Chapitre 1

Notions de théorie des ensembles

De nombreuses façons, les mathématiques s'intéressent à l'étude des structures et des applications entre elles. Par exemple, l'algèbre linéaire s'occupe des espaces vectoriels et de leurs homomorphismes ; une grande partie de l'analyse s'intéresse aux espaces vectoriels sur les réels et aux fonctions sur de tels espaces.

La plus simple des structures mathématiques est celle d'un ensemble. Ainsi, la théorie des ensembles est au cœur des mathématiques modernes. Les autres concepts, comme les fonctions ou les relations, peuvent s'obtenir à partir de cette théorie.

Durant la plus grande partie du $19^{\text{ème}}$ siècle, la théorie des ensembles était basée sur la définition intuitive d'un ensemble comme une collection d'objets. Et donc, toute collection d'objets pouvait former un ensemble. Néanmoins, vers la fin du siècle, les mathématiciens ont découvert de sérieuses contradictions dans ce modèle intuitif. L'exemple le plus connu est le paradoxe de Russell : soit un ensemble S dont les éléments sont tous les ensembles qui ne se contiennent pas eux-même. S contient-il S ? Si oui, il contient un ensemble qui se contient lui-même, ce qui contredit la définition de S. Si non, il ne contient pas tous les ensembles qui ne se contiennent pas eux-mêmes, encore une contradiction !

Pour résoudre cette difficulté, Ernst Zermelo a proposé en 1908 la première théorie axiomatique des ensembles, c'est-à-dire une théorie des ensembles basée sur un petit nombre d'axiomes. L'avantage de cette théorie est qu'à peu près toutes les mathématiques en découlent et qu'elle n'admet pas de contradictions comme le paradoxe de Russell. Cette théorie a ensuite été étoffée par Abraham Frænkel, indépendamment par Thoralf Skolem et aussi par Zermelo lui-même. Aujourd'hui, les axiomes de Zermelo-Fraenkel sont au cœur de la théorie des ensembles.

1.1. Les ensembles

Malgré les problèmes soulevés par une théorie intuitive des ensembles, nous avons choisi dans ces notes cette approche pour sa simplicité, tout en gardant à l'esprit que d'éventuels problèmes peuvent être résolus en utilisant la théorie axiomatique de Zermelo-Fraenkel.

Un ensemble est une collection non ordonnée d'objets, que l'on appelle ses *éléments*. Si un ensemble A contient un élément a, alors on écrit $a \in A$. Si a n'est pas un élément de A, on écrit $a \notin A$. Un ensemble est *fini* s'il contient un nombre fini d'éléments, sinon on dit qu'il est *infini*.

Exemple 1.1.
- L'ensemble $A = \{1, 0, \mathrm{Pomme}\}$ est fini et $1 \in A$ mais $\mathrm{Table} \notin A$.
- L'ensemble infini de tous les entiers relatifs est noté $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$.
- L'ensemble infini de tous les entiers naturels est noté $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- L'ensemble infini de tous les entiers strictement positifs est noté $\mathbb{N}^\star = \{1, 2, 3, \ldots\}$.
- L'ensemble infini des nombres rationnels est noté $\mathbb{Q}$.
- L'ensemble infini des nombres réels est noté $\mathbb{R}$.
- L'ensemble infini des nombres complexes est noté $\mathbb{C}$.

Un sous-ensemble S d'un ensemble A, noté $S \subseteq A$, est un ensemble avec la propriété suivante :

$$S \subseteq A \iff \forall x\colon (x \in S \implies x \in A).$$

C'est-à-dire qu'un sous-ensemble de A contient certains éléments de A (peut-être tous). L'*ensemble vide*, noté $\emptyset$, est un ensemble ne contenant aucun élément. Pour tout ensemble A, on a $\emptyset \subseteq A$ et $A \subseteq A$. Si S n'est pas un sous-ensemble de A, ou de manière équivalente s'il existe un élément $s \in S$ tel que $s \notin A$, alors on écrit $S \nsubseteq A$.

Il est commode de définir un sous-ensemble d'un ensemble T à l'aide d'une propriété P qui est soit vraie soit fausse pour chacun des éléments de T. On peut alors définir un ensemble $A \subseteq T$ par $A := \{x \mid x \in T, P(x) \text{ est vraie}\}$.

Exemple 1.2.
- Les ensembles $\{x \mid x \in \mathbb{N}, x^2 < 12\}$ et $\{0, 1, 2, 3\}$ sont égaux.
- $\mathbb{N} = \{x \mid x \in \mathbb{Z}, x \geq 0\}$.
- Soient $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4\}$, et $C = \{3, 4, 5\}$. Alors $B \subseteq A$, $C \nsubseteq A$, $B \nsubseteq C$, $C \nsubseteq B$.
- Soient A un ensemble et $B = \{A, \{A\}\}$. Alors $A \in B$, mais quand A est non vide $A \nsubseteq B$. De plus, $\{A\} \in B$, $\{A\} \subseteq B$ et $\{\{A\}\} \subseteq B$.

L'ensemble des parties (*power set* en anglais) $P(A)$ d'un ensemble A est l'ensemble de tous les sous-ensembles de A. Par exemple, si $A = \{1, 2\}$, alors $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

1.2. Opérations sur les ensembles

Si A et B sont des ensembles, alors leur *produit cartésien* $A \times B$ est défini par

$$A \times B = \{(a, b) \mid a \in A \text{ et } b \in B\}.$$

Le produit cartésien d'un nombre fini d'ensembles $A_1, \ldots, A_n$ est défini récursivement comme :

$$A_1 \times \cdots \times A_n := \begin{cases} A_1 & \text{si } n = 1, \\ A_1 \times A_2 & \text{si } n = 2, \\ (A_1 \times \cdots \times A_{n-1}) \times A_n & \text{si } n > 2. \end{cases}$$

La *différence* de deux ensembles A et B, notée $A \smallsetminus B$, est définie par $A \smallsetminus B := \{x \mid x \in A \text{ et } x \notin B\}$. Ainsi, $A \smallsetminus B$ contient les éléments qui sont dans A mais qui ne sont pas dans B.

Soient A un ensemble et U un autre ensemble qui contient A. Le *complément* de A par rapport à U, noté ${}_UA^c$, ou juste A^c si U est connu d'après le contexte, est défini par $A^c = U \smallsetminus A$. Remarquez que $(A^c)^c = A$ quel que soit l'ensemble U.

L'*intersection* et l'*union* de deux ensembles A et B sont définies comme

$$\begin{aligned} A \cap B &:= \{x \mid x \in A \text{ et } x \in B\}, \\ A \cup B &:= \{x \mid x \in A \text{ ou } x \in B\}. \end{aligned}$$

L'union et l'intersection d'un nombre fini d'ensembles sont définies récursivement de manière analogue à la définition pour le produit cartésien. Le lemme suivant est connu sous le nom de *Loi de De Morgan* en mémoire de Augustus De Morgan, mathématicien britannique du 19$^{\text{ème}}$ siècle.

Lemme 1.3. *Soit U un ensemble contenant les ensembles A et B. On a :*

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

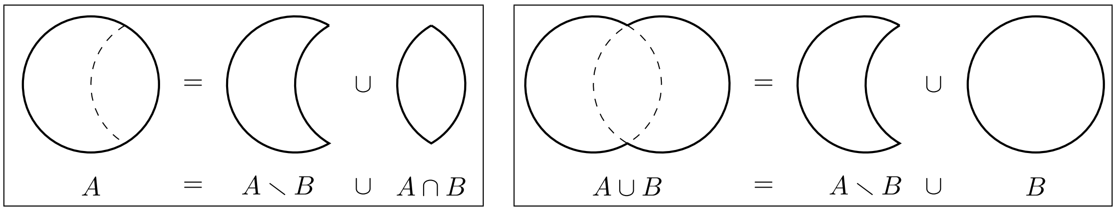
(2) $(A \cap B)^c = A^c \cup B^c$.

Démonstration. Nous ne prouvons que la partie (1), la seconde partie se prouve de manière analogue.

Pour montrer l'égalité de deux ensembles, on doit montrer que tout élément appartenant à l'un des ensembles appartient aussi à l'autre et *vice versa*. Soit $x \in (A \cup B)^c$. Alors $x \notin (A \cup B)$, donc $x \notin A$ et $x \notin B$, donc $x \in A^c$ et $x \in B^c$, donc $x \in A^c \cap B^c$.

Réciproquement, soit $x \in A^c \cap B^c$. Alors $x \in A^c$ et $x \in B^c$, donc $x \notin A$ et $x \notin B$, donc $x \notin A \cup B$, donc $x \in (A \cup B)^c$. □

Les opérations d'intersection et d'union satisfont certaines relations de commutativité et de distributivité indiquées dans la proposition suivante :



(a) (b)

Figure 1.1 – Description graphique de la démonstration du Lemme 1.5

Proposition 1.4. *Soient A, B et C des ensembles.*

(1) $A \cup A = A$, $A \cap A = A$,

(2) $A \cup B = B \cup A$, $A \cap B = B \cap A$.

(3) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.

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

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

Démonstration. Les assertion (1)–(3) sont triviales et les preuves de (4) et (5) sont similaires. On va donc se concentrer sur la démonstration de (4).

Soit $x \in A \cup (B \cap C)$. Alors $x \in A$ ou $x \in B \cap C$. Si $x \in A$, alors $x \in (A \cup C) \cap (A \cup B)$, ce qui montre que $A \cup (B \cap C) \subseteq (A \cup C) \cap (A \cup B)$. Si $x \in B \cap C$, alors $x \in B$ et $x \in C$, donc $x \in (A \cup C) \cap (A \cup B)$, ce qui montre encore que $A \cup (B \cap C) \subseteq (A \cup C) \cap (A \cup B)$.

Réciproquement, soit $x \in (A \cup C) \cap (A \cup B)$. Alors $x \in A \cup C$ et $x \in A \cup B$. Si $x \in A$, alors $x \in A \cup (B \cap C)$, donc $(A \cup C) \cap (A \cup B) \subseteq A \cup (B \cap C)$. Si $x \notin A$, alors $x \in C$ et $x \in B$, donc $x \in B \cap C$ et ainsi $x \in A \cup (B \cap C)$. Cela montre que $(A \cup B) \subseteq A \cup (B \cap C)$ et avec l'autre inclusion on obtient l'égalité des deux ensembles. □

La prochaine opération qui va nous intéresser et celle de l'*union disjointe*. Soient A et B des ensembles. L'*union disjointe* $A \sqcup B$ de A et B est définie comme

$$A \sqcup B = \{(a, 1) \mid a \in A\} \cup \{(b, 2) \mid b \in B\}.$$

De manière similaire, si $A_1, A_2, \ldots$ sont des ensembles, leur union disjointe est définie comme

$$\bigsqcup_{i=1}^{\infty} A_i := \bigcup_{i=1}^{\infty} \{(a, i) \mid a \in A_i\}.$$

On verra plus en détails certaines propriétés de l'union disjointe dans la prochaine section. Pour le moment, montrons juste le résultat suivant :

Lemme 1.5. *Soient A et B des ensembles.*

(a) $A = (A \smallsetminus B) \cup (A \cap B)$.

(b) $A \cup B = (A \smallsetminus B) \cup B$.

Démonstration. (a) L'ensemble à droite est trivialement contenu dans A, il suffit donc de montrer l'autre inclusion. Soit $x \in A$. Si $x \in A \cap B$, alors x est contenu dans $(A \smallsetminus B) \cup (A \cap B)$ et on a fini, supposons donc que $x \notin A \cap B$. Cela implique que $x \in A$, mais $x \notin B$, donc $x \in A \smallsetminus B$ par définition. Finalement $x \in (A \smallsetminus B) \cup (A \cap B)$ et on a fini.

(b) En utilisant (a), on sait que $A \cup B = (A \smallsetminus B) \cup (A \cap B) \cup B$. Mais $(A \cap B) \cup B = B$ et le résultat en découle. □

Une description graphique de la preuve de ce lemme est donné sur la figure 1.1.

1.3. Fonctions

La notion de fonction, et plus généralement celle de relation, sera vue dans le Chapitre 2. Néanmoins, nous en donnons ici une brève introduction pour pouvoir exposer plus clairement les concepts qui nous intéressent.

Soient A et B des ensembles. Intuitivement, une fonction f de A vers B est une procédure qui assigne à des éléments de A un élément de B. Cette définition n'est malheureusement pas assez précise dans notre contexte. Nous allons plutôt voir f comme un ensemble de paires telles que le premier élément est un argument de la fonction et le deuxième la valeur prise sur cet argument.

Plus précisément, le *graphe* de la fonction $f\colon A \to B$ de A dans B est un sous-ensemble de $G \subseteq A \times B$ tel que pour chaque $a \in A$, si (a, b) et (a, b') sont des éléments de G, alors $b = b'$. Cela revient à imposer qu'une fonction associe au plus une seule valeur pour un argument donné. On identifie une *fonction* avec son graphe et on note $b = f(a)$. On appelle a l'*antécédant* par f de b et b la *valeur* de f sur l'argument a. L'ensemble A est appelé l'*ensemble de départ* de f. L'ensemble des éléments $a \in A$ tels que $f(a)$ est défini est appelé *domaine de définition* de f et est noté $\mathrm{Dom}(f)$. Si le domaine de f est égal à A tout entier, on dit que f est une *application*. L'ensemble B est appelé l'*ensemble d'arrivée* de f. L'ensemble $f(A) := \{f(a) \mid a \in A\}$ est appelé l'*image* $\mathrm{Im}(f)$ de f.

Exemple 1.6. Voici quelques exemples de fonctions et d'objets qui n'en sont pas.
- Soit A un ensemble. L'ensemble $\{(a_1, a_2) \mid a_1, a_2 \in A \text{ et } a_1 = a_2\}$ est le graphe d'une fonction. Il s'agit de *la fonction identité* sur A.
- Soient A un ensemble et $P(A)$ l'ensemble de ses parties. L'ensemble $\{(a, S) \mid a \in S\} \subseteq A \times P(A)$ n'est pas le graphe d'une fonction à moins que A n'ait qu'un élément ou soit vide. Pour voir cela, notez que si a, b sont des éléments distincts de A, alors $(a, \{a\})$ et $(a, \{a, b\})$ sont tous deux dans cet ensemble, ce qui contredit la définition du graphe d'une fonction.

Une fonction $f\colon A \to B$ est dite *injective* si $f(a) = f(b)$ implique que $a = b$. Elle est dite *surjective* si pour tout $b \in B$ il existe $a \in A$ tel que $f(a) = b$. Elle est dite *bijective* si elle est à la fois surjective et injective.

Exemple 1.7. – Soit $f\colon \mathbb{Z} \to \mathbb{Z}$ définie par $f(z) := z + 1$. Alors, f est bijective.
- Soient A un ensemble fini et $f\colon A \to A$. Si f est injective, alors elle est bijective car comme $f(a) \neq f(b)$ pour $a \neq b$, la taille de $\mathrm{Im}(f)$ est égale à la taille de A ce qui montre la surjectivité.
- De manière similaire, si $f\colon A \to A$ est surjective et que A est fini alors f est bijective. Dans le cas contraire, s'il existe des éléments $a, b \in A$ distincts tel que $f(a) = f(b)$, cela montre que $\mathrm{Im}(f)$ a au moins un élément de moins que A ce qui contredit la surjectivité de f.
- Les deux points précédents sont faux si A est infini. La fonction $f\colon \mathbb{Z} \to \mathbb{Z}$ définie par $f(x) = 2x$ est clairement injective, mais elle n'est pas surjective.

Pour un ensemble fini A, le cardinal de A, noté $|A|$ ou $\#A$ est le nombre d'éléments dans A. L'ensemble de toutes les applications de A vers B est noté B^A. Cette notation est très bonne comme le montre le lemme suivant :

Lemme 1.8. *Si A et B sont finis, alors $|B^A| = |B|^{|A|}$.*

Démonstration. Une application $f\colon A \to B$ est déterminée de manière unique par son graphe $\{(a, f(a)) \mid a \in A\}$. Pour tout a, il y a $|B|$ possibilités pour $f(a)$. Comme il est possible de choisir $f(a)$ indépendamment pour chaque a, on voit qu'il y a $|B|^{|A|}$ possibilités pour l'application f. $\square$

Introduisons maintenant quelques notations que l'on va utiliser dans ce cours.
- Pour un nombre naturel n, l'ensemble $\underline{n}$ est défini comme $\{0, \ldots, n-1\}$. On définit également $\underline{0} := \emptyset$.
- Pour un ensemble fini A, on note n^A l'ensemble $\underline{n}^A$, c'est-à-dire l'ensemble de toutes les applications de A dans $\underline{n}$.
- Pour une fonction $f\colon A \to B$ et $b \in B$, on note $f^{-1}(b)$ la *fibre de f en b*, définie par

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

  Remarquez que cet ensemble peut être vide.
- Pour une fonction $f\colon A \to B$ et $S \subseteq A$, la *restriction de f sur S*, notée $f|_S$, est la fonction de S dans B qui associe à $s \in S$ l'élément $f(s)$.

Exemple 1.9. Montrons que pour un ensemble A, il existe une bijection φ de $P(A)$ dans 2^A. Soit $S \subseteq A$. On définit $f\colon A \to \underline{2}$ en posant $f(a) := 1$ ssi $a \in S$. On définit $\varphi(S) := f$. Pour montrer l'injectivité de φ, supposons que $\varphi(S) = \varphi(S') =: f$ pour deux ensembles distincts S, S' et soit $a \in S \setminus S'$. Alors $f(a) = 1$ car $a \in S$ et $f(a) = 0$ car $a \notin S'$, contradiction. Pour montrer que φ est surjective, soit $f \in 2^A$ et soit $S := f^{-1}(1)$. Il est alors trivial que $\varphi(S) = f$.

S'il existe une bijection entre deux ensembles A et B, on écrit $A \leftrightarrow B$. (Une notation plus naturelle serait d'écrire $A \simeq B$, mais elle est usuellement réservé pour des ensembles avec plus de structure, comme les espaces vectoriel, les groupes, les anneaux, etc.) On a le résultat suivant :

Proposition 1.10. *Soient A et B des ensembles.*

(a) *Il existe une application injective de $A \cup B$ dans $A \sqcup B$.*

(b) *Si $A \cap B = \emptyset$, alors $A \sqcup B \leftrightarrow A \cup B$.*

(c) *On a $A \leftrightarrow (A \setminus B) \sqcup (A \cap B)$.*

(d) *On a $A \cup B \leftrightarrow (A \setminus B) \sqcup B$.*

Démonstration. (a) En utilisant le lemme 1.5(b) on a $A \cup B = (A \setminus B) \cup B$. Soit $f\colon A \cup B \to A \sqcup B$ défini de la manière suivante : si $a \in B$, alors $f(a) := (a, 2)$ et si $a \in A \setminus B$ alors $f(a) := (a, 1)$. Cette application est une injection : si $f(a) = f(b)$, alors soit $a, b \in B$, soit $a, b \in A \setminus B$. Dans le premier cas, $(a, 2) = (b, 2)$, donc $a = b$. Dans le second cas, $(a, 1) = (b, 1)$, donc $a = b$.

(b) Dans cette situation, l'application f définie ci-dessus est surjective : pour $(a, 1) \in A \sqcup B$ on doit avoir $a \in A$ et $a \notin B$ (car $A \cap B = \emptyset$). Ainsi $(a, 1) = f(a)$. De manière similaire, $(b, 2) = f(b)$ pour tout $b \in B$, ce qui prouve la surjectivité de f.

(c) D'après le lemme 1.5(a) on sait que $A = (A \setminus B) \cup (A \cap B)$. Mais $(A \setminus B) \cap (A \cap B) = \emptyset$, donc (b) prouve le résultat.

(d) D'après le lemme 1.5(b) on sait que $A \cup B = (A \setminus B) \cup B$. Comme $(A \setminus B) \cap B = \emptyset$, (b) prouve le résultat. $\square$

1.4. Cardinal, ensembles dénombrables et indénombrables

Une bijection existe entre deux ensembles finis ssi ils ont le même cardinal.

Lemme 1.11. *Soient A et B des ensembles finis. Il existe une bijection entre A et B ssi $|A| = |B|$.*

Démonstration. Soit f une bijection entre A et B. Comme f est injective, la cardinal de $f(A)$ est le même que celui de A et par surjectivité $f(A) = B$.

Pour la réciproque, on peut supposer que $A = \{a_1, \dots, a_m\}$ et $B = \{b_1, \dots, b_m\}$ et définir l'application f par $f(a_1) = b_1, \dots, f(a_m) = b_m$. $\square$

Que se passe-t-il si A et B ont un nombre infini d'éléments ? Dans ce cas, il est difficile de donner une définition intuitive de $|A|$ et $|B|$. Une façon de s'en sortir est de ne pas essayer d'associer un nombre à $|A|$, mais de comparer la valeur relative du cardinal de deux ensembles.

Plus précisément, on dit que A et B ont le *même cardinal* ou encore que A et B sont *équipotents* et on note $|A| = |B|$, s'il existe une bijection $f\colon A \to B$.

Exemple 1.12. *L'ensemble des entiers $\mathbb{Z}$ et celui des nombres naturels $\mathbb{N}$ ont le même cardinal.* Pour prouver cela, considérons l'application $f\colon \mathbb{Z} \to \mathbb{N}$ définie par

$$f(z) := \begin{cases} -2z - 1 & \text{si } z < 0 \\ 2z & \text{si } z \geq 0. \end{cases}$$

Pour montrer que f est injective, supposons que $f(z_1) = f(z_2)$. Comme la valeur de f pour un argument négatif est impaire et celle pour un argument positif est pair, z_1 et z_2 sont nécessairement du même signe. Supposons par exemple qu'ils soient tous deux négatifs. Alors $f(z_1) = -2z_1 - 1 = -2z_2 - 1 = f(z_2)$, ce qui implique que $z_1 = z_2$. On arrive à la même conclusion si on les suppose tous deux positifs, ce qui montre l'injectivité de f.

Pour montrer la surjectivité de f, soit $m \in \mathbb{N}$. Si m est impair, il s'écrit $m = 2\ell - 1$ avec $\ell \in \mathbb{N}^\star$ et $m = f(-\ell)$. Si m est pair, il s'écrit $m = 2\ell$ avec $\ell \in \mathbb{N}$ et $m = f(\ell)$. L'application f est donc une bijection, ce qui termine la preuve.

On dit que $|A| < |B|$ s'il existe une application injective $f\colon A \to B$, mais qu'il n'existe *pas* de bijection $g\colon A \to B$. Montrer que $|A| < |B|$ est souvent plus difficile que de montrer $|A| = |B|$ car on doit prouver la non-existence d'un objet plutôt que son existence. On dit que $|A| \leq |B|$ s'il existe une application injective $f\colon A \to B$.

Un ensemble A est dit *dénombrable* si $|A| \leq |\mathbb{N}|$, c'est-à-dire s'il existe une injection de A dans $\mathbb{N}$. Une telle application est dite fonction de comptage.

Exemple 1.13. – Tout ensemble fini est dénombrable.
– De l'exemple précédent on en déduit que $\mathbb{Z}$ est dénombrable.

Théorème 1.14. *Les assertions suivantes sont vraies :*

(a) *Un sous-ensemble d'un ensemble dénombrable est dénombrable.*

(b) *Une union finie d'ensembles dénombrables est dénombrable.*

(c) *Si $A_1, A_2, \ldots$ sont dénombrables, alors l'union $\bigcup_{i\in\mathbb{N}} A_i$ est dénombrable.*

(d) *Si A et B sont dénombrables, alors $A \times B$ l'est aussi.*

(e) *L'ensemble $2^{\mathbb{N}}$ n'est pas dénombrable.*

(f) *L'ensemble des réels $\mathbb{R}$ n'est pas dénombrable.*

Démonstration. (a) Soient A dénombrable, $S \subseteq A$ et $f\colon A \to \mathbb{N}$ fonction de comptage pour A. La restriction $f|_S$ est une fonction de comptage pour S.

(b) L'assertion est trivialement vraie si l'union ne contient qu'un ensemble. Considérons ensuite le cas de deux ensembles dénombrables A et B, et considérons dans un premier temps le cas où les ensembles sont disjoints. Soient $f\colon A \to \mathbb{N}$ et $g\colon B \to \mathbb{N}$ des fonctions de comptage pour A et B. On définit alors une application $F\colon A \cup B \to \mathbb{N}$ par

$$F(x) := \begin{cases} 2f(x) - 1 & \text{si } x \in A, \\ 2g(x) & \text{si } x \in B. \end{cases}$$

On peut alors vérifier que F est bien définie, et injective (voir la preuve de l'exemple 1.12) et est donc une fonction de comptage pour $A \bigcup B$. Maintenant, pour montrer le cas ou les A et B sont arbitraires, remarquez qu'il existe toujours une injection d'une union d'ensembles dans leur union disjointe (voir 1.10(a)).

On termine ensuite la preuve par récurrence sur le nombre d'ensembles m. Pour $m \geq 3$ et $A_1, \ldots, A_m$ des ensembles dénombrables, par hypothèse de récurrence, $A_1 \cup A_2 \cup \cdots \cup A_{m-1}$ est dénombrable. En utilisant alors la preuve pour deux ensembles, on montre que

$$A_1 \cup A_2 \cup \cdots \cup A_m = (A_1 \cup A_2 \cup \cdots \cup A_{m-1}) \cup A_m$$

est dénombrable.

(c) Considérons dans un premier temps le cas où les ensembles sont disjoints. La preuve repose sur une méthode d'*énumération triangulaire*. Notons $f_1, f_2, \ldots$ les fonctions de comptage des ensembles $A_1, A_2, \ldots$. On peut alors ordonner les éléments de A_i comme $\{a_{i1}, a_{i2}, \ldots\}$, où les a_{ij} satisfont $f_i(a_{ij}) < f_i(a_{i,j+1})$ pour tout $j \geq 1$. On définit ensuite une application $F\colon \bigcup_{i\in\mathbb{N}} A_i \to \mathbb{N}$ par

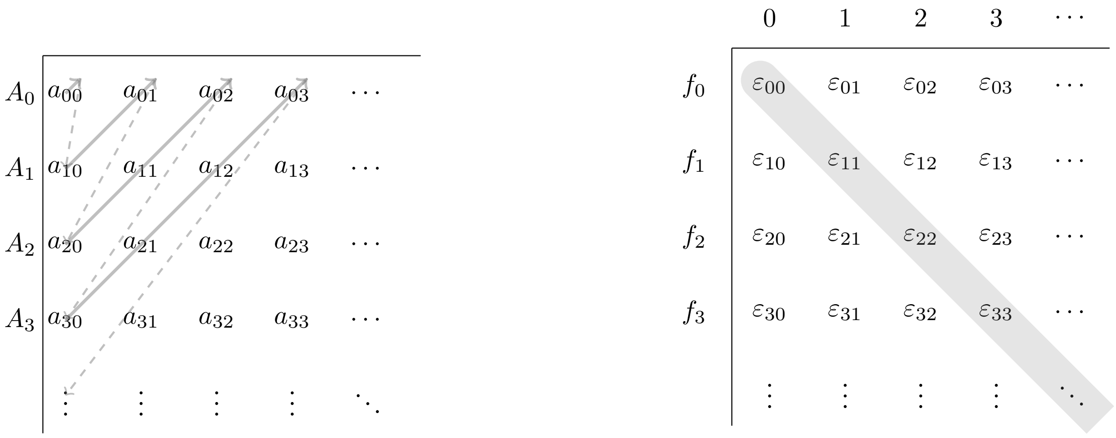
$$F(a_{ij}) := \frac{(i+j-2)(i+j-1)}{2} + j.$$

Remarquez que $F(a_{ij})$ est plus grand que $(i+j-2)(i+j-1)/2$ et inférieur ou égal à $(i+j-1)(i+j)/2$. Pour montrer que F est injective, il suffit de montrer que si $(i,j) \neq (i',j')$, alors $F(a_{ij}) \neq F(a_{i'j'})$. Si $i+j \neq i'+j'$, alors l'assertion est triviale à cause de la borne sur $F(a_{ij})$ mentionnée plus haut. Donc, supposons que $i+j = i'+j'$ et que $F(a_{ij}) = F(a_{i'j'})$. On en déduit alors que $j = j'$ et de là que $i = i'$. F est donc injective.

Maintenant, pour montrer le cas où les A_i sont arbitraires, remarquez qu'il existe toujours une injection d'une union d'ensembles dans leur union disjointe (voir 1.10(a)).

(d) Soient $A = \{a_0, a_1, a_2, \ldots\}$ et $B = \{b_0, b_1, b_2, \ldots\}$. Comme pour (c), on associe à (a_i, b_j) l'entier $(i+j)(i+j+1)/2 + j$. La preuve est alors la même que ci-dessus.

(e) La preuve est ici beaucoup moins facile car on essaie de montrer qu'une application n'existe pas plutôt que de simplement en construire une. On va utiliser une méthode connue sous le nom de « principe diagonal de Cantor » d'après le mathématicien allemand Georg Cantor qui l'a utilisée pour montrer que l'ensemble des réels dans l'intervalle $[0,1)$ est indénombrable.



(c) (e)

Figure 1.2 – Description graphique de la preuve du théorème 1.14(c) et (e).

Pour commencer, supposons que F est une fonction de comptage de l'ensemble $A = 2^{\mathbb{N}}$. On peut alors noter $n_0, n_1, \ldots \in \mathbb{N}$ avec $n_0 < n_1 < \cdots$ les éléments de l'image de F. On considère maintenant les applications $f_0, f_1, f_2 \ldots \in 2^{\mathbb{N}}$ telles que $F(f_i) = n_i$, $i = 0, 1, 2, \ldots$ et l'on pose

$$f_i(j) =: \varepsilon_{ij} \in \{0, 1\}.$$

Définissons alors $g \in 2^{\mathbb{N}}$ par

$$g(j) := \begin{cases} 1 & \text{si } \varepsilon_{jj} = 0, \\ 0 & \text{si } \varepsilon_{jj} = 1. \end{cases}$$

Par définition, on a $g(j) \neq \varepsilon_{jj}$. Comme $g \in 2^{\mathbb{N}}$, elle est nécessairement égale à l'une des f_ℓ pour un certain $\ell \in \mathbb{N}$. Mais alors $g(\ell) = f_\ell(\ell) = \varepsilon_{\ell,\ell}$, ce qui est en contradiction avec la définition de g.

(f) On va montrer que les réels de l'intervalle $[0, 1[$ ne sont pas dénombrables, ce qui implique l'assertion en utilisant la partie (a).

A toute suite $\epsilon = (\epsilon_1, \epsilon_2, \ldots)$ où $\epsilon_i \in \{0, 1\}$, on peut associer le réel $z = \sum_{i=1}^{\infty} \epsilon_i 2^{-i}$. Notons S_0 l'ensemble des suites qui deviennent constantes égales à 0 à partir d'un certain rang, S_1 l'ensemble des suites qui deviennent constantes égales à 1 à partir d'un certain rang et T les autres suites. L'ensemble $[0, 1[$ est en bijection avec $S_0 \cup T$. Nous avons déjà vu comment construire un réel à partir d'une suite. Réciproquement, tout réel z admet un développement dyadique que l'on peut construire par divisions euclidiennes successives. Dans cette construction, il est impossible qu'une suite de S_1 survienne car on a pour tout k, $2^{-k} = \sum_{i>k}^{\infty} 2^{-i}$. Comme $2^{\mathbb{N}} = T \cup S_0 \cup S_1$ n'est pas dénombrable et S_1 est dénombrable, $T \cup S_0$ ne peut pas être dénombrable car cela contredirait (b). Cela montre que $[0, 1[$ n'est pas dénombrable non plus. $\square$

La figure 1.2 donne une description graphique du procédé de comptage utilisé dans la preuve du théorème 1.14(c) et du principe diagonal de la preuve du théorème 1.14(e).

1.5. Le principe d'inclusion et d'exclusion

Comment compter le nombre d'éléments dans une union d'ensembles finis ? Si les ensembles sont disjoints, la solution est facile : le nombre d'éléments de l'union est la somme du nombres d'éléments de chaque ensemble qui apparaît dans l'union. Dans cette section, on développe une technique pour compter le nombre d'éléments dans une union. On ne considérera ici que le cas de 2 ou 3 ensembles, laissant le cas général en exercice.

Commençons par une simple observation.

Lemme 1.15. *Soient A et B des ensembles finis. Alors $|A \setminus B| = |A| - |A \cap B|$.*

Démonstration. En utilisant la proposition 1.10(c) on sait que $A \leftrightarrow (A \setminus B) \sqcup (A \cap B)$. Donc $|A| = |A \setminus B| + |A \cap B|$ ce qui montre le résultat. $\square$

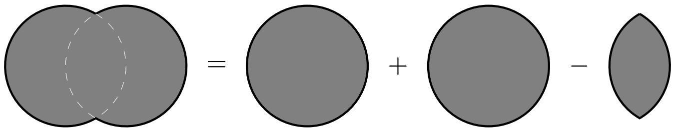


Figure 1.3 – Démonstration graphique de la proposition 1.16

Proposition 1.16. *Soient A et B des ensembles finis. Alors* $|A \cup B| = |A| + |B| - |A \cap B|$.

Démonstration. En utilisant la proposition 1.10(d) on a $A \cup B \leftrightarrow (A \setminus B) \sqcup B$. Ainsi $|A \cup B| = |A \setminus B| + |B|$ et le lemme 1.15 nous donne le résultat. □

Cette proposition est connue sous le nom de ≪ principe d'inclusion et d'exclusion ≫. En voici la raison : on commence par estimer la taille de $A \cup B$ par $|A| + |B|$. Mais de cette manière on a compté les éléments de $A \cap B$ deux fois, donc on doit les exclure de la somme, c'est-à-dire soustraire $|A \cap B|$.

Que faire pour trois ensembles ?

Proposition 1.17. *Soient A, B et C des ensembles finis. Alors,*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Démonstration. D'après la proposition 1.16 et la proposition 1.4(5) on a

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

□

Encore une fois, on peut voir pourquoi la méthode est connue comme principe d'inclusion et d'exclusion : On estime $|A \cup B \cup C|$ par $|A|+|B|+|C|$. Mais on a alors compté les éléments dans les intersections de deux ensembles deux fois, on doit donc les exclure. La nouvelle estimation est $|A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|$. Mais maintenant on a soustrait les éléments communs aux trois ensembles une fois de trop, on doit donc les inclure à nouveau.

Exemple 1.18. Un sondage a été effectué sur les méthodes de transports pour se rendre à l'EPFL. Les personnes interrogées pouvaient choisir ≪ vélo ≫, ≪ Tsol ≫ ou ≪ voiture ≫ et plusieurs réponses étaient possibles. La réponse ≪ vélo ≫ est apparue 30 fois, la réponse ≪ Tsol ≫ 100 fois, la réponse ≪ voiture ≫ 35 fois, les réponses ≪ vélo ≫ et ≪ voiture ≫ 15 fois ensemble, les réponses ≪ Tsol ≫ et ≪ voiture ≫ 15 fois ensemble, les réponses ≪ vélo ≫ et ≪ Tsol ≫ 20 fois ensemble et finalement seulement 5 personnes ont répondu les 3 moyens de transports. Combien de gens ont-ils été interrogés ?

Soient B, T et C les ensembles de questionnaires contenant respectivement les réponses ≪ Vélo ≫, ≪ Tsol ≫ et ≪ voiture ≫. La solution du problème est alors $|B \cup T \cup C|$. D'après l'énoncé on sait que $|B| = 30$, $|T| = 100$, $|C| = 35$, $|C \cap B| = 15$, $|T \cap C| = 15$, $|B \cap T| = 20$ et $|T \cap C \cap B| = 5$. Donc

$$|B \cup T \cup C| = 30 + 100 + 35 - 15 - 15 - 20 + 5 = 120,$$

et la réponse est 120.