si bien qu'il existe une bijection $f : (E \cup F) - \{x\} \to [[1, m]]$ pour un certain entier m. Définissons une application $g : E \cup F \to [[1, m + 1]]$ de la manière suivante : pour tout $y \in (E \cup F) - \{x\}$, on pose $g(y) = f(y)$, et on pose $g(x) = m + 1$. On vérifie aisément que g est une bijection, si bien que $E \cup F$ est fini. □

Remarque 3.1.9. Il paraît "évident" que la réunion de deux ensembles finis est un ensemble fini. Cependant, en choisissant de traduire l'intuition de ce qu'est un ensemble fini par la définition que nous avons adoptée, il devient nécessaire d'établir rigoureusement ce qui relève de l'intuition originelle.

Exercices de la section

Exercice 3.1.10. i) Démontrer que pour tout entier naturel n, l'ensemble $[[0, n]] = \{k \in \mathbb{N} : 0 \leq k \leq n\}$ est fini, de cardinal $n + 1$.
ii) Si E et F sont deux ensembles finis, de cardinaux respectifs m et n, montrer par récurrence sur n que le cardinal de $E \cup F$ est inférieur ou égal à $m + n$.

3.2 Les sous-ensembles d'un ensemble fini

Finitude des sous-ensembles et cardinaux

Comme corollaire de la proposition 3.1.7, nous pouvons démontrer la proposition essentielle suivante.

Corollaire 3.2.1. *Si E est un ensemble fini, alors tout sous-ensemble de E est fini. En particulier, l'intersection de deux ensembles finis est un ensemble fini.*

Démonstration. Raisonnons par récurrence sur le cardinal n de E. Si $n = 0$, alors E est vide, donc le seul sous-ensemble de E est E-lui-même, et tout sous-ensemble de E est donc fini. Supposons que la propriété soit vraie au rang n, et supposons que E possède $n + 1$ éléments : si $X \subseteq E$, soit $X = E$ et alors X est fini, soit $X \neq E$ donc il existe $x \in E - X$, si bien que $X \subseteq E - \{x\}$. Par la proposition 3.1.7, le cardinal

de $E - \{x\}$ est n, et comme X est alors un sous-ensemble d'un ensemble de cardinal n, par l'hypothèse de récurrence on en déduit que X est fini. Concernant la seconde assertion, si E et F sont deux ensembles finis, alors $E \cap F$ est un sous-ensemble de E, donc c'est un ensemble fini. □

La formule suivante des "cardinaux" est fondamentale.

Proposition 3.2.2. *Si E est F sont deux ensembles finis, alors on a $|E \cup F| = |E| + |F| - |E \cap F|$. Autrement dit, on a $|E \cup F| + |E \cap F| = |E| + |F|$.*

Démonstration. Nous commençons par le cas particulier où $E \cap F = \emptyset$. Comme E et F sont finis, il existe deux entiers naturels m, n et deux bijections $f : E \to [[1, m]]$, $g : F \to [[1, n]]$. Définissons une application $h : E \cup F \to [[1, m + n]]$ de la manière suivante : si $x \in E$, alors on pose $h(x) = f(x)$, tandis que si $x \in F$, on pose $h(x) = m + g(x)$; étant donné que E et F sont disjoints, on ne peut avoir $x \in E \cap F$ donc ces deux cas s'excluent mutuellement et h est bien définie comme application. Supposons que $x, y \in E \cup F$ et que $h(x) = h(y)$: si $x, y \in E$, alors $f(x) = f(y)$, donc $x = y$ car f est injective; si $x \in E$ et $y \in F$, alors $h(x) \leq m$ mais $h(y) > m$, ce qui est impossible : ce cas n'existe pas; si $x, y \in F$, alors $m + g(x) = m + g(y)$, donc $g(x) = g(y)$, si bien que $x = y$ car g est injective; dans tous les cas on a $x = y$, donc h est injective. Supposons que $i \in [[1, m + n]]$: si $i \leq m$, comme f est surjective il existe $x \in E$ tel que $h(x) = f(x) = i$; si $i > m$, on a $i \in [[m + 1, m + n]]$, donc $i - m \in [[1, n]]$, si bien que par surjectivité de g il existe $x \in F$ tel que $g(x) = i - m$, d'où $h(x) = m + g(x) = i$, et h est surjective. Nous avons ainsi démontré que $m + n = |E \cup F| = |E| + |F|$, ce qui est l'égalité énoncée dans ce cas particulier, puisque $|E \cap F| = 0$. Dans le cas général, on remarque que $E \cup F = E \cup (F - E)$ et que $F = (F \cap E) \cup (F - E)$: ce sont deux réunions d'ensembles disjoints, si bien que par le cas particulier on peut écrire $|E \cup F| = |E| + |F - E|$ et $|F| = |F \cap E| + |F - E|$; en combinant ces deux égalités, on obtient l'égalité voulue; nous laissons les détails à l'étudiant(e). □

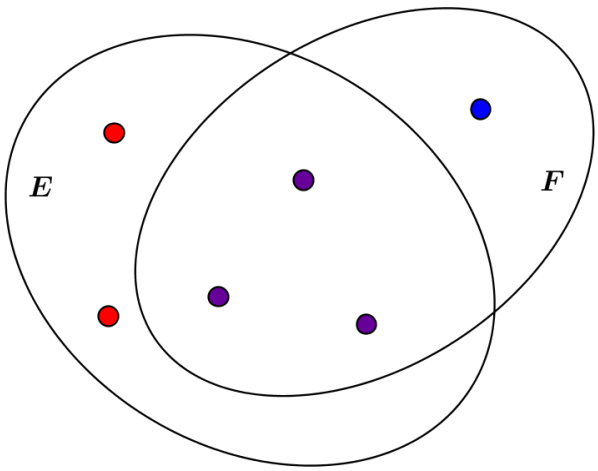

Figure 3.2: L'ensemble $E \cup F$ possède 6 éléments et l'ensemble $E \cap F$ en possède 3 : on vérifie que $9 = 6 + 3 = |E \cup F| + |E \cap F| = |E| + |F| = 5 + 4$.

Finitude de l'ensemble des parties

Dans la section 2.3, nous avons démontré le théorème de Cantor : l'ensemble des parties d'un ensemble E a toujours strictement plus d'éléments que E. Dans le cas des ensembles finis, nous pouvons préciser ce résultat en donnant le nombre d'éléments de $\mathscr{P}(E)$.

Proposition 3.2.3. *Si E est un ensemble fini à n éléments, alors l'ensemble $\mathscr{P}(E)$ est fini et possède 2^n éléments.*

Démonstration. Nous procédons par récurrence sur le nombre n d'éléments de E. Si $n = 0$, alors E est vide et $\mathscr{P}(E) = \{\emptyset\}$ est fini et ne possède qu'un seul élément. Supposons que la propriété soit vraie pour un entier naturel n, c'est-à-dire que tout ensemble fini à n éléments possède un ensemble fini de parties à 2^n éléments, et soit E un ensemble fini à $n+1$ éléments; en particulier, E n'est pas vide donc il existe $x \in E$. Soit $F = E - \{x\}$: F est fini et possède n éléments par la proposition 3.1.7, donc par hypothèse de récurrence $\mathscr{P}(F)$ est fini et possède 2^n éléments. Soit maintenant $X \subseteq E$ un sous-ensemble quelconque de E; on distingue deux cas : soit $x \in X$, soit $x \notin X$; si $x \notin X$, alors X est un sous-ensemble de F, tandis que si $x \in X$, alors $X - \{x\}$ est un sous-ensemble de F. Soit $\mathscr{P}_x(E) = \{X \in \mathscr{P}(E) : x \in X\}$ l'ensemble des parties de E dont x est un élément : on définit une application $f : \mathscr{P}_x(E) \to \mathscr{P}(F)$, en posant $f(X) = X - \{x\}$. Supposons que $X, X' \in \mathscr{P}_x(E)$ et que $f(X) = f(X')$: on a $X = f(X) \cup \{x\} = f(X') \cup \{x\} = X'$, donc f est injective; et si $X \in \mathscr{P}(F)$, par définition l'ensemble $Y = X \cup \{x\}$ est élément de $\mathscr{P}_x(E)$ et $f(Y) = X$, donc f est surjective, et finalement bijective, donc $\mathscr{P}_x(E)$ est fini et possède 2^n éléments. Or, on a $\mathscr{P}(E) = \mathscr{P}(F) \cup \mathscr{P}_x(E)$ (toute partie de E est soit une partie de F, soit la réunion d'une partie de F et de $\{x\}$), et $\mathscr{P}(F) \cap \mathscr{P}_x(E) = \emptyset$ (une partie de E qui contient x n'est pas une partie de F), si bien que $\mathscr{P}(E)$ est fini comme réunion de deux ensembles finis par le corollaire 3.1.8, et possède $2^n + 2^n = 2.(2^n) = 2^{n+1}$ éléments par la proposition 3.2.2, et la démonstration est complète par récurrence. □

Remarque 3.2.4. Rappelons que si a est un nombre complexe, donc en particulier un nombre entier naturel, pour $n \in \mathbb{N}$ le nombre a^n est *défini* par récurrence par $a^0 = 1$ et $a^{n+1} = a^n.a$ pour tout $n \in \mathbb{N}$ (voir le cours de logique mathématique naturelle : Cycle I, n° 2).

Dénombrement des parties et coefficients binomiaux

Si E est un ensemble fini à n éléments, les sous-ensembles de E sont finis par le corollaire 3.2.1. Par le lemme 3.1.3, on démontre facilement qu'un sous-ensemble F de E possède k éléments, avec $k \leq n$, ce qui est, encore une fois, intuitif, mais qu'il faudrait établir rigoureusement. Si on se donne un entier naturel $k \leq n$, pour dénombrer le nombre de sous-ensembles de E possédant exactement k éléments on utilise les nombres notés $C_n^k = \dfrac{n!}{(n-k)!}$, appelés *coefficients binomiaux*. La notation anglo-saxonne $\binom{n}{k}$ tend à s'imposer.

Remarque 3.2.5. Pour tout entier naturel n, le nombre entier naturel $n!$, appelé *factorielle* n, a été défini par récurrence dans le cours de logique mathématique naturelle, de la manière suivante. On pose $0! = 1$, et supposant que $n!$ a été défini, on pose $(n+1)! = (n+1) \times n!$: le nombre $n!$ est donc le produit des n premiers entiers naturels.

Proposition 3.2.6. *Si E est un ensemble fini à n éléments et $k \leq n$, alors l'ensemble (fini) $\mathscr{P}_k(E)$ de sous-ensembles de E à k éléments possède $C_n^k = \frac{n!}{k!(n-k)!}$ éléments : il existe exactement C_n^k parties de E à k éléments.*

Démonstration. On procède par récurrence sur n, comme une variation sur la démonstration de la proposition 3.2.3. Si $n = 0$, on a nécessairement $k = 0$, donc E est vide et $\mathscr{P}_k(E)$ contient un élément, $\emptyset$; comme $C_0^0 = \frac{0!}{0!0!}$, la propriété est vérifiée pour $n = 0$. Supposons qu'elle le soit pour un entier naturel n, et soit E un ensemble fini possédant $n+1$ éléments, ainsi que $k \leq n+1$. Nous distinguons trois cas : soit $k = n+1$, soit $0 < k < n+1$, soit $k = 0$. Si $k = n+1$, alors $\mathscr{P}_k(E)$ est l'ensemble des sous-ensembles de E ayant $n+1$ éléments; comme tout sous-ensemble propre (c'est-à-dire différent de l'ensemble lui-même) d'un ensemble fini possède "moins" d'éléments par la proposition 3.1.7, le seul élément de $\mathscr{P}_{n+1}(E)$ est E, et comme $C_{n+1}^{n+1} = \frac{(n+1)!}{(n+1)!0!} = \frac{(n+1)!}{(n+1)!} = 1$, la propriété est vérifiée dans ce cas. Si $k = 0$, alors $\mathscr{P}_0(E)$ est l'ensemble des parties de F à 0 éléments : il n'y en a qu'une, l'ensemble vide, et $C_{n+1}^0 = \frac{(n+1)!}{0!(n+1)!} = \frac{(n+1)!}{(n+1)!} = 1$, et la propriété est vérifiée dans ce cas également. Si maintenant $0 < k < n+1$ et $X \in \mathscr{P}_k(E)$, choisissons un élément x de X (qui est non vide par définition de k) et distinguons à nouveau deux cas, selon que $x \in X$ ou $x \notin X$. Si $x \notin X$, alors X est un sous-ensemble de $F = E - \{x\}$ avec k éléments, tandis que si $x \in X$, alors $X - \{x\}$ est un sous-ensemble de F avec $k-1$ éléments (attention !), car $k > 0$ et on a retiré un élément. Comme dans 3.2.3, on définit une application $f : \mathscr{P}_k(E) \to \mathscr{P}_k(F) \cup \mathscr{P}_{k-1}(F)$ en posant $f(X) = X$ si $x \notin X$, et $f(X) = X - \{x\}$ si $x \in X$; comme $\mathscr{P}_k(F)$ et $\mathscr{P}_{k-1}(F)$ sont disjoints, on peut définir une application $g : \mathscr{P}_k(F) \cup \mathscr{P}_{k-1}(F) \to \mathscr{P}_k(E)$, $Y \in \mathscr{P}_k(F) \mapsto Y$, $Y \in \mathscr{P}_{k-1}(F) \mapsto Y \cup \{x\}$: on vérifie facilement que $f \circ g = Id$ et $g \circ f = Id$, si bien que f est une bijection. Il nous reste à dénombrer $\mathscr{P}_k(F) \cup \mathscr{P}_{k-1}(F)$: par hypothèse de récurrence appliquée à F et $k-1, k \leq n$, l'ensemble $\mathscr{P}_k(F)$ possède C_n^k éléments et l'ensemble $\mathscr{P}_{k-1}(F)$ en possède C_n^{k-1}. Comme la réunion est disjointe, par la proposition 3.2.2 le nombre d'éléments de $\mathscr{P}_k(E)$ est $C_n^k + C_n^{k-1}$. Par réduction au même dénominateur, ce nombre est $\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!(n-k+1)}{k!(n-k)!(n-k+1)} + \frac{n!k}{(k-1)!(n-k+1)!k} = \frac{n!(n-k+1)+n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n+1-k)!} = C_{n+1}^k$. Ceci est la propriété au rang $n+1$ pour le troisième cas, et on peut donc conclure par récurrence. □

Remarque 3.2.7. Dans cette démonstration, on fait une disjonction de trois cas à l'intérieur d'un raisonnement par récurrence, et même une autre disjonction de deux cas à l'intérieur de l'un des cas ! Il est courant de combiner ainsi les types de raisonnement, non seulement les uns à la suite des autres, mais aussi les uns à l'intérieur des autres. La pratique et la reproduction de ces démonstrations permettent de se familiariser progressivement et naturellement avec ces procédés.

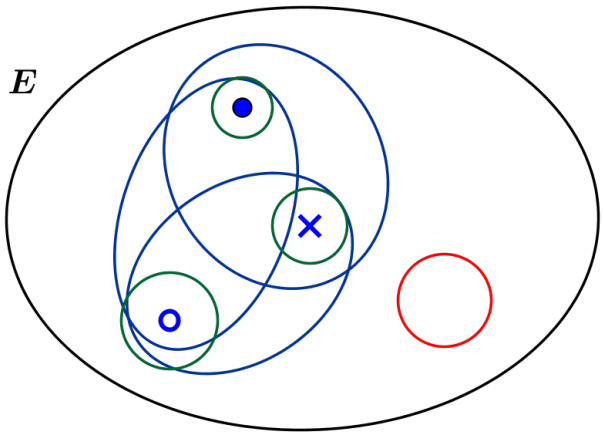

Figure 3.3: Un ensemble à 3 éléments possède $2^3 = 8$ parties : 1 partie vide, 3 parties à 1 élément, 3 parties à 2 éléments et 1 parties à 3 éléments. On a bien $1+3+3+1=8$.

Relations de Pascal et formule du binôme

Dans le cours de la preuve précédente, nous avons démontré la

Proposition 3.2.8. *Pour tous entiers naturels n, k tels que $0 < k \leq n$, on a $C_n^k + C_n^{k-1} = C_{n+1}^k$. Ces relations sont appelées* relations de Pascal, *du nom du mathématicien et philosophe français Blaise Pascal.*

Comme illustration, nous allons démontrer la *formule du binôme de Newton* : pour deux nombres complexes a et b et tout entier naturel n, on a $(a+b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$. L'apparition des coefficients binomiaux dans cette formule s'explique intuitivement comme suit. Considérons le cas $n = 2$: en développant, on a $(a+b)^2 = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$, et pour le cas $n = 3$, on a $(a+b)^3 = (a+b)(a+b)^2 = a^3 + a^2b + a^2b + ab^2 + ba^2 + ab^2 + ab^2 + b^3 = a^3 + 3a^2b + 3ab^2 + b^3$, et ainsi de suite. Intuitivement, quand on développe $(a+b)^n$, chaque terme de la somme obtenue est un produit de n facteurs, et on peut grouper les termes égaux selon les puissances de a qui apparaissent dans chacun d'eux. Pour tout $k \leq n$, a peut apparaître avec une puissance k, auquel cas c'est un terme de la forme $a^k b^{n-k}$; le nombre de fois où $a^k b^{n-k}$ apparaît dans le développement est alors exactement le nombre de manières de choisir k fois a dans les n facteurs $(a+b)$. Ceci revient intuitivement à choisir k éléments parmi n - ici les k facteurs d'où nous "extrayons" a - c'est-à-dire à choisir un sous-ensemble à k éléments dans un ensemble à n éléments.

Proposition 3.2.9 (Formule du binôme)**.** *Pour tous nombres complexes a, b et pour tout entier naturel n, on a $(a+b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$.*

Démonstration. On procède à nouveau par récurrence sur n. Si $n = 0$, par définition on a $(a+b)^n = (a+b)^0 = 1$, tandis que $\sum_{k=0}^n C_n^k a^k b^{n-k} = C_0^0 a^0 b^0 = 1.1 = 1$, donc la propriété est valide pour $n = 0$. Supposons que l'égalité soit vérifiée pour n, par hypothèse de récurrence nous pouvons alors écrire $(a+b)^{n+1} = (a+b)^n(a+b) = (\sum_{k=0}^n C_n^k a^k b^{n-k})(a+b) = (\sum_{k=0}^n C_n^k a^{k+1} b^{n-k}) + (\sum_{k=0}^n C_n^k a^k b^{n-k+1})$ en développant. En réindexant la première somme dans le développement pour obtenir des exposants

de a de la forme k plutôt que $k+1$ en exposant de a, on obtient $\sum_{k=0}^{n} C_n^k a^{k+1} b^{n-k} = \sum_{k=1}^{n+1} C_n^{k-1} a^k b^{n-k+1}$, d'où l'on peut réécrire

$$\begin{aligned}
(a+b)^{n+1} &= (\sum_{k=1}^{n+1} C_n^{k-1} a^k b^{n-k+1}) + (\sum_{k=0}^{n} C_n^k a^k b^{n-k+1}) \\
&= (\sum_{k=1}^{n} C_n^{k-1} a^k b^{n+1-k}) + C_n^n a^{n+1} b^0 + C_n^0 a^0 b^{n+1} + (\sum_{k=1}^{n} C_n^k a^k b^{n+1-k}) \\
&= a^{n+1} + (\sum_{k=1}^{n} (C_n^{k-1} + C_n^k) a^k b^{n+1-k}) + b^{n+1} \\
&= C_{n+1}^0 a^{n+1} + \sum_{k=1}^{n} C_{n+1}^k a^k b^{n+1-k} + C_{n+1}^{n+1} b^{n+1} \text{ (par 3.2.8)} \\
&= \sum_{k=0}^{n+1} C_{n+1}^k a^k b^{n+1-k},
\end{aligned}$$

ce qui est l'expression au rang $n+1$. Par récurrence, la démonstration est complète et la formule est valide pour tout entier naturel n. □

Nous concluons cette leçon en mentionnant une jolie relation entre tous ces résultats. Si E est un ensemble fini à n éléments, l'ensemble $\mathscr{P}(E)$ possède 2^n éléments par la proposition 3.2.3. Chaque sous-ensemble X de E étant fini, il possède un nombre déterminé k d'éléments, avec $k \leq n$, donc nous devrions avoir, par la proposition 3.2.6, $2^n = C_n^0 + C_n^1 + \ldots + C_n^k + \ldots C_n^{n-1} + C_n^n = \sum_{k=0}^{n} C_n^k$ (le nombre de parties de E est la somme des nombres de parties de E à k éléments, pour k variant de 0 à n). C'est en effet le cas par la formule du binôme 3.2.9, puisque $2^n = (1+1)^n = \sum_{k=0}^{n} C_n^k 1^k 1^{n-k} = \sum_{k=0}^{n} C_n^k$.

Exercices de la section

Exercice 3.2.10. i) Si E est un ensemble fini à n éléments, démontrer que le cardinal d'un sous-ensemble F de E est un entier $k \leq n$.
ii) Si E et F sont deux ensembles finis de cardinaux respectifs m et n, expliquer pourquoi $|E \cup F|$ peut prendre toutes les valeurs entre $\max\{m,n\}$ (le maximum de m et n), et $m+n$.
iii) Développer les expressions $(x+y)^4$ et $(x+y)^5$, où x et y dénotent des nombres complexes génériques.
v) Calculer de deux manière différentes le nombre de parties d'un ensemble à 4 éléments.
iv) Le *principe de récurrence* s'énonce comme suit : si S est une partie de $\mathbb{N}$ qui contient 0, et telle que pour tout $n \in \mathbb{N}$, $n+1 \in S$ dès que $n \in S$, alors $S = \mathbb{N}$. La démonstration par récurrence de la proposition 3.2.9 consiste à démontrer que pour tous $a, b \in \mathbb{C}$ et tout $n \in \mathbb{N}$, le triplet $(a, b, \sum_{k=0}^{n} C_n^k a^k b^{n-k})$ est dans le graphe de la fonction $(x, y, n) \in \mathbb{R}^2 \times \mathbb{N} \mapsto (x+y)^n$. Reformuler cette démonstration en appliquant le principe de récurrence (admis) à l'ensemble $S = \{n \in \mathbb{N} : \forall a, b \in \mathbb{R},\ (a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}\}$.

3.3 Applications entre ensembles finis

Le nombre d'applications entre deux ensembles finis

Proposition 3.3.1. *Si E et F sont deux ensembles finis ayant respectivement m et n éléments, alors le produit $E \times F$ est fini et possède $m.n$ éléments.*

Démonstration. Nous procédons par récurrence sur m, le cardinal de E, pour F un ensemble donné à n éléments. Si $m = 0$, alors $E = \emptyset$, et donc $E \times F$ est vide également, il est fini et possède aussi 0 éléments; comme $m.n = 0.n = 0$ dans ce cas, la propriété est valide pour $m = 0$. Supposons qu'elle le soit pour m, et que E possède $m + 1$ éléments; en particulier, E n'est pas vide, donc soit $x \in E$ et $E' = E - \{x\}$: on a $E \times F = (E' \cup \{x\}) \times F = (E' \times F) \cup (\{x\} \times F)$ (ce qui se démontre aisément par double inclusion). Par hypothèse de récurrence, l'ensemble $E' \times F$ est fini, de cardinal $m.n$, tandis que $\{x\} \times F$ est fini et possède n éléments, puisque l'application $F \to \{x\} \times F$, $y \mapsto (x, y)$ est une bijection (les détails sont laissés à l'étudiant(e)); la réunion est finie par le Corollaire 3.1.8 et comme les deux ensembles de la réunion sont disjoints (puisqu'un élément de $E' \times F$ ne peut pas être de la forme (x, y)), le nombre d'éléments de $E \times F$ est $m.n + n = (m + 1).n$ par la proposition 3.2.2, ce qui est la propriété au rang $m + 1$. Par récurrence sur m, on en conclut que la propriété est vraie pour tout m, et comme n a été choisi de manière arbitraire, la propriété est vraie pour tous m et n, et la proposition est démontrée. □

Remarque 3.3.2. La récurrence de la démonstration porte sur un seul des deux entiers, ici m, l'autre étant choisi arbitrairement. On aurait aussi pu, par symétrie, faire un raisonnement par récurrence sur n.

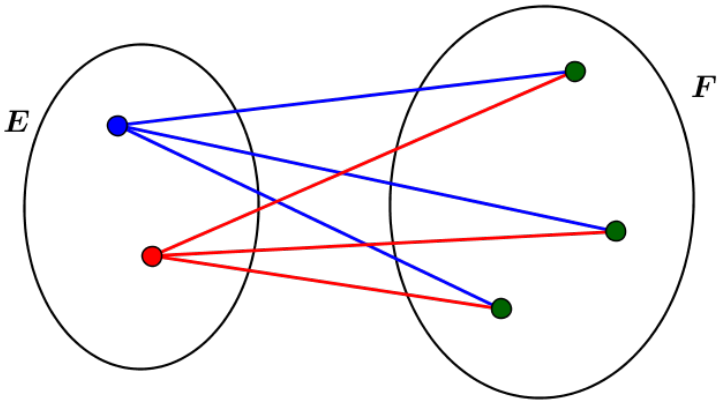

Figure 3.4: Si E a 2 éléments et F a 3 éléments, alors $E \times F$ a $2 \times 3 = 6$ éléments, lesquels sont représentés par toutes les manières d'apparier un élément de E à un élément de F.

Si E et F sont deux ensembles, **on note F^E l'ensemble des applications de E dans F**. La notation exponentielle n'est pas un hasard ; elle peut se comprendre à travers la proposition suivante :

Proposition 3.3.3. *Si E et F sont des ensembles finis ayant respectivement m et n éléments, alors l'ensemble F^E de toutes les applications de E dans F est fini et possède n^m éléments.*

Démonstration. Nous procédons par récurrence sur m. Si $m = 0$, alors E est vide, donc fini, et nous savons qu'il existe une seule application $f : \emptyset \to F$, celle dont le graphe est vide (voir le cours de théorie naïve des ensembles). Comme $n^m = n^0 = 1$ par définition dans ce cas, la propriété est valide pour $m = 0$. Supposons qu'elle le soit pour un entier naturel m et que E possède $m+1$ éléments. En particulier, E n'est pas vide, donc soient $x \in E$ et $E' = E - \{x\}$: l'ensemble $F^{E'}$ des applications de $E' = E - \{x\}$ dans F est fini et possède n^m éléments par hypothèse de récurrence, puisque le cardinal de E est m par la proposition 3.1.7. Soit $f : E \to F$ une application : l'idée est maintenant de considérer que f est "déterminée" par ses valeurs sur E' d'une part, par sa valeur en x d'autre part; il y a n^m possibilité pour la restriction $f|_{E'}$ de f à E' et n possibilités pour $f(x)$ (qui correspondent au choix de l'image de x par f, comme élément de F). Précisons cela en décrivant une bijection entre F^E et $F^{E'} \times F$. ! Si $f \in F^E$, on pose $\Phi(f) = (f|_{E'}, f(x))$, et ceci définit une application $\Phi : F^E \to F^{E'} \times F$. Pour montrer que Φ est une bijection, nous n'allons pas montrer qu'elle est injective et surjective, mais définir explicitement une bijection inverse : celle-ci doit "reconstruire" toute application $f : E \to F$ à partir des données de $f|_{E'}$ et de $f(x)$. Soit $\Psi : F^{E'} \times F \to F^E$ l'application définie, pour tout couple $(g, y) \in F^{E'} \times F$, par $\Psi((g, y)) = f$, où $f : E \to F$ est l'application $z \in E' \mapsto g(z)$ et $x \mapsto y$; il est clair que nous avons défini une application. Soit maintenant $f \in F^E$: on a $\Psi \circ \Phi(f) = \Psi(\Phi(f)) = \Psi((f|_{E'}), f(x)) = g$ disons; par définition de Ψ, pour $z \in E'$ on obtient $g(z) = f(z)$ et $g(x) = f(x)$, donc $g = f$, soit $\Psi \circ \Phi(f) = f$. Inversement, si $(g, y) \in F^{E'} \times F$, on a $\Phi \circ \Psi((g, y)) = f$, où $f : E \to F$ est l'application $z \in E' \mapsto g(z)$ et $x \mapsto y$, soit le couple $(f|_{E'}, f(x))$, qui par définition est (g, y) : on a $\Phi \circ \Psi((g, y)) = (g, y)$. En somme, $\Psi \circ \Phi$ est l'application identique de F^E , et $\Phi \circ \Psi$ est l'application identique de $F^{E'} \times F$, donc par caractérisation des applications bijectives, Φ et Ψ sont deux bijections réciproques. Par la proposition 3.3.1, l'ensemble $F^{E'} \times F$ est fini et possède $(n^m).n = n^{m+1}$ éléments, donc comme F^E et $F^{E'} \times F$ sont équipotents, F^E est également fini et possède aussi n^{m+1} éléments, et la démonstration est complète par récurrence : la propriété est vraie pour tous m et n. □

Remarque 3.3.4. i) Cette preuve est complexe. Il est normal d'éprouver des difficultés pour la comprendre complètement à la première lecture. Ici comme ailleurs, il faut la relire attentivement en essayant de l'analyser pas-à-pas, sans s'inquiéter des étapes qui demeurent incomprises, et qui s'éclairciront ultérieurement.
ii) La proposition 3.3.1 et cette proposition montrent que le rapport entre les ensembles finis et les entiers naturels, établi par la numération, fait correspondre certaines opérations sur les ensembles à des opérations analogues sur les nombres entiers naturels.

A partir de ce résultat, on peut retrouver le nombre de parties d'un ensemble fini à n éléments. En effet, si E est un ensemble quelconque et $S \subseteq E$ un sous-ensemble, on définit la *fonction caractéristique de S* comme l'application $f : E \to \{0, 1\}$ qui vaut 0 si $x \notin S$ et 1 si $x \in S$. On peut vérifier que l'application $\mathscr{P}(E) \to \{0, 1\}^E$,

qui associe à une partie S de E sa fonction caractéristique, est une bijection (voir les exercices). Comme $\{0,1\}$ possède 2 éléments, si E est fini et possède n éléments, l'ensemble $\{0,1\}^E$ des applications de E dans $\{0,1\}$ possède 2^n éléments par la proposition, donc $\mathscr{P}(E)$, qui lui est équipotent, possède aussi 2^n éléments.
Dans la section 2.4, nous avons introduit les puissances cartésiennes d'un ensemble E, et la représentation de leurs éléments par des multiplets. Dans le cas où l'ensemble E est fini, comme par définition l'ensemble $[[1,n]]$ possède n éléments, il est possible par la proposition 3.3.3 de dénombrer $E^{[[1,n]]}$, et donc E^n par la même occasion.

Corollaire 3.3.5. *Pour tout ensemble fini E et tout entier naturel n non nul, l'ensemble $E^{[[1,n]]}$ des n-uplets d'éléments de E, et la n-ième puissance cartésienne E^n de E, sont finis, de cardinal $|E|^n$.*

Les puissances E^n généralisent le produit cartésien $E \times E$. On peut généraliser à la fois le produit cartésien $E \times F$ de deux ensembles E et F quelconques et les puissances E^n d'un ensemble E par la notion suivante.

Définition 3.3.6. Si n est un entier naturel et $E_1, \ldots, E_n$ est un n-uplet d'ensembles, on définit par récurrence le produit $E_1 \times \ldots \times E_n$ de $E_1, \ldots, E_n$ comme suit. Si $n = 0$, par définition le produit est vide et vaut $\{\emptyset\}$. Si le produit de n ensembles est défini et $E_1, \ldots, E_{n+1}$ sont $n+1$ ensembles, on définit $E_1 \times \ldots \times E_{n+1}$ comme le produit cartésien $(E_1 \times \ldots \times E_n) \times E_{n+1}$.

Il est alors possible de dénombrer simplement le produit $E_1 \times \ldots \times E_n$ dans le cas où les ensembles $E_1, \ldots, E_n$ sont finis, puisque ce produit est fini.

Proposition 3.3.7. *Si n est un entier naturel et $E_1, \ldots, E_n$ est un n-uplet d'ensembles finis, alors leur produit $E_1 \times \ldots \times E_n$ est fini, de cardinal $|E_1| \times \ldots \times |E_n|$.*

Démonstration. On procède par récurrence sur n. Si $n = 0$, alors par définition le produit vaut $\{\emptyset\}$, fini et de cardinal 1, qui est bien le produit de 0 éléments, par définition. Supposons que $n \geq 0$ et que le produit $E_1 \times \ldots \times E_n$ de n ensembles finis quelconques $E_1, \ldots, E_n$ est fini, de cardinal $|E_1| \times \ldots \times |E_n|$, et soit $E_1, \ldots, E_{n+1}$ un $n+1$-uplet d'ensembles finis. Par la proposition 3.3.1 et par définition du produit de $n+1$ ensembles, le produit $E_1 \times \ldots E_{n+1} = (E_1 \times \ldots \mathcal{E}_n) \times E_{n+1}$ est fini, et son cardinal est $|E_1 \times \ldots \times E_{n+1}| = |(E_1 \times \ldots \times E_n) \times E_{n+1})| = |E_1 \times \ldots \times E_n|.|E_{n+1}| = |E_1| \times \ldots |E_n| \times |E_{n+1}|$, ce qui est la propriété au rang $n+1$, et la proposition est démontrée par récurrence. □

Exercices de la section

Exercice 3.3.8. i) Si E est F sont deux ensembles finis de cardinaux respectifs m et n, combien existe-t-il de relations entre E et F ?
ii) Si E et F sont deux ensembles, définir une application injective de l'ensemble F^E dans l'ensemble $\mathscr{P}(E \times F)$ en utilisant le graphe des applications de E dans F. En déduire que pour tous entiers naturels m, n, on a $n^m \leq 2^{n.m}$.
iii) En utilisant l'exercice (ii), définir l'image de l'application injective F^E à l'aide d'une clause symbolique.
iv) Montrer que pour tout ensemble E, l'application qui associe à une partie S de

E sa fonction caractéristique, est une bijection de $\mathscr{P}(E)$ sur $\{0,1\}^E$. Indication : pour la surjectivité, à partir d'une fonction $f : E \to \{0,1\}$, définir un sous-ensemble S de E dont f est la fonction caractéristique.
v) Représenter à l'aide de graphiques toutes les applications d'un ensemble à 2 éléments dans un ensemble à 3 éléments.

3.4 Permutations et arrangements

Nous avons dénombré les applications d'un ensemble fini dans un autre ensemble fini. Nous allons dans cette dernière section dénombrer les bijections et les injections entre ensembles finis.

Définition 3.4.1. Si E est un ensemble, une *permutation de E* est une bijection de E sur E lui-même. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E.

Pour dénombrer les bijections entre deux ensembles finis, et donc en particulier les permutations d'un ensemble fini, nous commençons par dénombrer les permutations d'un ensemble fini de la forme $[[1,n]]$; on note $\mathfrak{S}_n$ l'ensemble des permutations de $[[1,n]]$. Si $i,k \in [[1,n]]$, il existe une permutation σ ("sigma") de $[[1,n]]$ qui "échange" i et k : elle est définie par $\sigma(i) = k$, $\sigma(k) = i$, et $\sigma(j) = j$ pour tout $j \neq i,k$; si $i = k$, il s'agit de l'application identique de $[[1,n]]$. On appelle une telle permutation une *transposition*; notons que $\sigma^{-1} = \sigma$ par définition de σ : une transposition est sa propre bijection inverse.

Proposition 3.4.2. *Pour tout entier naturel n, l'ensemble des permutations $\mathfrak{S}_n$ de $[[1,n]]$ est fini et possède $n!$ éléments.*

Démonstration. Pour tout entier n, S_n est un sous-ensemble de l'ensemble $[[1,n]]^{[[1,n]]}$ des applications de $[[1,n]]$ dans lui-même : c'est donc un ensemble fini par la proposition 3.3.3 et le corollaire 3.2.1. Pour la cardinalité, on procède par récurrence sur n. Si $n = 0$, alors $[[1,n]] = \emptyset$, et il n'existe qu'une permutation de l'ensemble vide, l'application vide, donc $|\mathfrak{S}_0| = 1 = 0!$ par définition de $0!$, et la propriété est vérifiée au rang $n = 0$. Supposons qu'elle le soit au rang n, c'est-à-dire que $|\mathfrak{S}_n| = n!$, et soit $f \in \mathfrak{S}_{n+1}$ une permutation de $[[1,n+1]]$: distinguons deux cas, selon que $f(n+1) = n+1$ ou $f(n+1) < n+1$. Si $f(n+1) = n+1$, la restriction $g = f|_{[[1,n]]}$ de f à $[[1,n]]$ est une permutation de $[[1,n]]$, donc par hypothèse de récurrence il existe exactement $n!$ permutations f de $[[1,n+1]]$ telles que $f(n+1) = n+1$. Si $f(n+1) < n+1$, posons $k = f(n+1)$ et soit σ la transposition de $\mathfrak{S}_{n+1}$ qui échange $n+1$ et k : l'application $g = \sigma \circ f : [[1,n+1]] \to [[1,n+1]]$ est une permutation par composition, et on a $g(n+1) = \sigma(f(n+1)) = \sigma(k) = n+1$, si bien qu'on peut écrire $f = \sigma \circ g$, avec g une permutation de $[[1,n+1]]$ telle que $g(x) = x$. Par le cas précédent, il existe exactement $n!$ telles permutations f pour chaque valeur possible de $f(n+1)$ lorsque $f(n+1) \neq n+1$, donc au total $n.n!$ permutations dans ce cas et finalement, il existe $n! + n.n! = (n+1).n! = (n+1)!$ permutations de $[[1,n+1]]$, et la propriété est démontrée par récurrence.
Ecrivons de manière rigoureuse l'étape de récurrence en intégrant les deux cas. Si $f \in \mathfrak{S}_{n+1}$ est une permutation de $[[1,n+1]]$, on lui associe le couple $((\sigma \circ f)|_{[[1,n]]}, f(n+$

1)) $\in \mathfrak{S}_n \times [[1, n+1]]$, où σ est la transposition de $\mathfrak{S}_{n+1}$ qui échange $f(n+1)$ et $n+1$: ceci définit une application $\Phi : \mathfrak{S}_{n+1} \to \mathfrak{S}_n \times [[1, n+1]]$, et on veut montrer qu'il s'agit d'une bijection. Supposons que $g \in \mathfrak{S}_{n+1}$, et que $\Phi(g) = ((\tau \circ g)|_{[[1,n]]}, g(n+1))$ (τ est la lettre grecque "tau"). Si $\Phi(f) = \Phi(g)$, alors d'une part $f(n+1) = g(n+1)$, donc $\sigma = \tau$. D'autre part, si $i \in [[1, n]]$, on a $f(i) = \sigma \circ (\sigma \circ f)(i)$ (car σ est sa propre bijection inverse) $= \sigma((\sigma \circ f)(i)) = \tau((\tau \circ g)(i))$ (car $(\sigma \circ f)|_{[[1,n]]} = (\tau \circ g)|_{[[1,n]]}$ et $\sigma = \tau$) $= g(i)$, donc finalement, on a $f(i) = g(i)$ pour tout $i \in [[1, n+1]]$, donc $f = g$ et Φ est injective. Si maintenant $(h, k) \in \mathfrak{S}_n \times [[1, n+1]]$, alors on peut étendre h à $\overline{h} \in \mathfrak{S}_{n+1}$ en posant $\overline{h}(i) = h(i)$ pour $i \in [[1, n]]$ et $\overline{h}(n+1) = n+1$; soit alors σ la transposition de $\mathfrak{S}_{n+1}$ qui échange $n+1$ et k : on pose $f = \sigma \circ \overline{h} \in \mathfrak{S}_{n+1}$, et on veut montrer que $\Phi(f) = (h, k)$. D'une part, on a $f(n+1) = \sigma(\overline{h}(n+1)) = \sigma(n+1) = k$, d'autre part on a $(\sigma \circ f)|_{[[1,n]]} = \overline{h}|_{[[1,n]]} = h$, donc $\Phi(f) = (h, k)$ et Φ est surjective. Par conséquent, $\mathfrak{S}_{n+1}$ est équipotent à $\mathfrak{S}_n \times [[1, n+1]]$, qui est de cardinal $(n!) \times (n+1) = (n+1)!$ par la proposition 3.3.1, et $\mathfrak{S}_{n+1}$ est donc de cardinal $(n+1)!$, ce qui est la propriété au rang $n+1$. □

Remarque 3.4.3. Le début de la démonstration donne seulement l'idée de l'étape de récurrence, et pour obtenir une démonstration complètement rigoureuse, il faut décrire une bijection entre $\mathfrak{S}_{n+1}$ et un ensemble fini qu'on sait dénombrer grâce à l'hypothèse de récurrence. Cette deuxième partie est plus difficile à comprendre et intègre tous les concepts abordés jusqu'à présent dans ce cours.

Corollaire 3.4.4. *Si E et F sont deux ensembles finis de même cardinal n, alors il existe exactement $n!$ bijections différentes de E sur F. En particulier, si E est un ensemble fini à n éléments, alors il existe $n!$ permutations de E.*

Démonstration. Puisque E et F ont le même cardinal n, il existe une bijection $s : [[1, n]] \to E$ et une bijection $t : [[1, n]] \to F$. Notons $Bij(E, F)$ l'ensemble des bijections de E dans F : nous allons démontrer qu'il existe une bijection entre $Bij(E, F)$ et $\mathfrak{S}_n$. Soit $f : E \to F$ une bijection : l'application $t^{-1} \circ f \circ s : [[1, n]] \to E \to F \to [[1, n]]$ est une bijection comme composée de trois bijections, donc une permutation de $[[1, n]]$, et si on pose $\Phi(f) = t^{-1} \circ f \circ s$, on définit une application $\Phi : Bij(E, F) \to \mathfrak{S}_n$. Supposons que $g : E \to F$ est une autre bijection et que $\Phi(f) = \Phi(g)$: par définition on a $t^{-1} \circ f \circ s = t^{-1} \circ g \circ s$, d'où $f = (t \circ t^{-1}) \circ f \circ (s \circ s^{-1}) = t \circ (t^{-1} \circ f \circ s) \circ s^{-1} = t \circ (t^{-1} \circ g \circ s) \circ s^{-1} = (t \circ t^{-1}) \circ g \circ (s \circ s^{-1}) = g$, et Φ est injective. Par ailleurs, si $u \in \mathfrak{S}_n$ est une permutation de $[[1, n]]$, l'application $t \circ u \circ s^{-1} : E \to [[1, n]] \to [[1, n]] \to F$ est une bijection de E dans F par composition, et on a $\Phi(t \circ u \circ s^{-1}) = u$, si bien que Φ est surjective. Par conséquent, $Bij(E, F)$ et $\mathfrak{S}_n$ ont le même cardinal, c'est-à-dire $n!$ par la proposition 3.4.2. En choisissant $F = E$, on obtient le second énoncé. □

Remarque 3.4.5. On a utilisé ici la composition de plus de deux applications. La définition d'une telle composition est évidente : par exemple, si $f : E \to F$, $g : F \to G$ et $h : G \to H$ sont trois applications, par définition on a $h \circ g \circ f = h \circ (g \circ f)$. On peut montrer facilement que cette composition multiple est *associative*, c'est-à-dire que le groupement des compositions par deux fonctions donne toujours le même résultat, ce que nous avons exploité dans cette démonstration. Dans cet exemple, on a par exemple $(h \circ g) \circ f = h \circ (g \circ f)$, ce qu'on démontre en caractérisant l'égalité des deux fonctions sur chaque élément de E.

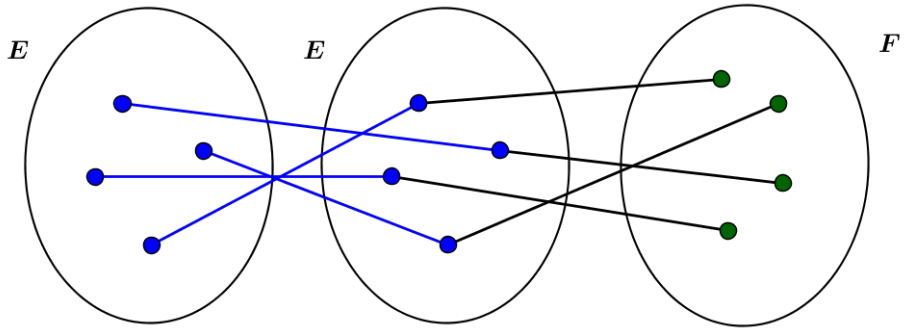

Figure 3.5: Pour toute bijection entre deux ensembles E et F de même cardinal (à droite), une permutation quelconque de l'ensemble E différente de l'application identique (à gauche) définit par composition une nouvelle bijection entre E et F.

Grâce au dénombrement des parties et des permutations d'un ensemble fini, nous pouvons désormais dénombrer les injections d'un ensemble fini dans un autre, ce par quoi nous terminons ce chapitre. C'est l'occasion de mentionner l'énoncé fondamental suivant.

Proposition 3.4.6. *Si E est un ensemble fini, alors toute application injective de E dans E est surjective, c'est-à-dire bijective.*

Démonstration. Supposons que $f : E \to E$ soit injective. En particulier, la corestriction g de f à son image est à la fois injective et surjective, c'est donc une bijection. On en déduit que $|Im(f)| = |E|$. Comme $Im(f) \subseteq E$, on en déduit que $Im(f) = E$, si bien que f est surjective, et donc bijective. □

Remarque 3.4.7. Ce résultat est utilisé notamment en algèbre linéaire, et donne lieu à des analogues en algèbre, notamment dans la théorie des corps finis.

Proposition 3.4.8. *Si E et F sont deux ensembles finis de cardinaux respectifs m et n, et si $m \leq n$, alors il existe $m!C_n^m = \frac{n!}{(n-m)!}$ applications injectives de E dans F.*

Démonstration. Soit $X \subseteq F$, de cardinal m : comme $|E| = m$ également, il existe une bijection f entre E et X, et son graphe est donc le graphe d'une *injection* $f_X : E \to X$ (soit l'application décrite de la même manière, mais dont F est le codomaine). Soit $\mathscr{P}_m(F)$ l'ensemble des sous ensembles de F possédant m éléments, de cardinal C_n^m par la proposition 3.2.6, et définissons une application $\Phi : \mathscr{P}_m(F) \times \mathfrak{S}(E) \to Inj(E, F)$, l'ensemble des injections de E dans F, de la manière suivante. Si $(X, \sigma) \in \mathscr{P}_m(F) \times \mathfrak{S}(E)$, on pose $\Phi(X, \sigma) = f_X \circ \sigma$, cette fonction de E dans F étant bien une injection comme composition de deux injections. Si $(Y, \tau) \in \mathscr{P}_m(F) \times \mathfrak{S}(E)$ et $\Phi(Y, \tau) = \Phi(X, \sigma)$, alors d'une part $Im(f_X \circ \sigma) = Im(f_Y \circ \tau)$, soit $X = Y$ et $f_X = f_Y$, et d'autre part pour tout $x \in E$ on a $f_X(\sigma(x) = f_X \circ \sigma(x) = f_X \circ \tau(x) = f_X(\tau(x))$ et comme f_X est injective, on en déduit que $\sigma(x) = \tau(x)$, si bien que $\sigma = \tau$ et finalement, les couples (X, σ) et $Y, \tau)$ sont égaux : Φ est injective. Supposons maintenant que $f \in Inj(E, F)$ et soit $X = Im(f)$: on définit une permutation $\sigma \in \mathfrak{S}(E)$ en posant pour $x \in E$, $\sigma(x) = y$, pour y l'élément de E tel que $f_X(y) = f(x)$; σ est bien définie puisque un tel y est unique par injectivité de

f_X. Pour tout $x \in E$, on a $f_X \circ \sigma(x) = f(x)$, et σ est injective : si $\sigma(x) = \sigma(y)$, alors $f(x) = f_X(\sigma(x)) = f_X(\sigma(y)) = f(y)$, d'où $x = y$ puisque f est injective; par la proposition 3.4.6, σ est une permutation de E et on a $\Phi(X, \sigma) = f$, donc Φ est une bijection. Par le corollaire 3.4.4 et la proposition 3.3.1, on en déduit que $|Inj(E, F)| = m! \times C_n^m$. □

Remarque 3.4.9. Dans toutes ces démonstrations, la difficulté pour établir le résultat de manière rigoureuse consiste à définir une bijection entre des ensembles construits à partir d'ensembles de fonctions : on a donc "deux niveaux d'abstraction" imbriqués.

Définition 3.4.10. Si $m \leq n$, le nombre d'injections $m!C_n^m$ d'un ensemble à m éléments dans un ensemble à n éléments est parfois appelé *nombre d'arrangements de m objets parmi n*, et noté alors A_n^m.

Exercices de la section

Exercice 3.4.11. i) Soient E, F, G trois ensembles et $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications. Démontrer que pour tout $x \in E$, on a $(h \circ g)(f(x)) = h((g \circ f)(x))$. En déduire que $h \circ (g \circ f) = (h \circ g) \circ f$.
ii) Adapter la démonstration de la proposition 3.4.8 en définissant une application $\Psi : Inj(E, F) \to \mathscr{P}_m(F) \times \mathfrak{S}(E)$ et en montrant que $\Psi \circ \Phi$ et $\Phi \circ \Psi$ sont les applications identiques de leurs domaines respectifs.
iii) A quelle condition, nécessaire et suffisante, existe-t-il une surjection d'un ensemble E à m éléments sur un ensemble F à n éléments ?

Chapitre 4

L'Infini Mathématique

4.1 Le premier ensemble infini

Rappelons que nous avons défini en 3.1.1 la notion d'ensemble *infini* comme un ensemble qui n'est pas fini. Notre étude de l'infini mathématique commence donc avec cette définition simple, et la place de l'ensemble $\mathbb{N}$, le plus "simple" des ensembles infinis, dans la théorie des ensembles finis et infinis. Il nous sera utile d'identifier les sous-ensembles finis de $\mathbb{N}$, pour *démontrer* que l'ensemble $\mathbb{N}$ est infini.

Proposition 4.1.1. *Si $X \subseteq \mathbb{N}$, alors X est fini si et seulement si il existe un entier $n \in \mathbb{N}$ tel que $X \subseteq [[0, n]] = \{i \in \mathbb{N} : i \leq n\}$.*

Démonstration. Supposons que X est fini, de cardinal m, et démontrons la propriété par récurrence sur m. Si $m = 0$, alors X est vide, et alors $X \subseteq [[0, 0]]$, donc la propriété est vérifiée au rang $m = 0$ avec $n = 0$. Supposons que X est de cardinal $m + 1$ et que la propriété est vérifiée au rang m, et soit x un élément de X (qui est non vide par hypothèse) : le cardinal de l'ensemble $Y = X - \{x\}$ est m par la proposition 3.1.7, donc par hypothèse de récurrence il existe un entier $n \in \mathbb{N}$ tel que $Y \subseteq [[0, n]]$. Par suite, si n' désigne le plus grand des entiers n et x, on a $X \subseteq [[0, n']]$, et la propriété est vérifiée au rang $m+1$. Par le principe de récurrence, elle est valide pour tout $m \in \mathbb{N}$, donc tout sous-ensemble fini de $\mathbb{N}$ est inclus dans un ensemble de la forme $[[0, n]]$ (appelé un *segment initial*. Réciproquement, supposons qu'il existe $n \in \mathbb{N}$ tel que $X \subseteq [[0, n]]$. L'ensemble $[[0, n]]$ est fini, puisque l'application $[[0, n]] \to [[1, n + 1]]$, $i \mapsto i + 1$ est une bijection, et X est alors un sous-ensemble d'un ensemble fini : il est donc fini par le corollaire 3.2.1. □

La première caractérisation de l'infini que nous donnerons s'appuie sur l'exemple fondamental d'ensemble infini, l'ensemble $\mathbb{N}$ des nombres entiers naturels. Toutefois, il nous faut déjà démontrer que cet ensemble est infini ! Nous aurons besoin du lemme suivant.

Lemme 4.1.2. *Si $f : E \to F$ est une application et si E est fini, alors $f(E)$ est fini (l'image d'un ensemble fini est un ensemble fini).*

Démonstration. Supposons que $y \in f(E)$: il existe $x \in E$ tel que $f(x) = y$; pour tout $y \in f(E)$ choisissons donc un élément x_y de E, que nous notons $g(y)$, et tel

que $f(x_y) = y$ (c'est-à-dire un antécédent de y par f). Nous définissons ainsi une application $g : f(E) \to E$, $y \mapsto g(y) = x_y$. Supposons que $y, y' \in f(E)$ et que $g(y) = g(y')$: par définition de g, on a $y = f(g(y)) = f(g(y')) = y'$, ce qui montre que g est injective. L'application g est donc une bijection de $f(E)$ sur un sous-ensemble $g(f(E))$ de E. Par le corollaire 3.2.1, l'ensemble $g(f(E))$ est fini, et on en conclut que $f(E)$ est fini. □

Théorème 4.1.3. *L'ensemble* $\mathbb{N}$ *des nombres entiers naturels est infini.*

Démonstration. Par définition, nous devons démontrer qu'il n'existe aucune bijection entre $\mathbb{N}$ et un ensemble de la forme $[[1, n]]$. Il suffit de montrer que pour tout entier naturel n, une application $f : [[1, n]] \to \mathbb{N}$ ne peut pas être surjective (il ne peut donc *a fortiori* pas exister de bijection de $[[1, n]]$ sur $\mathbb{N}$), ce qui vient directement du lemme 4.1.2. En effet, si $f : [[1, n]] \to \mathbb{N}$ est une telle application, par ce lemme le sous-ensemble $Im(f)$ de $\mathbb{N}$ est fini, et par la proposition 4.1.1 il existe un entier naturel k tel que $Im(f) \subseteq [[0, k]]$. Il s'ensuit que $k + 1$, par exemple, n'a pas d'antécédent par f, si bien que f ne peut pas être surjective. □

Il est important de comprendre que même si la (première) définition d'un ensemble infini adoptée ici n'est que la négation de celle d'un ensemble fini, cette définition est parfaitement valide, et que l'infinité de $\mathbb{N}$ est une "évidence" qu'il faut cependant démontrer.

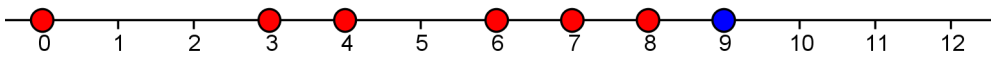

Figure 4.1: Un sous-ensemble fini de $\mathbb{N}$ (ici $\{0, 3, 4, 6, 7, 8\}$ en rouge) a toujours un plus grand élément, et on pourra donc toujours trouver un élément de $\mathbb{N}$ en-dehors d'un tel ensemble (ici 9 par exemple). L'image d'un sous-ensemble de la forme $[[1, n]]$ par une application injective dans $\mathbb{N}$ ne peut donc jamais être $\mathbb{N}$ tout entier.

Pour terminer cette section, nous rassemblons ici les postulats que nous avons adoptés jusqu'ici concernant la fonction successeur. Ils sont notre version de ce qu'on appelle les *axiomes de Peano*, qui déterminent de manière univoque les propriétés de cette fonction, et permettent de reconstituer toute la structure opératoire et relationnelle de l'ensemble $\mathbb{N}$. Nous aborderons en effet l'arithmétique naturelle de manière rigoureuse à partir de ces axiomes dans le cours suivant.

Axiome 1. 0 *n'est le successeur d'aucun entier naturel. En d'autres termes, il n'existe pas d'entier naturel* n *tel que* $s(n) = 0$.

En particulier, l'application successeur n'est pas surjective, puisque 0 ne possède pas d'antécédent.

Axiome 2. *Si deux entiers naturels* m *et* n *ont le même successeur, alors ils sont égaux. En d'autres termes, pour tous entiers naturels* m, n*, si* $s(m) = s(n)$ *alors* $m = n$.

On peut reformuler cet axiome en disant que l'application successeur *est injective*.

Axiome 3 (Principe de récurrence (ou d'induction))**.** *Si S est un sous-ensemble de $\mathbb{N}$ tel que :*
i) $0 \in S$
ii) pour tout $n \in S$, $s(n) \in S$ *("étape de récurrence"),*
alors on a $S = \mathbb{N}$.

Ce principe signifie intuitivement que l'ensemble $\mathbb{N}$ est entièrement "parcouru" si nous l'énumérons à partir de 0 et ajoutons chaque entier naturel successif, de manière indéfinie. Il fonde la pratique des démonstrations et définitions par récurrence.

Exercices de la section

Exercice 4.1.4. i) Trouver un sous-ensemble infini de $\mathbb{N}$ différent de $\mathbb{N}$. Démontrer qu'il est infini.
ii) Démontrer par récurrence que tout sous-ensemble fini non vide X de $\mathbb{N}$ possède un plus grand élément, c'est-à-dire qu'il existe $k \in X$ tel que pour tout $i \in X$, on ait $i \leq k$.
iii) Soit $X \subseteq \mathbb{N}$ un sous-ensemble non vide. Si $0 \notin X$, soient $Y = \{i \in \mathbb{N} : \forall x \in X,\ i < x\}$, et k le plus grand élément de Y par (ii). Démontrer que $k+1$ est le plus petit élément de X, c'est-à-dire que $k+1 \in X$, et que pour tout $x \in X$, on a $k+1 \leq x$. En déduire que toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

4.2 Caractérisation extrinsèque de l'infinité mathématique

Rappelons qu'une caractérisation d'une notion est une condition équivalente à cette notion, qui peut donc être choisie comme définition alternative. Il est possible de donner ici une première caractérisation des ensembles infinis, plus intéressante ou au moins plus suggestive, que la définition initiale, en utilisant l'ensemble $\mathbb{N}$. Nous parlons ici de caractérisation "extrinsèque", car nous la rapportons à un ensemble particulier "extérieur" à l'ensemble dont nous voulons caractériser l'infinité. Nous avons dans ce cours rappelé certaines définitions par récurrence, évoquées dans le cours de logique mathématique naturelle. Une telle définition consiste essentiellement à décrire une *suite* d'éléments d'un ensemble E, c'est-à-dire une application $f : \mathbb{N} \to E$. On définit d'abord l'image de 0, c'est-à-dire $f(0)$, en choisissant un élément de E (autrement dit, on commence par choisir un couple $(0, f(0))$ de $\mathbb{N} \times E$ pour "construire" le graphe de f), et on définit alors l'image de $n+1$ par f, *sous l'hypothèse* que nous avons défini l'image de n par f. En appliquant le principe de récurrence évoqué dans l'exercice 3.2.10(iv) et l'Axiome 3, l'ensemble E des entiers naturels n pour lesquels l'expression $f(n)$ est définie, est l'ensemble $\mathbb{N}$ tout entier, si bien que f est définie.

Remarque 4.2.1. Le raisonnement par récurrence ou la définition par récurrence s'appuient tous les deux sur le principe de récurrence. Dans la preuve par récurrence, on considère une propriété décrite par une clause $P(n)$: elle *définit* un sous-ensemble de $\mathbb{N}$, celui des entiers qui ont cette propriété, et on cherche précisément à montrer

"par récurrence" que c'est $\mathbb{N}$ tout entier. Dans la définition par récurrence on utilise le principe pour établir que la fonction est *définie* sur tout $\mathbb{N}$. Ce n'est plus une propriété qui est valide sur tout $\mathbb{N}$, mais une définition : le statut logico-mathématique du procédé est différent, mais on utilise le même principe.

Proposition 4.2.2. *L'image de l'application successeur $s : \mathbb{N} \to \mathbb{N}$ est l'ensemble $\mathbb{N}^*$.*

Démonstration. Soit S l'ensemble $\{0\} \cup Im(s) = \{0\} \cup \{n \in \mathbb{N} : \exists m \in \mathbb{N},\ n = s(m)\}$: si nous montrons que $S = \mathbb{N}$, alors tout entier naturel non nul est dans l'image de s, donc $Im(s) = \mathbb{N}^*$. Par définition, on a $0 \in S$, et supposons que n est un entier naturel, et que $n \in S$. Par définition, l'entier naturel $s(n)$ est dans S ! Par le principe de récurrence, l'ensemble S est $\mathbb{N}$ tout entier, et la proposition est démontrée. □

La co-restriction de l'application successeur à son image est donc une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$, partie propre de $\mathbb{N}$ (c'est-à-dire différente de $\mathbb{N}$). Nous verrons dans la section 4.4 que cette propriété caractérise de manière intrinsèque les ensembles infinis.

Théorème 4.2.3. *Un ensemble E est infini si et seulement si il existe une application injective $f : \mathbb{N} \hookrightarrow E$.*

Démonstration. Supposons que E est infini. En particulier, comme il n'existe pas de bijection entre E et $[[1, 0]] = \emptyset$, E n'est pas vide. Soit donc $x \in E$: on pose $f(0) = x$, et on va définir $f(n+1)$, sous l'hypothèse que $f(k)$ est défini pour tout $k \leq n$, et que $f(x_i) \neq f(x_j)$ pour tous $i, j \leq n$. L'ensemble $I = \{f(k) : k \leq n\}$ est fini, comme image d'un ensemble fini par le lemme 4.1.2 : il existe donc une bijection $g : [[1, m]] \cong I$ par définition d'un ensemble fini. Si $h : I \hookrightarrow E$ est l'inclusion de I dans E, $h \circ g : [[1, m]] \hookrightarrow E$ est alors une injection comme composition d'applications injectives, et comme E est infini, $h \circ g$ ne peut pas être surjective, donc il existe $y \in E - I$, et on pose $f(n+1) = y$. Par récurrence, nous avons défini une suite $f : \mathbb{N} \to E$, et nous devons vérifier qu'elle est injective. Pour cela, soient $m, n \in \mathbb{N}$, avec $m \neq n$: on a soit $m < n$, soit $n < m$, par exemple $m < n$ (l'autre cas est symétrique); comme $n \neq 0$, on peut écrire $n = s(n')$ pour un certain $n' \in \mathbb{N}$ par la proposition 4.2.2, et par définition on a $f(n) = f(n'+1) \notin f([[0, n']])$, donc $f(n) \neq f(m)$. Par contraposée, on a $f(m) = f(n) \Rightarrow m = n$, si bien que f est injective. Réciproquement, supposons qu'il existe une application injective $f : \mathbb{N} \hookrightarrow E$, mais que E est fini : il existe par définition un entier naturel n et une bijection $g : E \cong [[1, n]]$, de sorte que $g \circ f : \mathbb{N} \hookrightarrow [[1, n]]$ est une injection. En particulier, l'ensemble $Im(g \circ f)$ est fini par le corollaire 3.2.1 comme sous-ensemble d'un ensemble fini, donc il existe une bijection entre $\mathbb{N}$ et un ensemble fini, ce qui est impossible. Par l'absurde, E est infini. □

Remarque 4.2.4. Dans la seconde partie de la preuve, on utilise le raisonnement par l'absurde sous la forme suivante : elle consiste, pour démontrer un énoncé de la forme $P \Rightarrow Q$, à supposer que $P \wedge \neg Q$ (équivalent à la négation de $P \Rightarrow Q$, voir le cours de logique mathématique naturelle) est vrai, et à en tirer une contradiction : par l'absurde, cela signifie que $P \Rightarrow Q$ est vraie.

Corollaire 4.2.5. *Si E est un ensemble équipotent à un ensemble infini, ou contenant un ensemble infini, alors E est infini.*

Une conséquence immédiate de ce corollaire, c'est que si $f : E \to F$ est une application injective et E est infini, alors F lui-même est infini, contenant l'image infinie de E, équipotente à E. Ceci va nous permettre d'établir l'infinité des ensembles de multiplets d'éléments d'un ensemble infini, analogue de la proposition **??**.

Lemme 4.2.6. *Pour tous ensembles E infini et F non vide, le produit $E \times F$ est infini.*

Démonstration. Puisque F n'est pas vide, il en existe un élément y. Soit $f : E \to E \times F$ l'application définie par $f(x) = (x, y)$ pour tout $x \in E$. On vérifie facilement que f est injective, donc par ce qui précède, que $E \times F$ est infini. □

Proposition 4.2.7. *Si E est un ensemble infini et n un entier naturel non nul, alors l'ensemble E^n des n-uplets d'éléments de E est infini.*

Démonstration. On procède par récurrence sur $n \geq 1$. Si $n = 1$, alors $E^1 = E$ par définition, si bien que E^1 est infini. Supposons que E^n est infini pour $n \geq 1$: par définition, on a $E^{n+1} = E^n \times E$, et comme E^n est infini et E n'est pas vide, par le lemme 4.2.6 l'ensemble E^{n+1} est infini, d'où la propriété pour tout $n \geq 1$ par récurrence. □

L'étudiant(e) ou le lecteur cultivé(e) pourrait avoir une autre image de l'infini mathématique, par exemple celle des limites de fonctions "quand x tend vers l'infini". Cette infinité "géométrique" est différente de l'infinité présente, mais elle s'y ramène de manière fondamentale à travers l'infinité de $\mathbb{N}$ et notamment la construction de suites de nombres réels en analyse.
Voici quelques sous-ensembles finis de $\mathbb{N}$. Bien que $\mathbb{N}$ s'injecte (on dit aussi se "plonge") dans tout ensemble infini, cela n'exclut pas, en effet, qu'il contienne lui-même des ensembles infinis ! C'est un paradoxe de l'infini mathématique, qui nous servira à le caractériser d'une autre manière.

Exemple 4.2.8. i) L'ensemble $2\mathbb{N}$ des entiers naturels pairs est infini. En effet, l'application $D : \mathbb{N} \to 2\mathbb{N}$ de "multiplication par 2", $m \mapsto 2m$, est une bijection (en exercice). La même chose est vraie pour $m\mathbb{N}$, pour n'importe quel entier naturel non nul m, par le même argument, en remplaçant la multiplication par 2 par la multiplication par m.
ii) L'ensemble $2\mathbb{N}+1$ des entiers naturels impairs est infini : une bijection est donné par $I : \mathbb{N} \to 2\mathbb{N} + 1$, $m \mapsto 2m + 1$ (en exercice). Ceci montre que $\mathbb{N}$ est équipotent à de nombreux sous-ensembles propres, c'est-à-dire différents, de lui-même (en fait une infinité !) dont les compléments sont aussi infinis. En effet, nous avons vu que $2\mathbb{N}$ est infini, et $2\mathbb{N} + 1 = \mathbb{N} - 2\mathbb{N}$ aussi : on peut donc "partager" $\mathbb{N}$ en deux parties infinies qui ont la même taille que $\mathbb{N}$ lui-même !
iii) L'ensemble $\mathcal{P}$ des entiers naturels premiers est infini. Nous démontrerons ce fait rigoureusement dans le cours d'arithmétique.
iv) L'ensemble $\mathbb{N}$ est inclus dans tous les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$, ou du moins il existe une injection de $\mathbb{N}$ dans tous ces ensembles, si on les construit à partir de lui-même. Il s'ensuit que tous ces ensembles naturels sont eux-mêmes infinis.

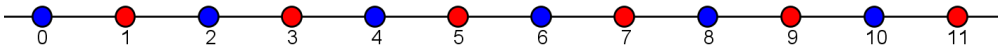

Figure 4.2: L'ensemble des entiers naturels pairs (en bleu) et l'ensemble des entiers naturels impairs (en rouge) sont deux sous-ensembles infinis et mutuellement complémentaires de $\mathbb{N}$, et chacun équipotent à $\mathbb{N}$.

La clause (ii) de l'exemple précédent, et plus généralement la définition même de l'infini, permettent d'exhiber des *paradoxes de l'infini mathématique* : il s'agit de contradictions *apparentes*, en ce qu'elles contreviennent à notre intuition, essentiellement *finie*, des quantités, mais il ne s'agit pas de contradictions réelles. Du moins, c'est ce que nous espérons et en fait "croyons" sous la forme des axiomes ou postulats que nous adoptons à propos de la fonction successeur, sans quoi nous devons perdre tout espoir de construire une théorie scientifique des nombres selon l'approche présente, et plus généralement une mathématique moderne. Mais ce saut dans l'infini, que nous avons fait comme un pas de foi dans la théorie naïve des ensembles, nous ouvre les portes de la mathématique supérieure.
Avant d'aller plus loin dans la caractérisation de l'infini mathématique, abordons un exemple fondamental d'ensemble infini associée à la topologie de la droite réelle. Un *intervalle* de l'ensemble $\mathbb{R}$ est un sous-ensemble I de $\mathbb{R}$ tel que pour tous $x, y \in I$, on a $[x, y] \subseteq I$, où $[a, b]$ est le *segment* $[a, b]$, soit l'ensemble $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$. Un intervalle I est dit *ouvert* s'il est de la forme $]a, b[$, $]a, +\infty[= \{x \in \mathbb{R} : a < x\}$, $]-\infty, b[= \{x \in \mathbb{R} : x < b\}$ ou $\mathbb{R}$, pour $a, b \in \mathbb{R}$. On renvoie par exemple au cours de logique mathématique naturelle pour la propriété d'Archimède et la définition de la partie entière d'un nombre réel.

Lemme 4.2.9. *Si a et b sont deux nombres réels tels que $a < b$, alors pour tout nombre réel $x > 0$, il existe un nombre rationnel r tel que $rx \in]a, b|$.*

Démonstration. Par la propriété d'Archimède, il existe un entier naturel $n > 0$ tel que $\frac{x}{b-a} < n$, d'où $\frac{x}{n} < (b-a)$, car $b-a > 0$ par hypothèse. Soit $k = E(\frac{an}{x})$ la partie entière de $\frac{an}{x}$: on a $\frac{k}{n}x \leq a < \frac{k+1}{n}x$, et $\frac{k+1}{n}x = \frac{k}{n}x + \frac{x}{n} \leq a + \frac{x}{n} < a + (b-a) = b$, d'où $\frac{k+1}{n}x \in]a, b|$, et le nombre rationnel $r = \frac{k+1}{n}$ convient, puisque comme $k \geq 0$, □

Proposition 4.2.10. *Si I est un intervalle ouvert non vide, alors I est infini.*

Démonstration. Si I est un intervalle ouvert non vide, alors il existe $a, b \in I$ tels que $a < b$; en effet, si ce n'est pas le cas, alors I ne possède qu'un élément et ne peut donc pas être un intervalle ouvert. Soient $x, y \in]a, b[$ tels que $x < y$ et considérons l'application $f : \mathbb{N} \to \mathbb{R}$, définie par $f(n) = a + \frac{b-a}{2^{n+1}}$: pour tout $n \in \mathbb{N}$, on a $f(n) \in]x, y[\subseteq]a, b[$ car $0 < \frac{y-x}{2^{n+1}} < y - x$, et si $n \neq m$, on a $f(n) \neq f(m)$: par exemple, si $n < m$, on a $2^{n+1} < 2^{m+1}$, d'où $\frac{y-x}{2^{m+1}} < \frac{b-a}{2^{n+1}}$. L'application f est donc injective, et par le théorème 4.2.3, I est infini.
Concernant la seconde assertion, par le lemme 4.2.9 appliqué à $x = 1$, il existe $r \in \mathbb{Q}$ tel que $r \in]a, b[$; en appliquant à nouveau le même lemme à l'intervalle $]r, b[$, il existe $s \in \mathbb{Q}$ tel que $s \in]r, b[$, d'où $]r, s| \subseteq]a, b[\subseteq I$. Appliquons le raisonnement précédent en remplaçant x et y par r et s respectivement : pour tout entier naturel n, le nombre

réel $r+\frac{s-r}{2^{n+1}}$ est rationnel, donc l'application injective $g :\in \mathbb{N} \mapsto r+\frac{s-r}{2^{n+1}}$ a pour image un sous-ensemble infini de nombres rationnels de I. Appliquons maintenant le lemme avec $x = \sqrt{2}$, dont on sait (voir le cours de logique mathématique naturelle) qu'il est irrationnel, et en notant que pour tout nombre rationnel r non nul, le nombre $r\sqrt{2}$ est irrationnel (sinon il existerait un nombre rationnel s tel que $r\sqrt{2} = s$, d'où $\sqrt{2} = \frac{r}{s} \in \mathbb{Q}$). Il existe comme avant deux nombres rationnels r et s tels que $r < s$ et $r\sqrt{2}, s\sqrt{2}[\subseteq]a, b[\subseteq I$, et l'application injective $h : n \in \mathbb{N} \mapsto r\sqrt{2} + \frac{(s-r)\sqrt{2}}{2^{n+1}} = \sqrt{2}(r + \frac{(s-r)}{2^{n+1}})$ a pour image un sous-ensemble infini de nombres irrationnels de I. □

Remarque 4.2.11. i) La démonstration, un peu exigeante, n'utilise que la propriété d'Archimède, la définition de la partie entière et l'irrationalité de $\sqrt{2}$, abordées dans le cours de logique mathématique naturelle. Cette proposition n'est pas essentielle pour la suite du présent cours.
ii) De même qu'il existe une infinité d'entiers pairs et d'entiers impairs dans $\mathbb{N}$, cette proposition montre qu'il existe une infinité de nombres rationnels et une infinité de nombres irrationnels dans $\mathbb{R}$. Cependant, il existe plus d'irrationnels que de rationnels : il y a plus de nombres réels que de nombres rationnels, et autant de nombres irrationnels que de nombres réels. Nous ne serons en mesure de démontrer cela qu'une fois abordés les développements des nombres réels dans une base numérique, ce qui sort du cadre du présent cours.

Définition 4.2.12. Un ensemble E est dit *dénombrable* si il existe une bijection entre $\mathbb{N}$ et E.

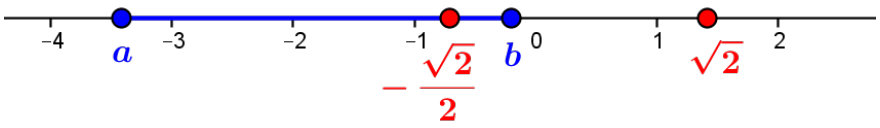

Figure 4.3: On a $b - a \geq 2$ et $1 \leq \sqrt{2} \leq 2$, donc $\frac{\sqrt{2}}{b-a} \leq 2/2 < 2$. Comme aussi $-4 \leq a \leq -3$, on a $-2 \leq \frac{a}{\sqrt{2}} \leq -3$, d'où $E(\frac{a}{\sqrt{2}}) = -2$, et le nombre rationnel $r = \frac{-2+1}{2} = -\frac{1}{2}$ vérifie donc $r\sqrt{2} = -\frac{\sqrt{2}}{2} \in]a, b[$.

Exercices de la section

Exercice 4.2.13. i) Soit n un entier naturel. Démontrer que l'ensemble $\{k \in \mathbb{N} : n \leq k\}$ est infini.
ii) On admet qu'il existe une bijection $f : \mathbb{N} \to \mathbb{Q}$, et qu'il n'existe pas de bijection de $\mathbb{N}$ sur $\mathbb{R}$. En supposant qu'il existe une bijection $g : \mathbb{N} \to \mathbb{R} - \mathbb{Q}$, montrer que l'application $h : \mathbb{N} \to \mathbb{R}$ définie par $h(2n) = f(n)$ et $h(2n + 1) = g(n)$ pour tout $n \in \mathbb{N}$, est une bijection. En conclure que l'ensemble $\mathbb{R} - \mathbb{Q}$ des nombres irrationnels n'est pas dénombrable.

4.3 Une énumération de $\mathbb{N}^2$

Parmi les ensembles infinis, on distingue l'ensemble $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$: on définit en effet une application injective $i : \mathbb{N} \hookrightarrow \mathbb{N}^2$ par $i(n) := (n, 0)$ pour tout $n \in \mathbb{N}$. Intuitivement, il semble qu'il existe "plus" d'éléments dans $\mathbb{N}^2$ que dans $\mathbb{N}$, correspondant aux couples (n, k) pour $k > 0$. Cependant, comme c'est le cas pour les entiers pairs et les entiers impairs, nous allons démontrer que $\mathbb{N}^2$ est *dénombrable*, c'est-à-dire qu'il existe une *bijection* de $\mathbb{N}$ sur $\mathbb{N}^2$. Cette section, plus difficile, peut-être passée ou survolée en première lecture.
Pour définir une telle bijection, on utilise l'intuition suivante : pour *énumérer* les couples d'entiers naturels, qu'on représente par les noeuds du quart de plan supérieur droite, on procède en énumérant les éléments des *diagonales* de ce quart de plan.

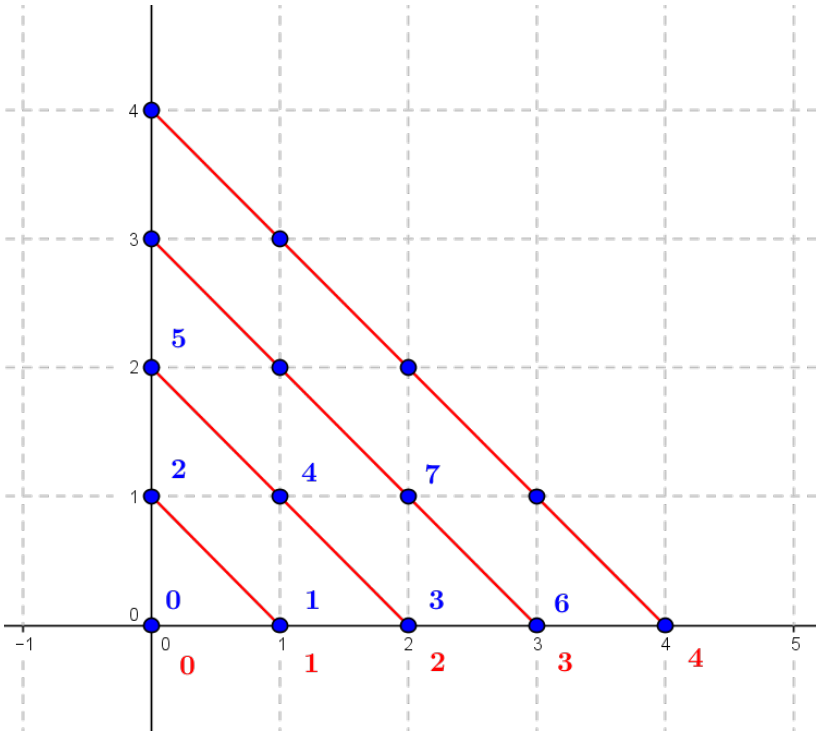

Figure 4.4: Représentation d'une énumération des couples d'entiers naturels par les entiers naturels (en bleu). Les diagonales (en rouge) sont aussi indexées par les entiers naturels : la diagonale d'indice n est l'ensemble des couples $(p, q) \in \mathbb{N}^2$ tels que $p + q = n$.

Le premier élément (d'indice 0) est l'origine $(0, 0)$, seul point de la "diagonale" d'indice 0. Les éléments suivants sont $(1, 0)$ et $(0, 1)$, points de la diagonale d'indice 1, et d'indices respectifs 1 et 2. On remarque que $1 + 0 = 0 + 1 = 1$; en fait, les points de la diagonale d'indice n sont les couples $(p, q) \in \mathbb{N}^2$ tels que $p + q = n$, et on commence à énumérer ceux-ci par $(n, 0)$, puis $(n - 1, 1)$, etc... jusqu'à $(1, n - 1)$ et n, et nous utiliserons cette intuition pour définir une bijection $\mathbb{N} \cong \mathbb{N}^2$. Tout d'abord, nous voulons associer à un couple $(p, q) \in \mathbb{N}^2$ un indice $m \in \mathbb{N}$ sous la forme d'une application $\varphi : \mathbb{N}^2 \to \mathbb{N}$ telle que $\varphi(p, q) = m$. En utilisant l'intuition précédente, (p, q) est sur la "diagonale d'indice n" tel que $n = p + q$, et il nous faut

donc identifier m à partir de là. La diagonale d'indice 0 correspond à un seul indice, le premier, c'est-à-dire 0; la diagonale d'indice 1 correspond à deux indices, 1 pour $(1,0)$ et 2 pour $(0,1)$: les indices correspondants aux diagonales 0 et 1 sont les nombres $0,1,2$, soit les nombres de 0 jusqu'à 2. En raisonnant de manière analogue, nous pouvons deviner que la diagonale d'indice k possède $k+1$ points (ce qu'on peut démontrer, mais nous n'avons besoin ici que de l'intuition pour construire φ), donc les indices correspondants aux diagonales d'indices $0,\dots,n$ devraient être les nombres de 0 jusqu'à $(1+2+\dots+(n+1))-1$. En effet, chaque diagonale d'indice k possédant $k+1$ points, elle "consomme" $k+1$ indices, donc on doit sommer les nombres $0+1, 1+1, \dots, n+1$ pour avoir le nombre total d'indices; comme on commence à compter à 0, on doit cependant retrancher 1).
Dans le cours de logique mathématique naturelle, nous démontrons par récurrence que la somme $1+2+\dots+n$ vaut $\frac{n(n+1)}{2}$, donc après la diagonale d'indice n on devrait avoir utilisé utilisé comme indices les entiers de 0 à $\frac{(n+1)(n+2)}{2}-1 = \frac{n^2+3n}{2} = \frac{n(n+3)}{2}$.
Par le même raisonnement, après la diagonale d'indice $n-1$ (si $n \geq 1$) on devrait avoir utilisé les entiers de 0 jusqu'à $\frac{(n-1)(n-1+3)}{2} = \frac{(n-1)(n+2)}{2} = \frac{n^2+n-2}{2} = \frac{n(n+1)}{2} - 1$: les indices correspondant à la diagonale d'indice n devraient être les entiers de $\frac{n(n+1)}{2}$ jusqu'à $\frac{n(n+3)}{2}$ inclus. Le raisonnement précédent permet maintenant de *conjecturer* ce que doit être l'indice m du couple (p,q) : si $n = p+q$, (p,q) est sur la diagonale d'indice n, et on commence à indexer les points de cette diagonale à partir de $(n,0)$, dont l'indice correspondant devrait donc être $\frac{n(n+1)}{2}$, ce qui nous amène à poser

$$\varphi(p,q) = \frac{n(n+1)}{2} + q = \frac{(p+q)(p+q+1)}{2} + q,$$

puisque c'est la deuxième composante, q, qui nous donne l'indice correspondant, en commençant pour $q=0$ à $\frac{n(n+1)}{2}$.
Vérifions ce que nous avons deviné précédemment : si $p+q=n$, par définition on a $\varphi(p,q) \geq \frac{n(n+1)}{2}$, et comme $q \leq n$, on a $\frac{n(n+3)}{2} - \varphi(p,q) = \frac{n(n+3)}{2} - \frac{n(n+1)}{2} - q = n - q \geq 0$, soit $\varphi(p,q) \leq \frac{n(n+3)}{2}$, donc on a bien $\varphi(p,q) \in [[\frac{n(n+1)}{2}, \frac{n(n+3)}{2}]]$ pour tout $(p,q) \in \mathbb{N}^2$, avec $p+q=n$.
Pour *démontrer* maintenant que cette indexation φ est une bijection, nous allons construire une bijection réciproque. Pour cela, si $n \in \mathbb{N}$ notons $I_n = [[\frac{n(n+1)}{2}, \frac{n(n+3)}{2}]]$.

Lemme 4.3.1. *i) Si $n, n' \in \mathbb{N}$ et $n \neq n'$, alors on a $I_n \cap I_{n'} = \emptyset$.*
ii) Pour tout $m \in \mathbb{N}$, il existe un unique $n \in \mathbb{N}$ tel que $m \in I_n$.

Démonstration. i) Supposons par exemple que $n < n'$: on a $\frac{n(n+3)}{2}+1 = \frac{(n+1)(n+2)}{2} \leq \frac{n'(n'+1)}{2}$, donc $\frac{n(n+3)}{2} < \frac{n'(n'+1)}{2}$, si bien que $I_n \cap I_{n'} = \emptyset$.
ii) Pour $m \in \mathbb{N}$, on a $\frac{0(0+1)}{2} = 0 \leq m$ et $m < \frac{m(m+1)}{2}$, si bien que l'ensemble $X = \{k \in \mathbb{N} : \frac{k(k+1)}{2} \leq m\}$ n'est pas vide (puisqu'il contient 0) et est majoré (puisque $m \notin X$). Par la proposition 4.1.1, l'ensemble X est fini, et par l'exercice 4.1.4(ii), il en existe un plus grand élément, notons-le n. On a $m \leq \frac{n(n+3)}{2}$: en effet, si $m > \frac{n(n+3)}{2}$ alors $m \geq \frac{n(n+3)}{2} + 1 = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$, si bien que $n+1 \in X$, ce qui contredit la définition de n. Par définition, on a $m \geq \frac{n(n+1)}{2}$, donc $m \in I_n$. Si $m \in I_{n'}$ pour un entier n', on a $I_n \cap I_{n'} \neq \emptyset$: par (i), cela signifie que $n = n'$, donc l'entier n tel que $m \in I_n$ est unique. □

Remarque 4.3.2. Avec les ensembles I_n, on "recouvre" l'ensemble $\mathbb{N}$ par des parties deux-à-deux disjointes : c'est ce qu'on appelle une *partition*.

Nous pouvons désormais définir ce que devrait être la bijection réciproque ψ de φ, à savoir l'énumération proprement dite, qui associe à un entier $m \in \mathbb{N}$ un couple d'entiers $(p, q) \in \mathbb{N}^2$. On considère par le lemme 4.3.1 l'entier $n \in \mathbb{N}$ unique tel que $m \in I_n$, dont tous les éléments devraient indexer les couples (p, q) tels que $p+q = n$, et la position de m dans I_n nous renseigne sur le couple (p, q) qui convient : si $m = \frac{n(n+1)}{2}$, m devrait indexer le "premier" couple, soit $(n, 0)$, ce qui nous amène à poser $q = m - \frac{n(n+1)}{2}$, $p = n - q$, et finalement on doit choisir $p = n - q = \frac{n(n+3)}{2} - m$, soit

$$\psi(m) = \left(\frac{n(n+3)}{2} - m, m - \frac{n(n+1)}{2} \right).$$

Par le travail fait précédemment sur les intervalles I_n, on voit que l'on définit ainsi une application de $\mathbb{N} \to \mathbb{N}^2$, puisque n est déterminé de manière unique pour chaque choix de m. Il nous reste à vérifier qu'on définit bien ainsi deux bijections réciproques.

Théorème 4.3.3. *L'application $\varphi : \mathbb{N}^2 \to \mathbb{N}$ est une bijection, de bijection réciproque $\psi : \mathbb{N} \to \mathbb{N}^2$.*

Démonstration. En écrivant par abus de notation Id les deux applications identiques de $\mathbb{N}^2$ et de $\mathbb{N}$, on doit montrer que $\varphi \circ \psi = Id$ et $\psi \circ \varphi = Id$. Si $m \in \mathbb{N}$, on a $\varphi \circ \psi(m) = \varphi(\frac{n(n+3)}{2} - m, m - \frac{n(n+1)}{2})$ (pour n l'entier tel que $m \in I_n$) $= \frac{n(n+1)}{2} + m - \frac{n(n+1)}{2} = m$, donc $\varphi \circ \psi = Id$. Inversement, si $(p, q) \in \mathbb{N}^2$ et $p + q = n$, on a $\psi \circ \varphi(p, q) = \psi(\frac{n(n+1)}{2} + q) = (\frac{n(n+3)}{2} - \frac{n(n+1)}{2} - q, q) = (p, q)$, donc $\psi \circ \varphi = Id$, et φ et ψ sont deux bijections réciproques l'une de l'autre. □

Remarque 4.3.4. i) Il y a donc "autant" de couples d'entiers naturels que d'entiers naturels.
ii) Cette énumération ψ de l'ensemble $\mathbb{N}^2$ est parfois appelée "appariement standard" ("standard pairing" en anglais) en logique mathématique.

4.4 Caractérisation intrinsèque de l'infinité mathématique

Si $f : E \to F$ est une application injective, la co-restriction de f à son image est injective et surjective, c'est donc une bijection $g : E \to f(E)$. Par exemple, l'application successeur $s : \mathbb{N} \to \mathbb{N}$ est injective, et sa co-restriction $t : \mathbb{N} \to \mathbb{N}^* = \mathbb{N} - \{0\}$ à $\mathbb{N}^*$ est bijective, puisque $Im(s) = \mathbb{N}^*$ par la proposition 4.2.2. Puisque $0 \notin \mathbb{N}^*$, il existe donc une bijection entre $\mathbb{N}$ et un sous-ensemble propre de $\mathbb{N}$ (rappelons qu'un sous-ensemble S d'un ensemble E est dit *propre* s'il est différent de E, c'est-à-dire si il existe $x \in E - S$). Cependant, notre intuition des ensembles finis nous dit que supprimer un élément d'un ensemble E produit un ensemble possédant *strictement* moins d'éléments. Par exemple, nous avons démontré dans la proposition 3.1.7 que si E possède n éléments, pour tout $x \in E$ l'ensemble $E' = E - \{x\}$ possède

$n-1$ éléments. Ce qui se produit avec la fonction successeur contrevient donc à l'intuition "finie" : nous ôtons un élément de $\mathbb{N}$, et nous obtenons pourtant un ensemble équipotent, c'est-à-dire qui possède le "même nombre d'éléments". Il est d'ailleurs possible, comme nous l'avons remarqué, d'ôter "une infinité d'éléments" à $\mathbb{N}$ et d'obtenir un sous-ensemble possédant le même nombre d'éléments, par exemple $2\mathbb{N}$, l'ensemble des entiers naturels pairs. Ou encore, d'ôter à l'ensemble $\mathbb{R}$ une infinité d'éléments (l'ensemble $\mathbb{Q}$), pour obtenir un sous-ensemble $\mathbb{R}-\mathbb{Q}$ possédant le même nombre d'éléments que $\mathbb{R}$.
Dans cette section, nous terminons ce cours en établissant que l'existence d'une bijection d'un ensemble avec une de ses parties propres délimite précisément la différence entre ensembles finis et ensembles infinis. Autrement dit, nous pouvons *caractériser* de manière intrinsèque ce qu'est un ensemble infini, c'est-à-dire sans référence à l'ensemble $\mathbb{N}$ ou aux ensembles finis.

Proposition 4.4.1. *Si E est un ensemble fini, alors il n'existe pas de bijection de E sur un sous-ensemble propre de E.*

Démonstration. Soit n le cardinal de E. On suppose au contraire, par l'absurde, qu'il existe un sous-ensemble propre F de E et une bijection $f : E \to F$. Comme $F \subseteq E$, par la proposition 3.2.1 F est fini, de cardinal $m < n$. Cependant, par définition du cardinal d'un ensemble fini il existe une bijection $g : [[1, n]] \to E$, donc l'application composée $f \circ g : [[1, n]] \to F$ est une bijection. En particulier, F possède aussi n éléments, ce qui contredit le fait que $|F| = m$. Par *reductio ad absurdum*, nous en concluons qu'il n'existe pas de bijection entre E et une partie propre de E. □

Proposition 4.4.2. *Si E est un ensemble infini, alors il existe un sous-ensemble propre F de E et une bijection de E sur F, et on peut choisir F de la forme $E-\{x\}$, pour $x \in E$.*

Démonstration. Supposons que E est infini : par le théorème 4.2.3, il existe une application injective $i : \mathbb{N} \hookrightarrow E$. Posant $E' = E - i(\mathbb{N}) = \{x \in E : x \notin i(\mathbb{N})\}$, nous avons $E = E' \cup i(\mathbb{N})$, une réunion disjointe, et nous définissons une application $g : E \to E - \{i(0)\}$ comme suit :
- si $x \in E'$, nous posons $g(x) = x$
- si $x \notin E'$, c'est-à-dire $x \in i(\mathbb{N})$, comme i est injective il existe un unique $n \in \mathbb{N}$ tel que $x = i(n)$, et nous posons $g(x) = i(n+1)$.

D'abord nous vérifions que g est injective : si $x, x' \in E$, distinguons trois cas. Si $x, x' \in E'$ et $g(x) = g(x')$, alors $x = g(x) = g(x') = x'$. Si $x \in E'$ et $x' \in i(\mathbb{N})$, alors $x \neq x'$ car $E' \cap i(\mathbb{N}) = \emptyset$, donc $g(x) \neq g(x')$ car $g(x) \in E'$ et $g(x') \in i(\mathbb{N})$. Si $x, x' \in i(\mathbb{N})$ et $g(x) = g(x')$, il existe des entiers naturels uniques m, n tels que $x = i(m)$ et $x' = i(n)$, donc $i(m+1) = g(i(m)) = g(x) = g(x') = g(i(n)) = i(n+1)$ et comme i est injective, on obtient $m+1 = n+1$, donc $m = n$ et on conclut que g est injective. Nous montrons ensuite que g est surjective : si $x \in E - \{i(0)\}$, soit $x \in E'$ et alors $x = g(x)$, soit $x \in i(\mathbb{N})$ et comme $x = \neg i(0)$, il existe $x \in \mathbb{N}$ tel que $x = i(n+1)$, si bien que $x = g(i(n))$ et dans les deux cas, x possède un antécédent par g, donc g est surjective. Finalement, g est une bijection de E sur une partie propre de E. □

Remarque 4.4.3. Deux cas de figure peuvent se présenter : soit E' est vide, auquel cas i est une bijection, soit $E' \neq \emptyset$, auquel cas $i(\mathbb{N})$ est une partie propre de E. La démonstration est uniforme dans les deux cas, car elle n'exploite E' que de manière "accessoire" en quelque sorte, pour définir g : c'est en "décalant" par g les images de i qu'on obtient une bijection de E sur une partie propre.

En combinant ces deux propositions, nous accédons à la seconde caractérisation, intrinsèque, des ensembles infinis, à partir des seuls concepts et principes de la théorie des ensembles.

Théorème 4.4.4. *Un ensemble E est* infini *si et seulement si il existe un sous-ensemble propre F de E et une bijection de E sur F.*

Démonstration. Si E est infini, alors par la proposition 4.4.2 il existe un sous-ensemble propre F de E et une bijection de E sur F. Inversement, supposons que E est fini : par la proposition 4.4.1, il n'existe pas de bijection de E sur un sous-ensemble propre de E; par contraposée, si une telle bijection existe, alors E est infini, et le théorème est démontré. □

Ce théorème fournit une description rigoureuse, authentique et intrinsèque de la notion *qualitative* d'infini mathématique. Il s'agit d'un accomplissement remarquable de la théorie naïve des ensembles, et la propriété pourrait servir de *définition* alternative à la notion d'ensemble infini. On définirait alors un ensemble *fini* comme un ensemble qui n'est pas infini ! Il faudrait cependant *démontrer* certaines propriétés des ensembles finis à partir de cette nouvelle définition, par exemple la propriété qui nous a servi à les définir ici. Une telle définition intrinsèque est esthétique, mais il pourrait sembler tortueux de définir la finitude à partir de l'infinité, alors que ce dernier concept est originellement la négation de la finitude, et est appréhendé à partir de l'intuition du "nombre d'éléments" des ensembles finis. Il faudrait par exemple démontrer qu'un ensemble est fini si et seulement si on peut le compter, alors que c'en est l'intuition fondamentale. Les deux approches sont néanmoins équivalentes, et l'étudiant(e) original(e) ou zélé(e) pourrait essayer de prendre ce chemin, ce qui constituerait d'ailleurs un excellent exercice. L'essentiel, ici comme ailleurs, est d'avoir des définitions claires et des résultats rigoureux.
Un dernier mot sur l'infini mathématique : nous introduirons dans un autre texte la construction de l'ensemble $\mathbb{R}$ des nombres réels, qui est infini en ce qu'il "contient" l'ensemble $\mathbb{N}$ des entiers naturels. Cependant, $\mathbb{R}$ possède *plus d'éléments* que $\mathbb{N}$, c'est-à-dire qu'il n'existe pas de bijection de $\mathbb{N}$ sur $\mathbb{R}$, comme nous l'avons déjà évoqué : ceci montre qu'il existe *différentes* quantités infinies, ce que nous avons déjà compris avec le théorème de Cantor. En fait, il est possible de développer une théorie *quantitative* de l'infini mathématique, à partir de "nombres" ordinaux ou cardinaux infinis - on dit plutôt "transfinis" - dans le cadre d'une théorie axiomatique des ensembles. La distinction entre les différentes quantités infinies prolonge alors la distinction entre les différentes quantités finies, et il est possible de calculer sur ces quantités infinies.

Exercices de la section

Exercice 4.4.5. i) En prenant comme définition d'un ensemble infini la propriété du théorème 4.4.4, montrer qu'un ensemble E est fini (c'est-à-dire n'est pas infini) si et seulement si il existe un entier naturel $n \in \mathbb{N}$ et une bijection $f : [[1, n]] \to E$.
ii) Utiliser la caractérisation du théorème 4.4.4 pour démontrer que si $E \subseteq F$ et E est infini, alors F lui-même est infini, sans utiliser la première caractérisation. Indication : choisir $x \in E$ et une bijection $E \to E - \{x\}$, et définir une bijection de F sur $F - \{x\}$.

Index