Cours préparatoire pour le BASI
Logique élémentaire et ensembles
2018–2019

Jean-Marc Schlenker

University of Luxembourg, UR en Mathématiques, Maison du nombre, 6 avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg

Email address: jean-marc.schlenker@uni.lu

Table des matières

Chapitre 1. Logique élémentaire 5
Un peu d'histoire 5
Objectifs du chapitre 5
1. Propositions et assertions 5
2. Opérations sur les assertions 6
3. Recettes intuitives pour manipuler des assertions 8
4. L'algèbre de Boole : le "calcul" logique 9
5. Implication et équivalence 10
6. Démonstrations 11
7. Quantificateurs 12
8. Exercices 13

Chapitre 2. Ensembles 17
Un peu d'histoire 17
Objectifs 17
1. Qu'est-ce qu'un ensemble ? 17
2. Opérations sur les ensembles et les sous-ensembles 19
3. Relation et applications 21
4. Cardinaux 22
5. Exercices 25

Bibliographie 29

Chapitre 1

Logique élémentaire

Un peu d'histoire

Les éléments de logique élémentaire présentés ici sont pour certains anciens, et connus sous une forme ou sous une autre jusqu'à l'antiquité grecque, et certaines notions ont été formalisées par Aristote (384–322 BC) ou par ses prédecesseurs, d'où le terme de "logique aristotélicienne".

La logique mathématique a néanmoins connu une évolution importante, voire une révolution, dans les dernières décennies du XIXe siècle. La découverte de paradoxes en mathématiques a obligé les mathématiciens de l'époque à remettre en question les fondements même de leur discipline, et à établir sur une base solide tant la logique que la théorie des ensembles. On peut mentionner par exemple l'introduction des quantificateurs par Gottlob Frege (1848-1925) en 1879, ou les travaux de Bertrand Russell (1872–1970) au tout début du XXe siècle. Nous référons à [**1**] pour un aperçu historique sous forme de bande dessinée des développements de la logique et de la théorie des ensembles de cette époque.

Une autre innovation importante est la découverte en 1854 par George Boole (1815-1864) de l'algèbre qui porte son nom. L'algèbre de Boole permet de traiter de manière algébrique sur des propositions, comme on sait le faire pour d'autres objets mathématiques comme par exemple les nombres ou les polynômes.

Les éléments élémentaires de logique présentés dans ce chapitre sont essentiels à la pratique des mathématiques comme de l'informatique. Au-delà, comprendre de manière un peu formelle les bases du raisonnement est indispensable pour qui veut réfléchir de manière rigoureuse à n'importe quel sujet, scientifique ou non. Nous renvoyons à [**2**] pour un approfondissement du sujet.

Objectifs du chapitre

A l'issue de ce chapitre, vous devrez connaître les notions de conjonction, disjonction, négation et les notations qui sont utilisées pour les désigner. Vous devrez savoir traiter de manière "algébrique" sur les prédicats, par exemple écrire la négation d'une assertion impliquant des conjonctions et des disjonctions.

Certaines définitions données dans ce chapitre seront volontairement informelles. Il s'agit en effet ici maîtriser des outils logiques qui vous seront utiles en pratique par la suite. Mais donner des définitions rigoureuses de notions logiques même élémentaires peut conduire de réelles difficultés.

1. Propositions et assertions

L'objectif de ce chapitre est de savoir opérer logiquement sur des propositions.

DÉFINITION 1.1. *Une* proposition*, ou* assertion*, est une phrase qui peut être vraie ou fausse.*

Les propositions peuvent être mathématiques, ou plus générales. Par exemple on peut considérer les assertions mathématiques suivantes :

— $3 \leq 4$

— $6 \geq 8$
— Dans le plan, deux droites quelconques se coupent toujours en un point.

Des exemples de propositions non mathématiques :
— Tous les chats sont gris.
— S'il fait beau demain, j'irai me promener.

Nous utiliserons les lettres capitales $A, B, \ldots$ pour désigner des assertions mathématiques.

On peut noter qu'un phrase en "langue naturelle" peut être vraie ou fausse, mais peut aussi ne pas avoir de valeur de vérité bien définie. Par exemple, les phrases :

Tous les moutons sont noirs.

ou

Paul est plus vieux que Jacques.

ont une valeur de vérité bien définie (du moins si on considère que les variables "Paul" et "Jacques" sont bien définies). Par contre, les phrases :

Aujourd'hui il fait beau.

ou

Marie chante mieux que Pauline.

peuvent être considérées comme vraies ou fausses par des personnes différentes.

De même, presque toutes les propositions mathématiques que vous rencontrerez sont vraies ou fausses, mais ça n'est pas le cas dans tous les cas. Quel que soit le système mathématique dans lequel on se place (on peut parler plus précisément de système axiomatique) il existe des propositions mathématiques qui sont *indécidables*, c'est-à-dire qu'on ne peut ni démontrer, ni infirmer. C'est le *Théorème d'incomplétude* de Gödel (1931). On verra dans le chapitre suivant un exemple d'énoncé indécidable dans le cadre de la théorie des ensembles usuelle.

Tautologies. Une *tautologie* est une assertion qui est vraie du fait de sa construction. L'assertion suivante est un exemple de tautologie :

Deux jours avant sa mort, il était encore en vie.

2. Opérations sur les assertions

2.1. Définitions. On dispose de trois opérations naturelles sur les assertions.

DÉFINITION 2.1. — *La négation d'une assertion A, notée $\neg A$, est l'assertion qui est vraie si A et fausse, et fausse si A est vraie.*
— *La conjonction de deux assertions A et B, notée $A \wedge B$, est l'assertion qui est vraie si et seulement si A et vraie et B est vraie. On la lit "et".*
— *La disjonction de deux assertions A et B, est l'assertion $A \vee B$ qui est vraie si et seulement si A est vraie ou B est vraie. On la lit "ou".*

Dans une expression composée, la négation prend la priorité sur $\vee$ et $\wedge$. Ainsi, l'expression

$$\neg A \wedge B$$

est équivalente à

$$(\neg A) \wedge B$$

et non pas à

$$\neg(A \wedge B) .$$

De même, certains auteurs (surtout dans le domaine de l'informatique) considère [1] que le $\wedge$ a priorité sur le $\vee$, mais il est également commun d'utiliser des parenthèses pour aider à décomposer une assertion composée. Par exemple, écrira $(A \vee B) \wedge B$ à la place de $A \vee B \wedge B$.

On note que $\wedge$ correspond bien au "et" usuel, par contre $\vee$ ne correspond pas nécessairement au "ou" usuel. En effet, $\vee$ est un *ou inclusif*, qui est vrai si A et B sont tous les deux vrais. Le "ou" usuel peut être soit inclusif, soit exclusif, en fonction du contexte. Ainsi si on lit dans le menu d'un restaurant la phrase :

> *Fromage ou dessert*

il faut comprendre qu'on peut prendre du fromage ou un dessert, mais pas le deux. Il s'agit alors d'un *ou exclusif*. Cet distinction entre le "ou" exclusif et le "ou" inclusif est aussi illustré dans la blague suivante (la mathématicienne utilise le "ou" inclusif, qui est toujours utilisé en mathématiques) :

> Une mathématicienne vient d'avoir un bébé. Elle rencontre une amie, qui lui demande : "C'est une fille ou un garçon ?"
> "Oui !", répond la mathématicienne.

On peut utiliser les opérations $\wedge$, $\vee$ et $\neg$ pour construire de nouvelles assertions à partir d'assertions existantes. Par exemple, si A et B sont des assertions, alors $(A \vee B) \wedge B$ est une assertion. Les assertions qui ne sont pas obtenues comme composition d'autre assertions sont appelées *propositions (ou assertions) atomiques*, ou *variables propositionnelles*.

2.2. Tables de vérité. Les *tables de vérité* sont un moyen efficace pour analyser une proposition composée C à partir de plusieurs assertions atomiques $A, B, \ldots$ Ce sont des tableaux ayant une ligne pour chaque valeur possible des assertions A, B, ... qui apparaissent dans C, et on met dans les cases correspondantes les valeurs de C. Ces valeurs sont obtenues à partir des valeurs des variables propositionnelles en utilisant les tables de vérités qui définissent les opérations $\wedge$, $\vee$ et $\neg$ (voir Tab. 1 à 3), et en utilisant les règles de priorités sur les opérations. On représente habituellement la valeur "vrai" par 1 et "faux" par 0, et on parle de *valeurs de vérités*.

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

TABLE 1. Table de vérité de "et" soit $\wedge$.

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

TABLE 2. Table de vérité de "ou" soit $\vee$.

1. Cette convention est justifiée par le fait que le $\wedge$ se comporte comme une multiplication, et le $\vee$ comme une addition.

A	$\neg A$
0	1
1	0

Table 3. Table de vérité de la négation soit $\neg$.

Exemple 2.2. La table de vérité de l'assertion $(A \vee B) \wedge B$ est explicitée dans la table. 4. On constate que cette proposition est équivalente à B car elle a la même table de vérité que B.

A	B	$(A \vee B)$	$(A \vee B) \wedge B$
0	0	0	0
0	1	1	1
1	0	1	0
1	1	1	1

Table 4. Table de vérité de "ou" soit $\vee$.

Ainsi, on peut reconnaître les tautologies comme les assertions dont la table de vérité ne contient que des 1, et les contradictions, celles dont la table de vérité ne contient que des 0.

3. Recettes intuitives pour manipuler des assertions

En composant les assertions en utilisant les opérations logiques comme expliqué dans la section précédente, on obtient ce qu'on appelle l'"algèbre de Boole des propositions", décrite dans la section suivante. Pour mieux comprendre les règles qui s'appliquent dans cette algèbre, on peut d'abord en décrire quelques unes en langue naturelle.

— On peut combiner deux *et* de n'importe quelle manière. Ainsi l'assertion

Il fait beau et chaud, et il est tard.

est équivalente à

Il fait beau et il est tard, et il fait chaud.

— De la même manière, on peut combiner deux *ou* de n'importe quelle manière. Ainsi

Ma prochaine voiture sera bleue ou rouge, ou verte

est équivalente à

Ma prochaine voiture sera bleue ou verte, ou rouge.

— L'ordre des éléments de part et d'autre d'un *et* n'a pas d'importance, ainsi

L'université est grande et belle

est équivalent à

L'université est belle et grande.

— De même pour l'ordre des éléments de part et d'autre de *ou*.

— On peut "distribuer" un *et* qui se trouve devant une assertion contenant un *ou*. Ainsi

Mon vélo préféré est rapide, et de plus il est gris ou noir

est équivalent à

Mon vélo préféré est rapide et gris, ou bien il est rapide et noir.

— La négation d'une assertion contenant un *et* est obtenue en prenant la négation des deux cotés, et en remplaçant le *et* par un *ou.* Ainsi, la négation de

Albert parle anglais et allemand

est

Albert ne parle pas anglais ou ne parle pas allemand.

— La négation d'une assertion contenant un *ou* est obtenue en prenant la négation des deux cotés, et en remplaçant le *ou* par un *et.* Ainsi, la négation de

le gagnant du tournoi sera Pierre ou Marie

est

le gagnant du tournoi ne sera ni Pierre ni Marie.

Les assertions qu'on vient de voir ne concernent que des objets uniquement déterminés, comme "Paul", "Pierre", ou "l'Université". On peut étendre considérablement nos capacités d'expression en utilisant des *quantificateurs* : "pour tout" ou "il existe". Ainsi une expression comme

La nuit, tous les chats sont gris

exprime une assertion qui s'applique non pas à un chat particulier, mais à tous les chats. De même pour l'expression :

L'année dernière, il y a eu un mois où il pleuvait tous les jours.

Cette expression contient *deux* quantificateurs.

Il faut noter que l'ordre des quantificateurs joue un rôle important. Par exemple il ne faut pas confondre :

Tous les jours, il y a un homme qui est touché par la foudre

et

Il y a un homme qui est touché par la foudre tous les jours.

On va retrouver cette distinction quand on verra les quantificateurs sous une forme plus précise plus loin.

4. L'algèbre de Boole : le "calcul" logique

Les opérations $\wedge$ et $\vee$ satisfont certaines propriétés algébriques élémentaires, qui permettent d'opérer sur des "formules" logiques. Ces propriétés sont analogues à celles que satisfont $+$ et $\times$ (à comparer respectivement à $\vee$ et $\wedge$). Ces propriétés formalisent les règles "intuitives" présentées dans la section précédente. Elles peuvent être formellement vérifiées (c'est un bon exercice) en établissant les tables de vérité des assertions qui les composent. Par exemple, la première règle $A \wedge (B \wedge C) = (A \wedge B) \wedge C$ signifie que les assertions $A \wedge (B \wedge C)$ et $(A \wedge B) \wedge C$ ont la même table de vérité. Voici une petite liste de ses propriétés.

— associativité de $\wedge$: $A \wedge (B \wedge C) = (A \wedge B) \wedge C$.
— associativité de $\vee$: $A \vee (B \vee C) = (A \vee B) \vee C$.
— commutativité de $\wedge$: $A \wedge B = B \wedge A$.
— commutativité de $\vee$: $A \vee B = B \vee A$.
— distributivité de $\wedge$ par rapport à $\vee$: $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$.
— l'assertion vraie 1 est élément neutre pour $\wedge$, et l'assertion fausse 0 est élément neutre pour $\vee$: quelle que soit l'assertion A, on a toujours

$$A \wedge 1 = A \ , \quad A \vee 0 = A \ .$$

— 0 annule toutes les proposition : on a pour toute assertion A que $A \wedge 0 = 0$.

D'autres propriétés n'ont pas d'analogue direct pour $+$ et $\times$, par exemple :

— distributivité de $\vee$ par rapport à $\wedge$: $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$.

Dans chaque cas, on peut démonter directement que les lois s'appliquent en montrant que les deux cotés de l'égalité prennent les mêmes valeurs quelle que soit les valeurs de vérité de A, B, C.

On a vu aussi l'opération $\neg$, la négation d'une assertion. Elle satisfait aussi des propriétés importantes en relation avec $\wedge$ et $\vee$.

— $\neg(\neg A) = A$.
— $\neg(A \vee B) = (\neg A) \wedge (\neg B)$.
— $\neg(A \wedge B) = (\neg A) \vee (\neg B)$ (ces deux lois portent le nom "de Morgan").
— $(\neg A) \wedge A = 0$.
— $(\neg A) \vee A = 1$.

Finalement, on dispose de deux règles simples qui permettent de simplifier les expressions logiques, elles portent le nom de "lois d'absorption".

— $(A \wedge B) \vee B = B$,
— $(A \vee B) \wedge B = B$.

5. Implication et équivalence

A partir des opérateurs $\neg, \wedge$ et $\vee$, on peut introduire d'autres opérateurs logiques utiles.

DÉFINITION 5.1. *On note $\Rightarrow$ l'opérateur "implication" défini pour deux assertions A et B quelconques par*

$$(A \Rightarrow B) \quad \textit{si et seulement si} \quad (\neg A) \vee B \ .$$

On dira que A implique B si l'assertion $A \Rightarrow B$ est vraie. On dit que A est l'antécédent, et que B est le conséquent, de l'implication $A \Rightarrow B$.

DÉFINITION 5.2. *L'implication $B \Rightarrow A$ est appelée* réciproque *de l'implication $A \Rightarrow B$.*

Il suit de la définition que $A \Rightarrow B$ est vraie *sauf* dans le cas où A est vraie et B est fausse. Ceci correspond à l'implication qu'on utilise dans le langage courant. Par exemple, la phrase

Si les poules avaient des dents, je serais pape

est vraie, parce que l'antécédent ("les poules ont des dents") est fausse.

On note aussi $\Leftarrow$ l'implication dans le sens inverse, c'est-à-dire que $B \Leftarrow A$ est équivalent à $A \Rightarrow B$.

On note donc que $A \Rightarrow B$ est équivalente à $B \Leftarrow A$, mais pas du tout à $B \Rightarrow A$!

DÉFINITION 5.3. *L'implication $(\neg B) \Rightarrow (\neg A)$ est appelée contraposée de l'implication $A \Rightarrow B$.*

PROPOSITION 5.4. *Une implication est équivalente à sa contraposée.*

DÉMONSTRATION. On veut montrer que $A \Rightarrow B$ est vraie si et seulement si $(\neg B) \Rightarrow (\neg A)$. Or $A \Rightarrow B$ est fausse si et seulement si A est vraie et B et fausse. Mais $(\neg B) \Rightarrow (\neg A)$ est fausse si et seulement si $(\neg B)$ est vraie et $(\neg A)$ est fausse, donc si et seulement si A est vraie et B est fausse. Les deux assertions ont donc exactement les mêmes valeurs de vérité, elles sont donc équivalentes. $\square$

Alternativement, on peut démontrer la proposition précédente en montrant que les deux assertions $A \Rightarrow B$ et $(\neg B) \Rightarrow (\neg A)$ ont la même table de vérité.

DÉFINITION 5.5. *On note $\Leftrightarrow$ la relation d'équivalence : $A \Leftrightarrow B$ si et seulement si $A \Leftarrow B$ et $B \Leftarrow A$.*

En d'autres termes, $A \Leftrightarrow B$ est vraie si et seulement si A et B ont la même valeur de vérité : soit A et B sont toutes deux vraies, soit A et B sont toutes deux fausses.

Dans certains cas, on utilisera aussi la notation suivante.

DÉFINITION 5.6. *La* disjonction exclusive*, ou "ou exclusif", notée $A \oplus B$, est définie comme suit : $A \oplus B$ est vraie si et seulement si*
— *soit A est vraie et B est fausse,*
— *soit A est fausse et B est vraie.*

Ainsi l'expression

Fromage ou dessert

sur un menu de restaurant correspond à un ou exclusif.

6. Démonstrations

Une démonstration mathématique est une suite d'assertions mathématiques, chacune découlant logiquement de la précédente, permettant de passer d'assertions admises comme étant vraies, vers une assertion finale qu'on souhaite démontrer.

Pour écrire une démonstration, la règle est donc très claire : il faut partir de ce qu'on connaît — un théorème tiré du cours, ou l'énoncé de l'exercice — et arriver à la conclusion, chaque étape découlant de manière parfaitement claire des précédentes. Si le passage d'une étape à la suivante n'est pas parfaitement clair, ça n'est pas une démonstration !

Démonstration par l'absurde. Dans certains cas, il est utile de "raisonner par l'absurde" : on suppose que la conclusion à laquelle on veut aboutir est fausse, et on en déduit une contradiction. Faire une démonstration par l'absurde revient donc à démontrer

$$(\neg B) \Rightarrow (\neg A)$$

pour en déduire que $A \Rightarrow B$.

Exemple. Montrons qu'il existe une infinité de nombres premiers (un nombre entier strictement positif est dit *premier* s'il est différent de 1 et n'est divisible que par 1 et par lui même). On admettra ici que tout nombre non premier est divisible par un nombre premier.

On suppose, en raisonnant par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers, qu'on note $p_1, p_2, \cdots, p_n$. On appelle p leur produit, $p = p_1 p_2 \cdots p_n$, et on sait que $n \geq 2$ puisque 2 et 3 sont des nombres premiers.

On remarque que $p + 1$ n'est pas divisible par p_1, car p_1 ne peut pas diviser deux nombre successifs. De même, $p+1$ n'est pas divisible par aucun des $p_i, 1 \leq i \leq n$. Donc $p+1$ n'est divisible par aucun des nombres premiers. Or tout nombre non premier est divisible par un nombre premier. Donc $p+1$ est premier. Or $p+1$ est strictement plus grand que tous les p_i (car $n \geq 2$). Ceci contredit notre hypothèse suivant laquelle $p_1, p_2, \cdots, p_n$ sont tous les nombres premiers.

On peut donc conclure que l'hypothèse de départ était fausse, et qu'il existe une infinité de nombres premiers.

Démonstration par récurrence. C'est un type particulier de preuve, utilisé pour démontrer des assertions dépendant d'un nombre entier n. Notons ainsi (A_n) une assertion dépendant de n. Pour démontrer que (A_n) est vraie pour tout n, il *suffit* de montrer que :
— (A_0) est vraie,
— pour tout $n \geq 0$, $(A_n) \Rightarrow (A_{n+1})$.
Dans certains cas, on pourra commencer à $n = 1$ au lieu de $n = 0$.

Exemple. Montrons par récurrence que pour tout $n \in \mathbb{N}_{>0}$, on a

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

On appelle (A_n) cette assertion.

On vérifie d'abord que (A_1) est vraie. En effet, pour $n = 1$, les deux cotés de l'équation sont égaux à 1.

Soit maintenant $n \geq 1$, supposons (A_n), et montrons (A_{n+1}). On remarque que

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+2)(n+1)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

et on peut donc en déduire (A_{n+1}). On voit ainsi que la propriété (A_n) est vraie pour tout $n \geq 1$.

7. Quantificateurs

7.1. Définitions. Le langage mathématique utilise souvent les quantificateurs suivants.

DÉFINITION 7.1. *Le* quantificateur universel*, $\forall$, se lit "pour tout". Si E est un ensemble et P un prédicat défini sur les éléments de E, l'assertion*

$$\forall x \in E, P(x)$$

affirme que $P(x)$ est vraie pour tous les éléments x de E.

DÉFINITION 7.2. *Le* quantificateur existentiel*, $\exists$, se lit "il existe". Si E est un ensemble et P un prédicat défini sur les éléments de E, l'assertion*

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

affirme qu'il existe un élément x de E tel que $P(x)$ est vraie.

EXEMPLE 7.3. Reprenons l'exemple où $P(n)$ est le prédicat défini sur l'ensemble des entiers par "n est pair". L'assertion $\exists n, P(n)$ stipule qu'il existe un entier pair. L'assertion $\forall n, P(n)$, qui est fausse, stipule que tous les entiers sont pairs.

On utilisera parfois une version modifiée de $\exists$ qui affirme l'existence d'un unique élément d'un ensemble satisfaisant un prédicat donné.

DÉFINITION 7.4. *Le quantificateur existentiel suivi d'un point d'exclamation, $\exists!$, se lit "il existe un unique". Si E est un ensemble et P un prédicat défini sur les éléments de E, l'assertion*

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

affirme qu'il existe un unique élément x de E tel que $P(x)$ est vraie.

7.2. Négation des quantificateurs. Si $P(x)$ est un prédicat, alors $\exists x, P(x)$ et $\forall x, P(x)$ sont des assertions. On peut donc combiner ces assertions à l'aide des opérations logiques $\vee, \wedge$ et $\neg$ pour former des assertions plus complexes. Il faut noter que les règles suivantes doivent être appliquées quand on veut déterminer la négation d'une assertion quantifiée.

PROPOSITION 7.5. *Soit E un ensemble, et P un prédicat défini pour les éléments de E.*

(1) $\neg(\forall x \in E, P(x)) = \exists x \in E, \neg P(x)$.

(2) $\neg(\exists x \in E, P(x)) = \forall x \in E, \neg P(x)$.

Ainsi, si E et F sont deux ensembles et P un prédicat de deux variables $x \in E$ et $y \in F$, la négation de

$$\forall x \in E, \exists y \in F, P(x,y)$$

est

$$\exists x \in X, \forall y \in F, \neg P(x,y)\ .$$

Ainsi, la négation de

Tous les moutons sont noirs

est l'assertion :

Il existe un mouton qui n'est pas noir

et réciproquement.

De même, la négation de

Tous les hommes ont au moins un ami

est

Il existe un homme qui n'a aucun ami.

En effet, si E est l'ensemble des hommes et $P(x,y)$ désigne "y est ami avec x" alors la première assertion se traduit par

$$\forall x \in E, \exists y \in E, P(x,y)\ ,$$

et sa négation est donc

$$\exists x \in E, \forall y \in E, \neg P(x,y)\ .$$

8. Exercices

Les exercices d'application directe du cours sont marqués par un "Δ". Si vous n'arrivez pas à les faire, vous devez revoir le cours ! Les exercices marqués "*" sont plus difficiles.

8.1. Δ Valeurs de vérité. Établir la valeur de vérité des propositions suivantes :

(1) (5 est un entier positif)
(2) $(3 < 4) \wedge (9 - 2 = 6)$
(3) $(4 \leq 4) \vee (9 - 2 = 6)$
(4) $(4 > 5) \vee \neg(9 - 2 = 6)$
(5) $(2 + 2 = 4) \Rightarrow (2 = 4 - 2)$
(6) $(5 > 3) \oplus (2 < 4)$
(7) $(5 > 3) \Leftrightarrow (1 \neq 0)$

8.2. △ Réciproque et contraposée. Écrivez la réciproque et la contraposée de chacune des implications suivantes :

(1) S'il ne fait pas beau, alors je vais au cinéma
(2) $(A \vee B) \Rightarrow C$
(3) Si $x > y$, alors $f(x) > f(y)$ et je suis le meilleur en maths
(4) $(A \wedge B) \Rightarrow (C \vee D)$

8.3. Tables de vérité. Soient A, B et C des assertions. Construire la table de vérité des assertions composées suivantes :

(1) $(A \wedge B) \vee (\neg A \vee C)$
(2) $(A \Leftarrow C) \Rightarrow B$
(3) $(A \Rightarrow B) \Leftrightarrow \neg(A \oplus B)$
(4) $(A \Rightarrow \neg(B \vee C)) \Rightarrow (B \wedge (A \Rightarrow \neg C))$

8.4. Ou exclusif. On rappelle la table de vérité du ou exclusif pour deux assertions A et B, ou "xor", notée $\oplus$:

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Montrer que pour n assertions $A_1, ..., A_n$,

$$vrai \oplus A_1 \oplus A_2 \oplus ... \oplus A_n = vrai \Leftrightarrow card(\{i \mid A_i = vrai\}) \text{ est pair.}$$

Indication : On pourra raisonner par récurrence sur n.

8.5. Simplification d'expression logique. Soient A, B, C et D des assertions. Simplifiez au maximum les expressions logiques suivantes :

(1) $(C \vee D) \wedge (A \vee B) \wedge \neg C \wedge \neg D$
(2) $((A \wedge \neg B) \wedge (B \wedge C))(\vee(A \wedge B) \vee (\neg B \wedge C))$
(3) $B \vee \neg(\neg A \vee \neg C) \vee \neg(C \wedge B) \vee \neg(A \vee \neg C)$

Vérifier le résultat à l'aide d'une table de vérité.

8.6. *Démonstration par l'absurde. Démontrer que $\sqrt{2}$ est irrationnel.

8.7. *Démonstration par récurrence.

(1) Prouver les formules suivantes, où n est un entier au moins égal à 1 :

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

(2) Montrer que le nombre $2^{3n} - 1$ est toujours divisible par 7 quel que soit le nombre entier positif ou nul n.

8.8. *Généralisation des lois de De Morgan. Soient $A_1, ..., A_n$ des assertions. Montrer les deux propositions suivantes, pour tout $n \geq 2$:

(1) $\neg \left(\bigwedge_{i=1}^{n} A_i \right) = \bigvee_{i=1}^{n} \neg A_i$, c'est-à-dire $\neg(A_1 \wedge A_2 \wedge ... \wedge A_n) = \neg A_1 \vee \neg A_2 \vee ... \vee \neg A_n$

(2) $\neg \left(\bigvee_{i=1}^{n} A_i \right) = \bigwedge_{i=1}^{n} \neg A_i$, c'est-à-dire $\neg(A_1 \vee A_2 \vee ... \vee A_n) = \neg A_1 \wedge \neg A_2 \wedge ... \wedge \neg A_n$

8.9. *Génération d'expression logique. Soient A, B et C des assertions. Proposer une expression logique e correspondant à la table de vérité suivante :

A	B	C	$e(A,B,C)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

8.10. *Connecteurs primitifs.

(1) Prouver qu'il est impossible d'exprimer toutes les opérations logiques comme compositions des opérations $\vee$ et $\Rightarrow$.

(2) On désigne par $\uparrow$ et $\downarrow$ les opérations dont les tables de vérités sont

A	B	$A \uparrow B$	$A \downarrow B$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

(a) Montrer qu'il est possible d'exprimer l'ensemble des opérations de la logique des assertions à l'aide de l'unique operation $\uparrow$.

(b) Montrer qu'il est possible d'exprimer l'ensemble des opérations de la logique des assertions à l'aide de l'unique connecteur $\downarrow$.

Chapitre 2

Ensembles

Un peu d'histoire

La notion d'ensemble en mathématiques est ancienne. Mais la théorie des ensembles moderne est née dans les années 1870, sous l'impulsion de mathématiciens comme Georg Cantor (1845-1918) et Richard Dedekind (1831-1916). La découvertes de paradoxes comme celui de Russell, présenté plus bas, a conduit au début du XXème siècle à formaliser la théorie des ensembles et à proposer différentes formulations axiomatiques, dont celle de Zermelo-Frankel qui est la plus utilisée aujourd'hui. La découverte par Cantor de la théorie des cardinaux pour les ensembles infinis a été considérée comme une véritable révolution à la fin du XIXè siècle.

La théorie des ensembles a connu des progrès considérables au cours du XXème siècle. On peut mentionner par exemple le théorème d'incomplétude de Kurt Gödel (1906-1978) ou la preuve en 1963 de l'hypothèse du continu (dont on verra l'énoncé) par Paul Cohen (1934-2007).

Objectifs

L'angle de présentation choisi ici est volontairement simple voire naïf. L'objectif est de :
- comprendre et savoir utiliser les principales notations sur les ensembles (intersection, union, etc),
- connaître et savoir utiliser les quantificateurs $\forall$ et $\exists$,
- savoir utiliser les expressions utilisant les quantificateurs, par exemple écrire la négation d'une proposition quantifiée,
- connaître et savoir utiliser les notions de relation, d'application, d'application injective, surjective et bijective.

1. Qu'est-ce qu'un ensemble ?

1.1. Une (non-)définition. On peut être tenté de définir un ensemble comme n'importe quelle collection d'éléments, sans se poser plus de question. C'est ce qu'on longtemps fait les mathématiciens. On peut ainsi parler de l'ensemble des nombres entiers positifs $\mathbb{N}$, de l'ensemble des parties de l'ensemble des nombres entiers positifs, ou de l'ensemble de tous les ensembles, ou de l'ensemble de tous les ensembles qui contiennent $\mathbb{N}$.

Malheureusement, cette approche naïve conduit à des paradoxes, et elle n'est donc pas utilisable mathématiquement, et il est donc indispensable de procéder avec précaution.

1.2. Le paradoxe de Russell. Le paradoxe de Russell, attribué à Bertand Russell (1872-1970), est le suivant. Soit E l'ensemble de tous les ensembles qui ne se contiennent pas eux-même comme élément, c'est-à-dire de tous les ensembles F tels que F n'est pas éléments de F. On considère alors l'assertion A suivante :

E est élément de E.

Alors :

— E n'est pas élément de E. Sinon, par définition, E serait élément de E. Donc, A est fausse.
— Mais alors, toujours par définition, E est élément de E. Donc, A est vraie.

On a ainsi défini une assertion A qui est à la fois vraie et fausse. Ceci est particulièrement grave, car on peut alors démontrer que *toute* assertion B est à la fois vraie et fausse. En effet, comme A est fausse, l'assertion $A \Rightarrow B$ est vraie, mais comme A est vraie, on peut en déduire que B est vraie.

1.3. Quelques ensembles importants. Pour éviter le paradoxe de Russell, on se contente de considérer des ensembles définis suivant des règles fixées, qui évitent les paradoxes. [1] Ainsi, on considèrera certains ensembles "bien connus", ceux définis en énumérant leurs éléments, ceux obtenus à partir de ceux-ci en leur appliquant certains opérateurs (en particulier en prenant l'ensemble de leurs parties) et enfin les ensembles obtenus à partir d'un autre ensemble en sélectionnant certains de ses éléments par un prédicat. Les éléments d'un ensemble sont deux à deux distincts et ne sont pas ordonnés.

1.4. Quelques ensembles essentiels en mathématiques. On admettra l'existence et les propriétés principales des ensembles suivants.
— $\mathbb{N}$, l'ensemble des entiers positifs $0, 1, 2, \cdots$.
— $\mathbb{Z}$, l'ensemble des entiers relatifs $\cdots, -2, -2, 0, 1, 2, \cdots$.
— $\mathbb{Q}$, l'ensemble des nombre rationnels, donc de la forme p/q, où p et q sont deux entiers relatifs et q est non nul.
— $\mathbb{R}$, l'ensemble des nombres réels.

1.5. Définition d'un ensemble en énumération. On peut définir un ensemble en énumérant la liste de ses éléments. On note alors l'ensemble sous la forme

$$E = \{A, B, \cdots, Z\} ,$$

où $A, B, \cdots, Z$ sont ses éléments.

On utilise une notation particulière pour l'ensemble vide, c'est-à-dire l'ensemble qui n'a aucun élément, on le note $\emptyset$. Comme les éléments d'un ensemble sont deux à deux distincts, on a $\{1, 1, 2\} = \{1, 2\}$ par exemple.

1.6. Appartenance, inclusion. On utilisera souvent les deux symboles suivants, qu'il est utile de savoir distinguer.

Définition 1.1 (appartenance). *Soit E un ensemble, on notera $x \in E$ si x est un élément de E.*

Définition 1.2 (inclusion). *Un ensemble F est un sous-ensemble (ou une partie) d'un ensemble E, et on note $F \subset E$, si tout élément de F est aussi un élément de E.* [2]

Par exemple, on a

$$A \in \{A, B, C\} ,$$

et

$$\{A\} \subset \{A, B, C\} .$$

On peut alors définir un sous-ensemble d'un ensemble donné.

1. Ou du moins on le pense. En fait il est essentiellement impossible de démontrer que le système obtenu ne contient pas de contradiction...
2. En anglais, on utilise la notation $F \subseteq E$.

DÉFINITION 1.3. *Un sous-ensemble d'un ensemble E est un ensemble F dont tous les éléments sont élément de E. On note alors $F \subset E$.*

EXEMPLE 1.4. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$: tout nombre entier naturel est un entier relatif, tout entier relatif est un nombre rationnel, tout nombre rationnel est un nombre réel.

1.7. Ensemble des parties d'un ensemble. On peut construire à partir d'un ensemble donné E un nouvel ensemble, "plus gros" que E.

DÉFINITION 1.5. *Etant donné un ensemble E, on notera $\mathcal{P}(E)$ l'ensemble des sous-ensembles de E, c'est-à-dire des ensembles dont tous les éléments sont des éléments de E.*

Par exemple, $\mathcal{P}(\emptyset) = \{\emptyset\}$ est un ensemble à un élément, alors que $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$ est un ensemble à deux éléments.

1.8. Prédicats. Un prédicat est une assertion $P(x)$ qui stipule une propriété d'un élément x d'un ensemble donné (dans le cas d'un prédicat unaire), ou d'un n-uplet (c'est à dire d'une suite ordonnée de n éléments) d'éléments de cet ensemble (dans le cas d'un prédicat n-aire où $n \geq 2$). Dans le prédicat $P(x)$, on considère x comme une variable qui peut être évaluée par n'importe quel élément de l'ensemble, et c'est cette évaluation qui donne la valeur de vérité au prédicat. Ainsi, un prédicat unaire sur un ensemble E peut être vu comme une fonction de E dans l'ensemble des valeurs de vérités $\{0, 1\}$ (pour rappel, 0 signifie "faux" et 1 signifie "vrai").

EXEMPLE 1.6. Le prédicat $P(n)$ défini par "n est pair" sur l'ensemble des entiers prend les valeurs suivantes en fonction de l'évaluation de n (avec 0 pour "faux" et 1 pour "vrai") : $P(0) = 1$, $P(1) = 0$, $P(2) = 1$, $P(3) = 0$, etc.

Le prédicat binaire $R(a, b)$ défini sur l'ensemble des nombres réels par "a est plus petit que b" est vrai si $a = 0$ et $b = 1$, mais est faux si $a = 4$ et $b = 2$. Bien-sûr, on préférera écrire le prédicat $R(a, b)$ par $a \leq b$.

1.9. Définition d'un ensemble en compréhension. Etant donné un prédicat P qui s'applique aux éléments d'un ensemble E, on peut définir un nouvel ensemble, dont les éléments sont exactement les éléments de E qui vérifient le prédicat P. On le note :

$$\{x \in E \mid P(x)\} .$$

EXEMPLE 1.7. On reprend l'exemple précédent où P est le prédicat "être pair". Alors

$$\{n \in \mathbb{N} \mid P(n)\}$$

est l'ensemble des entiers naturels (positifs) pairs, et

$$\{n \in \mathbb{N} \mid \neg P(n)\}$$

est l'ensemble des entiers naturels impairs.

2. Opérations sur les ensembles et les sous-ensembles

2.1. Union, intersection, complémentaire. On utilisera les opérations suivantes sur les ensembles, ou sur les sous-ensembles, suivantes.

DÉFINITION 2.1. *L'union de deux ensembles A et B, notée $A \cup B$, est l'ensemble des objets qui sont soit élément de A, soit élément de B.*

DÉFINITION 2.2. *L'intersection de deux ensembles A et B, notée $A \cap B$, est l'ensemble des éléments de A qui sont aussi élément de B.*

Définition 2.3. *Soit E un ensemble, et A un sous-ensemble de E. Le complément de A dans E, noté $\bar{A}^E$, est l'ensemble des éléments de E qui ne sont pas élément de A.*

Exemple 2.4. Considérons par exemple l'ensemble P des nombres entiers pairs et l'ensemble I des nombres entiers impairs. On a $P \subset \mathbb{N}$ et $I \subset \mathbb{N}$. Par ailleurs, $P \cap I = \emptyset$ et $P \cup I = \mathbb{N}$. On a en fait $\bar{P}^{\mathbb{N}} = I$.

Souvent, quand on considèrera le complémentaire d'un sous-ensemble, il n'y aura pas d'ambiguité sur l'ensemble dont il est sous-ensemble. On notera alors $\bar{A}$ au lieu de $\bar{A}^E$, sans qu'il y ait de confusion possible.

Il est utile de noter que $\cup, \cap$ et $\bar{}$ sont analogues respectivement des opérateurs $\vee, \wedge$ et $\neg$ pour les assertions. Ainsi, les opérations algébriques ci-dessous sont analogues aux règles de l'algèbre de Boole du premier chapitre.

2.2. Opérations algébriques sur les sous-ensemble. Les opérations $\cup$, $\cap$ et complémentaire satisfont certaines propriétés algébriques élémentaires, analogues à celles que satisfont $\vee$ et $\wedge$ (à comparer respectivement à $\cup$ et $\cap$).

— associativité de $\cap$: $A \cap (B \cap C) = (A \cap B) \cap C$.
— associativité de $\cup$: $A \cup (B \cup C) = (A \cup B) \cup C$.
— commutativité de $\cap$: $A \cap B = B \cap A$.
— commutativité de $\cup$: $A \cup B = B \cup A$.
— distributivité de $\cap$ par rapport à $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

D'autres propriétés n'ont pas d'analogue direct pour $+$ et $\times$, par exemple :

— distributivité de $\cup$ par rapport à $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Dans chaque cas, on peut démonter directement que les lois s'appliquent en montrant que les deux cotés de l'égalité contiennent les mêmes éléments.

On a vu aussi l'opération $\bar{}$, la négation d'une assertion. Elle satisfait aussi des propriétés importantes en relation avec $\cap$ et $\cup$.

— $\bar{\bar{A}} = A$.
— $\overline{A \cup B} = \bar{A} \cap \bar{B}$.
— $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
— $\bar{A}^E \cap A = \emptyset$.
— $\bar{A}^E \cup A = E$.

Définition 2.5. *On notera $\setminus$ la différence de deux ensembles : $E \setminus F$ est l'ensemble des éléments de E qui ne sont pas élément de F.*

2.3. Produit d'ensembles. Il existe une opération de produit d'ensembles, souvent appelée "produit cartésien".

Définition 2.6. *Soient E et F deux ensembles. Le produit (cartésien) de E et F, noté $E \times F$, est l'ensemble des couples (x, y), où x est un élément de E et y est un élément de F.*

Notons qu'un couple d'objets x et y, noté (x, y), est une suite de deux objets. Il tient compte de l'ordre des deux éléments. On distingue le couple (x, y) de la paire $\{x, y\}$, qui ne tient pas compte de l'ordre de x et y.

On peut généraliser ce produit à plus de deux ensembles. Ainsi, si E, F et G sont trois ensembles, le produit (cartésien) $E \times F \times G$ est l'ensemble des triplets (x, y, z) où $x \in E, y \in F$ et $z \in G$.

Définition 2.7. *Etant donné un ensemble E et un entier $n \in \mathbb{N}$, on notera*

$$E^n = E \times E \times \cdots \times E$$

(avec n facteurs) l'ensemble des n-uplets d'éléments de E.

3. Relation et applications

3.1. Relations. On va voir d'abord la notion de relation entre deux ensembles, puis se concentrer sur le cas particulier des applications.

DÉFINITION 3.1. *Une relation entre deux ensembles E et F est un sous ensemble R de $E \times F$. Etant donné une relation $R \subset E \times F$ entre E et F, on dit que deux éléments $x \in E$ et $y \in F$ sont en relation si $(x, y) \in R$.*

On utilisera les notions de domaine et d'image d'une relation.

DÉFINITION 3.2. *Soit $R \subset E \times F$ une relation. Le domaine de R est*

$$D(R) = \{x \in E \mid \exists y \in F, (x, y) \in R\} .$$

L'image de R est

$$Im(R) = \{y \in F \mid \exists x \in E, (x, y) \in R\} .$$

Ainsi le domaine de R est l'ensemble des éléments de E qui sont en relation avec au moins un élément de F, et l'image de R est l'ensemble des éléments de F qui sont en relation avec au moins un élément de E.

3.2. Applications.

DÉFINITION 3.3. *Soient E et F deux ensembles. Une application de E dans F est une relation $f \subset E \times F$ telle que tout élément $x \in E$ est en relation avec exactement un élément de F, qu'on notera $f(x)$. On notera $f : E \to F$ une applications de E dans F.*

EXEMPLE 3.4. Soit E un ensemble. On appellera *application identité* de E, et on notera id_E, l'application de E dans E qui à tout $x \in E$ associe x lui-même.

On pourra utiliser les notions suivantes.

DÉFINITION 3.5. *Soit $f : E \to F$ une application. L'image de f est l'image de f vue comme une relation, c'est-à-dire que*

$$Im(f) = \{y \in F \mid \exists x \in E, f(x) = y\} .$$

Pour tout $y \in F$, on dira que x est un antécédent de y par f si $f(x) = y$, et on notera $f^{-1}(\{y\})$ l'ensemble des antécédents de y par f.

Le vocabulaire suivant sera par ailleurs souvent utilisé, il est donc bon de le connaître.

DÉFINITION 3.6. *Une application $f : E \to F$ est :*
— *injective, si tout élément de F a au plus un antécédent par f,*
— *surjective, si tout élément de F a au moins un antécédent par f,*
— *bijective, si elle est injective et surjective.*

Ainsi une application $f : E \to F$ est injective si et seulement si

$$\forall x, x' \in E, x \neq x' \Rightarrow f(x) \neq f(x') ,$$

et surjective si et seulement si $Im(f) = F$. Elle est bijective si et seulement si tout élément de l'ensemble d'arrivée a exactement un antécédent.

Définition 3.7. *Soit* $f : E \to F$ *une application* bijective. *On note* $f^{-1} : F \to E$ *l'application qui à tout élément de* F *associe son unique antécédent dans* E*. On appelle* f^{-1} *l'application réciproque de* f*.*

On dispose aussi pour les applications d'une opération de composition, définie comme suit.

Définition 3.8. *Soient* E, F, G *trois ensembles, et soient* $f : E \to F$ *et* $g : F \to G$ *deux applications. On appelle composée de* f *et de* g*, et on note* $g \circ f$*, l'application* $g \circ f : E \to G$ *qui à* $x \in E$ *associe* $g(f(x)) \in G$*.*

Notez bien l'ordre des fonctions dans $g \circ f$: on note en premier l'application qui est appliquée en dernier.

Par exemple, on remarque que si $f : E \to F$ est une bijection, alors $f \circ f^{-1} = id_F$ et $f^{-1} \circ f = id_E$.

La loi de composition satisfait à la propriété d'associativité suivante.

Proposition 3.9. *Soient* $f : E \to F$*,* $g : F \to G$ *et* $h : G \to H$ *trois applications. Alors* $(h \circ g) \circ f = h \circ (g \circ f)$*.*

Démonstration. A faire en exercice. □

On laisse en exercice la preuve de la propriété suivante.

Proposition 3.10. *La composée de deux applications injectives est injective. La composée de deux applications surjectives est surjective.*

4. Cardinaux

4.1. Cardinaux des ensembles finis. On dira qu'un ensemble est fini s'il a un nombre fini d'éléments, c'est-à-dire si on peut établir une bijection entre cet ensemble et un ensemble de la forme

$$\{1, 2, \cdots, n\}$$

pour un certain $n \in \mathbb{N}$.

Définition 4.1. *Le cardinal d'un ensemble fini est le nombre de ses éléments. Soit* E *un ensemble fini, on notera* $|E|$*, ou* $\#(E)$*, son cardinal.*

On remarque que si E et F sont deux ensembles finis, alors :

— s'il existe une application injective de E dans F, alors $\#E \leq \#F$,

— s'il existe une application surjective de E dans F, alors $\#E \geq \#F$,

— s'il existe une application bijective de E dans F, alors $\#E = \#F$.

On a la règle d'addition suivante.

Proposition 4.2. *Soient* E *et* F *deux ensembles finis. Alors*

$$|E \cup F| + |E \cap F| = |E| + |F| \ .$$

Démonstration. On peut décomposer $E \cup F$ en la réunion de trois ensembles disjoints :

$$E \cup F = (E \cap F) \cup (E \setminus F) \cup (F \setminus E) \ .$$

Ainsi,

$$|E \cup F| = |E \cap F| + |E \setminus F| + |F \setminus E| \ .$$

Mais on a aussi l'union disjointe

$$E = (E \cap F) \cup (E \setminus F) \ ,$$

d'où il suit que

$$|E| = |E \cap F| + |E \setminus F| \ ,$$

et l'union disjointe

$$F = (E \cap F) \cup (F \setminus E) \ ,$$

qui montre que

$$|F| = |E \cap F| + |F \setminus E| \ ,$$

En ajoutant les deux dernières équations et en soustrayant la précédente, on obtient le résultat anoncé. □

Proposition 4.3. *Soient E et F deux ensembles finis. Alors $|E \times F| = |E| \times |F|$.*

Démonstration. A voir en exercice. □

Etant donné un ensemble fini E, le cardinal de l'ensemble de ses parties peut s'exprimer simplement en fonction du cardinal de E.

Proposition 4.4. *Soit E un ensemble fini, alors $\#\mathcal{P}(E) = 2^{\#E}$.*

Démonstration. On note $n = \#E$, et on appelle $e_1, \cdots, e_n$ les éléments de E. On note alors $\phi : \{0,1\}^n \to \mathcal{P}(E)$ l'application qui à un n-uplet $(\epsilon_1, \cdots, \epsilon_n) \in \{0,1\}^n$ associe le sous-ensemble $\phi(\epsilon_1, \cdots, \epsilon_n) \subset E$ qui contient e_i si et seulement si $\epsilon_i = 1$.

On peut alors facilement montrer que ϕ est injective et surjective, donc bijective. On en déduit que $|\mathcal{P}(E)| = |\{0,1\}|^n = 2^n$. □

En particulier, on note que $|\mathcal{P}(E)| > |E|$ dans tous les cas.

4.2. * Cardinaux infinis *. L'une des grandes découvertes du XIXème siècle est la réalisation par Georg Cantor (1845-1918) qu'il existe différents types d'infini : certains ensembles infinis sont "plus gros" que d'autres.

On admettra ici le résultat suivant (dont la preuve n'est pas excessivement difficile).

Théorème 4.5 (Admis). *Soient E et F deux ensembles (éventuellement infinis). S'il existe une application injective de E dans F et une application injective de F dans E, alors il existe une application bijective de E dans F.*

Ce résultat rend possible la définition suivante.

Définition 4.6. *Etant donné deux ensembles E et F, on dira que*
- *E a plus petit cardinal que F, s'il existe une application injective de E dans F,*
- *E a plus grand cardinal que F, s'il existe une application surjective de E dans F,*
- *E et F ont même cardinal, s'il existe une application bijective de E dans E.*

On peut vérifier assez facilement que cette notion de cardinal pour le ensembles infinis vérifie les principales propriétés souhaitables, par exemple si E a plus petit cardinal que F et F a plus petit cardinal que G alors E a plus petit cardinal que G.

Définition 4.7. *On dira qu'un ensemble E est dénombrable si E a même cardinal que $\mathbb{N}$, donc s'il existe une bijection de $\mathbb{N}$ sur E.*

Quelques exemples :
- $\mathbb{Z}$ est dénombrable, car on peut énumérer ses éléments, par exemple comme suit : $0, 1, -1, 2, -2, 3, -3, \cdots$.
- $\mathbb{N}^2$ est dénombrable, on peut aussi énumérer ses éléments, comme sur la Figure 1. De manière plus générale, $\mathbb{N}^n$ est dénombrable pour tout $n \geq 1$.

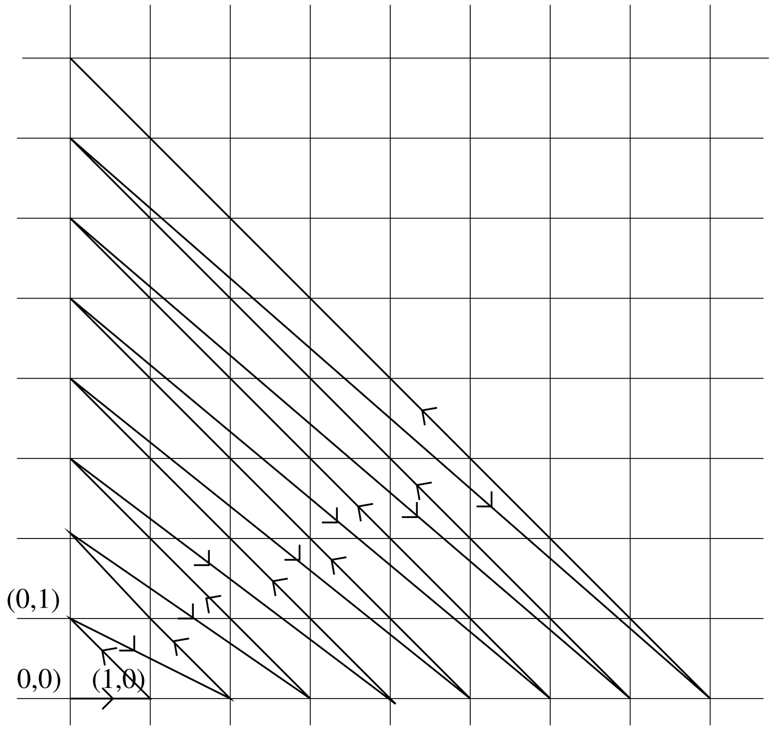

FIGURE 1. $\mathbb{N} \times \mathbb{N}$ est dénombrable

— en conséquence, $\mathbb{Z}^2$ est dénombrable, et de même pour $\mathbb{Z}^n$ pour tout $n \geq 1$.
— Il suit que $\mathbb{Q}$ est dénombrable, en effet on a une application surjective d'un sous-ensemble dénombrable de $\mathbb{Z}^2$ dans $\mathbb{Q}$, l'application qui à (p, q) associe p/q, définie pour $q \neq 0$.

Plus généralement :
— La réunion de deux ensembles dénombrables est dénombrable, car si $E = \{e_1, e_2, \cdots\}$ et $F = \{f_1, f_2, \cdots\}$, alors $E \cup F = \{e_1, f_1, e_2, f_2, \cdots\}$.
— Toute réunion dénombrable d'ensembles dénombrables est dénombrable : si $E_1, E_2, \cdots, E_n, \cdots$ sont des ensembles dénombrables, alors leur réunion

$$\cup_{n \in \mathbb{N}} E_i$$

est encore dénombrable.
— Si E et F sont dénombrables, alors $E \times F$ est dénombrable.

Le théorème suivant assure de l'existence d'un grand nombre de cardinaux infinis distincts.

THÉORÈME 4.8. *Soit E un ensemble, alors le cardinal de $\#\mathcal{P}(E)$ est strictement plus grand que celui de E, c'est-à-dire qu'il est plus grand et pas égal.*

IDÉE DE LA PREUVE. La preuve repose sur l'*argument diagonal de Cantor*. On considère une application $\phi : E \to \mathcal{P}(E)$, et on va montrer qu'elle ne peut pas être surjective. Pour cela, on définit un sous-ensemble $F \subset E$ comme suit : pour tout $e \in E$, $e \in F$ si et seulement si $e \notin \phi(e)$. On remarque alors que pour tout $e \in E, F \neq \phi(e)$, ce qui montre bien que ϕ n'est pas surjective. $\square$

Par exemple, l'ensemble des parties de $\mathbb{N}$ n'est pas dénombrable.

Proposition 4.9. *L'ensemble* $[0,1]$ *a même cardinal que* $\mathcal{P}(\mathbb{N})$.

Schéma de la preuve. On peut associer à tout élément $E \subset \mathbb{N}$ un nombre réel $r(E)$ qu'on définit par son écrire en base 2 comme suit : $r(E) = 0, r_1 r_2 \cdots$ avec $r_i \in \{0,1\}$ et $r_i = 1$ si et seulement si $i \in E$. On note que cette application est surjective. Elle n'est pas injective, car certains nombres ont deux écritures différentes en base 2, par exemple :

$$0,01 = 0,0100000000\cdots = 0,0011111111111\cdots$$

Mais ces nombres qui ont deux images réciproques par r forment un ensemble dénombrable. □

On peut en déduire que $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Ceci conduit naturellement à la question suivante, posée dès 1878 par Cantor.

Question 4.10 (Hypothèse du continu). *Est-il vrai que* $|\mathbb{R}|$ *est le plus petit cardinal strictement supérieur à* $|\mathbb{N}|$*, c'est-à-dire que tout ensemble infini non dénombrable a un cardinal au moins égal à celui de* $\mathbb{R}$ *?*

La réponse n'a été donnée qu'en 1963 par Paul Cohen : cet énoncé est *indécidable* dans le cadre de la théorie des ensembles usuelles, c'est-à-dire qu'on ne peut ni le démontrer, ni démontrer qu'il est faux.

5. Exercices

5.1. △ Valeurs de vérité. Quelles sont les propositions vraies parmi les suivantes ?

(1) $\emptyset \in \{\emptyset, \{\emptyset\}\}$.
(2) $\emptyset \subset \{\emptyset, \{\emptyset\}\}$.
(3) $4 \in \{\{4\}\}$.
(4) $\forall x \in \mathbb{Z} : (x \neq x^2)$.
(5) $(x \in A \wedge \neg(x \in B)) \Rightarrow x \in A \cap B$.
(6) $\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : \sqrt{x} - y = x$.

5.2. △ Définition d'un ensemble.

(1) Définir en énumération l'ensemble des nombres pairs compris entre 3 et 9.
(2) Définir en énumération l'ensemble $\{x \in \mathbb{N} \setminus \{0\} \mid \exists k \in \mathbb{Z} : x = 2k\}$.
(3) Définir en compréhension l'ensemble $\{2, 4, 8, 16, 32, 64, 128, ...\}$.
(4) Définir en compréhension l'ensemble $\{-2, -1, 0, 1, 2\}$.

5.3. Prédicats.

(1) Formuler les assertions suivantes en utilisants variables, connecteurs logiques et quantificateurs :
   (a) Personne n'est parfait.
   (b) Les absents n'on pas tous tort.
   (c) Tout nombre entier est un nombre réel.
(2) Ecrire la négation des assertions suivantes :
   (a) $\forall x, p(x) \Rightarrow q(x)$.
   (b) $\exists x, p(x) \wedge q(x)$.
   (c) $\exists x, \forall y : p(x,y) \Rightarrow q(x,y) \vee r(x,y)$.

(d) $\forall x > 0 \exists y((y > 0 \vee y = 1) \Rightarrow x + x < y)$.

(e) $\exists x \forall y(x + x = y \Rightarrow \forall z(z + y = x)) \Rightarrow \exists z \forall y(z \leq y)$.

(3) * Définir le quantificateur $\exists!$ à partir des autres quantificateurs et des opérations logiques.

(4) En utilisant uniquement le symbole $=$, les quantificateurs et les opérations logiques, écrire une assertion qui stipule que :

(a) un ensemble possède au moins trois éléments,

(b) un ensemble possède strictement moins de trois éléments,

(c) un ensemble possède exactement trois éléments.

5.4. Egalité, inclusion, opérations, cardinalité.

(1) On considère les ensembles suivants :

$$A = \{1, 2, 5\},\ B = \{\{1, 2\}, 5\},\ C = \{\{1, 2, 5\}\},\ D = \{\emptyset, 1, 2, 5\},$$
$$E = \{5, 1, 2\},\ F = \{\{1, 2\}, \{5\}\},\ G = \{\{1, 2\}, \{5\}, 5\},\ H = \{5, \{1\}, \{2\}\}.$$

(a) Quelles sont les relations d'égalité ou d'inclusion existantes entre ces ensembles ?

(b) Déterminer la cardinalité de chacun de ces ensembles.

(c) Déterminer $A \cap B$, $G \cup H$ et $E \setminus G$.

(2) On considère maintenant les quatres sous-ensembles de $\mathbb{N}$ suivants :

$$I = \{1, 2, 3, 4, 5, 6, 7\},\ J = \{1, 3, 5, 7\},\ K = \{2, 4, 6\}.$$

(a) Déterminer $\bar{J}^I$ et $\bar{K}^I$.

(b) On appelle différence symétrique de deux ensembles A et B, notée $A\Delta B$, l'ensemble constitué des éléments qui sont soit dans A, soit dans B, mais pas dans $A \cap B$. Déterminer $I\Delta J$ et $J\Delta K$.

5.5. Ensemble des parties. Donner les éléments de :

(1) $\mathcal{P}(\{0, 1, 2\})$.

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

(3) $\mathcal{P}(\mathcal{P}(\{1, 2\}))$.

5.6. Relations.

(1) Soient $E = F = \mathbb{R}$ et $R = \{(x, y) \in E \times F \,|\, x^2 + y^2 \leq 1\}$. Déterminer le domaine de définition de R.

(2) Soient f l'application de $\mathbb{N}$ dans $\mathbb{Z}$ définie par $f(n) = n^3$ et g l'application de $\mathbb{Z}$ dans $\mathbb{N}$ définie par $g(n) = n^2$. Calculer l'image de 2 par f et déterminer $f \circ g$.

(3) Soient f l'application de $E = \{1, 2, 3, 4\}$ dans $F = \{0, 1, 3, 5, 7, 10\}$ telle que $f(1) = 3, f(2) = 5, f(3) = 5$ et $f(4) = 0$. Déterminer $f^{-1}(\{5\})$, $f^{-1}(\{0, 1, 3\})$ et $f^{-1}(\{1, 10\})$. f est-elle injective, surjective, bijective ?

(4) Donner des exemples d'applications de $\mathbb{N}$ dans $\mathbb{N}$:

(a) bijective (autre que $id_{\mathbb{N}}$).

(b) injective mais pas surjective.

(c) surjective mais pas injective.

(5) * On considère la fonction

$$f:\mathbb{R}\to\mathbb{R}:x\mapsto\begin{cases}|x+1| \text{ si } x<0\\ |x-1| \text{ si } x\geq 0.\end{cases}$$

(a) La fonction f est-elle une bijection ?

(b) Déterminer une restriction g de f telle que g soit inversible.

(c) Déterminer l'inverse de g.

(6) Soit E un ensemble non vide et A et B deux parties de E.

(a) On définit

$$f:2^E\to 2^E:X\mapsto (A\cap X)\cup(B\cap\bar{X}).$$

Discuter et résoudre l'équation $f(X)=\emptyset$. En déduire une condition nécessaire pour que f soit bijective.

(b) On considère $B=\bar{A}$ dans la définition précédente. Dans ce cas, prouver que $f\circ f=\mathrm{id}$. En déduire que f est bijective.

5.7. * Démonstrations. Soient A, B, et C trois sous-ensembles.

(1) Montrer que si $A\subset B$ et $C\subset D$ alors $A\cap C\subset B\cap D$ et $A\cup C\subset B\cup D$.

(2) Montrer que $A\subset B\cap C$ si et seulement si $A\subset B$ et $A\subset C$.

(3) Montrer que $(A\setminus B)\setminus C=A\setminus(B\cup C)$.

(4) Montrer que la composée de deux applications injectives est injective.

(5) Montrer que si f est une application bijective de E sur F et g une application bijective de F sur G alors $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

5.8. Applications croissantes.

(1) Soit $I\subset\mathbb{R}$ et $J\subset\mathbb{R}$ deux intervalles de $\mathbb{R}$. Soit $f:I\longrightarrow J$ une fonction strictement croissante.

(a) Montrer que f est injective.
Indication : On pourra montrer la contraposée et on rappelle que $x_1\neq x_2$ équivant à $x_1<x_2$ ou $x_2<x_1$.

(b) Déterminer l'ensemble K tel que $f:I\longrightarrow K$ soit bijective.

Application de $\mathbb{N}$ dans $\mathbb{N}$. On considère une application $u:\mathbb{N}\to\mathbb{N}$ dont on suppose que

$$\forall k\in\mathbb{N}, u(k+1)>u(k)\ .$$

(1) Montrer rigoureusement, en justifiant chaque étape de votre raisonnement, que pour tout $k,l\in\mathbb{N}$ avec $k<l$, on a $u(k)<u(l)$.

(2) u est-elle nécessairement injective ? On justifiera la réponse par un argument précis ou par un contre-exemple.

(3) u est-elle nécessairement surjective ? On justifiera la réponse par un argument précis ou par un contre-exemple.

Bibliographie

[1] Apostolos Doxiadis and Christos H. Papadimitriou. *Logicomix*. Bloomsbury Press, New York, 2009. An epic search for truth, Character design and drawings by Alecos Papadatos, color by Annie Di Donna.

[2] Alfred Tarski. *Introduction to logic and to the methodology of deductive sciences*. Dover Publications, Inc., New York, 1995. Translated from the 1936 Polish original by Olaf Helmer, Reprint of the 1946 translation.