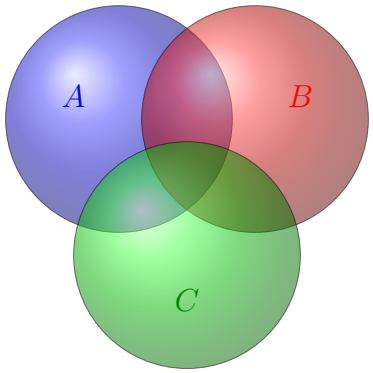
Fondements des mathématiques

MAT 2762

Automne 2014



Alistair Savage

Département de Mathématiques et de Statistique

Université d'Ottawa

Table des matières

Préface

Ce sont les notes pour le cours *Fondements des mathématiques* (MAT 2762) à l'Université d'Ottawa. C'est un cours pour les étudiants spécialisés en mathématiques. Il donne une introduction à la notion de preuves, la théorie des ensembles et les fondements des mathématiques. On commence avec la logique propositionnelle et les techniques de preuves. Puis on discute la théorie informelle des ensembles (fonctions, relations d'équivalence, relations d'ordre). On voit que cette théorie mène à des paradoxes. Pour résoudre ces paradoxes, on développe la théorie axiomatique des ensembles. Cela inclus l'Axiome du Choix, et le Lemme de Zorn. On conclut le cours avec la cardinalité des ensembles.

Remerciements : Chapitres 1, 2 et 9 sont des adaptations des notes de Daniel Daigle (avec seulement quelques petites changements). Chapitres 3 à 8 sont basées sur les notes [Nes] de Ali Nesin avec quelques parties aussi basées sur les notes de Daniel Daigle.

Alistair Savage Ottawa, 2014.

Site web du cours : `http://mysite.science.uottawa.ca/asavag2/mat2762/`

Chapitre 1

Logique propositionnelle

Dans ce chapitre, on présent la logique propositionnelle, incluant les propositions, les connecteurs, l'équivalence, et certaines méthodes de preuve.

1.1 Les propositions

Une *proposition* est une phrase qui est soit vraie, soit fausse.

Exemple 1.1.1.

(a) "La maison est blanche" est une proposition puisque cette phrase est soit vraie, soit fausse.

(b) L'expression mathématique "$7 - 4 = 3$" est une proposition, car c'est une affirmation qui est soit vraie, soit fausse (dans ce cas, c'est une proposition vraie).

(c) "$3^2 - 4 = 1$" est une proposition, parce que c'est une phrase qui est soit vraie, soit fausse (en fait c'est fausse).

(d) L'expression mathématique "$3^2 - 4$" n'est pas une proposition. En fait, "$3^2 - 4$" est le nombre 5, qui n'est ni vrai ni faux.

Les mots *proposition*, *affirmation*, et *assertion* veulent dire la même chose.

Lorsqu'une proposition est vraie, on dit que sa *valeur de vérité* est **V** (pour "vraie"). Lorsqu'elle est fausse, on dit que sa valeur de vérité est **F** (pour "fausse").

Souvent, on représent les propositions par des lettres. Par exemple, on peut écrire :

$$\begin{aligned} X &= \text{"le nombre 7 est pair"}, \\ Y &= \text{"le nombre 5 est impair"}, \\ Z &= \text{"}\sqrt{80} < 9\text{"}. \end{aligned}$$

Alors la proposition X est fausse, Y est vraie et Z est vraie. Autrement dit, les valeurs de vérités des propositions X, Y et Z sont **F**, **V** et **V** respectivement.

1.2 Les cinq connecteurs logiques

Un *connecteur logique* est un symbole ou un mot qui connecte une ou plusieurs propositions tel que le sens de la nouvelle phrase ne dépend que des propositions originales. Il y a cinq connecteurs logiques qu'on va utiliser dans ce cours.

1.2.1 Connecteur de conjonction ($\wedge$)

Le symbole $\wedge$ veut dire "et" et la formule $X \wedge Y$ se lit "X et Y". Ce connecteur s'appelle le *connecteur de conjonction*.

Si X et Y sont des propositions, la formule $X \wedge Y$ est une autre proposition. La valeur de vérité de $X \wedge Y$ est **V** si et seulement si les valeurs de vérité de X et Y sont toutes deux **V**.

On peut définer précisément le sens d'un connecteur avec un *table de verité*.

X	Y	$X \wedge Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**F**

Exemple 1.2.1. (a) La proposition "4 est impair et 2 est un nombre entier" est fausse, car cette phrase est

$$(4 \text{ est impair}) \wedge (2 \text{ est un nombre entier}) = \mathbf{F} \wedge \mathbf{V} = \mathbf{F}$$

(on a utilisé la troisième ligne de la table ci-dessus).

(b) La phrase "3 est impair et 4 est pair" est vraie, parce que cette phrase est

$$(3 \text{ est impair}) \wedge (4 \text{ est pair}) = \mathbf{V} \wedge \mathbf{V} = \mathbf{V}$$

(la premiére ligne de la table ci-dessus).

1.2.2 Connecteur de disjonction ($\vee$)

Le symbole $\vee$ veut dire "ou" et la formule $X \vee Y$ se lit "X ou Y". Ce connecteur s'appelle le *connecteur de disjonction*.

La proposition $X \vee Y$ est vraie si et seulement si X ou Y (ou les deux) sont vraie.

X	Y	$X \vee Y$
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

Exemple 1.2.2. (a) La phrase "3 est pair ou -2 est négatif" est vraie, car cette phrase est

$$(3 \text{ est pair}) \vee (-2 \text{ est négatif}) = \mathbf{F} \vee \mathbf{V} = \mathbf{V}$$

(on utilise la troisième ligne de la table ci-dessus).

(b) La phrase "3 est pair ou -2 est positif" est fausse, car cette phrase est

$$(3 \text{ est impair}) \vee (-2 \text{ est positif}) = \mathbf{F} \vee \mathbf{F} = \mathbf{F}$$

(on utilise la quatrième ligne).

1.2.3 Connecteur de négation ($\neg$)

La formule $\neg X$ se lit "non X". Ce connecteur s'appelle le *connecteur de négation*.

X	$\neg X$
V	**F**
F	**V**

Lorsqu'on veut remplacer une formule $\neg X$ par une phrase française on dit souvent "il est faux que X" au lieu de "non X".

Exemple 1.2.3. (a) Soit X la proposition "3 est impair". Donc $\neg X$ est la proposition "il est faux que 3 est impair". Par conséquent X est **V** et $\neg X$ est **F**.

(b) Soit Y la proposition "tout entier impair est divisible par 3". Donc $\neg Y$ est la proposition "il est faux que tout entier est divisible par 3". Dan ce cas, Y est **F** et $\neg Y$ est **V**.

1.2.4 Connecteur d'implication ($\Rightarrow$)

La formule $X \Rightarrow Y$ est appelée une *implication* ; elle se lit "X implique Y", ou encore "si X alors Y". On dit que X est l'*hypothèse* de cette implication et que Y est la *conclusion*. L'implication est définie par :

X	Y	$X \Rightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

Important :

- L'implication est vraie à chaque fois que l'hypothèse est fausse.
- L'implication est vraie à chaque fois que la conclusion est vraie.
- **Le seul cas où l'implication est fausse est celui où l'hypothèse est vraie et la conclusion est fausse.**

Exemple 1.2.4. Si ton ami dit :

"Si je suis à Ottawa, je viendrai à ta fête ce fin de semaine."

Supposons qu'il n'est pas à Ottawa et qu'il ne vient pas a ta fête. Alors peux-tu l'accuser d'avoir menti ?

Intuitivement, on pense qu'il n'a pas menti, puisqu'il n'avait rien promis du tout dans le cas où il ne serait pas à Ottawa. Donc notre intuition nous dit que la phrase qu'il a dit est vraie (sinon il aurait menti). Cette intuition est en accord avec la table de vérité, puisque la phrase prononcée est une implication du type ($\mathbf{F} \Rightarrow \mathbf{F}$), qui est $\mathbf{V}$ selon la table.

Exemple 1.2.5. Qu'est-ce que c'est la valeur de vérité des phrases suivantes ?

(a) "Si $3 > 4$ alors 3 est pair"

On simplifie la proposition, étape par étape.

$$(3 > 4) \Rightarrow (3 \text{ est pair})$$
$$\mathbf{F} \Rightarrow \mathbf{F}$$
$$\mathbf{V}$$

Donc, la proposition est $\mathbf{V}$.

(b)

$$\text{Si } 3^3 = 26 \text{ alors } 1 + 2 = 3$$
$$(3^3 = 26) \Rightarrow (1 + 2 = 3)$$
$$\mathbf{F} \Rightarrow \mathbf{V}$$
$$\mathbf{F}$$

(c)

$$\text{Si } 5 - 4 = 1 \text{ alors } 2^3 = 8$$
$$(5 - 4 = 1) \Rightarrow (2^3 = 8)$$
$$\mathbf{V} \Rightarrow \mathbf{V}$$
$$\mathbf{V}$$

Exemple 1.2.6. Montrons que l'implication $x < -2 \Rightarrow x^2 > 4$ est vraie **pour tout** $x \in \mathbb{Z}$.

Pour chaque entier x, on doit montrer que l'implication est vraie. Donc, si on veut, on peut diviser en deux cas. Si $x \in \mathbb{Z}$ alors x satisfait $x \geq -2$ ou $x < -2$.

- Dans le premier cas ($x \geq -2$), on a une implication avec hypothèse $\mathbf{F}$, donc l'implication est $\mathbf{V}$ (la valeur de vérité de la conclusion ne fait rien).
- Dans le deuxième cas ($x < -2$), on a $x^2 > 4$, donc on a une implication avec conclusion $\mathbf{V}$, donc l'implication est $\mathbf{V}$.

Ainsi, l'implication est $\mathbf{V}$ pour tout $x \in \mathbb{Z}$.

1.2.5 Le connecteur biconditionnel ($\Leftrightarrow$)

Le formule $X \Leftrightarrow Y$ se lit "X si et seulement si Y". Ce connecteur s'appelle le *connecteur biconditionnel*.

X	Y	$X \Leftrightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

Important :

- La formule $X \Leftrightarrow Y$ est vraie lorsque X et Y ont la même valeur de vérité (ce qui signifie que X et Y sont toutes les deux **V** ou toutes les deux **F**).
- La formule $X \Leftrightarrow Y$ est fausse lorsque X et Y ont des valeurs de vérité différentes.

Nous verrons plus tard que la formule $X \Leftrightarrow Y$ est équivalente à $(X \Rightarrow Y) \wedge (Y \Rightarrow X)$.

1.2.6 Formules complexes ou atomiques

Une formule logique qui contient au moins un connecteur est appelée une *formule complexe*, ou encore une *formule composée*. Une formule qui n'a aucun connecteur est appelée une *formule atomique* ou, plus simplement, un *atome*. Par exemple, X est une formule atomique et $\neg X$ est une formule complexe. On considère aussi que les symboles **V** et **F** sont des formules atomiques. La formule $X \wedge \mathbf{F}$ est complexe.

1.2.7 Connecteur principal

Considérons la formule $(X \wedge Z) \Rightarrow \neg Y$. On dit que $\Rightarrow$ est le *connecteur principal* de cette formule. On entend par là que $(X \wedge Z) \Rightarrow \neg Y$ est une implication : son hypothèse est $(X \wedge Z)$ est sa conclusion est $\neg Y$. Autrement dit, $(X \wedge Z) \Rightarrow \neg Y$ est une formule du type $\varphi \Rightarrow \psi$. Les formules $(X \wedge Z)$ est $\neg Y$ sont appelées les *composantes immédiates* de la formule.

La relation entre le connecteur principal est les composantes immédiates est un peux comme l'ordre des opérations pour l'arithmétique. L'operation qu'on fait premièrement est le connecteur principal.

Chaque formule complexe possède **exactement un** connecteur principal, et ce connecteur détermine soit une, soit deux composantes immédiates (dans le cas de $\neg$ il n'y a qu'une composante, dans les autres cas il y en a deux).

Exemple 1.2.7.

	formule	connecteur principal	composantes immédiates	
1	$(X \wedge Z) \Leftrightarrow \neg Y$	$\Leftrightarrow$	$(X \wedge Z)$	$\neg Y$
2	$X \wedge (Y \Rightarrow Z)$	$\wedge$	X	$(Y \Rightarrow Z)$
3	$(X \wedge Y) \Rightarrow Z$	$\Rightarrow$	$(X \wedge Y)$	Z
4	$\neg(X \Leftrightarrow (X \vee Y))$	$\neg$	$(X \Leftrightarrow (X \vee Y))$	

1.2.8 Tables de vérités

Si $X = \mathbf{F}$, $Y = \mathbf{V}$ et $Z = \mathbf{V}$, quelle est la valeur de vérité de la formule $\neg(X \wedge Y) \Leftrightarrow (Y \vee Z)$?

$$\begin{gathered}\neg(X \wedge Y) \Leftrightarrow (Y \vee Z)\\ \neg(\mathbf{F} \wedge \mathbf{V}) \Leftrightarrow (\mathbf{V} \vee \mathbf{V})\\ \neg\mathbf{F} \Leftrightarrow \mathbf{V}\\ \mathbf{V} \Leftrightarrow \mathbf{V}\\ \mathbf{V}\end{gathered}$$

Ainsi, lorsque $(X, Y, Z) = (\mathbf{F}, \mathbf{V}, \mathbf{V})$, la formule $\neg(X \wedge Y) \Leftrightarrow (Y \vee Z)$ est $\mathbf{V}$. On peut calculer la valeur de vérité de cette formule pour tous les valeurs de vérité de X, Y et Z et on obtiendrait la table suivante :

X	Y	Z	$\neg(X \wedge Y) \Leftrightarrow (Y \vee Z)$
V	**V**	**V**	**F**
V	**V**	**F**	**F**
V	**F**	**V**	**V**
V	**F**	**F**	**F**
F	**V**	**V**	**V**
F	**V**	**F**	**V**
F	**F**	**V**	**V**
F	**F**	**F**	**F**

La table ci-dessus est la *table de vérité* de $\neg(X \wedge Y) \Leftrightarrow (Y \vee Z)$. Toute formule a une table de vérité.

Exercices.

1.2.1. Répondez par **V** ou **F**.

(a) $3 + 4 = 7$ ou $2 \times 4 = 9$.

(b) $3 - 2 = 1$ et $3^2 = 9$.

(c) Il est faux que $2^3 = 8$.

(d) Si $3 - 5 = 1$ alors $1 + 1 = 3$.

(e) Si ($23^{354} + 2$ est un entier si et seulement si $2 \times 3 = 6$), alors $3 - 4 = -1$.

(f) Il est faux que ((si $3 + 5 = 7$ alors π est un entier) ou ($1 + 4 = 5$ si et seulement si $3 \times 5 = 15$)).

(g) Si $23^{341} + 3$ est divisible par 7 alors $2 + 3 = 5$. (*Indice :* Est-ce on doit savoir si $23^{341} + 3$ est divisible par 7 ou non ?)

(h) ($23^{341}+3$ est divisible par 7 et $1+1=3$) si et seulement si ($23^{341}+3$ est divisible par 7 ou $1+1=2$).

1.2.2. Calculez la table de vérité de la formule $(X \vee Z) \Rightarrow (X \wedge \neg Z)$.

1.3 Équivalence de formules

1.3.1 Équivalence

Définition 1.3.1. Deux formules sont *équivalentes* si elles ont la même table de vérité. Pour indiquer que des formules φ et ψ sont équivalentes, on écrit $\varphi \equiv \psi$.

Exemple 1.3.2. Les formules $X \Rightarrow Y$ et $\neg X \vee Y$ ont la même table de vérité :

X	Y	$X \Rightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

X	Y	$\neg X \vee Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

donc les deux formules sont équivalentes : $X \Rightarrow Y \equiv \neg X \vee Y$.

Exemple 1.3.3. Les tables

X	Y	$X \Rightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**F**

X	Y	$X \Leftrightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

ne sont pas identique. Donc, les formules $X \Rightarrow Y$ et $X \Leftrightarrow Y$ ne sont pas équivalentes : $X \Rightarrow Y \not\equiv X \Leftrightarrow Y$.

Exemple 1.3.4. Les tables

X	$\neg\neg X$
V	**V**
F	**F**

X	X
V	**V**
F	**F**

montrent que $\neg\neg X \equiv X$.

Exemple 1.3.5. Les tables

X	Y	$X \Leftrightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

X	Y	$(X \Rightarrow Y) \wedge (Y \Rightarrow X)$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

montrent que $X \Leftrightarrow Y \equiv (X \Rightarrow Y) \wedge (Y \Rightarrow X)$.

Exemple 1.3.6. Les tables

X	Y	$X \vee (Y \wedge \neg Y)$
V	**V**	**V**
V	**F**	**V**
F	**V**	**F**
F	**F**	**F**

X	Y	X
V	**V**	**V**
V	**F**	**V**
F	**V**	**F**
F	**F**	**F**

montrent que $X \vee (Y \wedge \neg Y) \equiv X$.

Voici maintenant une liste d'équivalences très utiles.

	Équivalence	Nom ou commentaire
(1)	$P \Rightarrow Q \equiv \neg P \vee Q$	
(3)	$P \Leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$	
(4)	$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$	
(5)	$P \vee \neg P \equiv \mathbf{V}$	Tiers exclu
(6)	$P \wedge \neg P \equiv \mathbf{F}$	Contradiction
(7)	$P \vee \mathbf{F} \equiv P$	**F** est neutre pour $\vee$
(8)	$P \wedge \mathbf{V} \equiv P$	**V** est neutre pour $\wedge$
(9)	$P \vee \mathbf{V} \equiv \mathbf{V}$	**V** est "absorbant" pour $\vee$
(10)	$P \wedge \mathbf{F} \equiv \mathbf{F}$	**F** est "absorbant" pour $\wedge$
(11)	$P \vee P \equiv P$	Idempotence
(12)	$P \wedge P \equiv P$	Idempotence
(13)	$\neg\neg P \equiv P$	Double négation
(14)	$P \vee Q \equiv Q \vee P$	Commutativité de $\vee$
(15)	$P \wedge Q \equiv Q \wedge P$	Commutativité de $\wedge$
(16)	$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$	Associativité de $\vee$
(17)	$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$	Associativité de $\wedge$
(18)	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	Distributivité de $\vee$ sur $\wedge$
(19)	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	Distributivité de $\wedge$ sur $\vee$
(20)	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	Loi de De Morgan
(21)	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	Loi de De Morgan

TABLE 1.1 – Liste d'équivalences très utiles

1.3.2 Preuves par manipulations algébriques

Nous allons maintenant utiliser une nouvelle méthode pour démontrer des équivalences de formules $\varphi \equiv \psi$. Au lieu de vérifier que les deux formules ont la même table de vérité on va plutôt procéder par "manipulations algébriques", en utilisant des équivalences du tableau ci-dessus.

Exemple 1.3.7. Montrons que $X \Rightarrow (X \Rightarrow Y) \equiv X \Rightarrow Y$:

$$\begin{aligned} X \Rightarrow (X \Rightarrow Y) &\overset{(1)}{\equiv} X \Rightarrow (\neg X \vee Y) \\ &\overset{(1)}{\equiv} \neg X \vee (\neg X \vee Y) \\ &\overset{(16)}{\equiv} (\neg X \vee \neg X) \vee Y \\ &\overset{(11)}{\equiv} \neg X \vee Y \\ &\overset{(1)}{\equiv} X \Rightarrow Y \end{aligned}$$

Exemple 1.3.8. Montrons que $X \vee (\neg X \wedge Y) \equiv X \vee Y$:

$$\begin{aligned} X \vee (\neg X \wedge Y) &\overset{(18)}{\equiv} (X \vee \neg X) \wedge (X \vee Y) \\ &\overset{(5)}{\equiv} \mathbf{V} \wedge (X \vee Y) \\ &\overset{(15)}{\equiv} (X \vee Y) \wedge \mathbf{V} \\ &\overset{(8)}{\equiv} X \vee Y \end{aligned}$$

Les équivalences de formules sont parfois utiles pour travailler avec des phrases écrites en français.

Exemple 1.3.9. Cherchons la négation de la phrase

"f est discontinue ou $f(1) \geq 0$".

On écrit une formule pour la négation et utilise la loi de De Morgan :

$$\begin{aligned} \neg((f \text{ est discontinue}) \vee (f(1) \geq 0)) &\overset{(21)}{\equiv} \neg(f \text{ est discontinue}) \wedge \neg(f(1) \geq 0) \\ &= (f \text{ est continue}) \wedge (f(1) < 0) \end{aligned}$$

donc la bonne réponse est "f est continue et $f(1) < 0$".

Exercices.

1.3.1. Chacun des équivalences de Table 1.1 peut être prouvée en utilisant les tables de vérité, comme dans les exemples qu'on a vus. Par exemple, prouvez la distributivité de $\vee$ sur $\wedge$.

1.3.2. Quelle est la négation de la phrase "$x \neq 2$ et $y = 1$" ?

1.4 Contraposée et réciproque d'une implication

Définition 1.4.1. La *contraposée* de $(X \Rightarrow Y)$ est $(\neg Y \Rightarrow \neg X)$. La *réciproque* de $(X \Rightarrow Y)$ est $(Y \Rightarrow X)$.

Comparons les tables de vérité de trois formules $X \Rightarrow Y$, $\neg Y \Rightarrow \neg X$ et $Y \Rightarrow X$:

X	Y	$X \Rightarrow Y$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

Contraposée de $X \Rightarrow Y$

X	Y	$\neg Y \Rightarrow \neg X$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

Réciproque de $X \Rightarrow Y$

X	Y	$Y \Rightarrow X$
V	**V**	**V**
V	**F**	**V**
F	**V**	**F**
F	**F**	**V**

Ces tables de vérité montrent que :

Une implication est équivalente à sa contraposée mais pas à sa réciproque.

Exemple 1.4.2. Les deux phrases :

(i) *Si un nombre est divisible par 6, il est divisible par 3.*

(ii) *Si un nombre n'est pas divisible par 3, il n'est pas divisible par 6.*

sont deux manières de dire la même chose. Ceci illustre le fait qu'une implication est équivalente à sa contraposée (chacune des phrases est la contraposée de l'autre). Comparez ensuite les deux phrases suivantes :

(i) *Si un nombre est divisible par 6, il est divisible par 3.*

(iii) *Si un nombre est divisible par 3, il est divisible par 6.*

Remarquez que (iii) est la réciproque de (i). Ces deux phrases ne disent pas la même chose ; en fait, (i) est **V** et (iii) est **F**.

Exercices.

1.4.1. Pour chacune des implications suivantes, donnez (i) la contraposée et (ii) la réciproque.

(a) Si x est pair alors xy est pair.

(b) Si $a < 0$ alors $a^2 > 0$. *Remarque :* la négation de $x > 0$ est $x \leq 0$.

(c) Si n est un multiple de 20 alors il est un multiple de 4.

(d) Si la matrice A est inversible, alors ses lignes sont linéairement indépendants.

(e) Si deux entiers sont pairs, alors leur somme est paire.

(f) Si une fonction est dérivable en $x = 2/3$, alors elle est continue en $x = 2/3$.

(g) Si la série $\sum_{n=1}^{\infty} a_n$ converge, alors la suite $\{a_n\}_{n=1}^{\infty}$ converge est sa limite est 0.

(h) Si les fonctions f et g sont continues, alors la fonction $f - g$ est continue.

1.5 Omission de parenthèses

Pourquoi l'expression $9 \div 3 \div 3$ est-elle ambiguë, tandis que $9 + 3 + 3$ ne l'est pas ?

L'ambiguïté de $9 \div 3 \div 3$ vient du fait que cette expression peut être interprétée de deux manières :

- $(9 \div 3) \div 3 = 3 \div 3 = 1$
- $9 \div (3 \div 3) = 9 \div 1 = 9$

Donc on ne sait pas si $9 \div 3 \div 3$ est égal à 1 ou à 9.

Dans le cas de $9 + 3 + 3$, les deux interprétations donnent la même résultat :

- $(9 + 3) + 3 = 12 + 3 = 15$
- $9 + (3 + 3) = 9 + 6 = 15$

Donc on sait que $9 + 3 + 3$ est égal à 15 et il n'y a pas d'ambiguïté.

En résumé, il est permis d'écrire $9 + 3 + 3$ sans parenthèses parce que l'addition est une opération associative :

$$(a + b) + c = a + (b + c) \text{ quels que soient } a, b, c.$$

Mais la division n'est pas associative, donc on doit écrire soit $(9 \div 3) \div 3$ soit $9 \div (3 \div 3)$.

Le connecteur $\wedge$ est associatif parce que

$$(X \wedge Y) \wedge Z \equiv X \wedge (Y \wedge Z).$$

Ceci nous donne le droit d'écrire $X \wedge Y \wedge Z$ sans parenthèses. On peut aussi écrire $X_1 \wedge X_2 \wedge X_3 \wedge \cdots \wedge X_n$ sans parenthèses parce que toutes les formules qu'on peut obtenir par l'insertion des parenthèses sont équivalentes.

Les connecteurs $\vee$ et $\Leftrightarrow$ sont eux aussi associatifs, donc on peut écrire des formules comme

- $X \vee Y \vee Z$
- $X \Leftrightarrow Y \Leftrightarrow Z$
- $X \vee (Y \Rightarrow Z) \vee Z \vee (X \wedge Z)$
- $(X \wedge Y) \Leftrightarrow Z \Leftrightarrow (X \Rightarrow Y) \Leftrightarrow (X \vee Y)$

sans parenthèses supplémentaires.

Par contre, $(X \Rightarrow Y) \Rightarrow Z \not\equiv X \Rightarrow (Y \Rightarrow Z)$ (considère $X = \mathbf{F}$, $Y = \mathbf{V}$, $Z = \mathbf{F}$), donc $\Rightarrow$ n'est pas associatif et les parenthèses sont obligatoires : il n'est pas permis d'écrire $X \Rightarrow Y \Rightarrow Z$.

Remarquez aussi que la formule $X \vee Y \wedge Z$ n'est pas "légale" : il faut écrire soit $(X \vee Y) \wedge Z$, soit $X \vee (Y \wedge Z)$ (considère $X = \mathbf{V}$, $Y = \mathbf{F}$, $Z = \mathbf{F}$).

On adopte la convention suivante, qui nous permet d'omettre certaines parenthèses :

Le connecteur de négation $\neg$ a un niveau de priorité plus élevé que les autres connecteurs.

Par exemple, $\neg X \vee Y$ signifie $(\neg X) \vee Y$ et non $\neg(X \vee Y)$. Remarquez qu'on a déjà utilisé cette convention sans le dire : par exemple lorsqu'on a dit que la contraposée de $X \Rightarrow Y$ est $\neg Y \Rightarrow \neg X$, on n'a pas eu besoin d'écrire $(\neg Y) \Rightarrow (\neg X)$.

1.6 Tautologies et contradictions

Définition 1.6.1.

- Une *tautologie* est une formule dont la table de vérité ne contient que des "**V**" (c'est à dire, une formule qui est équivalent à **V**).
- Une *contradiction* est une formule dont la table de vérité ne contient que des "**F**" (c'est à dire, une formule qui est équivalent à **F**).

Remarquez que la plupart des formules ne sont ni des tautologies ni des contradictions.

Exemple 1.6.2. La table

X	Y	$(X \wedge Y) \Rightarrow (X \vee Y)$
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**V**

montre que $(X \wedge Y) \Rightarrow (X \vee Y)$ est une tautologie.

Exemple 1.6.3. La table

X	$X \vee \neg X$
V	**V**
F	**V**

montre que $X \vee \neg X$ est une tautologie.

Exemple 1.6.4. La table

X	$X \wedge \neg X$
V	**F**
F	**F**

montre que $X \vee \neg X$ est une contradiction.

Exemple 1.6.5. La formule **V** est une tautologie et la formule **F** est une contradiction.

Exemple 1.6.6. La formule $(X \Rightarrow Y) \vee (Y \Rightarrow X)$ est-il une tautologie ?

X	Y	$(X \Rightarrow Y) \vee (Y \Rightarrow X)$
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**V**

Donc la réponse et oui, la formule est une tautologie.

Exercices.

1.6.1. La formule $X \Rightarrow \neg X$ est-elle une contradiction ? (Ne répondez pas trop vite !)

1.6.2. À l'aide de tables de vérité, décidez si les formules suivantes sont des tautologies, contradictions, on ni l'une ni l'autre.

(a) $(X \wedge Y) \Leftrightarrow \neg(X \Rightarrow \neg Y)$

(b) $(X \vee Y) \Leftrightarrow \neg(X \Rightarrow \neg Y)$

(c) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)$

(d) $\neg(A \Rightarrow (B \vee C)) \Leftrightarrow ((A \Rightarrow B) \vee (A \Rightarrow C))$

1.7 Méthodes de preuve

1.7.1 Preuve de $P \Rightarrow Q$

On va voir deux techniques : la preuve directe et la preuve de la contraposée.

Preuve directe

On suppose que P est vraie et on en déduit que Q est vraie.

Assertion : $P \Rightarrow Q$
Preuve. Supposons que P est vraie.
⋮
Donc Q est vraie. □

Voici un exemple.

Proposition 1.7.1. *Soit $n, m \in \mathbb{Z}$. Si n est divisible par 2 et m est divisible par 3 alors nm est divisible par 6.*

Preuve. Supposons que n est divisible par 2 et m est divisible par 3. Donc, il y a $a, b \in \mathbb{Z}$ tels que $n = 2a$ et $m = 3b$. Par conséquent, $nm = (2a)(3b) = 6ab$ et $ab \in \mathbb{Z}$. Donc nm est divisible par 6. □

Preuve de la contraposée

Rappelez-vous que $P \Rightarrow Q$ est équivalente a sa contraposée $\neg Q \Rightarrow \neg P$. Donc si une est vraie alors l'autre l'est aussi. La *preuve de la contraposée* consiste à faire une preuve directe de l'implication $\neg Q \Rightarrow \neg P$.

Assertion : $P \Rightarrow Q$

Preuve. Supposons que $\neg Q$ est vraie.

$\vdots$

Donc $\neg P$ est vraie.

Ceci montre que $\neg Q \Rightarrow \neg P$ est vraie, donc $P \Rightarrow Q$ est vraie. □

Proposition 1.7.2. *Soit* $x \in \mathbb{R}$. *Si* $x^3 + 2x^2 + x < 4$ *alors* $x < 1$.

Preuve. La contraposée est

$$\textit{Si } x \geq 1, \textit{ alors } x^3 + 2x^2 + x \geq 4. \tag{1.1}$$

On fait une preuve directe de (1.1). Supposons que $x \geq 1$. Alors $x^3 \geq 1$ et $x^2 \geq 1$. Donc

$$x^3 + 2x^2 + x \geq 1 + 2(1) + 1 = 4.$$

Ceci démontre (1.1), donc la proposition est démontrée. □

1.7.2 Preuve de $P \Leftrightarrow Q$

Pour prouver $P \Leftrightarrow Q$ on doit prouver les deux implications $P \Rightarrow Q$ et $Q \Rightarrow P$.

1.7.3 Preuve par séparation des cas

Supposons qu'on sait que $P_1 \vee P_2$ est **V**. On peut démontrer (exercice !)

$$Q \equiv [(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)]. \tag{1.2}$$

Par conséquent, si on veut démontrer Q sachant que $P_1 \vee P_2$ est vraie, la méthode par séparation des cas consiste à faire deux preuves :

- on prouve que si P_1 est vraie, alors Q est vraie,
- on prouve que si P_2 est vraie, alors Q est vraie.

Assertion : Q

Preuve. On sait que $P_1 \vee P_2$ est vraie.

- Supposons que P_1 est vraie, alors ..., donc Q est vraie.
- Supposons que P_2 est vraie, alors ..., donc Q est vraie.

Donc Q est démontrée. □

Voici un exemple. On utilise le symbole $\mathbb{R}^+$ pour l'ensemble $\{x \in \mathbb{R} : x > 0\}$ des nombres réels positifs et $\mathbb{N}^+$ pour l'ensemble $\{n \in \mathbb{N} : n > 0\}$ des nombres entiers positifs.

Proposition 1.7.3. *Soit* $x \in \mathbb{R}^+$. *Alors* $x^2 + \frac{1}{x} > x$.

Preuve. Supposons que $x \in \mathbb{R}^+$. On sait que $x \geq 1$ ou $0 < x < 1$.

- Si $x \geq 1$ alors $x^2 \geq x$ et $\frac{1}{x} > 0$. Donc $x^2 + \frac{1}{x} > x$.
- Si $0 < x < 1$ alors $\frac{1}{x} > x$ et $x^2 > 0$. Donc $x^2 + \frac{1}{x} > x$.

Donc $x^2 + \frac{1}{x} > x$. □

1.7.4 Preuve par contradiction

On utilise le fait que $\neg\neg P \equiv P$. Si on veut démontrer l'assertion P en utilisant la technique de preuve "par contradiction", on commence par supposer que P est fausse et on déduit de cette hypothèse une conséquence impossible. Ceci montre qu'il est impossible que P soit fausse, donc P est prouvée (c'est à dire que P est vraie).

Assertion : P
Preuve. Supposons $\neg P$.
⋮
Contradiction. □

Voici un exemple.

Proposition 1.7.4. *Il existe une infinité de nombres premiers.*

Preuve. Supposons que le nombre de nombre premiers est fini. Soit $p_1, p_2, \ldots, p_n$ les nombres premiers. Considérons le nombre $q = p_1 p_2 \ldots p_n + 1$. Le nombre q est soit premier soit composé. Si l'on divise par un des nombres premiers p_i, il reste 1 pour chaque $i = 1, \ldots, n$. Ainsi, q ne peut pas être composé. Donc q est un nombre premier, qui n'est pas parmi les nombres premiers dans notre liste (parce que $q > p_i$ pour chaque i). Cela contredit notre hypothèse selon laquelle tous les nombres premiers sont dans la liste $p_1, p_2, \ldots, p_n$. Ceci termine la preuve par contradiction. □

1.7.5 Preuve d'une implication $P \Rightarrow Q$ par contradiction

Ici on suppose que l'implication $P \Rightarrow Q$ est fausse et on en déduit une contradiction. Rappelez-vous que $P \Rightarrow Q$ est fausse lorsque P est vraie et Q est fausse.

Assertion : $P \Rightarrow Q$
Preuve. Supposons que P est vraie et que Q est fausse.
⋮
Contradiction. □

Voici un exemple.

Proposition 1.7.5. *Soit $n \in \mathbb{Z}$. Si n^2 est impair, alors n est impair.*

Preuve. Procédons par contradiction : supposons que n^2 est impair et que n est pair. Alors il existe $a, b \in \mathbb{Z}$ tels que

$$n^2 = 2a + 1, \quad \text{et} \quad n = 2b.$$

Alors $2a + 1 = n^2 = (2b)^2 = 4b^2$, donc

$$2(2b^2 - a) = 1.$$

Ceci est absurde, car 2 fois un entier ne peut pas être égal à 1. Cette contradiction complète la démonstration. □

Exercices.

1.7.1. Supposons que $P_1 \vee P_2$ et $\mathbf{V}$, démontrer 'équivalence (1.2)

1.7.2. Soient $a, b \in \mathbb{Z}$. Démontrez l'implication

Si ab est pair, alors au moins un des entiers a, b est pair.

Chapitre 2

Usage des quantificateurs en mathématiques

Dans ce chapitre on discute les quantificateurs, qui jouent un rôle très important dans la logique et les mathématiques.

2.1 Le quantificateur existentiel

Le symbole $\exists$ est appelé le *quantificateur existentiel* ; une expression du type

$$\exists_{a\in A}(\dots)$$

se traduit en français par :

Il existe au moins un élément a de A qui satisfait la condition $(\dots)$.

Exemple 2.1.1. L'expression

$$\exists_{x\in\mathbb{N}}\ (x \text{ est un nombre premier}) \tag{2.1}$$

se lit

Il existe au moins un élément x de $\mathbb{N}$ qui satisfait : "x est un nombre premier".

On peut simplifier cette phrase pour qu'elle soit plus agréable à lire et plus facile à comprendre :

Il existe au moins un élément de $\mathbb{N}$ qui est un nombre premier. (2.2)

La phrase (2.2) est une bonne traduction de (2.1). Une des raisons qui font que (2.2) est agréable et claire est qu'on a évité de nommer "x". Remarquez aussi que la phrase (2.2) est vraie, donc (2.1) est vraie.

Exemple 2.1.2. La traduction française de $\exists_{n\in\mathbb{N}}(n$ est un nombre premier) est encore la phrase (2.2). Autrement dit, les expression

$$\exists_{x\in\mathbb{N}}\ (x \text{ est un nombre premier}) \quad \text{et} \quad \exists_{n\in\mathbb{N}}\ (n \text{ est un nombre premier})$$

ont la même signification. Elles sont aussi la même valeur de vérité : les deux sont vraies.

Exemple 2.1.3. L'expression

$$\exists_{x\in\mathbb{R}}\ (x^2 < 0) \tag{2.3}$$

se traduit par :

Il existe au moins un nombre réel dont le carrée est negatif. (2.4)

La phrase (2.4) est fausse, donc (2.3) est fausse.

2.2 Le quantificateur universel

Le symbole $\forall$ est appelé le *quantificateur universel*. Une expression du type

$$\forall_{a\in A}\ (\dots)$$

se traduit en français par l'une des phrases suivantes :

- *Pour tout élément a de A, la condition $(\dots)$ est satisfaite.*
- *Pout chaque élément a de A, la condition $(\dots)$ est satisfaite.*
- *Quel que soit l'élément a de A, la condition $(\dots)$ est satisfaite.*
- *Tout élément a de A satisfait la condition $(\dots)$.*
- *Chaque élément a de A satisfait la condition $(\dots)$.*

Exemple 2.2.1. L'expression

$$\forall_{x\in\mathbb{R}}\ (|x| \geq 0)$$

se lit :

- *Pour tout $x \in \mathbb{R}$, la condition $|x| \geq 0$ est satisfaite.*
- *Tout $x \in \mathbb{R}$ satisfait $|x| \geq 0$.*
- *La valeur absolue de tout nombre réel est non-négatif.*

Notons que ces phrases (et donc la formule) est **V**.

Exemple 2.2.2. L'expression

$$\forall_{x\in\mathbb{R}}\ (|x| > 0)$$

est **F**.

Variantes

Remarquez la différence entre les phrases suivantes :

- $\forall_{x\in A}\ \varphi$: tout élément de A satisfait la condition φ,
- $\forall_x\ \varphi$: tout objet de l'univers satisfait la condition φ.

Ces deux phrases (donc ces deux formules) sont différentes.

Mais on a les équivalences suivantes :

$$\begin{aligned}\forall_{x\in A}\ \varphi &\equiv \forall_x\ [(x \in A) \Rightarrow \varphi],\\ \exists_{x\in A}\ \varphi &\equiv \exists_x\ [(x \in A) \wedge \varphi].\end{aligned}$$

Un principe de raisonnement fondamental est le *principe de l'instanciation* qui dit :

$$\boxed{\text{De } \forall_{x\in X}\, P(x), \text{ on peut conclure } P(a) \text{ pour tout } a \in X.}$$

Exemple 2.2.3. De

$$\forall_{n\in\mathbb{N}^+}\ (e^n \text{ est un nombre irrationnel})$$

on peut conclure que e^4 est un nombre irrationnel, puisque $4 \in \mathbb{N}^+$.

2.3 Négation d'un quantificateur

Il n'y a que deux règles :

$$\neg\forall_{x\in A}\ \varphi \ \equiv\ \exists_{x\in A}\ \neg\varphi \qquad \text{et} \qquad \neg\exists_{x\in A}\ \varphi \ \equiv\ \forall_{x\in A}\ \neg\varphi.$$

Exemple 2.3.1. La négation de la formule $\forall_{x\in\mathbb{Z}}\ (|x| \geq 0)$ est :

$$\begin{aligned}\neg\forall_{x\in\mathbb{Z}}\ (|x| \geq 0) &\equiv \exists_{x\in\mathbb{R}}\ \neg(|x| \geq 0)\\ &\equiv \exists_{x\in\mathbb{Z}}\ (|x| < 0)\end{aligned}$$

Notez que la formule $\exists_{x\in\mathbb{Z}}\ (|x| < 0)$ est **F**. Donc la formule $\forall_{x\in\mathbb{N}}\ (|x| \geq 0)$ est **V**.

Exemple 2.3.2. La négation de $\forall_{x\in\mathbb{R}}\ [(x < 0) \vee (x > 0)]$ est :

$$\begin{aligned}\neg\forall_{x\in\mathbb{R}}\ [(x < 0) \vee (x > 0)] &\equiv \exists_{x\in\mathbb{R}}\ \neg[(x < 0) \vee (x > 0)]\\ &\equiv \exists_{x\in\mathbb{R}}\ [(x \geq 0) \wedge (x \leq 0)]\\ &\equiv \exists_{x\in\mathbb{R}}\ (x = 0)\end{aligned}$$

La dernière formule est **V**, donc $\forall_{x\in\mathbb{R}}\ [(x < 0) \vee (x > 0)]$ est **F**.

2.4 Variables liées et variable libres

Considérons l'expression

$$\forall_{x\in\mathbb{R}}\ (x^2 > y). \tag{2.5}$$

Le quantificateur $\forall$ s'applique à x mais pas à y. On dit alors que la variable x est *liée* par le quantificateur $\forall$. Puisque y n'est pas liée par un quantificateur, on dit que y est un *variable libre*.

Question : Qu'est-ce que c'est la valeur de vérité de (2.5) ?

La valeur de vérité de (2.5) dépend de la valeur numérique de y. Par exemple, si $y = -1$, (2.5) est **V**, mais si $y = 2$, (2.5) est **F**. Donc on dit que la valeur de vérité de (2.5) n'est pas définie. C'est parce qu'il existe une variable libre que la valeur de vérité de (2.5) n'est pas définie.

On peut traduire (2.5) en évitant de nommer la variable liée x :

La carrée de tout nombre réel est supérieure à y.

Remarque 2.4.1. Lorsqu'on traduit une formule en français,

- les variables libres doivent **toujours** être nommées dans la traduction française, et

- si possible, on évite de nommer la variable liée (mais ce n'est pas obligatoire, et c'est parfois mieux de la nommer).

Définition 2.4.2. Un *énoncé* est une formule qui n'a aucune variable libre.

Remarque 2.4.3. Tout énoncé a une valeur de vérité bien définie (un énoncé est soit **V**, soit **F**).

2.5 Formules ayant plusieurs quantificateurs

2.5.1 Interprétation

Exemple 2.5.1. La formule

$$\exists_{x\in\mathbb{R}}\exists_{y\in\mathbb{N}}\ (x<y)$$

est équivalente à

Il existe au moins un $x\in\mathbb{R}$ *pour lequel la formule* $\exists_{y\in\mathbb{N}}\ (x<y)$ *est vraie*

ou

Il existe des éléments x *de* $\mathbb{R}$ *est* y *de* $\mathbb{N}$ *qui satisfont* $x<y$.

Cette formule et **V** parce que 3 et 5 sont des éléments de $\mathbb{R}$ et $\mathbb{N}$ (respectivement) qui satisfont $x<y$.

Exemple 2.5.2. La formule

$$\forall_{x\in\mathbb{R}}\forall_{y\in\mathbb{R}}\ (x^2+y^3\geq x+y)$$

doit être interprété des manières suivantes :

- *Pour chaque* $x\in\mathbb{R}$, *la formule* $\forall_{y\in\mathbb{R}}\ (x^2+y^3\geq x+y)$ *est vraie.*
- *Pour chaque* $x\in\mathbb{R}$ *et pour chaque* $y\in\mathbb{R}$, *la condition* $(x^2+y^3\geq x+y)$ *est satisfaite.*
- *Pour tout choix de deux nombre réels* x *et* y, *la condition* $(x^2+y^3\geq x+y)$ *est satisfaite.*

Remarquons que ceci est faux (considère $x=0$, $y=-2$).

2.5.2 Ordre des quantificateurs

Si $P(x,y)$ est une condition, alors on a les équivalences

$$\exists_{a\in A}\exists_{b\in B}\ P(a,b)\equiv\exists_{b\in B}\exists_{a\in A}P(a,b),$$
$$\forall_{a\in A}\forall_{b\in B}\ P(a,b)\equiv\forall_{b\in B}\forall_{a\in A}P(a,b).$$

Exemple 2.5.3. Les deux formules

$$\exists_{n\in\mathbb{N}}\exists_{m\in\mathbb{N}}\ (|m+n|<|m|+|n|)\quad\text{et}\quad\exists_{m\in\mathbb{N}}\exists_{n\in\mathbb{N}}\ (|m+n|<|m|+|n|)$$

disent la même chose :

Il existe (au moins un choix de) $m,n\in\mathbb{N}$ *pour lesquels la formule* $|m+n|<|m|+|n|$ *est vraie.*

Exemple 2.5.4. La situation est différente lorsqu'une formule contient $\exists$ et $\forall$. Par exemple, les formules

$$\forall_{x\in\mathbb{R}}\exists_{y\in\mathbb{R}}\ (x > y) \tag{2.6}$$

$$\exists_{y\in\mathbb{R}}\forall_{x\in\mathbb{R}}(x > y) \tag{2.7}$$

ne sont pas équivalentes. La formule (2.6) peut être remplacée par

Chaque nombre réel est inférieur à au moins un (autre) nombre réel.

qui est **V**. De l'autre côté, la formule (2.7) peut être remplacée par

Il existe un nombre réel qui est plus petit que tous les nombres réels

qui est **F**.

Notation.
- $\exists_{x,y\in A}\ (\dots)$ est une abréviation de $\exists_{x\in A}\exists_{y\in A}\ (\dots)$.
- $\forall_{x,y\in A}\ (\dots)$ est une abréviation de $\forall_{x\in A}\forall_{y\in A}\ (\dots)$.

Notation. $\exists!_{x\in A}\ P(x)$ se traduit en français par l'une ou l'autre des phrases :
- il existe un unique élément x de A qui satisfait la condition $P(x)$
- il existe précisement un élément x de A qui satisfait la condition $P(x)$
- il existe un et un seul élément x de A qui satisfait la condition $P(x)$

Remarque 2.5.5. On peut éviter la notation "$\exists!$" (si l'on veut) :

$$\exists!_{x\in A}\ P(x) \equiv \exists_{x\in A}\ P(x)\ \wedge\ \forall_{x_1,x_2\in A}[(P(x_1)\wedge P(x_2)) \Rightarrow x_1 = x_2] \tag{2.8}$$

2.5.3 Négation d'une formule ayant plusieurs quantificateurs

Exemple 2.5.6. La négation de

$$\exists_{x\in\mathbb{N}}\forall_{y\in\mathbb{R}}\ (x^2 \le y)$$

et

$$\begin{aligned}\neg\exists_{x\in\mathbb{N}}\forall_{y\in\mathbb{R}}\ (x^2 \le y) &\equiv \forall_{x\in\mathbb{N}}\ \neg\forall_{y\in\mathbb{R}}\ (x^2 \le y)\\ &\equiv \forall_{x\in\mathbb{N}}\exists_{y\in\mathbb{R}}\ \neg(x^2 \le y)\\ &\equiv \forall_{x\in\mathbb{N}}\exists_{y\in\mathbb{R}}\ (x^2 > y)\end{aligned}$$

Exercices.

2.5.1. Donnez la valeur de vérité.

(a) $\forall_{x\in\mathbb{Z}}\exists_{y\in\mathbb{Z}}\,(x + y = 0)$

(b) $\exists_{y\in\mathbb{Z}}\forall_{x\in\mathbb{Z}}\,(x+y=0)$

2.5.2. Écrivez la négation de chacune des formules suivantes :

(a) $\forall_{x\in\mathbb{Z}}\exists_{y\in\mathbb{Z}}\,(x+y=0)$

(b) $\exists_{y\in\mathbb{Z}}\forall_{x\in\mathbb{Z}}\,(x+y=0)$

2.5.3. Soit $\mathbb{R}^+=(0,\infty)$ l'ensemble des nombres réels positifs et soit $\mathbb{N}^+=\{1,2,3,4,5,\ldots\}$ l'ensemble des entiers positifs. Traduite en logique :

(a) Quels que soient les nombres réels positifs x et y, il existe un entier positif n satisfaisant $nx>y$.

(b) Quel que soit le nombre réel positif x, il existe un entier positif n tel que $\frac{1}{n}<x$.

(c) Quel que soit le nombre réel positif x, il existe un entier positif n tel que $\frac{1}{n}<x^n$.

2.5.4. Écrivez la négation de chaque formule logique que vous avez obtenue à l'Exercice 2.5.3.

2.5.5. Écrivez la négation de la formule logique (2.8) (la côté droite de l'équivalence).

2.5.6. Supposez que $P(x,y)$ est une condition. Démontrez que $\exists_x\,\forall_y\,P(x,y)$ implique $\forall_y\,\exists_x\,P(x,y)$, mais l'implication dans l'autre direction ne tient pas .

2.6 Preuve de $\exists_{x\in A}\,\varphi$

Pour prouver $\exists_{x\in A}\,\varphi$, on doit prouver qu'il existe au moins un élément de A qui satisfait la condition φ.

La meilleure manière de prouver qu'un tel élément existe, c'est de *montrer* un élément qui satisfait la condition. Dans ce cas, on dit qu'on a une *preuve constructive*.

Voici un exemple de preuve constructive.

Proposition 2.6.1. $\exists_{a,b\in\mathbb{Z}}\;|a+b|<|a|+|b|$

Preuve. Prenons $a=1$, $b=-1$, alors $|a+b|=0<2=|a|=|b|$. □

Il n'est pas toujours possible de faire un preuve constructive. Parfois, on peut prouver qu'un certain objet existe même si on n'est pas capable de montrer cet objet. On a alors une *preuve non constructive*. Voici un exemple.

Proposition 2.6.2. *Il existe un nombre irrationnel x tel que $x^{\sqrt{2}}\in\mathbb{Q}$.*

Preuve. On sait que $\sqrt{2}$ est irrationnel, mais on ne sait pas si $\sqrt{2}^{\sqrt{2}}$ est rationnel ou irrationnel. Examinons les deux cas.

- Si $\sqrt{2}^{\sqrt{2}}$ est rationnel, alors $x=\sqrt{2}$ est un nombre irrationnel tel que $x^{\sqrt{2}}\in\mathbb{Q}$.
- Si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, alors $x=\sqrt{2}^{\sqrt{2}}$ est un nombre irrationnel tel que

$$x^{\sqrt{2}}=\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}=\sqrt{2}^{\sqrt{2}\cdot\sqrt{2}}=\left(\sqrt{2}\right)^2=2\in\mathbb{Q}.$$

Nous pouvons donc affirmer avec certitude qu'un des deux nombres

$$\sqrt{2}, \quad \sqrt{2}^{\sqrt{2}}$$

satisfait la condition demandée, mais nous ne savons pas lequel.

□

Remarque 2.6.3. En fait, $\sqrt{2}^{\sqrt{2}}$ est irrationnel.

Exercices.

2.6.1. Prouvez qu'il existe deux matrices A, B de format 2×2 telles que $AB \neq BA$.

2.6.2. Prouvez : $\exists_{a,b\in\mathbb{Z}}\ (1, 9b^2 < a^2 < 2b^2)$

2.7 Preuve de $\forall_{x\in A}\ \varphi$

Pour prouver $\forall_{x\in A}\ \varphi$, on doit prouver que chaque élément de A satisfait la condition φ.

Une telle preuve commence souvent pas la phrase : "*Soit* $x \in A$" qui est une forme abrégée de :

"Soit x un élément quelconque de A."

Cette phrase est alors suivie d'un raisonnement qui montre que l'élément x considéré satisfait la condition φ. Ce raisonnement doit être valable quel que soit l'élément x de A.

Assertion : $\forall_{x\in A}\ \varphi$
Preuve. Soit $x \in A$.
⋮
...donc x satisfait la condition φ. □

Voici quelques exemples.

Proposition 2.7.1. $\forall_{x\in\mathbb{R}}\ (x^2 + 1 \geq 2x)$

Preuve. Soit $x \in \mathbb{R}$. Puis

$$\begin{aligned} (x-1)^2 &\geq 0 \\ x^2 - 2x + 1 &\geq 0 \\ x^2 + 1 &\geq 2x \end{aligned}$$

□

Proposition 2.7.2. $\forall_{x\in\mathbb{R}}\exists_{n\in\mathbb{N}}\ \left(\frac{x^4+x^3}{n+2} < \frac{1}{3}\right)$

Preuve. Soit $x \in \mathbb{R}$. À partir de maintenant, on considère que la valeur de x ne change plus : on traite x comme une constante. On doit montrer que ce nombre x satisfait la condition

$$\exists_{n\in\mathbb{N}}\ \left(\frac{x^4+x^3}{n+2} < \frac{1}{3}\right).$$

Il est clair que x satisfait $x^4 + x^3 \leq 0$ ou $x^4 + x^3 > 0$. On procède par séparation des cas.

Cas 1 : Si $x^4 + x^3 \leq 0$ on prend $n = 0$ est puis

$$\frac{x^4+x^3}{n+2} = \frac{x^4+x^3}{2} \leq 0 < \frac{1}{3}$$

et donc x satisfait la condition.

Cas 2 : Si $x^4 + x^3 > 0$, on a

$$3(x^4 + x^3) \in \mathbb{R}^+$$

et on peut choisir un nombre $n \in \mathbb{N}$ tel que $n > 3(x^4 + x^3)$. Donc

$$n + 2 > n > 3(x^4 + x^3)$$
$$\frac{x^4+x^3}{n+2} < \frac{1}{3}$$

et x satisfait la condition. □

Remarque 2.7.3. Le fait qu'il existe un $n \in \mathbb{N}$ tel que $n > 3(x^4 + x^3)$ est l'étape cruciale de la preuve ci-dessus, puisque c'est à cet endroit qu'on voit que n existe. C'est parce qu'on traite x comme une constante qu'on peut trouver un n qui satisfait cette inégalité.

Exercices.

2.7.1. Prouvez les affirmations suivantes :

(a) $\forall_{n\in\mathbb{N}}\ \left(\frac{n}{n+1} < \frac{n+1}{n+2}\right)$

(b) $\forall_{x\in\mathbb{R}}\exists_{n\in\mathbb{N}}\ \left(\frac{x^2+1}{n+1} < \frac{1}{2}\right)$

2.8 Réfutation de $\forall_{x\in A}\ \varphi$

Réfuter un énoncé P signifie prouver que P est faux (ce qui revient à prouver que $\neg P$ est vrai).

Rappelez-vous que la négation de $\forall_{x\in A}\ \varphi$ est $\exists_{x\in A}\ \neg\varphi$.

Important :
- Pour réfuter $\forall_{x\in A}\ \varphi$ il suffit de donner un exemple d'un $x \in A$ qui ne satisfait pas φ.
- Pour prouver que $\forall_{x\in A}\varphi$ est vrai, il ne suffit pas de donner un ou plusieurs exemples d'éléments de A qui satisfont φ.

Exemple 2.8.1. Pour réfuter $\forall_{x\in\mathbb{R}}\ (x^2 > x)$ il suffit de dire que $x = \frac{1}{2}$ est un nombre réel tel que $x^2 \leq x$.

Exercices.

2.8.1. Pour chacune des assertions suivantes,
- prouvez l'assertion si vous croyez qu'elle est vraie ; ou
- réfutez-la si vous croyez qu'elle est fausse.

(a) $\exists_{n\in\mathbb{N}}\ \frac{3n+4}{4n+3} < \frac{95}{124}$

(b) $\forall_{x\in\mathbb{R}}\ \frac{1}{2x^2+3} \leq \frac{3}{10}$

(c) $\forall_{x\in\mathbb{R}}\ \frac{1}{x^2+1} \leq 1$

2.8.2. Soient A et A' les sous-ensembles de $\mathbb{R}^2$ définis par

$$A = \{(x, y) \in \mathbb{R}^2 : y \geq 0 \text{ et } x \leq y^2\}, \quad A' = \{(x, y) \in \mathbb{R}^2 : x \leq y^2\}$$

et on considère l'addition usuelle des vecteurs dan $\mathbb{R}^2$:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

On se demande si A et A' sont fermés sous l'addition de $\mathbb{R}^2$. Montrez que l'assertion $\forall_{u,v\in A}\ (u + v \in A)$ est vraie, mais que $\forall_{u,v\in A'}\ (u + v \in A')$ est fausse.

2.8.3. Si (u_1, u_2, u_3) et (v_1, v_2, v_3) sont deux points de $\mathbb{R}^3$ alors on définit

$$(u_1, u_2, u_3) * (v_1, v_2, v_3) = (u_1 + v_1, u_2 + v_2, u_1 + 2u_3 + v_3).$$

(a) Réfutez l'assertion $\forall_{u,v\in\mathbb{R}^3}\ (u * v = v * u)$.

(b) Soit $L = \{(x, y, z) \in \mathbb{R}^3 : 2y - z = 3 \text{ et } x + 2y = 8\}$ (L est une droite dans $\mathbb{R}^3$). Prouvez ou réfutez l'assertion suivante :

$$\forall_{u,v\in L}\ (u * v = v * u).$$

Chapitre 3

La théorie des ensembles : concepts de base et exemples

Dans ce chapitre on discute la notion d'un ensemble avec quelques exemples importants.

3.1 Les ensembles

Un *ensemble* est un collection d'objets. Les objets de cette collection sont appelés les *éléments* (ou les *membres*) de l'ensemble.

Un ensemble qui a un nombre fini d'éléments $x_1, \ldots, x_n$ est noté $\{x_1, \ldots, x_n\}$. Un ensemble qui a exactement un élément est appelé un *singleton*. Par exemple, on a l'ensemble $\{2\}$. Remarquons que l'ensemble $\{2\}$ et le nombre 2 sont deux objets différents : $2 \neq \{2\}$.

On dit que deux ensembles sont *égaux* s'ils contiennent les mêmes éléments. Par exemple :

$$\{0, 1\} \neq \{0\}, \quad \{0\} \neq \{1\}.$$

Plus précisément, si A et B sont des ensembles, $A = B$ si et seulement si

$$\forall_x \, [x \in A \Leftrightarrow x \in B]$$

La négation de cette formule est :

$$\begin{aligned} \neg\forall_x[x \in A \Leftrightarrow x \in B] &\equiv \exists_x \, \neg[x \in A \Leftrightarrow x \in B] \\ &\equiv \exists_x \, \neg[(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)] \\ &\equiv \exists_x[\neg(x \in A \Rightarrow x \in B) \vee \neg(x \in B \Rightarrow x \in A)] \\ &\equiv \exists_x[(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)] \end{aligned}$$

Donc on a

(a) $A = B \;\Leftrightarrow\; \forall_x \, [x \in A \Leftrightarrow y \in B]$

(b) $A \neq B \;\Leftrightarrow\; \exists_x[(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)]$

Un ensemble peut être un élément d'un autre ensemble. Par exemple, $\mathbb{N}$ est l'ensemble des nombres naturels et $\{\mathbb{N}\}$ est un ensemble avec un élément (l'ensemble $\mathbb{N}$). Notons que $\mathbb{N} \neq \{\mathbb{N}\}$. En fait, on va voir que tout est un ensemble !

Un ensemble est *fini* s'il a un nombre fini d'éléments. Autrement, il est *infini*.

Exemple 3.1.1.
- L'ensemble $\mathbb{N} = \{0, 1, 2, \ldots\}$ est infini.
- Les ensembles $\{2, 2, 5\}$, $\{2, 5\}$ et $\{5, 2\}$ sont égaux.
- Les ensembles $\{a, b\}$ et $\{a\}$ sont égaux si $a = b$. Autrement, ils ne sont pas égaux.
- $\{\{0, 1\}, \{2\}, \{3, 4, 5\}\}$ est un ensemble avec trois éléments : $\{0, 1\}$, $\{2\}$ et $\{3, 4, 5\}$. Ces éléments sont des ensembles aussi (avec 2, 1 et 3 éléments respectivement).

Le nombre d'éléments d'un ensemble X est noté par $|X|$.

Exemple 3.1.2.
- $|\mathbb{N}| = \infty$
- $|\{2, 5, 7\}| = 3$
- $|\{\{2, 3\}, \{4, 5\}, \{7, 9\}, \{2, 5\}\}| = 4$

Un ensemble x est une *partie* ou un *sous-ensemble* d'un autre ensemble y si chaque élément de x est aussi un élément de y, et on écrit $x \subseteq y$. On dit quelquefois que y est un *surensemble* de x.

Précisément,

$$\forall_{x,y}(x \subseteq y \Leftrightarrow \forall_a[(a \in x) \Rightarrow (a \in y)]).$$

Exemple 3.1.3.
- $\{1, 3, 4\} \subseteq \{1, 2, 3, 4\}$, mais $\{1, 3, 4\} \nsubseteq \{1, 2, 3, 4\}$
- $\{1, 2\}$ n'est pas une partie de $\{1, \{1, 2\}, \{2, 4\}\}$, mais $\{1, 2\} \in \{1, \{1, 2\}, \{2, 4\}\}$
- L'ensemble des nombres naturels est un sous-ensemble de l'ensemble des nombres réels.
- Chaque ensemble est une partie de lui-même.

Deux ensembles x et y sont égaux si est seulement si $x \subseteq y$ et $y \subseteq x$:

$$x = y \;\Leftrightarrow\; [(x \subseteq y) \wedge (y \subseteq x)]$$

Si $x \subseteq y$ est $x \neq y$, on écrit $x \subsetneq y$. Par exemple $\mathbb{N} \subsetneq \mathbb{R}$.

Remarque 3.1.4. Le symbole $\subset$ est un peu ambigu. Dans certains textes, cela signifie $\subseteq$ et dans d'autres (par exemple, [Nes]) il signifie $\subsetneq$.

Si l'ensemble x n'est pas une partie de l'ensemble y, on écrit $x \nsubseteq y$. Par exemple, $\mathbb{N} \nsubseteq \mathbb{R}^+$. Notez la différence entres les symboles $\subsetneq$ et $\nsubseteq$.

Théorème 3.1.5. *Un ensemble ne contenant aucun élément est une partie de chaque ensemble.*

Preuve. Soit $\varnothing$ un ensemble sans éléments. Soit x un ensemble quelconque. Supposons que $\varnothing$ n'est pas une partie de x. Donc il y a un élément de $\varnothing$ qui n'est pas un élément de x. (On utilise ici le fait que la négation de $\forall_a[(a \in \varnothing) \Rightarrow (a \in x)]$ est $\exists_a[(a \in \varnothing) \wedge (a \notin x)]$). Mais $\varnothing$ n'a pas d'éléments. Ceci est une contradiction et donc $\varnothing \subseteq x$. □

Corollaire 3.1.6. *Il y a au plus un ensemble sans éléments.*

Preuve. Soient $\varnothing_1$ et $\varnothing_2$ deux ensembles ne contenant aucun élément. D'après le théorème ci-dessus, $\varnothing_1 \subseteq \varnothing_2$ et $\varnothing_2 \subseteq \varnothing_1$. Par conséquent, $\varnothing_1 = \varnothing_2$. □

L'ensemble qui ne contient aucun élément est appelé *l'ensemble vide* et on le désigne par le symbole $\varnothing$. Autrement dit, $\varnothing$ est l'unique ensemble qui satisfait $\forall_x\ (x \notin \varnothing)$.

Remarque 3.1.7. Notez bien que $\varnothing \neq \{\varnothing\}$, puisque $\{\varnothing\}$ n'est pas vide – on a $\varnothing \in \{\varnothing\}$.

L'ensemble des parties d'un ensemble X est noté par $\wp(X)$.

Exemple 3.1.8.

$$\wp(\{-1,2,5\}) = \{\varnothing,\ \{-1\},\ \{2\},\ \{5\},\ \{-1,2\},\ \{2,5\},\ \{-1,5\},\ \{-1,2,5\}\}$$

Exemple 3.1.9.

$$\wp(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$

Théorème 3.1.10. *Si $|X| = n$ est fini, alors $|\wp(X)| = 2^n$.*

Preuve. Supposons que $|X| = n$. En formant une partie de X, on doit décider quels éléments sont dans le sous-ensemble. Autrement dit, pour chaque élément de X, on doit décider "oui" ou "non". Puisqu'il y a n éléments de X et que pour chaque élément il y a deux décisions possibles, il existe 2^n sous-ensembles possibles de X. □

Exercices.

3.1.1. Soient $A = \{2,3\}$ et $B = \{A\}$. Alors A a combien d'éléments, et B a combien d'éléments ? A est-il égal à B ?

3.1.2. Quels que soient les ensembles A, B, C, si $A \subseteq B$ et $B \subseteq C$, alors $A \subseteq C$.

3.1.3. Soit $X = \{0,1\}$. Quels sont les éléments de $\{\wp(A) : A \in \wp(X)\}$?

3.1.4. Énumérer les 16 éléments de $\wp(\wp(\{0,1\}))$.

3.1.5. Montrez que $X \subseteq Y$ si et seulement si $\wp(X) \subseteq \wp(Y)$.

3.1.6. Montrez que pour tout ensemble X, $\{X\} \in \wp(\wp(X))$.

3.1.7. Montrez que $\{\wp(A) : A \subseteq X\} \in \wp(\wp(\wp(X)))$.

3.2 Les ensembles de nombres

On a déjà vu certains ensembles : $\mathbb{N}$, $\mathbb{N}^+$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}^+$. On a (par exemple) :

$$\mathbb{N}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

On peut additionner et multiplier deux nombre naturels. Donc on dit que $\mathbb{N}$ est *fermé* ou *stable* sous les opérations de l'addition et de la multiplication.

Exemple 3.2.1. Est-ce que les ensembles suivants sont fermés sous les opérations données (avec $\div$ on suppose qu'on ne divise pas par zéro) ?

	$\mathbb{N}$	$\mathbb{N}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{R}^+$
$+$	Oui	Oui	Oui	Oui	Oui	Oui
$\times$	Oui	Oui	Oui	Oui	Oui	Oui
$-$	Non	Non	Oui	Oui	Oui	Non
$\div$	Non	Non	Non	Oui	Oui	Oui

On voit que les nombres rationnels sont fermés sous les quatres opérations. Mais il y a des "trous" dans l'ensemble $\mathbb{Q}$.

Lemme 3.2.2. *Il n'existe aucun nombre rationnel q tel que $q^2 = 2$.*

Preuve. On va prouver le lemme par contradiction. Soit $q \in \mathbb{Q}$ tel que $q^2 = 2$. Soient $a, b \in \mathbb{Z}$ tels que $q = a/b$ et tels que a et b ne sont pas tous les deux divisibles par 2 (sinon, on simplifie). Donc

$$\frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = q^2 = 2$$

Par conséquent, $a^2 = 2b^2$. Donc a^2 est pair. Puisque le carré d'un nombre impair est toujours impair, a est pair. Donc on peut choisir $c \in \mathbb{Z}$ tel que $a = 2c$. Donc $4c^2 = (2c)^2 = a^2 = 2b^2$ et $2c^2 = b^2$. Par conséquent, b et aussi pair, ce qui est une contradiction. □

Ce lemme nous montre que les nombres rationnels ne sont pas fermés sous l'opération d'élever aux (rationnels) puissances (parce que $2^{1/2} = \sqrt{2} \notin \mathbb{Q}$).

Exercices.

3.2.1. Montrez que entre deux nombres rationnels quelconques, il existe un nombre rationnel.

3.2.2. Montrez qu'il n'y a pas de plus petit nombre rationnel > 0.

3.2.3. Soient $\epsilon > 0$ and $\alpha > 0$ des nombres rationnels. Montrez qu'il existe $n \in \mathbb{N}$ tel que $n\epsilon > \alpha$.

3.3 Les sous-ensembles définis par une propriété

Si P est une propriété et $P(x)$ signifie que x a la propriété P alors

$$\{x : P(x)\}$$

signifie l'ensemble dont les éléments sont précisément tous les objets qui satisfont P.

Si X est un ensemble,

$$\{x \in X : P(x)\}$$

signifie la partie de X constituée des éléments de X qui ont la propriété P. Une autre manière de dire la même chose est

$$\{x : x \in X,\ P(x)\}.$$

Par exemple,

$$\{x \in \mathbb{N} : x \text{ est pair}\}$$

est l'ensemble des nombres naturels pairs. On note le même ensemble par

$$\{2x : x \in \mathbb{N}\}$$

et on abrège cet ensemble comme $2\mathbb{N}$. De même, $2\mathbb{Z}$ est l'ensemble des entiers pairs.

Pour $r \in \mathbb{R}$, on définit $r\mathbb{N}$, $r\mathbb{Z}$, $r\mathbb{Q}$ par

$$r\mathbb{Z} := \{rn : n \in \mathbb{Z}\} = \{s \in \mathbb{R} : s = rn \text{ pour certain } n \in \mathbb{Z}\}, \quad \text{etc.}$$

Ils sont tous des parties de $\mathbb{R}$.

Remarque 3.3.1. Pour l'instant, on va supposer le principe suivant :

> Étant donnée une condition P, il existe un et un seul ensemble dont les éléments sont précisément tous les objets qui satisfont P.

Plus tard, on va voir que cette supposition peut causer des problèmes. Par exemple, est-ce que l'ensemble

$$U = \{x : x \text{ est un ensemble}\}$$

existe ? U est l'ensemble de tous les ensembles, donc en particulier $U \in U$. On reviendra sur ce point plus tard.

Intervalles

Pour $a, b \in \mathbb{R}$, on définit

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} : a < x < b\} \\
(a, b] &= \{x \in \mathbb{R} : a < x \leq b\} \\
[a, b) &= \{x \in \mathbb{R} : a \leq x < b\} \\
[a, b] &= \{x \in \mathbb{R} : a \leq b \leq b\} \\
(a, \infty) &= \{x \in \mathbb{R} : x > a\} \\
[a, \infty) &= \{x \in \mathbb{R} : x \geq a\} \\
(-\infty, a) &= \{x \in \mathbb{R} : x < a\} \\
(-\infty, a] &= \{x \in \mathbb{R} : x \leq a\} \\
(-\infty, \infty) &= \mathbb{R}
\end{aligned}$$

Ces ensembles sont appelés *intervalles* ou *segments*. Remarquez que $\mathbb{R}^+ = (0, \infty)$. On écrit aussi $\mathbb{R}^{>0}$ et $\mathbb{R}^{\geq 0}$ pour $(0, \infty)$ et $[0, \infty)$ respectivement.

Exercices.

3.3.1. Montrez que si $b \leq a$, alors $(a, b) = \varnothing$.

3.3.2. Trouvez les éléments de l'ensemble $\{x \in \mathbb{R} : x > n \text{ pour tout } n \in \mathbb{N}\}$.

3.3.3. Trouvez l'ensemble $\{x \in \mathbb{R} : x^2 \in (0, 1)\}$.

3.4 Les ensembles d'ensembles

Pour être à l'aise avec l'idée qu'un ensemble peut être un élément d'un autre ensemble, on considère quelques exemples.

Exemple 3.4.1. $X = \{(a, b) : a, b \in \mathbb{R}\}$ est un ensemble dont les éléments sont des intervalles. On a

$$\begin{aligned} (2, 3) &\in X \\ [4, 5) &\notin X \\ (2, \infty) &\notin X \\ 4 \in (-2, 7) &\in X \\ 4 &\notin X \end{aligned}$$

Exemple 3.4.2. Soit X l'ensemble des parties A de $\mathbb{R}$ tels que $0 \in A$:

$$X = \{A \subseteq \mathbb{R} : 0 \in A\}.$$

Donc on a

$$\begin{aligned} (2, 3) &\notin X \\ (-1, 4) &\in X \\ 0 &\notin X \\ \{0\} &\in X \\ (0, \infty) &\notin X \\ [0, \infty) &\in X \end{aligned}$$

Exercices.

3.4.1. Soit X un ensemble avec n éléments. Combien d'éléments y a-t-il dans l'ensemble $\{A \in \wp(X) : |A| = n - 1\}$.

3.4.2. Soit X un ensemble avec n éléments. Combien d'éléments y a-t-il dans l'ensemble $\{A \in \wp(X) : |A| \text{ est pair}\}$.

3.4.3. Soit U l'ensemble des parties X de $\mathbb{R}$ tels que pour quelque $\epsilon \in \mathbb{R}^+$, $(-\epsilon, \epsilon) \subseteq X$. Soit V l'ensemble des parties X de $\mathbb{R}$ tels que pour quelque $\epsilon \in \mathbb{R}^+$, $[-\epsilon, \epsilon] \subseteq X$. Soit W l'ensemble des parties X de $\mathbb{R}$ tels que pour quelque $\epsilon \in \mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$, $(-\epsilon, \epsilon) \subseteq X$. Montrez que $U = V = W$.

3.5 Les ensembles paramétrés

Considérons l'ensemble

$$\{4n + 3 : n \in \mathbb{N}\}.$$

On dit que l'ensemble est *paramétré* (ou *indexé*) par $\mathbb{N}$ et que $\mathbb{N}$ est *l'ensemble d'indices*.

Si X est un ensemble quelconque, on a $X = \{x : x \in X\}$ et puis chaque ensemble est paramétré par lui-même.

L'ensemble

$$\{[a, b) : a < 0 \text{ et } b > 4\}$$

est paramétré par un ensemble de paires a, b de nombre réels.

Parfois, un ensemble $\{x_i : i \in I\}$ est noté par $(x_i)_{i \in I}$ ou par $(x_i)_i$ lorsque l'ensemble d'indices est clair dans le contexte.

Chapitre 4

Opérations avec des ensembles

Dans ce chapitre on discute certaines opérations avec des ensembles.

4.1 Différence

Soient X et Y deux ensembles. On définit la *différence d'ensembles*

$$X \setminus Y := \{x \in X : x \notin Y\} \qquad \text{“}X \text{ moins } Y\text{”}.$$

Par exemple,
- $\{-1, 0, 2, 3, 6, 7\} \setminus \{-5, -1, 1, 3, 4, 6, 9\} = \{0, 2, 7\}$
- $\mathbb{N} \setminus 2\mathbb{N}$ est l'ensemble des nombres naturels impairs.
- $\mathbb{R} \setminus \mathbb{R}^+ = (-\infty, 0]$.

Pour tous les ensembles x et y,

(a) $x \setminus x = \varnothing$

(b) $x \setminus y \subseteq x$

(c) $x \setminus \varnothing = x$

(d) $x \setminus y = \varnothing$ si et seulement si $x \subseteq y$

Si X est un ensemble fixe, pour chaque partie Y de X on écrit Y^c pour $X \setminus Y$. On utilise la notation Y^c seulement quand le surensemble X est clair dans le contexte. L'ensemble Y^c est appelé le *complémentaire* de Y (dans X).

Si on fixe un surensemble X, on a

(a) $(Y^c)^c = Y$

(b) $X^c = \varnothing$

(c) $\varnothing^c = X$

4.2 Intersection

Si X et Y sont des ensembles, on définit *l'intersection* de X et Y par

$$X \cap Y := \{a : (a \in X) \wedge (a \in Y)\}.$$

Par exemple, si $X = \{1, 2, 3, 4, 5, 6\}$, $Y = \{4, 5, 6, 7, 8, 9\}$ alors $X \cap Y = \{4, 5, 6\}$.
Un autre exemple : $\mathbb{R}^+ \cap \mathbb{Z} = \mathbb{N}^+$.
On dit que deux ensembles X et Y sont *disjoints* si $X \cap Y = \varnothing$.
L'intersection satisfait les propriétés suivantes (exercices) :

(a) $x \cap x = x$

(b) $x \cap y \subseteq x$

(c) $x \cap y = y \cap x$ (l'intersection est commutative)

(d) $x \cap y = x$ si et seulement si $x \subseteq y$

(e) $(x \cap y) \cap z = x \cap (y \cap z)$ (l'intersection est associative)

(f) $x \cap \varnothing = \varnothing$

(g) $(x \setminus y) \cap (y \setminus x) = \varnothing$

À cause de la commutativité de l'intersection on n'a pas besoin de parenthèses quand on prend l'intersection de plusieurs ensembles. Par exemple, on peut écrire :

$$x \cap y \cap z \cap t$$

On peut aussi former l'intersection d'un nombre infini d'ensembles. Si A_i est un ensemble pour chaque $i \in I$ (I est un ensemble d'indices),

$$\bigcap_{i \in I} A_i := \{x : x \in A_i \text{ pour chaque } i \in I\}.$$

On écrit $\bigcap_{n=1}^{\infty} A_n$ pour $\bigcap_{n \in \mathbb{N}} A_n$.
Si X est un ensemble d'ensembles, on écrit $\cap X$ pour $\cap_{x \in X} x$.

Exemple 4.2.1. (a) $\bigcap_{n=1}^{\infty} (-1/n, 1/n) = \{0\}$

(b) $\bigcap_{r \in \mathbb{R}^+} (0, r] = \varnothing$

(c) $\bigcap_{r \in \mathbb{R}^+} [0, r) = \{0\}$

(d) $\bigcap_{r \in \mathbb{Q}} (r, \infty) = \varnothing$

(e) Soit $X = \{\mathbb{N}, \mathbb{R}^+, (-\infty, 5)\}$. Alors $\cap X = \{1, 2, 3, 4\}$.

Exercices.

4.2.1. Montrez que $x \setminus y = x$ si et seulement si $x \cap y = \varnothing$ et que $x \setminus y = \varnothing$ si et seulement si $x \subseteq y$.

4.2.2. Montrez que $\bigcap_{n=1}^{\infty} (-1/n, 1 + 1/n) = [0, 1]$.

4.2.3. Montrez que $\bigcap_{r,s \in \mathbb{R},\, r<1 \text{ et } 2<s} (r, s) = [1, 2]$.

4.3 Union

Si X et Y sont des ensembles, on définit *l'union* (ou *la réunion*) de X et Y par

$$X \cup Y := \{a : (a \in X) \vee (a \in Y)\}.$$

Par exemple, si $X = \{1, 2, 3, 4, 5, 6\}$, $Y = \{4, 5, 6, 7, 8, 9\}$ alors $X \cup Y = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
Un autre exemple : $(-3, 5] \cup [0, \infty) = (-3, \infty)$.
L'union satisfait les propriétés suivantes (exercices) :

(a) $x \cup x = x$

(b) $x \subseteq x \cup y$

(c) $x \cup y = y \cup x$ (l'union est commutative)

(d) $x \cup y = x$ si et seulement si $y \subseteq x$

(e) $(x \cup y) \cup z = x \cup (y \cup z)$ (l'union est associative)

(f) $x \cup \varnothing = x$

À cause de la commutativité de l'union on n'a pas besoin de parenthèses quand on prend l'intersection de plusieurs ensembles. Par exemple, on peut écrire :

$$x \cup y \cup z \cup t$$

On peut aussi former l'union d'un nombre infini d'ensembles. Si A_i est un ensemble pour chaque $i \in I$ (I est un ensemble d'indices),

$$\bigcup_{i \in I} A_i := \{x : x \in A_i \text{ pour au moins un } i \in I\}.$$

On écrit $\bigcup_{n=1}^{\infty} A_n$ pour $\bigcup_{n \in \mathbb{N}} A_n$.

Si X est un ensemble d'ensembles, on écrit $\cup X$ pour $\cup_{x \in X} x$. Par exemple, si $X = \{\varnothing, \{0\}, \{2, 1\}, \{0, 1\}\}$, alors $\cup X = \{0, 1, 2\}$.

Exemple 4.3.1. Démontrons que $\bigcup_{n=1}^{\infty}(1/n, 1 - 1/n) = (0, 1)$. On doit prouver

$$\bigcup_{n=1}^{\infty}(1/n, 1 - 1/n) \subseteq (0, 1) \quad \text{et} \quad (0, 1) \subseteq \bigcup_{n=1}^{\infty}(1/n, 1 - 1/n).$$

Puisque $0 < 1/n$ et $1 - 1/n < 1$ pour chaque nombre naturel n, la première inclusion est satisfaite. Soit $x \in (0, 1)$. Donc $0 < x < 1$. On peut choisir un nombre n_1 tel que $1/n_1 < x$ et un nombre n_2 tel que $1/n_2 < 1 - x$. Soit n le maximum de n_1 et n_2. Donc

$$1/n \leq 1/n_1 < x \quad \text{et} \quad 1/n \leq 1/n_2 < 1 - x \Rightarrow x < 1 - 1/n.$$

Par conséquent, $x \in (1/n, 1 - 1/n)$. On a démontré que chaque $x \in (0, 1)$ est un élément de $(1/n, 1 - 1/n)$ pour un certain n. Donc on a démontré que $(0, 1) \subseteq \bigcup_{n=1}^{\infty}(1/n, 1 - 1/n)$.

Exemple 4.3.2.

(a) $\bigcup_{n=1}^{\infty}(-1/n, 1/n) = (-1, 1)$
(b) $\bigcup_{n=1}^{\infty}(1/n, 1 - 1/n] = (0, 1)$
(c) $\bigcup_{n=1}^{\infty}[1/n, n) = (0, \infty)$
(d) $\bigcup_{r\in\mathbb{Q}}(r, \infty) = \mathbb{R}$

Il y a deux relations entre $\cap$ et $\cup$ appelées la *Loi de De Morgan* (rappelez-vous la Loi de De Morgan dans la logique propositionnelle, qui est différente) :

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$$
$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$$

Pour deux ensembles X et Y,

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$$

est la *différence symétrique* de X et Y.

Exemple 4.3.3. Si

$$A = \{1, 2, 3, 4, 5, 6\} \quad \text{et} \quad B = \{4, 5, 6, 7, 8, 9\},$$

alors

$$A \Delta B = \{1, 2, 3, 7, 8, 9\}.$$

Exercices.

4.3.1. Soit A et B des parties d'un surensemble X. Montrez que $(A \setminus B)^c = A^c \cup B$.

4.3.2. Montrez que pour des ensembles quelconques x, y, z,

$$y \cap (x \setminus y) = \varnothing$$
$$(x \cap y) \setminus z = (x \setminus z) \cap (y \setminus z)$$
$$(x \setminus y) \setminus z = x \setminus (y \cup z)$$

4.3.3. Trouvez $\bigcup_{n\in\mathbb{N}}[n, n^2]$.

4.3.4. Trouvez $\bigcup_{n\in\mathbb{N}}(n, n^2)$.

4.3.5. Soit X un ensemble et pour $i \in I$ soit $Y_i \subseteq X$. Montrez que $(\bigcup_i Y_i)^c = \bigcap_i Y_i^c$ et que $(\bigcap_i Y_i)^c = \bigcup_i Y_i^c$.

4.3.6. Montrez que $\bigcup_{r>0}[r, \infty) = (0, \infty)$.

4.3.7. Soit A un ensemble et X un ensemble d'ensembles. Montrez que $\left(\bigcup_{x\in X} x\right) \setminus A = \bigcup_{x\in X}(x \setminus A)$.

4.3.8. Soient X et Y deux ensembles non-vides d'ensembles. Montrez que

$$\left(\bigcup_{x\in X} x\right) \cap \left(\bigcup_{y\in Y} y\right) = \bigcup_{x\in X,\, y\in Y}(x \cap y),$$
$$\left(\bigcap_{x\in X} x\right) \cup \left(\bigcap_{y\in Y} y\right) = \bigcap_{x\in X,\, y\in Y}(x \cup y).$$

4.3.9. Pour deux ensembles X et Y, montrez que

(a) $X\Delta(Y\Delta Z) = (X\Delta Y)\Delta Z$.

(b) $X\Delta Y = Y\Delta X$.

(c) $X\Delta\varnothing = \varnothing\Delta X = X$.

(d) $X\Delta X = \varnothing$.

4.4 Produit cartésien

Rappelez-vous qu'on paramètre le plan $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ par des couples des nombres réels (x, y). Chaque point P du plan $\mathbb{R} \times \mathbb{R}$ est représenté par deux coordonnées x et y et on écrit $P = (x, y)$.

Mais qu'est-ce que c'est un couple (x, y) ? Qu'est-ce ça veut dire ? La propriété dont on a besoin est la suivante :

$$(x, y) = (z, t) \text{ si et seulement si } x = z \text{ et } y = t.$$

Donc, on veut une définition d'un pair (x, y) avec cette propriété. L'ensemble $\{x, y\}$ n'a pas cette propriété parce que $\{x, y\} = \{y, x\}$ (même si $x \neq y$).

Mais l'ensemble $\{\{x\}, \{x, y\}\}$ a cette propriété.

Lemme 4.4.1. $\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}$ *si et seulement si* $x = z$ *et* $y = t$.

Preuve. Si $x = z$ et $y = t$, alors $\{x\} = \{z\}$ et $\{x, y\} = \{z, t\}$. Donc $\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}$. On a demontré :

$$(x = z \text{ et } y = t) \Rightarrow \{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}.$$

Supposons que $\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}$. On sait que $x = y$ ou $x \neq y$. On montre que $x = z$ et $y = t$ par séparation des cas. Supposons que $x = y$. Alors $\{\{x\}, \{x, y\}\} = \{\{x\}\}$. Donc $\{\{z\}, \{z, t\}\} = \{\{x\}\}$ a seulement un élément. Par conséquent, $\{z, t\} = \{z\}$ et donc $z = t$. Puis $\{z\} = \{x\}$ et donc $z = x$. Donc $y = x = z = t$ aussi.

Maintenant, supposons que $x \neq y$. On sait que $\{z\} \in \{\{x\}, \{x, y\}\}$ et donc $\{z\} = \{x\}$ ou $\{z\} = \{x, y\}$. Mais l'ensemble $\{x, y\}$ a deux éléments parce que $x \neq y$. Par conséquent $\{z\} \neq \{x, y\}$ et donc $\{z\} = \{x\}$. Puis $z = x$. Aussi, il faut que $\{x, y\} = \{z, t\}$ et çela implique que $y = t$. On a démontré l'autre implication :

$$\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\} \Rightarrow (x = z \text{ et } y = t).$$

□

Définition 4.4.2. Le couple (x, y) est l'ensemble $\{\{x\}, \{x, y\}\}$. On dit que x est la *première coordonnée* et que y est la *deuxième coordonnée*. Pour deux ensembles X et Y,

$$X \times Y = \{(x, y) : x \in X,\ y \in Y\}.$$

L'ensemble $X \times Y$ est appelé le *produit cartésien* de X et Y.

Lemme 4.4.3. *Si X et Y sont des ensembles, alors $X \times Y \subseteq \wp(\wp(X \cup Y))$.*

Preuve. Soient $x \in X$ et $y \in Y$. Alors $x, y \in X \cup Y$. Donc $\{x\}, \{x, y\} \in \wp(X \cup Y)$. Par conséquent $\{\{x\}, \{x, y\}\}$ est un sous-ensemble de $\wp(X \cup Y)$, et donc un élément de $\wp(\wp(X \cup Y))$. Puis $X \times Y \subseteq \wp(\wp(X \cup Y))$. □

Corollaire 4.4.4. *Si X et Y sont des ensembles,*

$$X \times Y = \{\ \alpha \in \wp(\wp(X \cup Y)) : \exists_{x \in X}\, \exists_{y \in Y}\, \alpha = \{\{x\}, \{x, y\}\}\ \}.$$

Donc $X \times Y$ est un sous-ensemble de $\wp(\wp(X \cup Y))$ défini par une propriété.

On écrit (x, y, z) pour $((x, y), z)$. On va donner une définition meilleure plus tard.

Exercices.

4.4.1. Écrivez les éléments de $((x, y), z)$.

4.4.2. Si $|X| = n$ et $|Y| = m$, combien d'éléments $X \times Y$ a-t-il ?

4.4.3. Trouvez $\cap(x, y)$, $\cup(x, y)$, $\cap\cap(x, y)$, $\cap\cup(x, y)$, $\cup\cap(x, y)$, et $\cup\cup(x, y)$.

4.4.4. Trouvez $((\cup\cup(x, y)) \setminus (\cup\cap(x, y))) \cup (\cap\cup(x, y))$.

4.4.5. Qu'est-ce c'est $X \times \varnothing$?

4.4.6. Montrez que $\cup\cup(X \times Y) = X \cup Y$ si $X \neq \varnothing$ et $Y \neq \varnothing$.

4.4.7. Montrez que $X \times Y = \varnothing$ si et seulement si un de X ou Y est vide.

4.4.8. Montrez que $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$, $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$ et $(X \setminus Y) \times Z = (X \times Z) \setminus (Y \times Z)$.

4.4.9. Trouvez des égalités similar pour $(\cup_i X_i) \times Z$ et $(\cap_i X_i) \times Z$.

Chapitre 5

Les fonctions

Dans ce chapitre on discute la définition précise d'une fonction. On voit aussi quelques opérations sur les fonctions.

5.1 Les fonctions

Intuitivement, une *fonction* ou une *application* d'un ensemble X vers un ensemble Y est un "règle" qui assigne à **chaque** élément x de X un élément **unique** $f(x)$ de Y. L'ensemble $\operatorname{dom} f := X$ est appelé le *domaine* et $\operatorname{codom} f := Y$ est appelé le *codomaine* (ou *l'ensemble d'arrivée*).

Remarquez qu'une fonction peut assigner le même élément du codomaine a deux (ou plus) éléments du domaine. Aussi, ce n'est pas nécessaire que chaque élément du codomaine est associé à un élément du domaine (mais chaque élément du domaine est associé à un élément du codomaine).

Par exemple, la fonction de $\mathbb{R}$ vers $\mathbb{R}$ qui assigne à chaque nombre réel son carré assign le nombre 1 (du codomaine) à 1 et -1 (du domaine). Et il n'existe aucun nombre du domaine associé à -1 (du codomaine).

Si f est une fonction de X vers Y, on écrit $f\colon X \to Y$. Si on veut donner la règle, on écrit $x \mapsto f(x)$.

Par exemple,

$$f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2 \tag{5.1}$$

est la fonction qui assigne a chaque nombre réel son carré.

Si $A \subseteq X$ et $f\colon X \to Y$ est une fonction,

$$f(A) := \{f(x) : x \in A\} = \{y \in Y : y = f(a) \text{ pour quelque } a \in A\}.$$

est *l'image* de A sous f. L'ensemble $f(X)$ est *l'image* de f. Si $B \subseteq Y$,

$$f^{-1}(B) := \{x \in X : f(x) \in B\}$$

est *l'image réciproque* de B sous f. On écrite souvent $f^{-1}(y)$ $f^{-1}(\{y\})$. Notez que, ici, f^{-1} est seulement une partie de la notation. Cela n'implique pas que f est inversible.

Remarquez que le codomaine et l'image peuvent être différent. Par example, si f est la fonction définie par (5.1), l'image est $[0,\infty)$ mais le codomaine est $\mathbb{R}$. Aussi, $f((-2,2)) = [0,4)$ et $f^{-1}([-1,9)) = (-3,3)$.

Le domaine et le codomaine sont des parties de la définition d'une fonction. Par example, les fonctions

$$\begin{aligned} f\colon \mathbb{R} \to \mathbb{R}, &\quad f(x) = x^2, \\ f_1\colon \mathbb{R} \to (-1,\infty), &\quad f(x) = x^2, \\ f_2\colon \mathbb{R} \to [0,\infty), &\quad f(x) = x^2, \end{aligned}$$

sont différents parce qu'ils ont des codomaines différents. Cependant, parfois on utilisera la même notation f pour tous ces fonctions.

Si $f\colon X \to Y$ et Y_1 est un ensemble tel que $f(X) \subseteq Y_1$, on peut former une autre fonction $f_1\colon X \to Y_1$ avec la même règle.

Deux fonctions $f\colon X \to Y$ et $g\colon X_1 \to Y_1$ sont égaux si et seulement si $X = X_1$, $Y = Y_1$ et $f(x) = g(x)$ pour tout $x \in X$.

Par exemple, les fonctions

$$\begin{aligned} f\colon \mathbb{R} \to \mathbb{R}, &\quad f(x) = 4x^2, \\ g\colon \mathbb{R} \to \mathbb{R}, &\quad g(x) = (2x)^2, \end{aligned}$$

sont égaux.

L'ensemble des fonctions de X vers Y sera désigné par $\mathrm{Fonc}(X,Y)$.

Exemples 5.1.1. (a) Pour chaque ensemble X, il existe la *fonction identique* $\mathrm{Id}_X\colon X \to X$ définie par $\mathrm{Id}_X(x) = x$.

(b) Soient X et Y des ensembles et soit b un élément fixe de Y. La fonction $x \mapsto b$ qui envoie chaque élément de X à b est appelée la *fonction constante de valeur b*.

(c) Soient X, Y, Z trois ensembles et soient $f\colon X \to Y$ et $g\colon Y \to Z$ deux fonctions. On définit la fonction

$$g \circ f\colon X \to Z$$

par la règle

$$(g \circ f)(x) = g(f(x)).$$

La fonction $g \circ f$ est appelée la *composé* de f et g. L'operation $\circ$ est appelée la *composition*.

Remarquez que $f \circ g$ peut pas être définie (à moins que $X = Z$) et même quand elle est définie, l'égalité $f \circ g = g \circ f$ peut être fausse.

Si $X = Y$ on peut composer f avec lui-même plusieurs fois. On écrit f^n pour $f \circ \cdots \circ f$ (n fois). Remarquez que $f^n \circ f^m = f^{n+m}$.

(d) Soient $f\colon X \to Y$ une fonction et $A \subseteq X$. Ensuite, il y a une fonction $f|_A\colon A \to Y$ tel que $f|_A(a) = f(a)$ pour tous $a \in A$.

La fonction $f|_A$ est appelée la *restriction* de f à A.

(e) Soient X et Y deux ensembles. Les fonctions $\pi_1 \colon X \times Y \to X$ et $\pi_2 \colon X \times Y \to Y$ définies par $\pi_1(x, y) = x$ et $\pi_2(x, y) = y$ sont appelées les *première* et *deuxième projections* respectivement.

Lemme 5.1.2. *Soient X, Y, Z, T des ensembles et $f \colon X \to Y$, $g \colon Y \to Z$ et $h \colon Z \to T$ des fonctions. Alors*

(a) $h \circ (g \circ f) = (h \circ g) \circ f$. *(*associativité*)*

(b) $f \circ \mathrm{Id}_X = f$ *et* $\mathrm{Id}_Y \circ f = f$.

Preuve.

(a) Premièrement, remarquez que les domaines de $h \circ (g \circ f)$ est $(h \circ g) \circ f$ sont tous les deux X et les codomaines sont tous les deux Z. Ensuite, pour chaque $x \in X$,

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))), \quad \text{et}$$
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Donc $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ pour tout $x \in X$ et cela veut dire que $h \circ (g \circ f) = (h \circ g) \circ f$.

(b) Premièrement, remarquez que les domaines de $f \circ \mathrm{Id}_X$, $\mathrm{Id}_Y \circ f$, et f sont tous X et leurs codomaines sont tous Y. Ensuite, pour chaque $x \in X$, on remarquez que

$$(f \circ \mathrm{Id}_X)(x) = f(\mathrm{Id}_X(x)) = f(x), \quad \text{et}$$
$$(\mathrm{Id}_Y \circ f)(x) = \mathrm{Id}_Y(f(x)) = f(x).$$

□

Définition 5.1.3. Si $f \colon X \to Y$ est une fonction, son *graphe* est l'ensemble

$$\mathrm{Gph}(f) = \{(x, f(x)) : x \in X\} = \{(x, y) \in X \times Y : y = f(x)\}.$$

L'ensemble $\mathrm{Gph}(f)$ a les propriétés suivantes :

(a) $\mathrm{Gph}(f) \subseteq X \times Y$,

(b) Pour chaque $x \in X$ il existe un élément unique $y \in Y$ tel que $(x, y) \in \mathrm{Gph}(f)$.

Inversement, supposons que F est un ensemble qui satisfait ces deux propriétés :

(a) $F \subseteq X \times Y$,

(b) Pour chaque $x \in X$ il existe un élément unique $y \in Y$ tel que $(x, y) \in F$.

Alors on peut définir une fonction $f \colon X \to Y$ tel que $F = \mathrm{Gph}(f)$. On définit $f \colon X \to Y$ par la règle

$$f(x) = y \text{ si et seulement si } (x, y) \in F.$$

Exercices.

Dans les exercices suivantes, f est une fonction.

5.1.1. Combien de fonctions y a-t-il d'un ensemble de n éléments dans un ensemble de m éléments ?

5.1.2. Que pouvez-vous dire au sujet de la relation entre $f(A \setminus B)$ et $f(A) \setminus f(B)$?

5.1.3. Montrez que $f(\varnothing) = \varnothing$.

5.1.4. Soit $f\colon \mathbb{N} \to \mathbb{N}$ la fonction définie par $f(x) = 2x+1$. Par exemple $f(3) = 7$, $f(f(3)) = f(7) = 15$.

(a) Trouvez $f(\mathbb{N})$, $f(f(\mathbb{N}))$, $f(f(f(\mathbb{N})))$.

(b) Trouvez $f^n(\mathbb{N})$.

5.1.5. Soit $f\colon X \to Y$ une fonction.

(a) Montrez que si $(B_i)_i$ est une famille de parties de Y, alors

$$f^{-1}\left(\bigcup_i B_i\right) = \bigcup_i f^{-1}(B_i),$$

et

$$f^{-1}\left(\bigcap_i B_i\right) = \bigcap_i f^{-1}(B_i)$$

et si $B \subseteq Y$ alors $f^{-1}(B^c) = f^{-1}(B)^c$.

(b) Montrez que si $(A_i)_i$ est une famille de parties de X, alors $f(\bigcup_i A_i) = \bigcup_i f(A_i)$ et $f(\bigcap_i A_i) \subseteq \bigcap_i f(A_i)$.

(c) Trouvez un example où la dernière inclusion n'est pas une égalité.

(d) Si $A \subseteq X$, qu'est-ce c'est la relation entre $f(A^c)$ et $f(A)^c$?

5.1.6. (a) Trouvez une fonction $f\colon \wp(\mathbb{N}) \to \mathbb{N}$ tel que si $x \in \wp(\mathbb{N}) \setminus \{\varnothing\}$ alors $f(x) \in x$.

(b) Trouvez une fonction $g\colon \wp(\mathbb{Z}) \to \mathbb{Z}$ tel que si $x \in \wp(\mathbb{Z}) \setminus \{\varnothing\}$ alors $g(x) \in x$.

(c) Est-ce qu'il est possible de trouvez une fonction $h\colon \wp(\mathbb{Q}) \to \mathbb{Z}$ tel que si $x \in \wp(\mathbb{Q}) \setminus \{\varnothing\}$ alors $h(x) \in x$?

5.2 Les fonctions : Une définition plus précise

On a dit qu'une fonction $f\colon X \to Y$ est une "règle" que assigne a chaque élément de X un élément de Y. Mais cette définition n'est pas assez précise. Plus précisément, on a la définition suivante.

Définition 5.2.1. Une fonction est un ensemble de la forme (X, Y, F) tel que X et Y sont deux ensembles et F est un sous-ensemble de $X \times Y$ qui satisfait la propriété suivante :

Pour chaque $x \in X$, il existe un unique $y \in Y$ tel que $(x, y) \in F$.

Puis notre "règle" $f(x) = y$ est définie par

$$f(x) = y \text{ si et seulement si } (x, y) \in F.$$

Avec la nouvelle définition d'une fonction donnée ci-dessus, étant donné deux fonctions (X, Y, F) et (Y, Z, G), qu'est-ce c'est la composé $(Y, Z, G) \circ (X, Y, F)$?

Par définition, pour chaque $x \in X$, il existe un unique $f(x) = y \in Y$ tel que $(x, y) \in F$. Puis il existe un unique $g(f(x)) = g(y) = z \in Z$ tel que $(y, z) \in F$. Donc on définit un nouveaux ensemble H par

$$H = \{(x, z) \in X \times Z : \exists_{y \in Y} [((x, y) \in F) \wedge ((y, z) \in G)]\}.$$

Puis on définit

$$(Y, Z, G) \circ (X, Y, F) := (X, Z, H).$$

Dans ce cours, on va continuer d'utiliser la notation $f \colon X \to Y$ pour une fonction de X vers Y, et on va penser des fonction en termes des règles. Mais maintenant on sait que cette notion est basée sur une idée précise.

Exercices.

5.2.1. Soit (X, Y, F) une fonction. Montrez que l'ensemble X est uniquement déterminée par Y et F. En d'autres termes, si (X, Y, F) et (X_1, Y, F) sont des fonctions, alors $X = X_1$. Cet exercice montre qu'une fonction peut être définie comme une paire (Y, F) tel que pour tout x il existe au plus un $y \in Y$ tel que $(x, y) \in F$ et on peut retrouver l'ensemble de définition comme l'ensemble des $x \in X$ tels que $(x, y) \in F$ pour au moins un $y \in Y$.

5.3 Les opérations binaires

Définition 5.3.1. Soit X un ensemble. Une *opération binaire* sur X est une fonction $f \colon X \times X \to X$. Pour $x, y \in X$, au lieu de $f(x, y)$ on écrit souvent $x \star y$, $x \cdot y$, $x + y$, $x \odot y$, $x \otimes y$, etc. ou même xy. Si l'opération n'a pas de nom, le résultat $x \star y$ est souvent appelé le *produit* des éléments x et y. Un ensemble X avec une opération binaire $\star$ est noté $(X, \star)$.

Exemples 5.3.2. (a) Soit $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$. Alors l'addition et la multiplication sont des opérations binaires sur X. Si $X = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$ alors la soustraction est une opération binaire. Si $X = \mathbb{Q} \setminus \{0\}$ ou $\mathbb{R} \setminus \{0\}$ alors la division est une opération binaire sur X.

(b) Soit X un ensemble. Alors $\cap, \cup, \setminus, \Delta$ sont des opérations binaires sur $\wp(X)$.

Propriétés potentielles des opération binaires. Soit $\star$ une opération binaire définie sur un ensemble X.

(a) **Associativité.** Si $(x \star y) \star z = x \star (y \star z)$ pour tous choix de $x, y, z \in X$, alors on dit que $\star$ est *associative*. Si $\star$ est associative, on peut écrire des produits $x \star y \star z$ sans parenthèses. Si $\star$ n'est pas associative, même les produits $(x \star x) \star x$ et $x \star (x \star x)$ peuvent être différent et donc x^3 n'a pas du sens.

(b) **Commutativité.** Si $x \star y = y \star x$ pour tous choix de $x, y \in X$, alors on dit que $\star$ est *commutative*.

(c) **Élément unité.** S'il y a un $e \in X$ tel que $x \star e = x$ pour tout $x \in X$, alors on dit que e est une *unité à droite* pour $\star$. S'il y a un $f \in X$ tel que $f \star x = x$ pour tout $x \in X$, alors on dit que f est une *unité à gauche* pour $\star$. Un élément qui est une unité à droite **et** une unité à gauche est une *unité* (ou *élément neutre*) de l'opération binaire $\star$.

Supposons que $\star$ a une unité à gauche f et une unité à droite e. Donc $f = f \star e = e$. Par conséquent, X a une unité et cet élément est unique.

(d) **Élément inverse.** Supposons que $(X, \star)$ a une unité e. Soit $x \in X$. S'il existe $y \in X$ tel que $x \star y = e$, alors y est appelé un *inverse à droite* de x. S'il existe $z \in X$ tel que $z \star x = e$, alors z est appelé un *inverse à gauche* de x. Si $\star$ est associative est si $x \in X$ a un élément inverse à gauche z et un élément inverse à droite y, alors

$$y = e \star y = (z \star x) \star y = z \star (x \star y) = z \star e = z$$

et donc $y = z$ est un *inverse* de x.

Exemples 5.3.3. (a) $X = \wp(A)$ avec l'opération d'intersection $\cap$. On a vu que cette opération est associative et commutative. Puisque $B \cap A = A \cap B = B$ pour tous $B \in \wp(A)$ (c.-à-d. $B \subseteq A$), A est une unité. Seulement A a un inverse (qui est A lui-même) parce que si $B \subsetneq A$, alors $B \cap C \subseteq B \neq A$ pour tous $C \in \wp(A)$.

(b) $\mathbb{Z}$ avec $+$. Cette opération est associative et commutative et 0 est un élément unité. L'inverse de $n \in \mathbb{Z}$ est $-n$.

(c) $\mathbb{Z}$ avec $\times$. Cette opération est associative et commutative et 1 est un élément unité. Seulement 1 et -1 a des inverses (qui sont 1 et -1 respectivement). Aucun autre élément a un inverse (à gauche ou à droite).

(d) $\mathbb{Q} \setminus \{0\}$ avec division. Cette opération n'est ni associative ni commutative. Par exemple,

$$1/2 \neq 2/1, \quad \text{et} \quad 1/(2/2) \neq (1/2)/2.$$

1 est une unité à droite mais il n'y a pas d'unité à gauche (et donc pas d'unité).

Exercices.

5.3.1. Pour les opérations binaires suivantes, déterminer si les opérations sont associatives et/ou commutatives. Aussi, déterminez s'il existe des éléments unités à droite ou à gauche et si oui, déterminez s'il existe des éléments inverses à droite ou à gauche.

(a) $X = \wp(A)$ avec l'opération d'union $\cup$.
(b) $X = \wp(A)$ avec la différence $\setminus$.
(c) $X = \wp(A)$ avec la différence symétrique Δ.
(d) $X = \mathbb{N}, \mathbb{Q}, \mathbb{R}$ avec $+$ ou $\times$.
(e) $X = \mathbb{N} \setminus \{0\}$, $\mathbb{Z} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ avec la division.
(f) $X = 2\mathbb{Z}$ avec $+$.
(g) $X = \mathbb{R}$, $a \in R$ un élément fixe et $x \star y = x + y - a$.
(h) X un ensemble quelconque, $e \in X$ un élément fixe, $x \star y = e$ pour tous $x, y \in X$.
(i) X un ensemble quelconque, $x \star y = x$ pour tous $x, y \in X$.
(j) $X = \mathbb{R}$ et $x \star y = \max\{x, y\}$.
(k) $X = \mathbb{R}$ et $x \star y = x - y$.
(l) $X = \mathbb{R}$ et $x \star y = |x - y|$.

5.4 Les opérations avec des fonctions

On va voir comment utiliser les anciennes fonctions pour créer des nouvelles fonctions.

Exemples 5.4.1. (a) Soient f et g des fonctions d'un ensemble X vers $\mathbb{R}$. On peut définir

$$f + g \colon X \to \mathbb{R}, \quad (f + g)(x) = f(x) + g(x) \text{ pour tout } x \in X.$$

On dit que $f + g$ est définie par *addition termes à termes*. On peut aussi définir

$$fg \colon X \to \mathbb{R}, \quad (fg)(x) = f(x)g(x) \text{ pour tout } x \in X$$

On dit que fg est définie par *multiplication termes à termes*. En général, si $f, g \colon X \to Y$ sont des fonctions et $\star$ est une opération binaire sur Y, alors on peut définir

$$f \star g \colon X \to Y, \quad (f \star g)(x) = f(x) \star g(x), \quad x \in X.$$

Donc $\star$ nous donne une opération binaire sur $\mathrm{Fonc}(X, Y)$, encore noté par $\star$. Des propriétés de $(Y, \star)$ devient des propriétés de $(\mathrm{Fonc}(X, Y), \star)$. Par example, si $(Y, \star)$ est commutative, alors pour tous choix de $f, g \in \mathrm{Fonc}(X, Y)$,

$$(f \star g)(x) = f(x) \star g(x) = g(x) \star f(x) = (g \star f)(x) \text{ pour tout } x \in X.$$

Par conséquent $f \star g = g \star f$ pour tout choix de $\mathrm{Fonc}(X, Y)$. Donc $(\mathrm{Fonc}(X, Y), \star)$ est commutative. Voir Exercice 5.4.1 pour les autres propriétés.

(b) Si $f \colon X \to X_1$ et $g \colon Y \to Y_1$ sont des fonctions, on peut définir la fonction

$$f \times g \colon X \times Y \to X_1 \times Y_1, \quad (f \times g)(x, y) = (f(x), g(y)).$$

(c) Pour chaque fonction $f \colon X \to Y$, on peut définir la fonction

$$\tilde{f} \colon \wp(X) \to \wp(Y), \quad \tilde{f}(A) = f(A) := \{f(a) : a \in A\} \text{ pour tout } A \in \wp(X).$$

(d) Soit $f\colon X \to Y$ une fonction. On peut définir une fonction

$$\tilde{f}^{-1}\colon \wp(Y) \to \wp(X),$$
$$\tilde{f}^{-1}(B) = f^{-1}(B) := \{x \in X : f(x) \in B\} \text{ pour tout } B \in \wp(Y).$$

(e) Soient $f\colon X \to X_1$ et $g\colon Y \to Y_1$ deux fonctions. Supposez que $X \cap Y = \varnothing$. Alors on peut définir la fonction $f \cup g\colon X \cup Y \to X_1 \cup Y_1$, *l'union* de f et g, par la règle

$$(f \cup g)(z) = \begin{cases} f(z) & \text{if } z \in X, \\ g(z) & \text{if } z \in Y. \end{cases}$$

(f) On peut généraliser l'exemple ci-dessus. Soient $f\colon X \to X_1$ et $g\colon Y \to Y_1$ deux fonctions. Supposez que pour tout $z \in X \cap Y$, $f(z) = g(z)$. Alors on peut définir la fonction $f \cup g\colon X \cup Y \to X_1 \cup Y_1$, *l'union* de f et g, par la règle

$$(f \cup g)(z) = \begin{cases} f(z) & \text{if } z \in X, \\ g(z) & \text{if } z \in Y. \end{cases}$$

Si $X \cap Y = \varnothing$, cette définition est d'accord avec l'ancien.

Exercices.

5.4.1. Supposez que X et Y sont des ensembles et $\star$ est un opération binaire sur Y.

(a) Montrez que si $(Y, \star)$ est associative, alors $(\mathrm{Fonc}(X, Y), \star)$ est associative.

(b) Montrez que si $(Y, \star)$ a une unité à gauche (resp. à droite), alors $(\mathrm{Fonc}(X, Y), \star)$ a une unité à gauche (resp. à droite).

(c) Montrez que si $(Y, \star)$ a une unité et si chaque element de Y est inversible, alors $(\mathrm{Fonc}(X, Y), \star)$ a les mêmes propriétés.

5.4.2. Soient f et g deux fonctions d'un ensemble X vers $\mathbb{R}$. Montrez que si $s\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est définie par $s(x, y) = x + y$, alors $f + g = s \circ (f \times g)$. Montrez que si $p\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est définie par $p(x, y) = xy$, alors $fg = p \circ (f \times g)$.

5.5 Les injections, surjections, et bijections

5.5.1 Injections

Définition 5.5.1. Une fonction $f\colon X \to Y$ est *injective* si

$$\forall_{x_1, x_2 \in X}[(f(x_1) = f(x_2)) \implies (x_1 = x_2)].$$

On dit aussi que f est une *injection*.

Exemples 5.5.2. (a) La fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$$

n'est pas injective. Cependant, la fonction

$$f\colon [0, \infty) \to \mathbb{R}, \quad f(x) = x^2$$

est injective.

(b) Si X et Y sont des ensembles non-vides et $x_0 \in X$ est fixe, alors la fonction $f\colon Y \to X \times Y$ définie par $f(y) = (x_0, y)$ est injective.

(c) Soit $a \in \mathbb{N}$. La fonction

$$f\colon \mathbb{N} \to \mathbb{N}, \quad f(n) = n + a$$

est injective.

(d) Soit $r \in \mathbb{R}$. La fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = rx$$

est injective si et seulement si $r \neq 0$.

(e) Si $f_1\colon X_1 \to Y_1$ et $f_2\colon X_2 \to Y_2$ sont des fonctions injectives, alors la fonction

$$f_1 \times f_2\colon X_1 \times X_2 \to Y_1 \times Y_2, \quad (f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2))$$

est aussi injective.

Lemme 5.5.3. *(a) La composition de deux injections est une injection.*

(b) Si $f \circ g$ est une injection, alors g est un injection.

Preuve.

(a) Soient f et g deux injections. Pour tous choix de x_1, x_2,

$$\begin{aligned} (f \circ g)(x_1) = (f \circ g)(x_2) &\implies f(g(x_1)) = f(g(x_2)) && \text{(définition de composition)} \\ &\implies g(x_1) = g(x_2) && (f \text{ est injective}) \\ &\implies x_1 = x_2 && (g \text{ est injective}) \end{aligned}$$

Donc $f \circ g$ est injective.

(b) Supposez que $f \circ g$ est une injection et que $g(x_1) = g(x_2)$. Donc $f(g(x_1)) = f(g(x_2))$. En d'autres termes $(f \circ g)(x_1) = (f \circ g)(x_2)$. Puisque $f \circ g$ est une injection, cela implique $x_1 = x_2$.

□

Remarquez que c'est possible d'avoir une injection $f \circ g$ où f n'est pas une injection. Par exemple, si

$$g\colon \{0\} \to \{0, 1\},\ g(0) = 0 \quad \text{et} \quad f\colon \{0, 1\} \to \{0\},\ f(0) = f(1) = 0,$$

alors $f \circ g\colon \{0\} \to \{0\}$ est l'identité, qui est injective, mais f n'est pas injective.

5.5.2 Surjections

Définition 5.5.4. Une fonction $f\colon X \to Y$ est une *surjection* si

$$\forall_{y\in Y}\exists_{x\in X}[f(x) = y]$$

c.-à-d. $f(X) = Y$. On dit aussi que f est une *surjection*.

Exemples 5.5.5. (a) La fonction

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$$

n'est pas surjective, mais

$$g\colon \mathbb{R} \to [0,\infty), \quad g(x) = x^2, \quad \text{et} \quad h\colon [-5,10] \to [0,100], \quad h(x) = x^2,$$

sont surjectives.

(b) La fonction $f\colon \mathbb{R} \to \mathbb{Z}$ définie par

$$f(x) = \lfloor x \rfloor := \text{le plus grand entier qui est inférieur ou égal a } x$$

est surjective (mais pas injective).

(c) La fonction $f\colon \mathbb{Z} \to \mathbb{N}$, $f(x) = |x|$, est surjective.

(d) Si $f_1\colon X_1 \to Y_1$ et $f_2\colon X_2 \to Y_2$ sont surjectives, alors la fonction

$$f_1 \times f_2\colon X_1 \times X_2 \to Y_1 \times Y_2, \quad (f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2)),$$

est surjective aussi.

Lemme 5.5.6. *(a) La composition de deux surjections est une surjection.*

(b) Si $g \circ f$ est une surjection, alors g est une surjection.

(c) Si $f\colon X \to Y$ est une fonction quelconque, alors la fonction $f\colon X \to f(X)$ est une surjection.

(d) La projection $\pi_1\colon X \times Y \to X$ (resp. $\pi_2\colon X \times Y \to Y$) est une surjection si $Y \neq \varnothing$ (resp. $X \neq \varnothing$).

Preuve.

(a) Supposons que $f\colon X \to Y$ et $g\colon Y \to Z$ sont deux surjections. On a

$$(g \circ f)(X) = g(f(X)) = g(Y) = Z$$

et donc $g \circ f$ est une surjection.

(b) Supposons que $f\colon X \to Y$ et $g\colon Y \to Z$ sont des fonctions et que $g \circ f$ est une surjection. Alors $Z = g(f(X)) \subseteq g(Y)$. Puisque on a toujours $g(Y) \subseteq Z$, on déduit que $g(Y) = Z$ et donc g est une surjection.

(c) Exercice.

(d) Exercice.

□

Remarquez que c'est possible d'avoir une surjection $g \circ f$ où f n'est pas une surjection. Par exemple, si

$$f\colon \{0\} \to \{0,1\},\ f(0) = 0 \quad \text{et} \quad g\colon \{0,1\} \to \{0\},\ g(0) = g(1) = 0,$$

alors $g \circ f\colon \{0\} \to \{0\}$ est l'identité, qui est surjective, mais f n'est pas surjective.

5.5.3 Bijections

Définition 5.5.7. Une fonction $f\colon X \to Y$ est appelée une *bijection* (et on dit que f est *bijective*) si elle est injective et surjective. Si X et Y sont des ensembles pour lesquels il existe une bijection de X vers Y, on dit que X et Y sont en *correspondance bijective*.

Lemme 5.5.8. *(a) La composition de deux bijections est une bijection.*

(b) Si $f \circ g$ est une bijection, alors g est une injection est f est une surjection.

(c) Si $f\colon X \to Y$ est une injection, alors $f\colon X \to f(X)$ est une bijection.

Preuve. Le résultat découle de Lemmes 5.5.3 et 5.5.6. □

Lemme 5.5.9 (Inverse)**.** *Soit $f\colon X \to Y$ une bijection. Alors il existe une bijection unique $f^{-1}\colon Y \to X$ tel que pour tous choix de $x \in X$ et $y \in Y$,*

$$f^{-1}(y) = x \iff f(x) = y.$$

On a

$$f \circ f^{-1} = \mathrm{Id}_Y, \quad \text{et} \quad f^{-1} \circ f = \mathrm{Id}_X.$$

De plus, si $g\colon Y \to X$ satisfait

$$f \circ g = \mathrm{Id}_Y \quad \text{ou} \quad g \circ f = \mathrm{Id}_X,$$

alors $g = f^{-1}$.

Preuve. Les deux premières affirmations sont des exercices. Si f est une bijection est $g\colon Y \to X$ satisfait $f \circ g = \mathrm{Id}_Y$, alors

$$g = \mathrm{Id}_X \circ g = f^{-1} \circ f \circ g = f^{-1} \circ \mathrm{Id}_Y = f^{-1}.$$

Le cas où $g\colon Y \to X$ satisfait $g \circ f = \mathrm{Id}_X$ est similaire. □

Si $f\colon X \to Y$ est un bijection, la bijection $f^{-1}\colon X \to Y$ du lemme ci-dessus est appelée *l'inverse* de f.

Lemme 5.5.10. *Supposons qu'une fonction $f\colon X \to Y$ possède une inverse, c'est-à-dire, il existe une fonction $g\colon Y \to X$ tel que $f \circ g = \mathrm{Id}_Y$ et $g \circ f = \mathrm{Id}_X$. Alors f est une bijection.*

Preuve. Exercice. □

Lemme 5.5.11. *(a) Soit $f\colon X \to Y$ une bijection. Alors $(f^{-1})^{-1} = f$.*
(b) Soient $f\colon X \to Y$ et $g\colon Y \to Z$ des bijections. Alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Preuve. Exercice. □

Exercices.

5.5.1. Démontrez Lemma 5.5.6(c) et (d).

5.5.2. (a) Trouvez tous les bijections de $\{0, 1, 2\}$ vers $\{0, 1, 2\}$.
(b) Trouvez tous les bijections de $\{0, 1, 2, 3\}$ vers $\{0, 1, 2, 3\}$.
(c) Trouvez tous les injections de $\{0, 1, 2\}$ vers $\{0, 1, 2, 3\}$.
(d) Trouver tous les surjections de $\{0, 1, 2\}$ vers $\{0, 1\}$.
(e) Combiens de surjections de $\{0, 1, 2, 3\}$ vers $\{0, 1, 2\}$ y a-t-il ?

5.5.3. Soit $f\colon X \to Y$ une bijection. Montrez que pour tous choix de $A, B \subseteq X$,
(a) $f(A \cap B) = f(A) \cap f(B)$
(b) $f(A \cup B) = f(A) \cup f(B)$
(c) $f(A \setminus B) = f(A) \setminus f(B)$
(d) Montrez que la fonction induite $\tilde{f}\colon \wp(X) \to \wp(Y)$ est aussi une bijection.

5.5.4. Soit X un ensemble. Montrez que les ensembles $\mathrm{Fonc}(\{0, 1\}, X)$ et $X \times X$ sont en correspondance bijective.

Chapitre 6

Les relations

Dans ce chapitre, on discute les relations, incluant les relation d'équivalences et les ordres partiels.

6.1 Définitions

Définition 6.1.1. Soit X un ensemble. Une *relation binaire* R sur X (ou entre les éléments de X) est un sous-ensemble de $X \times X$. Pour $x, y \in X$, on écrit xRy si $(x, y) \in R$ et on écrit $x \not R y$ si $(x, y) \notin R$. Les symboles usuels pour les relations sont $<, \leq, \prec, \preceq, \gg, \subset, \subseteq, \sqsubseteq, \sim, \simeq, \approx, \equiv, \perp, \lhd, \trianglelefteq$, etc.

Exemples 6.1.2. (a) Soit $X = \{0, 1, 2, 3\}$. On définit

$$< = \{(0,1),\, (0,2),\, (1,2),\, (0,3)\,(1,3),\, (2,3)\} = \{(i,j) : i < j\}.$$

Alors $<$ est une relation. C'est la relation familière d'ordre.

(b) Soit $X = \mathbb{R}$. Alors

$$< = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}$$

est la relation d'ordre sur $\mathbb{R}$.

(c) Soit X un ensemble. Alors $\varnothing$ et $X \times X$ sont des relations binaires sur X. Dans le premier, il n'existe pas deux éléments de X qui sont reliés. Dans le deuxième, chaque deux éléments de X sont reliés.

(d) Soit X un ensemble. Alors

$$\{(x, y) \in X \times X : x = y\} = \{(x, x) : x \in X\}$$

est une relation binaire sur X (c'est l'égalité !).

(e) Soit $X \in \mathbb{Z}$. Alors $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \text{ divise } y\}$ est une relation binaire sur $\mathbb{Z}$.

(f) Soit U un ensemble et soit X l'ensemble des parties finies de U. Alors

$$\{(A, B) \in X \times X : |A| = |B|\}$$

est une relation binaire sur X.

(g) Soit U un ensemble et soit $X = \wp(U)$. Alors on a les relations binaires suivantes.
   i. $\{(A, B) \in X \times X : \text{il existe une bijection } f\colon A \to B\}$
   ii. $\{(A, B) \in X \times X : A \subseteq B\}$
   iii. $\{(A, B) \in X \times X : A \cap B \neq \varnothing\}$
   iv. $\{(A, B) \in X \times X : A \cap B = \varnothing\}$

(h) Si $f\colon X \to X$ est une fonction, alors le graphe de f est une relation de X.

On peut définir les propriétés suivantes d'une relation R sur X :

(a) *Réflexive* : $\forall_{x \in X}\, xRx$

(b) *Irréflexive* : $\forall_{x \in X}\, x \not R x$

(c) *Symétrique* : $\forall_{x,y \in X}\, (xRy \Rightarrow yRx)$

(d) *Antisymétrique* : $\forall_{x,y \in X}\, [(xRy \wedge yRx) \Rightarrow (x = y)]$

(e) *Transitive* : $\forall_{x,y,z \in X}\, [(xRy \wedge yRz) \Rightarrow xRz]$

Exemples 6.1.3. (a) L'égalité (sur un ensemble non-vide) est une relation réflexive, symétrique, antisymétrique et transitive. Elle n'est pas irréflexive.

(b) La relation $\leq$ sur $\mathbb{R}$ est réflexive, antisymétrique et transitive. Elle n'est ni irréflexive ni symétrique.

(c) La relation $<$ sur $\mathbb{R}$ est irréflexive, antisymétrique et transitive. Elle n'est ni réflexive ni symétrique.

(d) La relation $\neq$ sur $\mathbb{R}$ est irréflexive et symétrique. Elle n'est ni réflexive, ni antisymétrique, ni transitive.

Exemple 6.1.4. Soit R une relations binaire sur X. Alors, il existe une relation réflexive S minimum qui contient R. Précisément,

$$S = R \cup \{(x, x) : x \in X\}.$$

On dit que S est la *clôture réflexive* de R. Ici, "plus petite" veut dire que toute relation réflexive qui contient R contient S aussi.

On peut définir aussi la *clôture symétrique* et *clôture transitive* d'une relation R (voir les exercices).

Exercices.

6.1.1. Déterminez si les relations binaires de l'Exemple 6.1.2 sont réflexives, irréflexives, symétriques, antisymétriques, ou transitives.

6.1.2. Soit R une relation sur un ensemble X. Montrez qu'il existe une relation symétrique S minimum qui contient R (c.-à-d. une relation symétrique qui contient R et qui est contenue dans chaque relation symétrique qui contient R). On dit que S est la *clôture symétrique* de R.

6.1.3. Soit R une relation sur un ensemble X. Montrez qu'il existe une relation transitive S minimum qui contient R. On dit que S est la *clôture transitive* de R.

6.2 Les relations d'équivalence

Définition 6.2.1. Une *relation d'équivalence* est une relation binaire qui est réflexive, symétrique et transitive. Une relation d'équivalence est souvent noté par $\equiv, \sim, \simeq, \approx, \cong$.

Selon la définition, une relation binaire $\equiv$ sur un ensemble X est une relation d'équivalence si et seulement si :

(a) **Réflexivité.** Pour tout $x \in X$, $x \equiv x$.

(b) **Symétrie.** Pour tous choix de $x, y \in X$, si $x \equiv y$ alors $y \equiv x$.

(c) **Transitivité.** Pour tous choix de $x, y, z \in X$, si $x \equiv y$ et $y \equiv z$, alors $x \equiv z$.

Exemples 6.2.2. (a) Égalité est une relation d'équivalence sur tout ensemble.

(b) Les relations $<$ et $\leq$ (par exemple, sur $\mathbb{R}$) ne sont pas des relations d'équivalence.

(c) La relation définie par $\forall_{x,y \in X}\, xRy$ (c.-à-d la relation $X \times X$) est une relation d'équivalence pour tout ensemble X.

(d) Si X est un sous-ensemble de $\mathbb{R}$ ou $\mathbb{C}$, la relation définie par xRy si et seulement si $|x| = |y|$ est une relation d'équivalence sur X.

(e) Soit $n > 0$ un nombre naturel. Sur $\mathbb{Z}$, la relation $\equiv_n$ définie par

$$x \equiv_n y \iff n \text{ divise } x - y$$

est une relation d'équivalence.

Preuve. On doit montrer que la relation est réflexive, symétrique, et transitive.

i. *Réflexive.* Pour tout $x \in \mathbb{Z}$, on a $x - x = 0 = 0 \cdot n$ est donc $x \equiv_n x$.

ii. *Symétrique.* Supposons que $x, y \in \mathbb{Z}$ tel que $x \equiv_n y$. Donc il existe $k \in \mathbb{Z}$ tel que $x - y = kn$ (parce que $x - y$ est divisible par n). Par conséquent, $y - x = (-k)n$ est divisible par n et donc $y \equiv_n x$.

iii. *Transitive.* Supposons que $x, y, z \in \mathbb{Z}$ tel que $x \equiv_n y$ et $y \equiv_n z$. Donc il existe $k, m \in \mathbb{Z}$ tel que $x - y = kn$ et $y - z = mn$. Par conséquent,

$$x - z = (x - y) + (y - z) = kn + mn = (k + m)n$$

est donc $x - z$ est divisible par n. Donc $x \equiv_n z$.

□

(f) Si X est l'ensemble $\mathbb{R}$ ou $\mathbb{Q}$, alors la relation définie par $x \equiv y$ si et seulement si $x - y \in \mathbb{Z}$ est une relation d'équivalence.

(g) Soient X et Y deux ensembles et $A \subseteq X$. La relation $\equiv_A$ définie sur $\text{Fonc}(X, Y)$ par

$$f \equiv g \iff f|_A = g|_A$$

est une relation d'équivalence.

(h) On définit une relation sur $\text{Fonc}(\mathbb{R}, \mathbb{R})$ par

$$f \equiv g \iff \exists_{x \in \mathbb{R}} [f(x) = g(x)].$$

Alors $\equiv$ n'est pas une relation d'équivalence parce que elle n'est pas transitive. Par exemple, si

$$f(x) = 1, \quad g(x) = x^2, \quad h(x) = 0, \quad x \in X,$$

alors $f \equiv g$ et $g \equiv h$ mais $f \not\equiv h$.

(i) Si X et Y sont des ensembles et F est un ensemble de fonctions de X vers Y, alors la relation sur X définie par

$$x \equiv_A y \iff \forall_{f \in F} [f(x) = f(y)]$$

est une relation d'équivalence sur X.

Définition 6.2.3. Si $\equiv$ est une relation d'équivalence sur un ensemble X et $a \in X$, on définit la *classe d'équivalence* $\bar{a}$ de a par

$$\bar{a} = \{x \in X : a \equiv x\}.$$

Parfois, on écrit $[a]$ ou $\tilde{a}$ (ou quelque autre symbole) pour la classe d'équivalence de a.

Définition 6.2.4. Une *partition* P d'un ensemble X est un ensemble de parties de X (c.-à-d. $P \in \wp(\wp(X))$) tel que

(a) $\cup P = X$, et

(b) pour tous choix de $A, B \in P$, si $A \neq B$ alors $A \cap B = \varnothing$.

Exemples 6.2.5. (a) Les ensembles $\{\{0\}, \{1, 3\}, \{2, 4\}\}$ et $\{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\}$ sont des partitions de $\{0, 1, 2, 3, 4\}$.

(b) Les ensembles $\{[n, n + 1) : n \in \mathbb{Z}\}$ et $\{(2n, 2n + 2] : n \in \mathbb{Z}\}$ sont des partitions de $\mathbb{R}$.

(c) Les ensembles

i. $\{[n, n + 1] : n \in \mathbb{Z}\}$

ii. $\{[n, n + 2) : n \in \mathbb{Z}\}$

iii. $\{[2n, 2n + 1) : n \in \mathbb{N}\}$

ne sont pas des partitions de $\mathbb{R}$.

Lemme 6.2.6. *Soit $\equiv$ une relation d'équivalence sur un ensemble X. Alors l'ensemble $\{\bar{x} : x \in X\}$ est une partition de X. Inversement, toute partition P de X donne une relation d'équivalence sur X définie par*

$$x \equiv y \iff \exists_{A \in P} (x \in A \wedge y \in A).$$

Donc il existe une correspondance bijective entre l'ensemble des partitions de X et l'ensemble des relations d'équivalence sur X.

Preuve. Soit $\equiv$ une relation d'équivalence sur X. Puisque $x \equiv x$ pour tout $x \in X$, on a $x \in \bar{x}$. Donc $\cup\{\bar{x} \mid x \in X\} = X$. Maintenant, on prouve que pour tous choix de $x, y \in X$, soit $\bar{x} = \bar{y}$ ou $\bar{x} \cap \bar{y} = \varnothing$. On montre que si $\bar{x} \cap \bar{y} \neq \varnothing$, alors $\bar{x} = \bar{y}$. Puisque $\bar{x} \cap \bar{y} \neq \varnothing$, on peut choisir $z \in \bar{x} \cap \bar{y}$. Donc $z \equiv x$ et $z \equiv y$. Soit $t \in \bar{x}$. Alors $t \equiv x$. Puisque $\equiv$ est symétrique, on a

$$t \equiv x$$
$$x \equiv z$$
$$z \equiv y$$

Par transitivité, on obtient $t \equiv y$, c.-à-d. $t \in \bar{y}$. On a montré que chaque élément t de $\bar{x}$ est un élément de $\bar{y}$ et donc $\bar{x} \subseteq \bar{y}$. Par le même argument, on voit que $\bar{y} \subseteq \bar{x}$. Donc $\bar{x} = \bar{y}$. Par conséquent, $\{\bar{x} : x \in X\}$ est une partition de X.

Inversement, soit P une partition de X. On définit une relation $\equiv$ par :

$$x \equiv y \iff \exists_{A \in P} (x \in A \wedge y \in A).$$

On peut montrer que $\equiv$ est une relation d'équivalence (exercice). □

Pour $a, b \in \mathbb{R}$, on définit

$$a\mathbb{Z} + b = \{an + b : n \in \mathbb{Z}\}.$$

Exemple 6.2.7. Soit $\equiv_5$ la relation sur $\mathbb{Z}$ définie par

$$x \equiv_5 y \iff (x - y) \text{ est divisible par } 5.$$

Alors $\equiv_5$ est une relation d'équivalence. La partition correspondante est

$$\{A_0, A_1, A_2, A_3, A_4\}$$

où

$$A_i = \{5n + i : n \in \mathbb{Z}\} = 5\mathbb{Z} + i, \quad i = 0, 1, 2, 3, 4,$$

est l'ensemble des entiers dont le reste sur la division par 5 est i.

Définition 6.2.8. Soit $\equiv$ une relation d'équivalence sur un ensemble X. L'ensemble

$$X/\equiv := \{\bar{x} : x \in X\}$$

est *l'ensemble quotient*. Les éléments de $X/\equiv$ sont des sous-ensembles de X est deux éléments distincts de $X/\equiv$ sont des sous-ensembles disjoint de X.

Exemples 6.2.9. (a) L'égalité est une relation d'équivalence sur un ensemble X. Alors l'ensemble quotient est $\{\{x\} : x \in X\}$ et il est en correspondance bijective avec X.

(b) Soit X un ensemble. On définit une relation d'équivalence par $x \equiv y$ pour tous choix de $x, y \in X$. Alors $(X/\equiv) = \{X\}$ a seulement un élément.

(c) Sur $\mathbb{R}$, on a la relation d'équivalence définie par

$$x \equiv y \iff x^2 = y^2.$$

Pour tout $x \in X$, $\bar{x} = \{x, -x\}$. Il y a une bijection entre $\mathbb{R}/\equiv$ est $\mathbb{R}^{\geq 0}$ définie par $\bar{r} \mapsto |r|$.

(d) Soit $n > 0$ un nombre naturel. Sur $\mathbb{Z}$, on définit une relation d'équivalence $\equiv_n$ par

$$x \equiv_n y \iff n \text{ divise } x - y.$$

Alors pour tout $i \in \mathbb{Z}$, $\bar{i} = n\mathbb{Z} + i = n\mathbb{Z} + j$ où $j \in \{0, 1, \ldots, n-1\}$ est le reste quand on divise i par n. Donc

$$\mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

et $|\,\mathbb{Z}/\equiv_n\,| = n$.

(e) Sur $\mathbb{R}$, on définit la relation d'équivalence $\equiv$ par

$$x \equiv y \iff x - y \in \mathbb{Z}.$$

Alors pour chaque $r \in \mathbb{R}$, $\bar{r} = r + \mathbb{Z} = s + \mathbb{Z}$ pour un unique $s \in [0, 1)$. Donc $\mathbb{R}/\equiv$ est en correspondance bijective avec l'intervalle $[0, 1)$.

(f) Sur $\mathbb{R}$, on définit la relation d'équivalence $\equiv$ par

$$x \equiv y \iff x - y \in \mathbb{Q}.$$

Alors pour chaque $r \in \mathbb{R}$, $\bar{r} = r + \mathbb{Q}$. Dans ce cas, on ne peut pas trouver en ensemble bien connu qui est en correspondance bijective avec $\mathbb{R}/\equiv$ (mais il existe un tel ensemble – on va le voir plus tard).

(g) Soient X et Y deux ensembles et $a \in X$. On peut définir la relation d'équivalence $\equiv_a$ sur $\mathrm{Fonc}(X, Y)$ par

$$f \equiv_a g \iff f(a) = g(a).$$

Pour $f \in \mathrm{Fonc}(X, Y)$,

$$\bar{f} = \{g \in \mathrm{Fonc}(X, Y) : f(a) = g(a)\}.$$

Il y a une bijection entre $\mathrm{Fonc}(X, Y)/\equiv$ est Y définie par $\bar{f} \mapsto f(a)$. Il existe aussi une bijection entre $\mathrm{Fonc}(X, Y)/\equiv$ et l'ensemble des fonctions constantes de X sur Y.

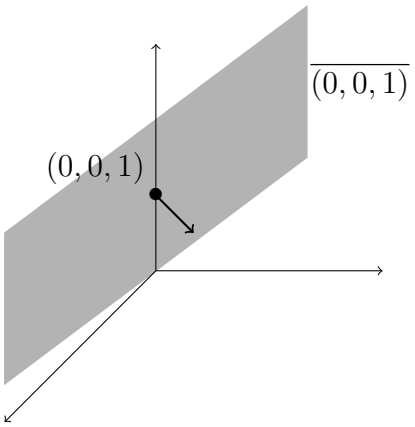
(h) Sur $X := \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$, on peut définir une relation d'équivalence $\equiv$ par

$$(x, y, z) \equiv (x_1, y_1, z_1) \iff 2(x - x_1) + 3(y - y_1) - (z - z_1) = 0.$$

Alors

$$\overline{(x, y, z)} = \{(x_1, y_1, z_1) : 2x + 3y - z = 2x_1 + 3y_1 - z_1\}.$$

Les classes d'équivalences sont des plans. En particulier, la classe d'équivalence $\overline{(x, y, z)}$ est le plan avec vecteur normal $(2, 3, -1)$ qui contient le point (x, y, z).

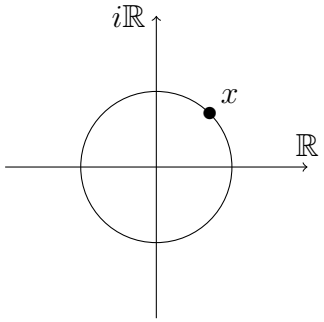


Il y a une correspondance bijective entre $\mathbb{R}^3/\equiv$ et $\mathbb{R}^2$ définie par $(x,y,z)\mapsto(x,y)$ (il existe des autres aussi).

(i) Sur $\mathbb{C}$, on a la relation d'équivalence définie par

$$x \equiv y \iff |x| = |y|.$$

Alors, la classe d'équivalence de $x \in \mathbb{C}$ est $[x] = \{y \in \mathbb{C} : |x| = |y|\}$ et il y a une correspondance bijective entre $\mathbb{C}/\equiv$ et $\mathbb{R}^{\geq 0}$ donné par $[x] \mapsto |x|$. La classe d'équivalence qui corresponde à $|x|$ est le cercle de centre 0 et rayon $|x|$.



Surjection canonique. Si $\equiv$ est une relation d'équivalence sur l'ensemble X, alors la fonction de X vers $X/\equiv$ définie par $x \mapsto \bar{x}$ est appelée la *surjection canonique* de X vers $X/\equiv$. Souvent, on note la surjection canonique par π. Donc, pour tout $x \in Z$, $\pi(x) = \bar{x} = \{y \in X : x \equiv y\} \in X/\equiv$.

Fonction induite. Soit X un ensemble et $\equiv$ une relation d'équivalence sur X. Soit Y un ensemble et soit $f\colon X \to Y$ une fonction tel que pour tous choix de $x, y \in X$, si $x \equiv y$, alors $f(x) = f(y)$. Alors la fonction $f\colon X \to Y$ induit une fonction $\tilde{f}\colon X/\equiv \to Y$ définie par $\tilde{f}(\bar{x}) = f(x)$.

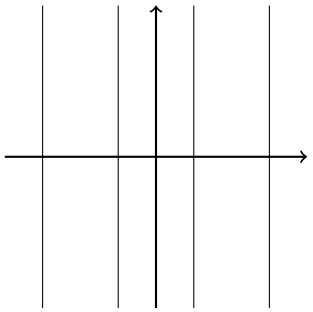
Exemple 6.2.10. Soit $X = \mathbb{R}^2$, $Y = \mathbb{R}$ et $f\colon X \to Y$ une fonction définie par $f((x,y)) = 2x$. Soit $\equiv$ la relation d'équivalence sur X définie par

$$(x,y) \equiv (x',y') \iff x = x'.$$

Alors

$$(x,y) \equiv (x',y') \implies x = x' \implies f((x,y)) = 2x = 2x' = f((x',y'))$$

est donc f induit une fonction $\tilde{f}\colon X/\equiv \to Y$ définie par $f\big(\overline{(x,y)}\big) = 2x$. Remarquez que les éléments de $X/\equiv$ sont les lignes verticales dans $\mathbb{R}^2$ (c.-à-d. les lignes parallèles à l'axe y).



Exercices.

6.2.1. Soit $X = \mathbb{R}$ (ou $\mathbb{C}$). Montrez que

$$x \equiv y \iff \exists_{r\in X\setminus\{0\}}\, x = ry$$

définit une relation d'équivalence sur X. Combien de classes d'équivalence y a-t-il ?

6.2.2. Soit X un ensemble.

(a) Pour $i \in I$ (où I est un ensemble d'indices), soit R_i une relation d'équivalence sur X. Donc $R_i \subseteq X \times X$ pour chaque $i \in I$. Montrez que $\bigcap_{i\in I} R_i$ est une relation d'équivalence.

(b) Concluez que pour toute relation R sur X, il existe une relation d'équivalence S minimum qui contient R (c.-à-d. S est un relation d'équivalence qui contient R et qui est contenue dans toute relation d'équivalence qui contient R). Cette relation d'équivalence est appelée la relation d'équivalence *engendrée* par R. *Indice :* Considérez l'intersection de toutes les relations d'équivalence qui contiennent R.

(c) Soit $X = \bigcup_{n\in\mathbb{N}}\{(x,y) \in \mathbb{R}^2 : 2n+1 \le x^2+y^2 \le 2n+2\}$. On définit R sur X par : Pour tous choix de $A, B \in X$, $A\,R\,B$ si et seulement si le segment de ligne AB est dans X. Montrez que cela n'est pas une relation d'équivalence. Trouvez la relation d'équivalence engendrée par cette relation. Trouvez son ensemble des classes d'équivalence.

6.2.3. Soit X l'ensemble des fonctions de $\mathbb{R}$ vers $\mathbb{R}$. Soit $a \in \mathbb{R}$. Définissez la relation suivante sur X : $f \equiv g$ si et seulement s'il existe un $\varepsilon > 0$ tel que $f(x) = g(x)$ pour tout $x \in (a-\varepsilon, a+\varepsilon)$. Montrez que c'est une relation d'équivalence. Montrez que les fonctions données par deux polynômes distincts ne sont pas équivalents.

6.2.4. Soit X un ensemble. Pour deux ensembles A et B de X, définissez

$$A \equiv B \iff \text{il existe un bijection } f\colon A \to B.$$

Montrez que c'est une relation d'équivalence sur $\wp(X)$.

6.2.5. Soit X un ensemble. Pour deux sous-ensembles A et B de X définissez

$$A \equiv B \iff A\Delta B \text{ est fini.}$$

(a) Montrez que c'est une relation d'équivalence sur $\wp(X)$.

(b) Montrez que $\wp(X)/\equiv$ a seulement un élément si X est fini.

(c) Réciproquement, montrez que si $\wp(X)/\equiv$ a seulement un élément, alors X est fini.

(d) Montrez que $\wp(\mathbb{N})/\equiv$ est infini.

Supposons que $A, B, A_1, B_1 \subseteq X$ tel que $A \equiv A_1$ et $B \equiv B_1$. Montrez que :

(e) $A \cap B \equiv A_1 \cap B_1$.

(f) $A \cup B \equiv A_1 \cup B_1$.

(g) $A^c \equiv A_1^c$.

(h) $A \setminus B \equiv A_1 \setminus B_1$.

(i) $A\Delta B \equiv A_1\Delta B_1$.

6.3 Les ordres partiels

Définition 6.3.1. Soit X un ensemble.

(a) Un *ordre partiel* sur X est une relation binaire "$\leq$" qui satisfait

i. **(réflexivité)** $\forall_{x\in X}\,(x \leq x)$,

ii. **(transitivité)** $\forall_{x,y,z\in X}\,[(x \leq y \wedge y \leq z) \Rightarrow x \leq z]$,

iii. **(antisymétrie)** $\forall_{x,y\in X}\,[(x \leq y \wedge y \leq x) \Rightarrow x = y]$.

On utilise les symboles $\leq, \preceq, \subseteq, \trianglelefteq$ pour les ordres partiels.

(b) Un *ordre partiel strict* sur X est une relation binaire "$<$" sur X qui satisfait

i. **(transitivité)** $\forall_{x,y,z\in X}\,[(x < y \wedge y < z) \Rightarrow x < z]$,

ii. $\nexists_{x,y\in X}\,(x < y \wedge y < x)$.

On utilise les symboles $<, \prec, \subset, \triangleleft$ pour les ordres partiels stricts.

Un *ensemble (partiellement) ordonné* est une paire $(X, \leq)$ où X est un ensemble et $\leq$ est un ordre partiel sur X.

Lemme 6.3.2. *Soit X un ensemble. Une relation $<$ sur X est un ordre partiel strict si et seulement si elle est irréflexive et transitive.*

Preuve. Soit $<$ un ordre partiel strict sur X. Alors $<$ est transitive par définition. Supposons que $<$ n'est pas irréflexive. Alors il existe $x \in X$ tel que $x < x$. Mais cela contredit la deuxième propriété dans la définition d'un ordre partiel strict (avec $x = y$). Donc $<$ doit être irréflexive.

Supposons que $<$ est une relation irréflexive et transitive sur X. Pour montrer que $<$ est un ordre partiel strict, on doit seulement montrer que $<$ satisfait la deuxième propriété dans la définition. Supposons qu'il existe $x, y \in X$ tel que $x < y$ et $y < x$. Par transitivité, on a $x < x$ qui est une contradiction parce que $<$ est irréflexive. □

Exemples 6.3.3. (a) La relation $<$ ("inférieur à") est un ordre partiel strict sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(b) La relation $\leq$ ("inférieur ou égal à") est un ordre partiel sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(c) Soit X un ensemble. L'inclusion $\subseteq$ est un ordre partiel sur $\wp(X)$ et $\subsetneq$ est un ordre partiel strict sur $\wp(X)$.

(d) Sur $\mathbb{Z}$ définissons

$$x \prec y \iff y < x.$$

Alors $\prec$ est un ordre partiel strict. En général, l'inverse d'un ordre partiel (strict) est un ordre partiel (strict).

(e) Sur $\mathbb{R}$, la relation

$$x \prec y \iff |x| < |y|$$

est un ordre partiel strict.

(f) Sur $\mathbb{N}^+$, la relation

$$x \preceq y \iff x \text{ divise } y \iff \exists_{z \in \mathbb{Z}} (y = xz)$$

est un ordre partiel. Remarquez que ce n'est pas un ordre partiel sur $\mathbb{Z}$ (parce que, par exemple, on a $-2 \preceq 2$ et $2 \preceq -2$).

Rappelons-nous que les relations sur X sont des sous-ensembles de $X \times X$. Donc, une relation R peut contient une autre relation S. Puisque les ordres sont des relations, un ordre peut contient un autre. Remarquez que l'égalité est contenu dans tout ordre partiel (à cause de réflexivité). Donc, l'égalité est le "plus petit" ordre partiel sur un ensemble. Remarquez aussi que la relation vide et un ordre partiel strict sur tout ensemble X (exercice). Donc, la relation vide est le "plus petit" ordre partiel strict.

Lemme 6.3.4. *(a) Si $\leq$ est un ordre partiel sur X et si on définit $<$ par*

$$x < y \iff x \leq y \text{ et } x \neq y,$$

alors $<$ est un ordre partiel strict sur X.

(b) Réciproquement, si $<$ est un ordre partiel strict sur X et si on définit $\leq$ par

$$x \leq y \iff x < y \text{ ou } x = y,$$

alors $\leq$ est un ordre partiel sur X.

Preuve.

(a) Supposons que $\leq$ est un ordre partiel sur X et définissons $<$ comme ci-dessus. On doit montrer que $<$ est transitive et irréflexive.

i. *Transitive.* Soient $x, y, z \in X$ tels que $x < y$ et $y < z$. Par définition, on a $x \leq y$ et $y \leq z$. Puisque $\leq$ est transitive, $x \leq z$. Supposons que $x = z$. Alors, par la réflexivité de $\leq$, $z \leq x$. Donc, par la transitivité de $\leq$ (et le fait que $x \leq y$), $z \leq y$. Donc on a $y \leq z$ et $z \leq y$. Par l'antisymétrie de $\leq$, on a $z = y$ qui contredit le fait que $y < z$. Donc $x \neq z$ et puis $x < z$.

ii. *Irréflexive.* La relation $<$ est irréflexive par définition : pout tout $x \in X$, $x \not< x$ parce que $x = x$.

(b) Supposons que $<$ est un ordre partiel strict sur X et définissons $\leq$ comme ci-dessus. On doit montrer que $\leq$ est réflexive, transitive, et antisymétrique.

i. *Réflexive.* La relation $\leq$ est réflexive par définition : $x \leq x$ parce que $x = x$.

ii. *Transitive.* Soient $x, y, z \in X$ tels que $x \leq y$ et $y \leq z$. Il y a quatre cas :

(1) $x = y$ et $y = z$. Alors $x = z$ et donc $x \leq z$.

(2) $x = y$ et $y < z$. Alors $x < z$ et donc $x \leq z$.

(3) $x < y$ et $y = z$. Alors $x < z$ et donc $x \leq z$.

(4) $x < y$ et $y < z$. Alors $x < z$ par la transitivité de $<$ et donc $x \leq z$.

iii. *Antisymétrique.* On prouve que $\leq$ est antisymétrique par contradiction. Soient $x, y \in X$ tels que $x \leq y$, $y \leq x$ et $x \neq y$. Donc $x < y$ et $y < x$. Mais cela contredit la deuxième propriété dans la définition d'un ordre partiel strict.

□

Lemme 6.3.4 nous montre qu'il y a une correspondance entre les ordres partiels et les ordres partiels stricts. On peut changer entre les deux lorsqu'on veut.

Définition 6.3.5. Soit $(X, \leq)$ un ensemble partiellement ordonné.

(a) Un *élément maximum* de $(X, \leq)$ est un $x_0 \in X$ satisfaisant $\forall_{x \in X}\, (x \leq x_0)$.

(b) Un *élément maximal* de $(X, \leq)$ est un $x_0 \in X$ satisfaisant $\nexists_{x \in X}\, (x_0 < x)$.

(c) Un *élément minimum* de $(X, \leq)$ est un $x_0 \in X$ satisfaisant $\forall_{x \in X}\, (x_0 \leq x)$.

(d) Un *élément minimal* de $(X, \leq)$ est un $x_0 \in X$ satisfaisant $\nexists_{x \in X}\, (x < x_0)$.

Exemple 6.3.6. Soit $A = \{1, 2, 3\}$ et soit $X_1 = \wp(A)$. Alors $\subseteq$ est un ordre partiel sur X_1, donc $(X_1, \subseteq)$ est un ensemble partiellement ordonné. L'élément A de X_1 est élément maximum (et maximal) de $(X_1, \subseteq)$. Soit aussi

$$X_2 = X_1 \setminus \{A\} = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

Alors $\subseteq$ est un ordre partiel sur X_2, donc $(X_2, \subseteq)$ est un ensemble partiellement ordonné. On voit que $(X_2, \subseteq)$ n'a aucun élément maximum. Cependant, $(X_2, \subseteq)$ possède trois éléments maximaux : $\{1, 2\}$, $\{1, 3\}$ et $\{2, 3\}$.

Exemple 6.3.7. Soit $X = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Alors

$$(x_1, y_1) \prec (x_2, y_2) \iff x_1 < x_2$$

définit un ordre partiel strict sur X. Donc

$$(x_1, y_1) \preceq (x_2, y_2) \iff [x_1 < x_2 \ \vee \ (x_1, y_1) = (x_2, y_2)]$$

définit un ordre partiel sur X. On voit que X n'a pas d'élément maximum, maximal, minimum ou minimal. Soit

$$Y = \{(-1, 5), (0, 0), (0, 1), (0, 3), (1, 3), (2, -3), (2, 0), (2, 4)\} \subseteq X.$$

Alors $\preceq$ induit un ordre sur Y. L'élément $(-1, 5)$ est un élément minimum et minimal. L'ensemble Y n'a aucun élément maximum mais il a trois éléments maximaux : $(2, -3)$, $(2, 0)$ et $(2, 4)$.

Important : On a vu qu'un ensemble partiellement ordonné peut avoir plusieurs éléments maximaux (ou minimaux), ou en avoir un seul, on n'en avoir aucun.

Lemme 6.3.8. *Si un ensemble partiellement ordonné possède un élément maximum (resp. minimum), alors cet élément est unique, est maximal (resp. minimal), et est en fait le seul élément maximal (resp. minimal).*

Preuve. On prouve seulement le lemme pour les éléments maximum/maximal. Le résultat pour les élément minimum/minimal est analogue. Supposons que $(X, \leq)$ est un ensemble partiellement ordonné et x_0 est un élément maximum. On prouve premièrement que x_0 est l'unique élément maximum. Supposons que x_0' est maximum. Alors $x_0 \leq x_0'$ (parce que x_0' est maximum) et $x_0 \leq x_0'$ (parce que x_0 est maximum). Alors, par l'antisymétrie de $\leq$, on a $x_0 = x_0'$. Donc x_0 est l'unique élément maximum.

Maintenant on prouve que x_0 est maximal. Puisque x_0 est maximum, pour chaque élément $x \in X$, on a $x \leq x_0$. Supposons qu'il existe $x \in X$ tel que $x_0 < x$. Alors $x_0 \leq x$ et donc, par l'antisymétrie de $\leq$, on a $x = x_0$. Mais cela contredit le fait que $x_0 \neq x$ (parce que $x_0 < x$. Donc x_0 est maximal.

Finalement, on prouve que x_0 est l'unique élément maximal. Supposons que $y \in X$ tel que $y \neq x_0$. Puisque x_0 est maximum, on a $y \leq x_0$ et donc $y < x_0$ parce que $y \neq x_0$. Par conséquent, y n'est pas maximal. Donc x_0 est l'unique élément maximal. □

En particulier remarquez qu'un élément maximum est nécessairement maximal, mas que la réciproque n'est pas vraie.

Définition 6.3.9. Soit $(X, \leq)$ un ensemble partiellement ordonné. Deux éléments $x, y \in X$ sont *comparable* s'ils satisfont $x \leq y$ ou $y \leq x$.

Exemple 6.3.10. Considérez $(X_2, \subseteq)$ comme dans Exemple 6.3.6, et soient $x = \{1, 2\}$, $y = \{1, 3\}$ et $z = \{1\}$. Alors $x \not\subseteq y$ et $y \not\subseteq x$, donc les éléments x et y de X_2 ne sont pas comparables. Cependant $z \subseteq x$ et donc x et z sont comparables.

Notation. Si $(X, \leq)$ est un ensemble partiellement ordonné, et $x, y \in X$, $x \geq y$ signifie $y \leq x$ et $x > y$ signifie $y < x$.

Définition 6.3.11. Un ensemble partiellement ordonné $(X, \leq)$ qui satisfait

$$\forall_{x,y \in X} \, (x \leq y \ \vee \ x \geq y)$$

est appelé *totalement ordonné* ou *linéairement ordonné* est $\leq$ est appelé un *ordre total*.

Exemple 6.3.12. $(\mathbb{R}, \leq)$ est totalement ordonné, mais $(\wp(\mathbb{R}), \subseteq)$ n'est pas totalement ordonné. (*Remarque :* Ici nous trichons. Nous n'avons défini ni $\mathbb{R}$ ni sa relation d'ordre, donc nous ne devrions pas en parler. Nous allons continuer à tricher, parce que cela nous permet de donner des exemples intéressants.)

Soit $(X, \leq)$ un ensemble partiellement ordonné et soit $A \subseteq X$. Alors la restriction de $\leq$ à A (c.-à-d. $\leq \cap (A \times A)$) est un ordre partiel sur A, donc $(A, \leq)$ est un ensemble partiellement ordonné. Il se peut que $(A, \leq)$ ait un élément minimum, comme il se peut qu'il n'en ait pas. Remarquez qu'un élément minimum de $(A, \leq)$, s'il existe, est un x_0 qui satisfait

$$x_0 \in A \quad \text{et} \quad \forall_{x \in A} \, (x_0 \leq x).$$

S'il existe un x_0 qui satisfait ces propriétés, on écrit $x_0 = \min(A)$.

Définition 6.3.13. Si $(X, \leq)$ est un ensemble partiellement ordonné qui satisfait

tout sous-ensemble non vide de X possède un élément minimum,

on dit que $(X, \leq)$ est *bien ordonné* et on dit que $\leq$ est un *bon ordre*.

Exemples 6.3.14. (a) Soit $X = \{0, 1, 2\}$ et soit $\leq$ la relation "inférieur ou égal à". Alors $(X, \leq)$ est bien ordonné parce que tout sous-ensemble non vide de X possède un élément minimum comme on peut voir dans la table suivante.

Sous-ensemble	Minimum
{0}	0
{1}	1
{2}	2
{0,1}	0
{0,2}	0
{1,2}	1
{1,2,3}	1

(b) On va voir que $(\mathbb{N}, \leq)$ est bien ordonné.

(c) $(\mathbb{R}, \leq)$ n'est pas bien ordonné. Par exemple $(0, 1)$ est un sous-ensemble de $\mathbb{R}$ qui n'a aucun élément minimum.

Proposition 6.3.15. *Tout ensemble bien ordonné est totalement ordonné.*

Preuve. Soit $(X, \leq)$ un ensemble bien ordonné. On doit monter $\forall_{x,y \in X} \, (x \leq y \ \vee \ y \leq x)$. Soient $x, y \in X$. Alors $\{x, y\}$ est un sous-ensemble non vide de X. Puisque $(X, \leq)$ est bien ordonné, ce sous-ensemble a un élément minimum qui doit être x ou y. Si x est minium, alors $x \leq y$. Si y est minimum, alors $y \leq x$. □

Remarquez qu'il existe des ensembles totalement ordonné qui ne sont pas bien ordonné (par exemple $(\mathbb{R}, \leq)$).

Définition 6.3.16. Soit $(X, \leq)$ un ensemble partiellement ordonné et $A \subseteq X$.

(a) $x \in X$ est un *minorant* de A si $\forall_{a \in A} \, x \leq a$.

(b) $x \in X$ est un *majorant* de A si $\forall_{a \in A} \, a \leq x$.

Si A possède un majorant (resp. minorant), alors on dit que A est une *partie majorée* (resp. *partie minorée*). Remarquez que un minorant/majorant de $A \subseteq X$ n'est pas nécessairement un élément de A.

(c) x est un *infimum* (ou *plus grande limite inférieure*) de A si
- x est un minorant de $A : \forall_{a\in A}\, x \leq a$, et
- x est plus grand que ou égal à tous les minorants de $A : \forall_{y\in X}[(\forall_{a\in A}\, y \leq a) \Rightarrow (y \leq x)]$.

On écrit $x = \inf A$.

(d) x est un *supremum* (ou *plus petite limite supérieure*) de A si
- x est un majorant de $A : \forall_{a\in A}\, a \leq x$, et
- x est plus petit que ou égal à tous les majorants de $A : \forall_{y\in X}[(\forall_{a\in A}\, a \leq y) \Rightarrow (x \leq y)]$.

On écrit $x = \sup A$.

Exemples 6.3.17. (a) $(\mathbb{R}, \leq)$ est un ensemble partiellement ordonné et $A = (0, 1) \subseteq \mathbb{R}$. Un élément $x \in \mathbb{R}$ est un minorant de A si et seulement si $x \leq 0$. Donc $x = 0$ est l'infimum de A. Un élément $x \in \mathbb{R}$ est un majorant de A si et seulement si $x \geq 1$. Donc $x = 1$ est le supremum de A.

(b) Soit $A = \{1/n : n \in \mathbb{N}\}$. Comme un sous-ensemble de $\mathbb{R}$, l'infimum de A est 0 est le supremum est 1. Comme un sous-ensemble de $\mathbb{R}_{>0}$, le supremeum de A est 1 est A n'a pas d'infimum.

(c) Comme un sous-ensemble de $\mathbb{R}$, l'ensemble $\mathbb{Z}$ n'a ni un infimum ni un supremum.

Exercices.

6.3.1. Soient $(X, \leq)$ et $(Y, \leq)$ deux ensembles partiellement ordonnés. On définit une relation $\preceq$ sur l'ensemble $X \times Y$ par la condition suivante : étant donnés $(x, y), (x', y') \in X \times Y$,

$$(x, y) \preceq (x', y') \iff [x < x' \ \vee \ (x = x' \ \wedge \ y \leq y')].$$

(a) Montrez que $\preceq$ est un ordre partiel sur $X \times Y$. (On l'appelle *l'ordre lexicographique*.)

(b) Montrez que si $(X, \leq)$ et $(Y, \leq)$ sont totalement ordonnés, alors $(X \times Y, \preceq)$ est totalement ordonné.

(c) Montrez que si $(X, \leq)$ et $(Y, \leq)$ sont bien ordonnés, alors $(X \times Y, \preceq)$ est bien ordonné.

6.3.2. Soit $<$ un ordre partiel strict sur un ensemble Y. Soit $f\colon X \to Y$ une fonction. Montrez que la relation $<$ sur X défini par

$$x_1 < x_2 \iff f(x_1) < f(x_2)$$

est un ordre partiel strict sur X.

6.3.3. Soit $<$ un ordre partiel strict sur un ensemble Y. Soient X un ensemble et $A \subseteq X$. Montrez que

$$f < g \iff \forall_{a\in A}\, [f(a) < g(a)]$$

définit un ordre partiel strict sur $\mathrm{Fonc}(X, Y)$.

6.3.4. Trouvez le supremum et infimum (s'ils existent) des ensemble suivants :

(a) $\{x \in \mathbb{R} : x^2 + x - 1 < 0\}$,

(b) $\{x \in \mathbb{R} : x^2 + x - 1 > 0\}$,

(c) $\{\frac{1}{n} + (-1)^n : n \in \mathbb{N},\ n > 0\}$,

(d) $\{\frac{1}{1-x} : x \in \mathbb{R},\ x > 1\}$,

(e) $\{\frac{1}{1-x} : x \in \mathbb{R},\ x < 1\}$.

6.3.5. Supposons que x_0 est un élément maximal de l'ensemble totalement ordonné $(X, \leq)$. Montrez que x_0 est un élément maximum de $(X, \leq)$.

6.3.6. Soit A une partie de $\mathbb{R}$. Si chaque partie non vide de A possède un élément minimum (sous la relation d'ordre $\leq$ de $\mathbb{R}$), alors on dit que A est une *partie bien ordonnée* de $\mathbb{R}$. On définit

$$\mathcal{B}(\mathbb{R}) = \{A \in \wp(\mathbb{R}) : A \text{ est une partie bien ordonnée de } \mathbb{R}\}.$$

Remarquez que $\mathcal{B}(\mathbb{R}) \subseteq \wp(\mathbb{R})$. Par exemple on a $\mathbb{N} \in \mathcal{B}(\mathbb{R})$, mais $\mathbb{R} \notin \mathcal{B}(\mathbb{R})$.

(a) Montrez que si $A, B \in \mathcal{B}(\mathbb{R})$, alors $A \cup B \in \mathcal{B}(\mathbb{R})$.

(b) Supposons que $\{A_i\}_{i \in I}$ est une famille de parties bien ordonnées de $\mathbb{R}$, c'est à dire que $\forall_{i \in I} [\, A_i \in \mathcal{B}(\mathbb{R}) \,]$. S'ensuit-il nécessairement que $\bigcup_{i \in I} A_i \in \mathcal{B}(\mathbb{R})$? Si oui, donnez une preuve ; si non, donnez un contre-example.

(c) Montrez qui si $A \in \mathcal{B}(\mathbb{R})$ alors toute partie de A est élément de $\mathcal{B}(\mathbb{R})$.

Chapitre 7

L'induction

Dans ce chapitre on discute le principe d'induction transfinie et les deux cas particuliers, l'induction simple et l'induction forte.

7.1 L'induction transfinie

Si $(X, \leq)$ est un ensemble partiellement ordonné et $a \in X$, on définit

$$(-\infty, a) = \{x \in X : x < a\}.$$

Théorème 7.1.1. *Soit $(X, \leq)$ un ensemble bien ordonné. Supposons que S est une partie de X ($S \subseteq X$) qui satisfait*

$$\forall_{a \in X} \left[(-\infty, a) \subseteq S \implies a \in S\right]. \tag{7.1}$$

Alors $S = X$.

Preuve. Supposons que S satisfait (7.1) et montrons que $S = X$. Par contradiction, supposons que $S \neq X$. Alors $X \setminus S$ est une partie non vide de X, donc possède un élément minimum : il existe $a \in X \setminus S$ tel que $\forall_{x \in X \setminus S} (a \leq x)$. On a alors $(-\infty, a) \subseteq S$. Puisque S satisfait (7.1), il s'ensuit que $a \in S$, ce qui contredit $a \in X \setminus S$. □

Le théorème ci-dessus est appelé le *principe d'induction transfinie*. C'est un principe d'induction valide dans n'importe quel ensemble bien ordonné. On peut le reformuler de la manière suivante :

Corollaire 7.1.2. *Soit $(X, \leq)$ un ensemble bien ordonné et soit $P(x)$ une condition sur x. Supposons que pour chaque $a \in X$, l'implication suivante est vraie :*

$$\textit{Si } P(x) \textit{ est vraie pour tout } x \in (-\infty, a), \textit{ alors } P(a) \textit{ est vraie.} \tag{7.2}$$

Alors $\forall_{x \in X} P(x)$.

Preuve. Supposons que (7.2) est vraie pour chaque $a \in X$. Alors l'ensemble

$$S = \{x \in X : P(x)\}$$

est une partie de X qui satisfait (7.1), donc le Théorème 7.1.1 implique que $S = X$, donc $\forall_{x\in X} P(x)$. □

Remarque 7.1.3. Supposons que $(X, \leq)$ est un ensemble bien ordonné et que $X \neq \varnothing$. Remarquez que X possède un élément minimum ; soit $a_0 = \min(X)$. Si vous voulez utiliser Corollaire 7.1.2 pour démontrer que $\forall_{x\in X} P(x)$, vous devez vérifier que chaque $a \in X$ satisfait (7.2), donc en particulier vous devez montrer que a_0 satisfait (7.2), ce qui revient à montrer que $P(a_0)$ est vraie (en effet, a_0 satisfait (7.2) $\iff$ $P(a_0)$ est vraie, montrez ceci en exercice). Autrement dit, la vérification que chaque $a \in X$ satisfait (7.2) peut se diviser en deux parties :

(a) montrer que $P(a_0)$ est vraie,

(b) montrer que chaque $a \in X \setminus \{a_0\}$ satisfait (7.2).

7.2 L'induction

Puisque $\mathbb{N}$ est un ensemble bien ordonné, on peut appliquer le principe d'induction transfinie avec $X = \mathbb{N}$ dans Théorème 7.1.1. Si on veut démontrer la proposition

$$\phi(n) \text{ pour tout } n \in \mathbb{N}$$

on peut faire ce qui suit :

(a) On montre que $\phi(n)$ est vraie pour $n = 0$ (c.-à-d. on montre $\phi(0)$).

(b) On montre $\forall_{n\in\mathbb{N}} (P(n) \Rightarrow P(n+1))$ (*l'induction simple*).

ou

On montre $\forall_{n\in\mathbb{N}} [(\forall_{k\leq n} P(k)) \Rightarrow P(n+1)]$ (*l'induction forte*).

Exemple 7.2.1. Montrons que pour tout $n \in \mathbb{N}$,

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Soit $\phi(n)$ la proposition

$$\text{“ } 0 + 1 + 2 + \cdots + n = \tfrac{n(n+1)}{2}. \text{ ”}$$

(a) $\phi(0)$ **est vraie.** Puisque la somme des nombre naturels de 0 à 0 est $0 = 0(0+1)/2$, on voit que $\phi(0)$ est vraie.

(b) **Si** $\phi(n)$ **est vraie, alors** $\phi(n+1)$ **est vraie.** Supposons que $\phi(n)$ est vraie. Donc

$$0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Par conséquent,

$$0 + 1 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Donc $\phi(x)$ est vraie pour tout $x \in \mathbb{N}$.

Exemple 7.2.2. Montrons que tout nombre naturel plus grand que 1 est un produit de nombres premiers. Donc on veut montrer que

$$P(n) = \text{“}n \text{ est un produit de nombres premiers”}$$

est vraie pour tout entier $n > 1$.

On sait que 2 est un nombre premier (et donc un produit de nombres premiers). Donc $P(2)$ est vraie. Supposons que $P(k)$ est vraie pout tout k tel que $1 \leq k < n$. C'est-à-dire, chaque nombre naturel plus grand que 1 et plus petit que n est un produit de nombres premiers. On veut montrer que n est un produit de nombres premiers. Si n est premier, on a finit. Sinon, $n = ab$ pour $a, b \in \mathbb{N}$ tels que $a, b > 1$ (par la définition d'un nombre premier). Il s'ensuit que $a, b < n$. Par supposition, a et b sont produits de nombres premiers. Par conséquent, $n = ab$ est un produit de nombres premiers. On a montré que

$$[\forall_{1 \leq k < n} P(k)] \implies P(n)$$

et donc on a montrer $\forall_{n>1} P(n)$ par l'induction forte.

Remarquez que dans Exemple 7.2.2 on a utilisé vraiment l'induction avec l'ensemble $\mathbb{N}_{\geq 2} = \{n \in \mathbb{N} : n \geq 2\}$ qui est bien ordonné.

Exemple 7.2.3. Soient $t_1 = 2$, $t_2 = 4$, et $t_3 = 8$, et, pour $n \geq 1$, définissons $t_{n+3} = t_{n+2} + t_{n+1} + 2t_n$. Démontrons que $t_n = 2^n$ pour tout entier $n \geq 1$.

On le prouve par induction forte. Puisque

$$t_1 = 2 = 2^1, \quad t_2 = 4 = 2^2, \quad t_3 = 8 = 2^3,$$

on a $t_n = 2^n$ pour $n = 1, 2, 3$. Soit $n \geq 4$ un entier. On suppose que $t_k = 2^k$ pour $k < n$. Donc

$$\begin{aligned} t_n &= t_{n-1} + t_{n-2} + 2t_{n-3} \\ &= 2^{n-1} + 2^{n-2} + 2 \cdot 2^{n-3} \\ &= 2^{n-1} + 2^{n-2} + 2^{n-2} \\ &= 2^{n-1} + 2 \cdot 2^{n-2} \\ &= 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n. \end{aligned}$$

Par conséquent, on a prouvé $\forall_{n \in \mathbb{N}_+} (t_n = 2^n)$ par induction forte. Remarquez qu'on a dû prouver les premier trois cas de base puisque notre étape inductive fonctionne seulement pour $n \geq 4$ (puisque il faut que $n - 3 \geq 1$).

Exercices.

7.2.1. Montrez que si $0 < x < 1$ et $n > 0$ est un nombre naturel, alors

$$(1-x)^n \leq 1 - nx + \frac{n(n-1)}{2}x^2.$$

7.2.2. Montrez que $n! > 2^n$ pour tous n suffisamment grands. C'est-à-dire, montrez qu'il existe un $N \in \mathbb{N}$ tel que $n! > 2^n$ pour tout $n \geq N$.

7.2.3. Montrez que $(x-1)^n \geq x^n - nx^{n-1}$ pour tous choix de $n \in \mathbb{N}$ et $x > 1$.

7.2.4. Montrez que pour tout $n \in \mathbb{N}^+$, $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

7.2.5. Montrez que pour tout $n \in \mathbb{N}^+$, $1^4 + 2^4 + \cdots + n^4 = \frac{n(n+1)(6n^3+9n^2+n-1)}{30}$.

7.2.6. On définit la *suite de Finonacci* par $F_1 = F_2 = 1$ et

$$F_n = F_{n-1} + F_{n-2} \quad \text{pour} \quad n \geq 3.$$

Soient

$$\phi_+ = \frac{1+\sqrt{5}}{2}, \quad \phi_- = \frac{1-\sqrt{5}}{2}.$$

Montrez que

$$F_n = \frac{(\phi_+)^n - (\phi_-)^n}{\phi_+ - \phi_-} = \frac{(\phi_+)^n - (\phi_-)^n}{\sqrt{5}}.$$

Chapitre 8

La théorie axiomatique des ensembles

Dans ce chapitre, on parle brièvement de la théorie axiomatique des ensembles. Ce chapitre est basé sur les notes [Dai] de Daniel Daigle et plus de détails peuvent être trouvés là.

8.1 La théorie des ensembles de Cantor et le paradoxe de Russell

George Cantor (1845–1918) est considéré comme l'inventeur de la théorie des ensembles. La théorie de Cantor reposait sur deux principes, que nous avons accepté.

I. Deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments.

II. Étant donnée une condition P, il existe un et un seul ensemble dont les éléments sont précisément tous les objets qui satisfont P.

En 1901, Bertrand Russell a trouvé le paradoxe suivant :

Paradoxe de Russell. Soit P la propriété

$$P(X) = \text{“}X \text{ est un ensemble et } X \notin X\text{”}$$

D'après le Principe II ci-dessus, l'ensemble

$$R = \{X : P(X)\} = \{X : X \text{ est un ensemble et } X \notin X\}$$

existe. En particulier, R est l'ensemble de tous les ensembles qui ne sont pas éléments d'eux-même. Il y a alors deux possibilités : soit $R \in R$, soit $R \notin R$.

Si $R \in R$ alors R satisfait P (car chaque élément de R satisfait cette condition par définition). Donc R est un ensemble qui n'est pas élément de lui-même, puis $R \notin R$, donc

$$R \in R \quad \text{et} \quad R \notin R.$$

Si $R \notin R$ alors R est un ensemble qui n'est pas élément de lui-même, autrement dit R satisfait P. Mais alors $R \in R$ car tout objet qui satisfait la condition P est élément de R. Donc on arrive à la même conclusion :

$$R \in R \quad \text{et} \quad R \notin R.$$

Donc, dans un cas comme dans l'autre, R satisfait $R \in R$ et $R \notin R$.

En résumé, le principe ci-dessus implique qu'il existe un ensemble R qui satisfait les deux condition $R \in R$ et $R \notin R$, ce qui est impossible (la loi de contradiction dans la logique propositionnelle).

D'autres paradoxes ont été découverts, dont au moins un par Cantor lui-même. Au tournant de siècle, il était devenu clair que la théorie des ensembles se contredisait elle-même et qu'il était nécessaire de la reconstruire sur des bases logiques plus solides. Cette période est connue sous le nom de la crise des fondements (parce que toutes les mathématiques s'appuient sur la théorie des ensembles).

8.2 L'introduction à la théorie ZFC

On a vu que les Principes I et II de Cantor donnent lieu à une théorie des ensembles qui se contredit elle-même. Pour résoudre cette difficulté, Zermelo proposa en 1908 une liste d'axiomes destinée à remplacer les deux principes de Cantor ; en 1922 Fraenkel et Skolem apportèrent quelques améliorations aux axiomes de Zermelo et le système d'axiomes qui en résulta est connu sous le nom de la théorie "ZF" des ensembles (pour Zermelo-Fraenkel). Plus tard on ajouta un axiome supplémentaire à la liste : l'axiome du choix. "ZFC" désigne le système d'axiomes ZF auquel on a ajouté l'axiome du choix. C'est le système qui est utilisé aujourd'hui, donc toutes les mathématiques s'appuient sur ZFC.

Dans notre système on a deux choses :

- des objets
- une relation $\in$ entre ces objets.

Ces objets et cette relation forment ce que on appellera *l'univers*. Pour l'instant, la seule chose qu'on sait à propos de cet univers c'est que si x et y sont des objets quelconques alors on a soit $x \in y$, soit $\neg(x \in y)$ par la loi de tier exclu. On écrit "$x \notin y$" comme abréviation de $\neg(x \in y)$. Les axiomes de ZFC sont des conditions que les objets et la relation $\in$ doivent satisfaire. La théorie des ensembles est l'étude des univers qui satisfont **tous** les axiomes de ZFC.

Pour parler de l'univers il est commode d'utiliser des mots connus : les objets seront appelés des *ensembles*, et lorsque $x \in y$, on dira que x *est un élément de* y. Il vaut la peine d'insister : **tous** les objets de l'univers sont des ensembles, donc il n'existe rien d'autre que des ensembles et nous ne rencontrerons jamais une "chose" qui n'est pas un ensemble. En particulier tous les éléments d'un ensemble donné sont eux-mêmes des ensembles. Lorsqu'on écrit "$x \in y$", non seulement y est un ensemble mais x aussi. Une formule $\forall_x (\dots)$ doit toujours être interprétée de la manière suivante :

"tout objet x de l'univers satisfait la condition $(\dots)$"

et puisque "ensemble" est synonyme de "objet", la même formule peut aussi être traduite par

"tout ensemble x satisfait la condition $(\dots)$".

Similairement, $\exists_x (\dots)$ se traduit par "il existe au moins un objet x de l'univers qui satisfait la condition $(\dots)$", ou encore par "il existe au moins un ensemble x qui satisfait la condition $(\dots)$."

On a dit que "$\in$" était la seule relation entre les objets mais évidemment on a aussi la relation d'égalité : deux objects x et y peuvent être égaux, $x = y$, et comme d'habitude ceci signifie que x et y sont en fait le même objet (on n'a pas deux objets mais un seul, qu'on a nommé deux fois).

8.3 Les trois premiers axiomes de ZFC

Le premier axiome est exactement le Principe I de Cantor :

ZFC Axiome 1 (Axiome d'extensionalité). Deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments.

$$\forall_{x,y}\,[x = y \iff \forall_z\,(z \in x \iff z \in y)]$$

Exemple 8.3.1. Considérez un univers que a précisément trois objets distincts a, b_1, b_2 et tel que $\in$ est définie par :

$$a \in b_1, \quad a \in b_2, \quad a \notin a, \quad (\text{et } x \notin y \text{ dans tous les cas qui ne sont pas nommés}).$$

Alors $b_1 \neq b_2$ mais b_1, b_2 ont les mêmes éléments, donc cet univers ne satisfait pas l'Axiome 1.

Le deuxième axiome est une version affaiblie du Principe II de Cantor :

ZFC Axiome 2 (Axiome de spécification). Étant donnés un ensemble A et une condition $P(x)$ sur x, il existe un ensemble B dont les éléments sont précisément les éléments x de A qui satisfont la condition $P(x)$.

Ainsi, étant donnés A et $P(x)$, l'axiome affirme l'existence d'un ensemble B qui satisfait

$$\forall_x\,(x \in B \iff [x \in A \ \wedge\ P(x)]).$$

Cet ensemble B est unique, en vertu de l'axiome d'extensionalité. On le désigne par la notation suivante :

$$B = \{x \in A : P(x)\}.$$

La différence entre l'Axiome 2 et le Principe II de Cantor est celle-ci : au lieu de former un ensemble avec *tous les objets x de l'univers* qui satisfont la condition $P(x)$, on se restreint maintenant aux éléments d'un ensemble A.

Exemple 8.3.2. L'axiome de spécification implique que si A est un ensemble alors l'ensemble $\{x \in A : x \notin x\}$ existe, mais l'axiome ne permet pas d'affirmer que $\{x : x \notin x\}$ existe.

Exemple 8.3.3. Considérez un univers dans lequel il y a exactement trois objets, a, b, c, et tel que $\in$ est définie par

$$a \in c,\ b \in c,\ b \in b \quad (\text{et } x \notin y \text{ dans tous les cas qui ne sont pas nommés}).$$

- Remarquez que a n'a aucun élément, b a un seul élément, et c a deux éléments ; donc il n'existe pas deux objets différents qui ont les mêmes éléments, donc cet univers satisfait l'Axiome 1.
- Dans cet univers il n'existe aucun objet x qui satisfait : "$a \in x$ et a est le seul élément de x" ; autrement dit, le singleton $\{a\}$ n'existe pas.
- Cet univers ne satisfait pas l'Axiome 2. En effet, si cet axiome était satisfait alors l'ensemble $B = \{x \in c : x \notin x\}$ existerait, et en fait B serait le singleton $\{a\}$ (car il existe exactement un élément x de c que satisfait $x \notin x$, et cet élément est $x = a$). Puisque $\{a\}$ n'existe pas, l'Axiome 2 n'est pas satisfait.

Pour compléter la présentation de l'Axiome 2 il nous reste à préciser qu'est-ce qu'on entend par "une condition $P(x)$ sur x". Nous dirons que $P(x)$ est une condition sur x si $P(x)$ est une formule dont la seule variable libre est x. Par exemple, "$x \notin x$" est une formule dont la seule variable libre est x, donc est une condition sur x. Voici un exemple plus compliqué : l'expression

$$\exists_{y,z} (x \in y \ \wedge \ y \in z)$$

est une condition sur x (car c'est une formule dont la seule variable libre est x). On peut donc utiliser cette condition avec l'Axiome 2 pour définir des ensembles : l'axiome affirme que si A est un ensemble alors l'ensemble $\{x \in A : \exists_{y,z} (x \in y \ \wedge \ y \in z)\}$ existe.

Voici un autre exemple. La formule $x \notin y$ a deux variables libres x, y, mais si on remplace la variable y par un ensemble spécifique B on obtient une formule $x \notin B$ dont la seule variable libre est x. Donc $x \notin B$ est une condition sur x et peut donc être utilisée avec l'Axiome 2 pour définir des ensembles : si A est un ensemble alors l'ensemble $\{x \in A : x \notin B\}$ existe. L'ensemble $\{x \in A : x \notin B\}$ est désigné par $A \setminus B$. Remarquez que

$$\forall_x [x \in A \setminus B \iff (x \in A \ \wedge \ x \notin B)].$$

Similairement, l'Axiome 2 implique que si A et B sont des ensembles alors l'ensemble $\{x \in A : x \in B\}$ existe et il est désigné par $A \cap B$. Il satisfait :

$$\forall_x [x \in A \cap B \iff (x \in A \ \wedge \ x \in B)].$$

Remarque 8.3.4. Les axiomes qu'on a vus jusqu'ici ne nous permettent **pas** d'affirmer que si A et B sont des ensembles alors l'ensemble $A \cup B$ existe. En effet, considérez un univers avec trois objets a_0, a_1, a_2 et tel que $a_i \in a_j \iff j = i + 1$. Cet univers satisfait les axiomes 1 et 2 (et aussi 3 ci-dessous), mais $a_1 \cup a_2$ n'existe pas.

Proposition 8.3.5. *Il n'existe pas d'ensemble A qui satisfait $\forall_x (x \in A)$.*

Preuve. Supposons qu'il existe un ensemble A tel que $\forall_x (x \in A)$. Puisque A est un ensemble et puisque $x \notin x$ est un condition sur x, l'axiome de spécification implique que l'ensemble $R = \{x \in A : x \notin x\}$ existe. En particulier, R est l'ensemble de tous les ensembles qui ne contiennent pas eux-même. Mais on a deja vu que l'existence de cet ensemble est une contradiction. □

L'univers vide (aucun objet) satisfait les axiomes 1 et 2. Donc pour s'assurer qu'il existe au moins un ensemble, nous avons besoin d'un nouvel axiome :

ZFC Axiome 3 (Axiome d'existence). Il existe au moins un ensemble.

$$\exists_x (x = x)$$

Proposition 8.3.6. *Il existe un et un seul ensemble qui n'a aucun élément. On l'appelle l'ensemble vide, et on le désigne par le symbole* $\varnothing$*.*

Preuve. En vertu de l'axiome d'existence, il existe au moins un ensemble ; disons que A est un ensemble. Alors l'axiome de spécification affirme que l'ensemble suivant existe :

$$B = \{t \in A : t \neq t\}.$$

Les éléments de B sont les éléments t de A qui satisfont $t \neq t$, donc B n'a aucun élément. Ceci montre qu'il existe *au moins un* ensemble qui n'a aucun élément. Si B, B' sont des ensembles qui n'ont aucun élément alors $B = B'$ en vertu de l'axiome d'extensionalité. Donc il existe *exactement un* ensemble qui n'a aucun élément. □

Proposition 8.3.7. *Si A est un ensemble non vide alors il existe un et un seul ensemble V dont les éléments sont précisément tous les ensembles x qui satisfont :*

$$x \text{ est élément de chaque élément de } A.$$

On écrit $V = \cap A$ *ou* $V = \bigcap_{X \in A} X$*.*

Preuve. Puisque $A \neq \varnothing$, on peut choisir E tel que $E \in A$. Puisque E est un ensemble et $\forall_a (a \in A \implies x \in a)$ est une condition sur x, l'axiome de spécification implique que

$$V = \{x \in E : \forall_a (a \in A \implies x \in a)\}$$

est un ensemble. Pour un ensemble x quelconque, on a :

$$\begin{aligned} x \in V &\iff x \in E \text{ et } \forall_a (a \in A \implies x \in a) \\ &\iff x \in E \text{ et } x \text{ est élément de chaque élément de } A \\ &\iff x \text{ est élément de chaque élément de } A. \end{aligned}$$

Donc l'ensemble V a la propriété voulue. L'axiome d'extensionalité implique que V est unique. □

Exercices.

8.3.1. Imaginez un univers avec un seul objet a, et tel que $a \in a$. Montrez que les axiomes 1 et 3 sont satisfaits mais pas 2.

8.3.2. Considérez un univers avec un seul objet a, et tel que $a \notin a$ (autrement dit, le seul objet de l'univers est l'ensemble vide). Montrez que les trois axiomes 1, 2 et 3 sont satisfaits.

8.3.3. Considérez un univers avec deux objets $a \neq b$, et tel que

$$a \in b, \quad a \notin a, \quad b \notin b, \quad b \notin a.$$

Montrez que les trois axiomes 1, 2 et 3 sont satisfaits.

8.4 Les axiomes 4–6 de ZFC

ZFC Axiome 4 (Axiome de la paire). Étant donnés des ensembles x et y, il existe un ensemble z tel que $x \in z$ et $y \in z$.

$$\forall_{x,y} \exists_z (x \in z \ \wedge \ y \in z)$$

Proposition 8.4.1. *(a) Si a est un ensemble alors l'ensemble $\{a\}$ existe.*
(b) Si a et b sont des ensembles alors l'ensemble $\{a, b\}$ existe.

Preuve. Prouvons d'abord l'assertion (b). Soient a et b des ensembles. En vertu de l'axiom de la paire, il existe un ensemble c' qui satisfait $a \in c'$ et $b \in c'$. Alors l'axiome de spécification affirme que l'ensemble suivant existe :

$$c = \{x \in c' : x = a \ \vee \ x = b\}.$$

Alors a et b sont éléments de c, et sont les seuls éléments de c. Donc $c = \{a, b\}$, donc l'ensemble $\{a, b\}$ existe et (b) est démontré. Pour démontrer (a) il suffit de remarquer que l'assertion (b) est aussi valide dans le cas où $a = b$. □

ZFC Axiome 5 (Axiome de la réunion). Quel que soit l'ensemble A, il existe au moins un ensemble W qui satisfait : tout élément d'un élément de A est élément de W.

$$\forall_A \exists_W \forall_x (\exists_a (a \in A \ \wedge \ x \in a) \implies x \in W)$$

Proposition 8.4.2. *Si A est un ensemble alors il existe un et un seul ensemble W dont les éléments sont précisément tous les ensembles x qui satisfont :*

x est élément d'au moins un élément de A.

On écrit $W = \cup A$ *ou encore* $W = \bigcup_{X \in A} X$.

Preuve. En vertu de l'axiome de la réunion, il existe un ensemble W' qui satisfait : tout élément d'un élément de A est élément de W'. Autrement dit, pour tout objet x l'implication suivante est vraie :

$$\exists_a (a \in A \ \wedge \ x \in a) \implies x \in W'. \tag{8.1}$$

Puisque W' est un ensemble et $\exists_a (a \in A \ \wedge \ x \in a)$ est une condition sur x, l'axiome de spécification affirme que l'ensemble suivant existe :

$$W = \{x \in W' : \exists_a (a \in A \ \wedge \ x \in a)\}.$$

Alors quel que soit l'objet x on a

$$\begin{aligned} x \in W &\iff x \in W' \text{ et } \exists_a (a \in A \ \wedge \ x \in a) \\ &\overset{(8.1)}{\iff} \exists_a (a \in A \ \wedge \ x \in a) \\ &\iff x \text{ est élément d'au moins un élément de } A. \end{aligned}$$

Donc l'ensemble W a la propriété voulue. En vertu de l'axiome d'extensionalité, il ne peut y avoir qu'un seul W ayant cette propriété. □

Remarque 8.4.3. On peut montrer avec Axiomes 1–4 que $\wp(z)$ existe pour tout ensemble fini z (voir [Dai, Proposition 7.5]). Mais pour les ensembles infinis, on a besoin d'un autre axiome.

ZFC Axiome 6 (Axiome de l'ensemble des parties). Quel que soit l'ensemble z, il existe au moins un ensemble p ayant la propriété suivante : tout sous-ensemble de z est élément de p.

$$\forall_z \exists_p \forall_x (x \subseteq z \implies x \in p)$$

Proposition 8.4.4. *Quel que soit l'ensemble* z, $\wp(z)$ *existe.*

Preuve. Soit z un ensemble. L'Axiome 6 implique qu'il existe au moins un ensemble p' qui satisfait : tout sous-ensemble de z est élément de p'. On choisit un tel ensemble p', alors on a :

$$\forall_x (x \subseteq z \implies x \in p'). \tag{8.2}$$

Puisque p' est un ensemble et "$x \subseteq z$" est une condition sur x, l'axiome de spécification implique que l'ensemble suivant existe :

$$p = \{x \in p' : x \subseteq z\}.$$

Pour un ensemble x quelconque,

$$x \in p \iff (x \in p' \ \wedge \ x \subseteq z) \overset{8.2}{\iff} x \subseteq z$$

donc l'ensemble p satisfait la condition $\forall_x (x \in p \iff x \subseteq z)$, donc $p = \wp(z)$. □

Exercices.

8.4.1. Montrez que $\{\varnothing\} \neq \{\{\varnothing\}\}$ et que $\{\{\varnothing\}\} \neq \{\{\{\varnothing\}\}\}$.

8.4.2. Par induction sur n, démontrez que si $x_1, \ldots, x_n$ sont des ensembles, alors l'ensemble $\{x_1, \ldots, x_n\}$ existe.

8.5 L'axiome de l'infini

En vertu des cinq premiers axiomes, si y est un ensemble quelconque alors l'ensemble $y \cup \{y\}$ existe et est unique. Écrivons $y^+ = y \cup \{y\}$ comme abréviation. On dit que y^+ est le *successeur* de y. Par exemple, on a

$$\varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\} \quad \text{et} \quad \{\varnothing\}^+ = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}.$$

Définition 8.5.1. On dit qu'un ensemble A est *inductif* s'il satisfait les deux conditions

$$\varnothing \in A \quad \text{et} \quad \forall_y \, (y \in A \implies y^+ \in A).$$

La preuve du lemme suivant est une exercice.

Lemme 8.5.2. *Supposons que E est un ensemble non vide qui satisfait :*

Chaque élément de E est un ensemble inductif.

Alors $\cap E$ est un ensemble inductif.

ZFC Axiome 7 (Axiome de l'infini). Il existe au moins un ensemble inductif.

Théorème 8.5.3. *Il existe exactement un ensemble ω qui satisfait les deux conditions suivantes :*

- *ω est un ensemble inductif,*
- *ω est inclus ($\subseteq$) dans tout ensemble inductif.*

Preuve. En vertu de l'Axiome 7, il existe un ensemble inductif A. Considérons l'ensemble

$$E = \{x \in \wp(A) : x \text{ est un ensemble inductif}\}.$$

Cet ensemble existe par l'axiome de spécification. Notons que $E \neq \varnothing$ (puisque $A \in E$), et que chaque élément de E est un ensemble inductif. Donc le Lemme 8.5.2 implique que $\cap E$ est un ensemble inductif. On définit

$$\omega = \cap E.$$

Il reste à montrer que ω est inclus dans tout ensemble inductif. Soit B un ensemble inductif quelconque. Alors $A \cap B$ est un ensemble inductif (Exercice 8.5.3) et $A \cap B \in \wp(A)$, donc $A \cap B \in E$. Puisque $\cap E \subseteq C$ pour tout $C \in E$, on a $\cap E \subseteq A \cap B \subseteq B$, donc $\omega \subseteq B$.

On a montré l'existence d'au moins au ensemble inductif ω qui est inclus dans tout ensemble inductif. Un tel ensemble est forcément unique. En effet, supposons que ω' est aussi un ensemble inductif inclus dans tout ensemble inductif. Alors on a $\omega \subseteq \omega'$ et $\omega' \subseteq \omega$, donc $\omega = \omega'$. □

Définition 8.5.4. Les éléments de ω sont appelés les *nombres naturels*.

En particulier, on définit les nombres naturels 0, 1, 2, 3, 4, 5 de la manière suivante :

$$\begin{aligned}
&0 = \varnothing,\\
&1 = \varnothing^+ = 0 \cup \{0\} = \{0\} = \{\varnothing\},\\
&2 = 1^+ = 1 \cup \{1\} = \{0, 1\} = \{\varnothing, \{\varnothing\}\},\\
&3 = 2^+ = 2 \cup \{2\} = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\\
&4 = 3^+,\\
&5 = 4^+, \dots .
\end{aligned}$$

Maintenant, avec les axiomes, on peut définir l'ordre $\leq$ sur l'ensemble $\mathbb{N} = \omega$ et prouver que $(\omega, \leq)$ est bien ordonné. Parce que on n'a pas le temps, on ne le fera pas en classe. Mais maintenant vous avez les connaissances pour comprendre les preuves (voir [Dai, Section 13]). On peut aussi définir l'arithmétique (voir [Dai, Section 14]) et les ensembles de nombres $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ (voir [Dai, Section 15]).

Exercices.

8.5.1. Montrez que pour tout ensemble y on a $y \in y^+$ et $y \subseteq y^+$.

8.5.2. Démontrez le lemme 8.5.2.

8.5.3. Montrez que si A et B sont des ensembles inductifs alors $A \cap B$ est un ensemble inductif.

8.5.4. Prouvez que $2 \neq 3$.

8.6 Les deux derniers axiomes de ZF

ZFC Axiome 8 (Axiome de fondation). Pour tout ensemble x non vide, il existe au moins un élément $y \in x$ qui satisfait $y \cap x = \varnothing$.

$$\forall_x \left[x \neq \varnothing \implies \exists_{y \in x} \left(y \cap x = \varnothing\right)\right]$$

Proposition 8.6.1. *Aucun ensemble n'est élément de lui-même.*

Preuve. On procède par contradiction : supposons qu'il existe un ensemble a qui satisfait $a \in a$. On sait que l'ensemble $\{a\}$ existe. Puisque $\{a\} \neq \varnothing$, l'axiome de fondation implique qu'il existe $y \in \{a\}$ tel que $y \cap \{a\} = \varnothing$. On a forcément $y = a$, donc $a \cap \{a\} = \varnothing$. Cependant, $a \in a \cap \{a\}$, contradiction. □

ZFC Axiome 9 (Axiome de remplacement). Étant donnés un ensemble A et une formule $Q(x, y)$ avec variables libres x, y si l'énoncé

$$\forall_{a \in A} \exists!_b \, Q(a, b)$$

est vrai alors il existe un ensemble B tel que

$$\forall_{a \in A} \exists!_{b \in B} \, Q(a, b).$$

8.7 L'Axiome du Choix

Les 9 axiomes qu'on a vus ci-dessus constituent la théorie "ZF" des ensembles (l'axiomatization de Zermelo et Fraenkel). La théorie ZFC des ensembles est obtenue en ajoutant aux axiomes de ZF un axiome supplémentaire, appelé l'Axiome du Choix. On ne va pas parler beaucoup de l'Axiome du Choix dans ce cours, mais pour être complet, on le donne ici.

Axiome du Choix (Version 1). Soit $(A_i)_{i \in I}$ une famille d'ensembles telle que $\forall_{i \in I} \, (A_i \neq \varnothing)$. Alors il existe au moins une famille $(a_i)_{i \in I}$ (indicée par le même ensemble I) satisfaisant $\forall_{i \in I} \, (a_i \in A_i)$.

Axiome du Choix (Version 2). Soit $(A_i)_{i \in I}$ une famille d'ensembles telle que $\forall_{i \in I} \, (A_i \neq \varnothing)$. Alors il existe au moins une fonction $c \colon I \to \bigcup_{i \in I} A_i$ telle que $\forall_{i \in I}, (c(i) \in A_i)$.

L'Axiome du Choix est équivalent au Lemme de Zorn.

Lemme de Zorn. Supposons que $(X, \leq)$ est un ensemble partiellement ordonné satisfaisant les deux conditions suivantes :

(a) $X \neq \varnothing$

(b) Pour toute chaîne (c.-à-d. sous-ensemble totalement ordonné) $C \subseteq X$ telle que $C \neq \varnothing$, il existe au moins un $y \in X$ satisfaisant $\forall_{x \in C} \; x \leq y$.

Alors $(X, \leq)$ a au moins un élément maximal.

L'application la plus connue de l'Axiome du Choix (ou du Lemme de Zorn) est le preuve que tout espace vectoriel possède une base. Voir [Dai, Sections 17–19].

Chapitre 9

La cardinalité des ensembles

Dans ce chapitre on discute la notion de la cardinalité des ensembles.

9.1 La cardinalité

Si on dit que deux ensembles ont le même nombre d'éléments, qu'est-ce ça veut dire ? Si les ensembles sont finis, c'est facile. Si deux ensembles A et B sont finis, alors $|A|$ et $|B|$ sont des nombres naturels (le nombre d'éléments de A et B) et on dit que A et B ont le même nombre d'éléments si $|A| = |B|$. Mais, qu'est ce qu'on fait si les ensembles sont infinis ? Par exemple, les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{R}$ ont-ils le même nombre d'éléments ?

Une approche possible est de développer une théorie des nombres infiniment grands. C'est possible, mais c'est un peu compliqué. Il y a une autre approche qu'on va développer, une approche plus simple, qui est basée sur l'idée de bijection. On peut répondre à la question "$\mathbb{N}$ et $\mathbb{Q}$ ont-ils le même nombre d'éléments ?" sans jamais parler du nombre d'éléments de ces ensembles.

Définition 9.1.1. Étant donnés des ensembles A et B, on écrit $A \sim B$ si et seulement s'il existe au moins une bijection de A vers B. On dit que des ensembles qui satisfont $A \sim B$ sont *équipotents* et que A et B *ont la même cardinalité*.

Si on veut utiliser l'idée de bijection pour dire que deux ensembles ont le même nombre d'éléments, on devrait vérifier que cette notation coïncide avec la définition normale pour des ensemble finis.

Lemme 9.1.2. *Si A et B sont des ensemble finis, alors l'énoncé $A \sim B$ est vrai si et seulement si A et B ont le même nombre d'éléments.*

Preuve. Exercice. Cela va s'ensuivre des résultats qui viennent aussi. □

Exemples 9.1.3. (a) Si $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 7, 9\}$ et $C = \{2, 8, 12\}$ alors il existe une bijection de A vers B donc $A \sim B$. Cependant, il n'existe aucune bijection de A vers C donc $A \not\sim C$.

(b) Considérons le sous-ensemble $I = \{1, 3, 5, 7, 9, \ldots\}$ (les nombres impairs) de $\mathbb{N}$. Soit $f\colon \mathbb{N} \to I$ définie par $f(x) = 2x + 1$. Alors f est bijective, ce qui démontre que $\mathbb{N} \sim I$.

(c) Soit $f\colon \mathbb{N} \to \mathbb{Z}$ définie par

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ est pair,} \\ -(n+1)/2 & \text{si } n \text{ est impair.} \end{cases}$$

Alors f est bijective, ce qui démontre que $\mathbb{N} \sim \mathbb{Z}$ (même si $\mathbb{N} \subsetneq \mathbb{Z}$).

Proposition 9.1.4. *Quels que soient les ensembles A, B, C, on a :*

(a) $A \sim A$

(b) $A \sim B \implies B \sim A$

(c) $A \sim B$ *et* $B \sim C \implies A \sim C$

Preuve.

(a) $\mathrm{Id}_A\colon A \to A$ est une bijection. Donc $A \sim A$.

(b) Si $A \sim B$, alors il existe une bijection $f\colon A \to B$. Alors $f^{-1}\colon B \to A$ est un bijection, donc $B \sim A$.

(c) Si $A \sim B$ et $B \sim C$, alors il existe des bijections $f\colon A \to B$ et $g\colon B \to C$. Puisque $g \circ f\colon A \to C$ est un bijection (on a vu que la composition de deux bijections est une bijection) on a $A \sim C$.

□

Remarque 9.1.5. Est-ce que $\sim$ est une relation d'équivalence ? Si oui, sur quel ensemble ? Rappelez-vous qu'il n'existe pas un ensemble de tous les ensembles ! Mais si X est un ensemble de *quelques* ensembles, alors oui, $\sim$ est une relation d'équivalence sur X.

Proposition 9.1.6. *Si $A \subseteq \mathbb{N}$ et A est infini, alors $\mathbb{N} \sim A$.*

Preuve. On peut énumérer les éléments de A en ordre croissant : soit a_0 le plus petit élément de A, soit a_1 le plus petit élément de $A \setminus \{a_0\}$, soit a_2 le plus petit élément de $A \setminus \{a_0, a_1\}$, etc. (ici on utilise le fait que $(\mathbb{N}, \leq)$ est bien ordonné). Ainsi, les éléments de A sont :

$$a_0 < a_1 < a_2 < a_3 < \ldots$$

Soit $f\colon \mathbb{N} \to A$ définie par $f(n) = a_n$. Ceci est une bijection, donc $\mathbb{N} \sim A$. □

Corollaire 9.1.7. *Soit A l'ensemble des nombres premiers. Alors $A \sim \mathbb{N}$.*

Preuve. On a $A \subseteq \mathbb{N}$ et on sait par la proposition 1.7.4 que A est infini. Donc, par la proposition 9.1.6 on sait que $\mathbb{N} \sim A$. Puis par la proposition 9.1.4, $A \sim \mathbb{N}$. □

Proposition 9.1.8. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Remarque 9.1.9. En classe on a démontré la proposition à l'aide d'un dessin. Ci-dessous on voit une autre démonstration, mais plusieurs détails sont omis et c'est à vous de compléter le travail.

Preuve. Pour chaque $k \in \mathbb{N}$, on définit

$$T_k = 1 + 2 + \cdots + k = \frac{k(k+1)}{2} \in \mathbb{N}.$$

Donc $0 = T_0 < T_1 < T_2 < \cdots < \cdots$ et l'assertion suivante est vraie :

Pour chaque $n \in \mathbb{N}$, il existe exactement un $k \in \mathbb{N}$ tel que $T_k \leq n < T_{k+1}$.

Donc on peut définir une fonction $\alpha\colon \mathbb{N} \to \mathbb{N}$ par la règle suivante :

$$\alpha(n) = \text{l'unique } k \in \mathbb{N} \text{ qui satisfait } T_k \leq n < T_{k+1}.$$

Il est clair que

$$\textit{pour chaque } n \in \mathbb{N},\ T_{\alpha(n)} \leq n < T_{\alpha(n)+1},$$

donc

$$\textit{pour chaque } n \in \mathbb{N},\ (T_{\alpha(n)+1} - n - 1, n - T_{\alpha(n)}) \in \mathbb{N}^2.$$

On peut donc définir une fonction $g\colon \mathbb{N} \to \mathbb{N}^2$ par $g(n) = (T_{\alpha(n)+1} - n - 1, n - T_{\alpha(n)})$.

On définit aussi $f\colon \mathbb{N}^2 \to \mathbb{N}$ par $f(x, y) = y + T_{x+y}$. Vous pouvez vérifier que $f \circ g$ et $g \circ f$ sont les fonctions identiques sur $\mathbb{N}$ et sur $\mathbb{N}^2$ respectivement. Donc $f\colon \mathbb{N}^2 \to \mathbb{N}$ est une bijection. □

Proposition 9.1.10. *Quels que soient les ensembles A, A', B, B', on a :*

$$(A \sim A \text{ et } B \sim B') \implies A \times B \sim A' \times B'.$$

Preuve. Supposons que $A \sim A'$ et $B \sim B'$. On choisit deux bijections $f\colon A \to A'$ et $g\colon B \to B'$, et on définit une fonction $h\colon A \times B \to A' \times B'$ par $h(a, b) = (f(a), g(b))$. On doit montrer que h est bijective. Soit $(a', b') \in A' \times B'$. Puisque f et g sont surjectives, il existe $a \in A$ et $b \in B$ tels que $f(a) = a'$ et $g(b) = b'$. Donc $h(a, b) = (f(a), g(b)) = (a', b')$. Par conséquent, h est surjective. Pour montrer que h est injective, supposons que $h(a_1, b_1) = h(a_2, b_2)$. Alors $(f(a_1), g(b_1)) = (f(a_2), g(b_2))$. Donc $f(a_1) = f(a_2)$ et $g(b_1) = g(b_2)$. Puisque f et g sont injectives, on a $a_1 = a_2$ et $b_1 = b_2$. Donc $(a_1, b_1) = (a_2, b_2)$. Par conséquent, h est injective aussi et donc h est bijective. Donc $A \times B \sim A' \times B'$. □

Corollaire 9.1.11. $\mathbb{Z}^n \sim \mathbb{N}$ *pour tout* $n \geq 1$.

Preuve. Par induction sur n. Le cas $n = 1$ est vrai, parce que on a déjà montré que $\mathbb{Z} \sim \mathbb{N}$. Supposons que $n \geq 1$ est un entier pour lequel $\mathbb{Z}^n \sim \mathbb{N}$ est vrai, et montrons que $\mathbb{Z}^{n+1} \sim \mathbb{N}$.

En vertu de la proposition 9.1.10, $\mathbb{Z}^n \sim \mathbb{N}$ et $\mathbb{Z} \sim \mathbb{N}$ impliquent $\mathbb{Z}^n \times \mathbb{Z} \sim \mathbb{N} \times \mathbb{N}$, donc

$$\mathbb{Z}^{n+1} \sim \mathbb{Z}^n \times \mathbb{Z} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N},$$

donc $\mathbb{Z}^{n+1} \sim \mathbb{N}$. □

Définition 9.1.12. Pour deux ensembles A et B, on écrit $A \preceq B$ s'il existe au moins une injection de A vers B.

Exemples 9.1.13. (a) Les assertions $\{2,5,8\} \preceq \{1,5,9\}$ et $\{2,3\} \preceq \{4,8,23,56\}$ sont vraies mais $\{5,7,10\} \preceq \{3,12\}$ est fausse.

(b) $\{1,3,7,12\} \preceq \mathbb{N}$ et $\{-2,5,12,\pi\} \preceq \mathbb{N}$.

(c) $\mathbb{N} \preceq \mathbb{Z}$ et $\mathbb{Z} \preceq \mathbb{N}$.

La preuve de la proposition suivante est une exercice.

Proposition 9.1.14. *Quels que soient les ensembles A, B et C, on a :*

(a) $A \preceq A$

(b) $A \preceq B$ *et* $B \preceq C \implies A \preceq C$

(c) $A \subseteq B \implies A \preceq B$

(d) $A \sim B \implies A \preceq B$ *et* $B \preceq A$

Remarque 9.1.15. La proposition ci-dessus **ne répond pas** aux questions suivantes :

(a) L'implication

$$A \preceq B \text{ et } B \preceq A \implies A \sim B$$

est-elle vraie ?

(b) Est-il vrai que, quels que soient les ensembles A et B, au moins une des conditions

$$A \preceq B, \quad B \preceq A$$

doit être satisfaite ?

Ce questions sont difficiles et nous remettons à plus tard leur solution (nous verrons que la réponse est "oui" dans les deux cas). Remarquez que la première question demande si la récriproque de la proposition 9.1.14(d) est vraie. Concernant cette question, considérez l'exemple suivant.

Exemple 9.1.16. Soient les intervalles $A = (0,1)$ et $B = [0,1]$.

- Puisque $A \subseteq B$, il est clair que $A \preceq B$.
- Si $x \in B$ alors $(x+1)/3 \in [1/3, 2/3]$, donc $(x+1)/3 \in A$. Ainsi, une fonction $g\colon B \to A$ est définie par $g(x) = (x+1)/3$. Cette fonction est strictement croissante, donc injective, donc $B \preceq A$.

On a montré que $(0,1) \preceq [0,1]$ et $[0,1] \preceq (0,1)$. S'ensuit-il que $(0,1) \sim [0,1]$? Autrement dit, existe-t-il une bijection de $(0,1)$ vers $[0,1]$? Nous verrons plus tard un théorème qui répond "oui" à cette question, mais si vous essayez de définir une bijection de $(0,1)$ vers $[0,1]$ vous verrez que c'est loin d'être évident.

Proposition 9.1.17. *Étant donnés des ensembles A et B non vides, les conditions suivantes sont équivalentes :*

(1) Il existe au moins une injection de A vers B (autrement dit, $A \preceq B$).

(2) Il existe au moins une surjection de B vers A.

Preuve.

$(1 \Rightarrow 2)$ Supposons qu'il existe une injection $f\colon A \to B$. Remarquons que si $y \in f(A)$ alors $f^{-1}(y)$ est un élément bien défini de A, car f est injective. Puisque $A \neq \varnothing$ par hypothèse, on peut choisir un élément $a_0 \in A$ et définir une fonction $g\colon B \to A$ par

$$g(y) = \begin{cases} f^{-1}(y), & \text{si } y \in f(A), \\ a_0, & \text{si } y \in B \setminus f(A). \end{cases}$$

On a alors $g(f(x)) = x$ pour tout $x \in A$, donc $g\colon B \to A$ est surjective, donc (2) est satisfaite.

$(2 \Rightarrow 1)$ Supposons qu'il existe une surjection $g\colon B \to A$. Alors pour chaque $x \in A$ on peut choisir un élément $b_x \in B$ qui satisfait $g(b_x) = x$. En vertu de l'axiome du choix, $x \mapsto b_x$ définit une fonction $f\colon A \to B$, $f(x) = b_x$. Supposons que $x, y \in A$ tels que $f(x) = f(y)$. Alors

$$y = g(b_y) = g(f(y)) = g(f(x)) = g(b_x) = x.$$

Donc f est injective et (1) est satisfaite. □

Exercices.

9.1.1. Donnez une preuve directe du lemme 9.1.2.

9.1.2. Démontrer la proposition 9.1.14.

9.1.3. Considérez les intervalles $A = (0, 1)$ et $B = [0, 1]$. On a vu en l'exemple 9.1.16 qu'il existe une injection $B \to A$, donc en vertu de la proposition 9.1.17 il existe une surjection $A \to B$. Donnez un exemple concret d'une telle surjection. (*Suggestion* : imitez la démonstration de la proposition 9.1.17.)

9.1.4. Rappelez-vous que pour deux ensembles A et B, $\mathrm{Fonc}(A, B)$ est l'ensemble des fonctions de A vers B.

(a) Soient A, B_1 et B_2 trois ensembles tels que $B_1 \preceq B_2$. Montrez que

$$\mathrm{Fonc}(A, B_1) \preceq \mathrm{Fonc}(A, B_2).$$

Indice : Pensez à la composition des fonctions.

(b) Soient A_1, A_2 et B trois ensembles tels que $A_1 \preceq A_2$ et $A_1 \neq \varnothing$. Montrez que

$$\mathrm{Fonc}(A_1, B) \preceq \mathrm{Fonc}(A_2, B).$$

Indice : Utilisez la proposition 9.1.17.

9.2 Les ensembles dénombrables

Définition 9.2.1. Un ensemble A est *dénombrable* s'il satisfait $A \preceq \mathbb{N}$.

Exemples 9.2.2. (a) Tout ensemble fini est dénombrable.

(b) On a vu que $\mathbb{Z}^n \sim \mathbb{N}$, donc $\mathbb{Z}^n$ est dénombrable.

(c) Tout sous-ensemble d'un ensemble dénombrable est dénombrable.

Remarque 9.2.3. Il y a des textes qui utilisent une définition différent de dénombrables. Ils disent qu'un ensemble A est dénombrable s'il satisfait $A \sim \mathbb{N}$. Donc, pour eux, les ensembles finis ne sont pas dénombrables. Mais dans ce cours, on utilisera la définition ci-dessus.

Proposition 9.2.4. *Si A est dénombrable et infini alors $A \sim \mathbb{N}$.*

Preuve. Supposons que A est dénombrable et infini. Puisque $A \preceq \mathbb{N}$, il existe une injection $f\colon A \to \mathbb{N}$. Soit $B = f(A)$, alors $A \sim B$. Puisque B est une partie infinie de $\mathbb{N}$, on a $B \sim \mathbb{N}$ en vertu de Proposition 9.1.6. Donc $A \sim \mathbb{N}$. □

Donc on voit que

Un ensemble est dénombrable si et seulement si il est fini ou équipotent à $\mathbb{N}$.

Théorème 9.2.5. $\mathbb{Q} \sim \mathbb{N}$.

Preuve. Il suffit de montrer que $\mathbb{Q} \preceq \mathbb{Z}^2$. En effet, si ceci est vrai alors

$$\mathbb{Q} \preceq \mathbb{Z}^2 \text{ et } \mathbb{Z}^2 \sim \mathbb{N} \quad \Longrightarrow \quad \mathbb{Q} \preceq \mathbb{Z}^2 \text{ et } \mathbb{Z}^2 \preceq \mathbb{N} \quad \Longrightarrow \quad \mathbb{Q} \preceq \mathbb{N},$$

donc $\mathbb{Q}$ est dénombrable et infini, donc $\mathbb{Q} \sim \mathbb{N}$ en vertu de la proposition 9.2.4.

Il reste à montrer que $\mathbb{Q} \preceq \mathbb{Z}^2$. Il est bien connue qu'on peut écrire tout nombre rationnel comme une fraction a/b où $a, b \in \mathbb{Z}$, $b > 0$ et a, b sont relativement premiers. De manière précise, on peut énoncer :

> *Pour chaque $x \in \mathbb{Q}$, il existe une et une seule paire $(a, b) \in \mathbb{Z}^2$ satisfaisant les conditions*
>
> *(i) $b > 0$, (ii) a, b sont relativement premiers, (iii) $x = a/b$.*

Ceci signifie que nous pouvons définir une fonction $f\colon \mathbb{Q} \to \mathbb{Z}^2$ par la règle suivante :

$$f(x) = \text{l'unique } (a, b) \in \mathbb{Z}^2 \text{ satisfaisant les conditions (i), (ii), (iii) ci-dessus.}$$

Remarquons en particulier que si $f(x) = (a, b)$ alors $x = a/b$, puisque (a, b) satisfait (iii). Donc si $x_1, x_2 \in \mathbb{Q}$ sont tels que $f(x_1) = (a, b) = f(x_2)$, alors $x_1 = a/b = x_2$. Donc f est injective.

On a montré que $\mathbb{Q} \preceq \mathbb{Z}^2$, donc la démonstration est terminée. □

Corollaire 9.2.6. $\mathbb{Q}^n \sim \mathbb{N}$ *pour tout* $n \geq 1$.

Preuve. On le prouve par induction sur n. On vient de montrer que $\mathbb{Q} \sim \mathbb{N}$. Supposons que $\mathbb{Q}^n \sim \mathbb{N}$. Alors

$$\mathbb{Q}^{n+1} = \mathbb{Q}^n \times \mathbb{Q} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}.$$

Puisque $\sim$ est transitive, on a $\mathbb{Q}^{n+1} \sim \mathbb{N}$. □

La preuve de la proposition suivante est une exercice.

Proposition 9.2.7. *Quels que soient les ensembles A, A', B, B', on a :*

$$A \preceq A' \text{ et } B \preceq B' \quad \Longrightarrow \quad A \times B \preceq A' \times B'.$$

Corollaire 9.2.8. *Si A et B sont des ensembles dénombrables, alors $A \times B$ est dénombrable.*

Preuve. Si A et B sont des ensembles dénombrables, on a $A \preceq \mathbb{N}$ et $B \preceq \mathbb{N}$. Donc, par la corollaire 9.2.8, on a $A \times B \preceq \mathbb{N} \times \mathbb{N}$. Puisque $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, on obtient $A \times B \preceq \mathbb{N}$. □

Proposition 9.2.9. *Soit $A = \bigcup_{i \in I} A_i$ où I est dénombrable et chacun des A_i est dénombrable. Alors A est dénombrable.*

Preuve. Pour chaque $x \in A$, on peut choisir un élément $j(x) \in I$ tel que $x \in A_{j(x)}$. Donc, par l'axiome du choix, il existe une fonction $j \colon A \to I$, $x \mapsto j(x)$, qui satisfait :

$$\text{Pour tout } x \in A,\ x \in A_{j(x)}.$$

D'autre part, pour chaque $i \in I$ il existe une injection $f_i \colon A_i \to \mathbb{N}$ (puisque A_i est dénombrable). On définit une fonction $F \colon A \to I \times \mathbb{N}$ par

$$F(x) = (j(x), f_{j(x)}(x)) \quad \text{pour chaque } x \in A.$$

On montre que F est injective. Soient $x, y \in A$ tels que

$$(j(x), f_{j(x)}(x)) = F(x) = F(y) = (j(y), f_{j(y)}(y)).$$

Alors $j(x) = j(y)$, donc $x, y \in A_{j(x)}$. Puis on a $f_{j(x)}(x) = f_{j(x)}(y)$. Puisque $f_{j(x)}$ est injective, on a $x = y$. Donc F est injective. Puis $A \preceq I \times \mathbb{N}$. Puisque I est dénombrable, $I \times \mathbb{N} \preceq \mathbb{N}$, et puisque "$\preceq$" est transitive, $A \preceq \mathbb{N}$. □

On a montré que

Une réunion dénombrable d'ensembles dénombrables est dénombrable.

Exemple 9.2.10. Soit A un sous-ensemble de $\mathbb{R}$ qui satisfait :

$$A \cap [-n, n] \text{ est dénombrable pour tout } n \in \mathbb{N}.$$

On montre que A est dénombrable. Puisque

$$\bigcup_{n \in \mathbb{N}} [-n, n] = \mathbb{R},$$

on a

$$A = \bigcup_{n\in\mathbb{N}} \big(A \cap [-n, n]\big).$$

On sait que $A\cap[-n, n]$ est dénombrable pout tout $n \in \mathbb{N}$. Donc A est une réunion dénombrable d'ensembles dénombrables. Ainsi A est dénombrable.

Existe-t-il des ensembles non-dénombrables ? On va voir que $\mathbb{R}$ n'est pas dénombrable. Avant de voir la preuve, discutons un peu de la représentation décimale des nombre réels.

Considérons l'intervalle $I = [0, 1)$. Chaque $x \in I$ a **au moins une** représentation décimale $x = 0.c_1c_2c_3\ldots$. Remarquez que la notation "$x = 0.c_1c_2c_3\ldots...$" signifie que $(c_1, c_2, c_3, \ldots)$ est une suite infinie d'éléments de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ satisfaisant l'égalité $x = \sum_{n=1}^{\infty} \frac{c_n}{10^n}$.

Chaque $x \in I$ a **au plus deux** représentations décimales. Si x a deux représentations, alors l'une d'elles a une queue de 0 et l'autre a une queue de 9. Par exemple,

$$\frac{1}{2} = 0.500000\ldots = 0.499999\ldots.$$

Convention : Nous rejetons les représentations qui ont une queue de 9. Cette convention nous permet d'écrire :

Chaque $x \in I$ a une et une seule représentation décimale.

Ceci nous permet de parler de **la** représentation décimale d'un nombre $x \in I$. Par exemple, la représentation décimale de $\frac{1}{2}$ est $0.5000\ldots$.

Lemme 9.2.11. *Il n'existe aucune fonction surjective* $\mathbb{N} \to I$.

Preuve. Il revient au même de montrer qu'il n'existe aucune fonction surjective $A \to I$, où $A = \mathbb{N} \setminus \{0\}$ (puisqu'il existe une bijection de A vers $\mathbb{N}$. Soit $f\colon A \to I$ une fonction quelconque. Montrons que f n'est pas surjective.

Pour chaque $n \in A$, on considère la représentation décimale (unique, en vertu de la convention) du nombre $f(n) \in I$,

$$\begin{aligned} f(1) &= 0.c_{11}c_{12}c_{13}c_{14}\ldots \\ f(2) &= 0.c_{21}c_{22}c_{23}c_{24}\ldots \\ &\vdots \\ f(n) &= 0.c_{n1}c_{n2}c_{n3}c_{n4}\ldots \\ &\vdots \end{aligned}$$

On définit une suite infinie $(c_1, c_2, c_3, \ldots)$ par la règle

$$c_n = \begin{cases} 2 & \text{si } c_{nn} \neq 2, \\ 3 & \text{si } c_{nn} = 2. \end{cases}$$

Alors :

(a) $(c_1, c_2, c_3, \dots)$ est une suite d'éléments de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ qui n'a pas une "queue de 9",

(b) $c_n \neq c_{nn}$ pour tout $n \geq 1$.

Soit y le nombre de I dont la représentation décimale est $y = 0.c_1c_2c_3\dots$. Montrons que $y \notin f(A)$.

Supposons qu'il existe $n \in A$ tel que $y = f(n)$. Alors $y = 0.c_1c_2c_3\dots$ et $y = 0.c_{n1}c_{n2}c_{n3}\dots$. Puisque y a une seule représentation décimale, il s'ensuite que $c_1 = c_{n1}$, $c_2 = c_{n2}$, etc., et en particulier, $c_n = c_{nn}$. Ceci contredit la définition de la suite $(c_1, c_2, \dots)$, et cette contradiction montre qu'il n'existe aucun $n \in A$ tel que $f(n) = y$. Donc f n'est pas surjective. □

Remarque 9.2.12. Dans la preuve ci-dessus, la définition de la suite $(c_1, c_2, \dots)$ utilise une idée de Cantor qu'on appelle "l'argument de la diagonale."

Théorème 9.2.13 (Cantor, 1873)**.** *L'ensemble $\mathbb{R}$ des nombres réels n'est pas dénombrable.*

Preuve. Si $\mathbb{R}$ est dénombrable alors I l'est aussi (puisque $I \subseteq \mathbb{R}$), donc $I \sim \mathbb{N}$ puisque I est infini. En particulier il existe une fonction surjective $\mathbb{N} \to I$, ce qui contredit la lemme 9.2.11. □

Exercices.

9.2.1. Donnez une preuve de la proposition 9.2.7. On a déjà vu une proposition similaire avec $\sim$ au lieu de $\preceq$. Imiter la démonstration.

9.2.2. Pour $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ et $r \in \mathbb{R}$ tel que $r \geq 0$, soit

$$B_{x,r} = \{(y_1, y_2, y_3) \in \mathbb{R}^3 \mid (x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 \leq r^2\}$$

la boule de rayon r et centre x. Supposez que A est une sous-ensemble de $\mathbb{R}^3$ tel que $A \cap B_{x,r}$ est un ensemble dénombrable pour tous choix de $x \in \mathbb{R}^3$ et $r \in \mathbb{R}$ tel que $r \geq 0$. Montrez que A est un ensemble dénombrable.

9.2.3. Supposons que $f\colon A \to B$ est une fonction satisfaisant : pour chaque $b \in B$, l'ensemble $f^{-1}(b) = \{x \in A : f(x) = b\}$ est dénombrable. Montrez que si B est dénombrable alors A l'est aussi.

9.3 Le Théorème de Schröder-Bernstein et Applications

Théorème 9.3.1 (Schröder–Bernstein)**.** *Quels que soient les ensembles A et B,*

$$(A \preceq B \text{ et } B \preceq A) \implies A \sim B.$$

Preuve. Il y a deux parties à la démonstration :

(i) Montrer que si le théorème est vrai dans le cas particulier où $A \cap B = \varnothing$, alors il est vrai en général.

(ii) Montrer que le théorème est vrai dans le cas particulier où $A \cap B = \varnothing$.

On commence par (i). Supposons que le théorème est vrai dans le cas particulier où $A \cap B = \varnothing$. Considérons des ensembles A, B satisfaisant $A \preceq B$ et $B \preceq A$. On doit montrer que $A \sim B$, sans supposer que A, B sont disjoints. Définissons des ensembles A' et B' par $A' = \{0\} \times A$ et $B' = \{1\} \times B$. Alors $A' \cap B' = \varnothing$. On a aussi $A' \sim A$ et $B' \sim B$, donc :

$$\begin{aligned} A' \sim A \text{ et } A \preceq B \text{ et } B \sim B' &\implies A' \preceq B' \\ B' \sim B \text{ et } B \preceq A \text{ et } A \sim A' &\implies B' \preceq A'. \end{aligned}$$

On a donc $A' \preceq B'$, $B' \preceq A'$ et $A' \cap B' = \varnothing$. Puisque le théorème est supposé vrai dans le cas particulier des ensembles disjoints, on déduit que $A' \sim B'$. Mais alors

$$A \sim A' \text{ et } A' \sim B' \text{ et } B' \sim B \implies A \sim B,$$

donc on a montré que $A \sim B$, et la preuve de la partie (i) est terminée.

Pour la partie (ii), on suppose que les ensembles A, B satisfont

$$A \preceq B,\ B \preceq A \text{ et } A \cap B = \varnothing$$

et on doit montrer que $A \sim B$. Puisque $A \preceq B$ et $B \preceq A$, il existe une injection $f\colon A \to B$ et il existe une injection $g\colon B \to A$. Remarquez que ces fonctions ne sont pas nécessairement surjectives (voir l'exemple 9.1.16).

Soit $x_0 \in A$; s'il existe $x_1 \in B$ tel que $g(x_1) = x_0$, alors x_1 est unique (puisque g est injective) et nous dirons que x_1 est *le parent de* x_0. Notez que si $x_0 \notin g(B)$, alors x_0 n'a aucun parent.

Soit $x_0 \in B$; s'il existe $x_1 \in A$ tel que $f(x_1) = x_0$, alors x_1 est unique et est appelé *le parent de* x_0. Comme dans le premier cas, il se peut que x_0 n'ait aucun parent.

Ainsi, chaque élément x_0 de $A \cup B$ a *au plus un* parent (car $A \cap B = \varnothing$). Si x_0 a un parent, désignons-le par $x_1 \in A \cup B$; si x_1 a un parent, désignons-le par $x_2 \in A \cup B$; etc. Ainsi, chaque élément x_0 de $A \cup B$ détermine une suite $(x_0, x_1, x_2, \dots)$ d'éléments de $A \cup B$ telle que chaque terme x_{i+1} de la suite est le parent du terme précédent x_i. Cette suite peut être finie ou infinie, et on la désignera par le symbole $\alpha(x_0)$. Par exemple, supposons que $x_0 \in A \cup B$ a un parent x_1, que x_1 a un parent x_2, et que x_2 n'a aucun parent ; alors $\alpha(x_0) = (x_0, x_1, x_2)$. Autre exemple : si $x_0 \in A \cup B$ n'a aucun parent alors $\alpha(x_0) = (x_0)$. Lorsque $\alpha(x_0)$ est une suite finie, $\alpha(x_0) = (x_0, x_1, \dots, x_n)$, alors x_n n'a aucun parent. Lorsque la suite est infinie, $\alpha(x_0) = (x_0, x_1, x_2, \dots)$, alors chaque x_i a un parent.

On définit ensuite le "type" de chaque élément x_0 de $A \cup B$ (il y a trois types possibles). On dira que x_0 est de type ∞ si $\alpha(x_0)$ est une suite infinie ; que x_0 est de type A si $\alpha(x_0) = (x_0, \dots, x_n)$ et $x_n \in A$; et que x_0 est de type B si $\alpha(x_0) = (x_0, \dots, x_n)$ et $x_n \in B$. Remarquez que nous avons eu besoin du fait que $A \cap B = \varnothing$ pour définir le type de x_0. En effet, si $\alpha(x_0) = (x_0, \dots, x_n)$ alors x_n appartient soit à A soit à B, mais ne peut pas appartenir aux

deux ensembles, donc le type de x_0 est bien défini. Enfin, on définit

$$\begin{array}{ll} A_\infty = \{x \in A : x \text{ est de type } \infty\}, & B_\infty = \{x \in B : x \text{ est de type } \infty\}, \\ A_A = \{x \in A : x \text{ est de type } A\}, & B_A = \{x \in B : x \text{ est de type } A\}, \\ A_B = \{x \in A : x \text{ est de type } B\}, & B_B = \{x \in B : x \text{ est de type } B\}, \end{array}$$

et on note que ces six ensembles sont deux à deux disjoints. Vérifiez les affirmations suivantes :

$$f\big(A_\infty\big) = B_\infty, \qquad f\big(A_A\big) = B_A, \qquad g\big(B_B\big) = A_B.$$

Donc les trois fonctions suivantes sont bien définies et bijectives :

$$\begin{array}{rcl} A_\infty & \to & B_\infty \\ x & \mapsto & f(x) \end{array} \qquad \begin{array}{rcl} A_A & \to & B_A \\ x & \mapsto & f(x) \end{array} \qquad \begin{array}{rcl} B_B & \to & A_B \\ x & \mapsto & g(x) \end{array}$$

Puisque A est la réunion disjointe $A = A_\infty \cup A_A \cup A_B$ et que B est la réunion disjointe $B = B_\infty \cup B_A \cup B_B$, on conclut que la fonction suivante est bien définie et est bijective :

$$h : A \to B, \quad h(x) = \begin{cases} f(x), & \text{si } x \in A_\infty \\ f(x) & \text{si } x \in A_A \\ g^{-1}(x) & \text{si } x \in A_B. \end{cases}$$

Donc $A \sim B$. □

On a déjà vu que $A \sim B \implies (A \preceq B \ \wedge \ B \preceq A)$. Donc on obtient

$$\boxed{A \sim B \iff (A \preceq B \ \wedge \ B \preceq A)}$$

Corollaire 9.3.2. *Supposons que E est un sous-ensemble de $\mathbb{R}$ satisfaisant :*

Il existe des nombres réels $a < b$ tels que $(a, b) \subseteq E$.

Alors $E \sim \mathbb{R}$.

Preuve. La fonction arctan: $\mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$ est strictement croissante, donc injective. En fait c'est une bijection puisque pour tout $y \in (-\frac{\pi}{2}, \frac{\pi}{2})$ on a $\arctan(\tan y) = y$. Donc $\mathbb{R} \sim (-\frac{\pi}{2}, \frac{\pi}{2})$. C'est facile a voir que $(-\frac{\pi}{2}, \frac{\pi}{2}) \sim (a, b)$ puisque

$$x \mapsto a + \left(x + \frac{\pi}{2}\right) \cdot \frac{b-a}{\pi}$$

est une bijection $(-\frac{\pi}{2}, \frac{\pi}{2}) \to (a, b)$. Donc $\mathbb{R} \sim (a, b)$. Puisque $(a, b) \subseteq E$, on a $(a, b) \preceq E$, donc $\mathbb{R} \preceq E$. On a aussi $E \preceq \mathbb{R}$ puisque $E \subseteq \mathbb{R}$, donc le Théorème de Schröder-Bernstein implique que $E \sim \mathbb{R}$. □

Lemme 9.3.3. *Soit S un ensemble tel que $S \sim \mathbb{N}$. Alors il existe des sous-ensembles S_0, S_1 de S satisfaisant*

$$S = S_0 \cup S_1, \quad S_0 \cap S_1 = \varnothing, \quad S_0 \sim \mathbb{N} \sim S_1.$$

Preuve. Soient $P = \{0, 2, 4, 6, \ldots\}$ et $I = \{1, 3, 5, 7, \ldots\}$. On choisit une bijection $f\colon \mathbb{N} \to S$, alors les ensembles $S_0 = f(P)$ et $S_1 = f(I)$ satisfont la condition du lemme. □

Proposition 9.3.4. *Si A est un ensemble infini et D est un ensemble dénombrable, alors $D \cup A \sim A$.*

Preuve. Puisque A est infini, il existe une injection $f\colon \mathbb{N} \to A$. Soit $S = f(\mathbb{N})$ et par Lemme 9.3.3 on peut choisir des sous-ensembles S_0, S_1 de S satisfaisant

$$S = S_0 \cup S_1, \quad S_0 \cap S_1 = \varnothing, \quad S_0 \sim \mathbb{N} \sim S_1.$$

Alors

$$D \setminus A \preceq D \preceq \mathbb{N} \preceq S_0,$$

donc il existe une injection $g_0\colon D \setminus A \to S_0$. D'autre part, $S \sim \mathbb{N} \sim S_1$ implique qu'il existe une bijection $g_1\colon S \to S_1$. On définit $g\colon D \cup A \to A$ par

$$g(x) = \begin{cases} g_0(x), & \text{si } x \in D \setminus A, \\ g_1(x), & \text{si } x \in S, \\ x, & \text{si } x \in A \setminus S. \end{cases}$$

Puisque g est injective, on a $D \cup A \preceq A$. Puisque $A \subseteq D \cup A$, on a $A \preceq D \cup A$. Alors le Théorème de Schröder-Bernstein implique $D \cup A \sim A$. □

Corollaire 9.3.5. *Soit A un ensemble non dénombrable et soit D une partie dénombrable de A. Alors $A \setminus D \sim A$.*

Preuve. On a $(A \setminus D) \cup D = A$. Puisque A n'est pas dénombrable, mais D est dénombrable, on sait que $(A \setminus D)$ n'est pas dénombrable (puisqu'on sait que la réunion de deux ensembles dénombrables est dénombrable). En particulier, $A \setminus D$ est infini. Alors le résultat s'ensuit de la proposition. □

Exemple 9.3.6. Si D est une partie dénombrable de $\mathbb{R}$, alors $\mathbb{R}/D \sim \mathbb{R}$. En particulier $R\setminus\mathbb{Q} \sim \mathbb{R}$. Il y a beaucoup plus de nombres irrationnels que nombre rationnels !

Exercices.

9.3.1. Soit S un ensemble qui est équipotent à $\mathbb{N}$ et soit $n \in \mathbb{N}$. Démontrez qu'il existe des sous-ensembles $S_0, S_1, \ldots, S_n$ de S satisfaisant

$$S = \bigcup_{i=0}^{n} S_i, \quad S_i \cap S_j = \varnothing \text{ pour tout } i \neq j, \quad S_i \sim \mathbb{N} \text{ pour tout } i.$$

9.3.2. Soient $A = (-\infty, 0) = \{x \in \mathbb{R} : x < 0\}$ et $B = [0, \infty) = \{x \in \mathbb{R} : x \geq 0\}$. Vérifiez que

$$f\colon A \to B, \quad x \mapsto -x,$$
$$g\colon B \to A, \quad x \mapsto -x - 1,$$

sont des fonctions bien définies et sont injectives. Remarquez que $A \preceq B$, $B \preceq A$ et $A \cap B = \varnothing$. Suivez pas à pas la partie (ii) du théorème 9.3.1 en utilisant A, B, f, g qu'on vient de définir. En particulier, vérifiez :

$$A_\infty = \varnothing, \quad A_A = \bigcup_{n\in\mathbb{N}} (-n-1, -n), \quad A_B = \{-1, -2, -3, -4, \dots\},$$
$$B_\infty = \varnothing, \quad B_A = \bigcup_{n\in\mathbb{N}} (n, n+1), \quad B_B = \mathbb{N},$$

et décrivez la bijection $h\colon A \to B$ donnée par la preuve.

9.4 Le Principe de Trichotomie

Théorème 9.4.1. *Toute paire d'ensembles A et B satisfait $A \preceq B$ ou $B \preceq A$.*

Preuve. Soient A, B des ensembles. Soit Ω l'ensemble de toutes les fonctions f qui satisfont :

$$\operatorname{dom} f \subseteq A \quad \wedge \quad \operatorname{codom} f = B \quad \wedge \quad f \text{ est injective.}$$

Si $f, g \in \Omega$ satisfont

$$\operatorname{dom} f \subseteq \operatorname{dom} g \ \text{ et } \ \forall_{x\in\operatorname{dom} f}\, (f(x) = g(x))$$

alors on dit que *f est une restriction de g* et on écrit $f \leq g$. Alors $(\Omega, \leq)$ est un ensemble partiellement ordonné. Vérifions que $(\Omega, \leq)$ satisfait les deux hypothèses du Lemme de Zorn.

La première hypothèse est que $\Omega \neq \varnothing$. Ceci est vrai, car l'unique fonction de $\varnothing$ vers B est un élément de Ω.

Pour vérifier la deuxième hypothèse on considère un sous-ensemble $C \subseteq \Omega$ qui satisfait $C \neq \varnothing$ et $\forall_{f,g\in C}\, (f \leq g \ \vee \ g \leq f)$; on doit montrer qu'il existe $h \in \Omega$ tel que $\forall_{f\in C}\, (f \leq h)$. Soit $U = \bigcup_{f\in C} \operatorname{dom} f$ et soit $h : U \to B$ la fonction définie par :

> *Étant donné $x \in U$, on définit $h(x) = f(x)$ où f est n'importe quel élément de C satisfaisant $x \in \operatorname{dom} f$.*

Pour s'assurer que $h : U \to B$ est une fonction bien définie, on doit vérifier que pour chaque $x \in U$ les deux conditions suivantes sont satisfaites :

(i) il existe au moins un $f \in C$ satisfaisant $x \in \operatorname{dom} f$

(ii) si $f_1, f_2 \in C$ satisfont $x \in \operatorname{dom} f_1$ et $x \in \operatorname{dom} f_2$, alors $f_1(x) = f_2(x)$.

La condition (i) est satisfaite, en vertu de la définition de U. Pour la condition (ii) on remarque d'abord que $f_1, f_2 \in C$ implique $f_1 \leq f_2$ ou $f_2 \leq f_1$, donc la définition de $\leq$ implique $f_1(x) = f_2(x)$, donc (ii) est satisfaite. Ainsi, $h : U \to B$ est une fonction bien définie.

Montrons que h est injective. Supposons que $x_1, x_2 \in U$ satisfont $h(x_1) = h(x_2)$. Pour chaque $i = 1, 2$, il existe $f_i \in C$ telle que $x_i \in \operatorname{dom} f_i$. On a alors $f_1 \leq f_2$ ou $f_2 \leq f_1$, donc $\operatorname{dom} f_1 \subseteq \operatorname{dom} f_2$ ou $\operatorname{dom} f_2 \subseteq \operatorname{dom} f_1$. Donc on a $x_1, x_2 \in \operatorname{dom} f_j$ pour un choix approprié de $j \in \{1, 2\}$. Mais alors la définition de h nous permet d'écrire $h(x_1) = f_j(x_1)$ et $h(x_2) = f_j(x_2)$, d'où

$$f_j(x_1) = h(x_1) = h(x_2) = f_j(x_2).$$

Puisque $f_j \in C \subseteq \Omega$ est une fonction injective, on obtient $x_1 = x_2$. Donc h est injective et il s'ensuit que $h \in \Omega$. On a donc prouvé l'existence d'un élément $h \in \Omega$ qui satisfait $\forall_{f \in C}\, (f \leq h)$.

On conclut que $(\Omega, \leq)$ satisfait les deux hypothèses du Lemme de Zorn. Conséquemment, il existe un élément maximal $F \in \Omega$. Il y a deux possibilités : $\operatorname{dom}(F)$ est, ou n'est pas égal à A.

i) Si $\operatorname{dom}(F) = A$ alors F est une injection de A vers B, donc $A \preceq B$.

ii) Supposons que $\operatorname{dom}(F) \neq A$ et écrivons $A_0 = \operatorname{dom}(F)$. Alors $F : A_0 \to B$ doit être surjective. En effet, si F n'est pas surjective alors on peut choisir $a \in A \setminus A_0$ et $b \in B \setminus F(A_0)$, et définir une fonction $G : A_0 \cup \{a\} \to B$ par

$$G(x) = \begin{cases} F(x) & \text{si } x \in A_0 \\ b & \text{si } x = a. \end{cases}$$

Alors $G : A_0 \cup \{a\} \to B$ est injective, donc $G \in \Omega$ et $F < G$, contredisant la maximalité de F. Ainsi, $F : A_0 \to B$ doit être surjective, donc bijective, donc $B \sim A_0 \preceq A$.

On a montré que si $\operatorname{dom}(F) = A$ alors $A \preceq B$, et que si $\operatorname{dom}(F) \neq A$ alors $B \preceq A$. □

Corollaire 9.4.2. *Si A est un ensemble infini alors $\mathbb{N} \preceq A$.*

Preuve. Par le théorème ci-dessus, on a $\mathbb{N} \preceq A$ ou $A \preceq \mathbb{N}$. Si $A \preceq \mathbb{N}$ alors A est infini est dénombrable, donc $A \sim \mathbb{N}$. Donc $\mathbb{N} \preceq A$. □

La corollaire 9.4.2 dit que le nombre d'éléments de $\mathbb{N}$ est plus petit que ou égal au nombre d'éléments de tout ensemble infini.

Définition 9.4.3. Étant donnés des ensembles A et B,

$$A \prec B \text{ signifie : } A \preceq B \text{ et } A \not\sim B.$$

Donc $A \prec B$ signifie qu'il existe au moins une injection $A \to B$ mais aucune bijection.

Exemples 9.4.4. (a) $\varnothing \prec \{1, 2\} \prec \{1, 2, 3\}$

(b) Si A est un ensemble fini, alors $F \prec \mathbb{N}$.

(c) $\mathbb{N} \prec \mathbb{R}$ ($\mathbb{N} \subseteq \mathbb{R}$ implique $N \preceq \mathbb{R}$ et on a vue que $\mathbb{N} \not\sim \mathbb{R}$).

Exemple 9.4.5. Est-ce l'assertion $\mathbb{N} \prec \mathbb{Z}$ est vraie ? Non ! On a vu qu'il existe une bijection $\mathbb{N} \to \mathbb{Z}$.

Proposition 9.4.6. *Quels que soient les ensembles A, B et C,*

(a) $A \prec B$ *et* $B \prec C \implies A \prec C$ *(transitivité de* $\prec$*),*
(b) $A \prec B$ *et* $B \preceq C \implies A \prec C$*,*
(c) $A \preceq B$ *et* $B \prec C \implies A \prec C$*.*

Preuve. On commence par prouver l'implication (c) par contradiction. Supposons que $A \preceq B$ et $B \prec C$ et $\neg(A \prec C)$. On a

$$A \preceq B \text{ et } B \prec C \implies A \preceq B \text{ et } B \preceq C \implies A \preceq C.$$

Donc on a $A \preceq C$ et $\neg(A \prec C)$. Donc $A \sim C$ par la définition de $\prec$. En particulier, on a

$$A \preceq B \text{ et } B \preceq C \text{ et } C \preceq A.$$

Donc

$$B \preceq C \ \wedge\ (C \preceq A \ \wedge\ A \preceq B) \implies B \preceq C \ \wedge\ C \preceq B \overset{\text{TSB}}{\implies} B \sim C,$$

qui contredit l'hypothèse $B \prec C$. Donc l'implication (c) est vraie.

Puisque

$$A \prec C \ \wedge\ B \prec C \implies A \preceq B \ \wedge\ B \prec C \overset{(c)}{\implies} A \prec C,$$

l'implication (a) est également vraie. La preuve de l'implication (b) est presque identique à celle de (c). □

Théorème 9.4.7 (Principe de Trichotomie)**.** *Toute paire d'ensembles* A *et* B *satisfait exactement une des conditions suivantes :*

$$A \prec B, \quad A \sim B, \quad B \prec A. \tag{$*$}$$

Preuve. Par le théorème 9.4.1, on a $A \preceq B$ ou $B \preceq A$. Donc une des trois conditions $(*)$ est satisfaite. Par définition de $\prec$, il n'est pas possible que $(A \prec B \ \wedge\ A \sim B)$ soit vraie ou que $(A \sim B \ \wedge\ B \prec A)$ soit vraie. Si $(A \prec B \ \wedge\ B \prec A)$ est vraie alors par transitivité de $\prec$ on obtient $A \prec A$, donc $A \not\sim A$, qui est absurde. □

Exercices.

9.4.1. Démontrez partie (b) de la proposition 9.4.6.

9.4.2. Est-ce que la tentative suivante d'une démonstration de la proposition 9.4.6(a) est valide ?

"Supposons que $A \prec B$ et $B \prec C$. Alors il existe deux fonctions $f\colon A \to B$ et $g\colon B \to C$ qui sont injectives mais pas surjectives. Alors $g \circ f\colon A \to C$ est une fonction injective (puisque la composition de deux surjections est surjective) qui n'est pas surjective (puisque g n'est pas surjective), donc pas bijective. Donc $A \prec C$."

9.4.3. Si X est un ensemble d'ensembles, est-ce $\preceq$ un ordre totale sur X ?

9.5 Les cardinalités infinies

Terminologie. On a vue que $\mathbb{N} \prec \mathbb{R}$. Soit A un ensemble.

(a) Si $A \sim \mathbb{N}$, on dit que A est *infini dénombrable*.

(b) Si $A \sim \mathbb{R}$, on dit que A *a la puissance du continu*.

Question : Est-ce que tout ensemble infini est d'un de ces deux types ? Si non, est-ce qu'il y a des ensembles "entre les deux" ?

Proposition 9.5.1. *Supposons que A est un ensemble infini qui ne satisfait ni $A \sim \mathbb{N}$ ni $A \sim \mathbb{R}$. Alors $\mathbb{N} \prec A \prec \mathbb{R}$ ou $\mathbb{R} \prec A$.*

Preuve. Puisque A est infini, on a $\mathbb{N} \preceq A$. Puisque $\mathbb{N} \not\sim A$, on a

$$\mathbb{N} \prec A. \tag{9.1}$$

Le principe de trichotomie implique

$$A \prec \mathbb{R} \text{ ou } \mathbb{R} \prec A \tag{9.2}$$

(puisque $A \not\sim \mathbb{R}$ par hypothèse). Enfin, (9.1) et (9.2) impliquent que A satisfait $\mathbb{N} \prec A \prec \mathbb{R}$ ou $\mathbb{R} \prec A$. □

Donc nous voyons que notre question se subdivise en deux :

(i) Existe-t-il un ensemble A tel que $\mathbb{N} \prec A \prec \mathbb{R}$?

(ii) Existe-t-il un ensemble A tel que $\mathbb{R} \prec A$?

Théorème 9.5.2 (Cantor)**.** *On a $\mathbb{R}^2 \sim \mathbb{R}$.*

Preuve. Considérons la représentation décimale des éléments de $I = [0, 1)$. Définissons une fonction $f\colon I \times I \to I$ par

$$f(0.x_1x_2x_3\ldots, 0.y_1y_2y_3\ldots) = 0.x_1y_1x_2y_2x_3y_3\ldots.$$

Puisque la représentation décimale $0.x_1y_1x_2y_2x_3y_3\ldots$ détermine la paire (x, y) de manière unique, f est injective. Donc $I^2 \preceq I$.

La fonction $g\colon I \to I^2$ définie par $g(x) = (x, 0)$ est injective, donc $I \preceq I^2$. Alors le Théorème de Schröder-Bernstein implique $I^2 \sim I$. Par le corollaire 9.3.2, $\mathbb{R} \sim I$, donc $\mathbb{R}^2 \sim I^2$. Ainsi $\mathbb{R}^2 \sim I^2 \sim I \sim \mathbb{R}$. □

La démonstration du corollaire suivant est une exercice.

Corollaire 9.5.3. *On a $\mathbb{R}^n \sim \mathbb{R}$ pour tout $n \geq 1$.*

Théorème 9.5.4. *Si A est un ensemble, alors $A \prec \wp(A)$.*

Preuve. Soit A un ensemble. La fonction

$$A \to \wp(A), \quad a \mapsto \{a\},$$

est injective. Donc $A \preceq \wp(A)$. Rappelez-vous que $\wp(A) \sim A$ implique $\wp(A) \preceq A$, et que $\wp(A) \preceq A$ si et seulement s'il existe une surjection $A \to \wp(A)$. Donc, pour montrer que $A \prec \wp(A)$ (c.-à-d. $A \not\sim \wp(A)$), il suffit de montrer qu'il n'existe aucune fonction surjective $A \to \wp(A)$.

Soit $f\colon A \to \wp(A)$ une fonction quelconque et montrons que f n'est pas surjective. On trouve un élément $Y \in \wp(A)$ qui n'est pas dans l'image de f. Soit

$$Y = \{a \in A : a \notin f(a)\}.$$

Prouvons par contradiction que $Y \notin f(A)$. Supposons que $Y \in f(A)$. Donc il existe $a_0 \in A$ tel que $f(a_a) = Y$. On sait que soit $a_0 \in Y$, soit $a_0 \notin Y$.

- Si $a_0 \in Y = f(a_0)$, alors $a_0 \notin \{a \in A : a \notin f(a)\} = Y$. Donc $a_0 \in Y$ et $a_0 \notin Y$, une contradiction.
- Si $a_0 \notin Y = f(a_0)$, alors $a_0 \in \{a \in A : a \notin f(a)\} = Y$. Donc $a_0 \in Y$ et $a_0 \notin Y$, une contradiction.

Donc $Y \notin f(A)$ et f n'est pas surjective. □

Corollaire 9.5.5.

(a) $\mathbb{N} \prec \wp(\mathbb{N}) \prec \wp(\wp(\mathbb{N})) \prec \dots$

(b) $\mathbb{R} \prec \wp(\mathbb{R}) \prec \wp(\wp(\mathbb{R})) \prec \dots$

Remarque 9.5.6. Remarquons que le théorème 9.5.4 s'applique aux ensembles finis aussi.

- $\varnothing \prec \wp(\varnothing) = \{\varnothing\}$
- Si un ensemble A a n éléments, alors $\wp(A)$ a 2^n éléments. Puisque $n < 2^n$ pour $n \geq 0$ (exercice), on a $A \prec \wp(A)$.

Rappelez-vous que $\mathbb{N} \prec \mathbb{R}$. Maintenant, on voit qu'il existe des ensembles "plus grands" que $\mathbb{R}$ (par exemple, $\wp(\mathbb{R})$). Est-ce qu'il existe des ensembles "entre les deux" ? C'est-à-dire, est-ce "l'hypothèse du continu" est vrai ou faux :

$$\textit{Il n'existe aucun ensemble } A \textit{ satisfaisant } \mathbb{N} \prec A \prec \mathbb{R}. \tag{HC}$$

Théorème 9.5.7 (Gödel, 1938)**.** *Si ZFC est non contradictoire, alors ZFC+(HC) est non contradictoire.*

Théorème 9.5.8 (Cohen, 1963)**.** *Si ZFC est non contradictoire, alors ZFC+¬(HC) est non contradictoire.*

Donc, l'assertion (HC) est *indécidable* : à partir des axiomes de ZFC, il est impossible de prouver (HC) et il est impossible de prouver ¬(HC).

Exercices.

9.5.1. Démontrez Corollaire 9.5.3.

9.5.2. Soient A et B des ensembles tels que $A \preceq B$. Démontrez que $\wp(A) \preceq \wp(B)$.

9.6 Les parties de $\mathbb{N}$

Par le principe de trichotomie, on sait qu'exactement une des conditions

$$\wp(\mathbb{N}) \prec \mathbb{R}, \quad \wp(\mathbb{N}) \sim \mathbb{R}, \quad \mathbb{R} \prec \wp(\mathbb{N})$$

est vraie. Laquelle ? On va démontrer :

Théorème 9.6.1. *On a $\wp(\mathbb{N}) \sim \mathbb{R}$.*

Par le corollaire 9.3.2, on sait que $\mathbb{R} \sim [a, b)$ pour tous $a, b \in \mathbb{R}$, $a < b$. Soit

$$J = [0, 2).$$

Donc $\mathbb{R} \sim J$ et il suffit de montrer que $J \sim \wp(\mathbb{N})$.

Représentations binaires. Un *représentation binaire* de $x \in J$ est une suite $x_0, x_1, x_2, \ldots$ tel que

$$x = \sum_{n=0}^{\infty} \frac{x_n}{2^n}.$$

On écrit

$$x = x_0.x_1x_2x_3\ldots.$$

Comme dans le cas des représentations décimales, chaque $x \in J$ a **au moins une** et **au plus deux** représentations binaires. Si x a deux représentations binaires, alors l'une d'elles a une queue de 0 et l'autre a une queue de 1. Par exemple,

$$\begin{aligned}\frac{1}{4} &= \frac{0}{2^0} + \frac{0}{2^1} + \frac{1}{2^2} = 0.010000\ldots \\ \frac{1}{4} &= \frac{0}{2^0} + \frac{0}{2^1} + \frac{0}{2^2} + \sum_{n=3}^{\infty} \frac{1}{2^n} = 0.001111\ldots.\end{aligned}$$

Si on rejette les représentations binaires avec un queue de 1, on a

$$\begin{aligned}J &\sim \{\text{représentations binaires sans queue de 1}\} \\ &= \{\text{représentation binaires contenant une infinité de zéros}\}.\end{aligned}$$

Pour chaque élément $x \in J$, on définit un ensemble B_x comme suit : Si $x = x_0.x_1x_2\ldots$ est la représentation binaire de x (sans queue de 1), alors

$$B_x = \{n \in \mathbb{N} : x_n = 0\}.$$

Puisque la représentation binaire contient une infinité de zéros, il s'ensuit que B_x est un ensemble infini. Donc on a défini une fonction

$$\begin{aligned}f\colon J &\to \{B \in \wp(\mathbb{N}) : B \text{ est infini}\}, \\ x &\mapsto B_x.\end{aligned}$$

Par exemple, soit $x = 1/3 \in J$. Alors

$$x = x_0.x_1x_2x_3\cdots = 0.0101010101\ldots \quad \text{(périodique)},$$

donc $x_n = 0$ lorsque $n \in \{0, 1, 3, 5, 7, \ldots\}$, donc

$$f\left(\frac{1}{3}\right) = B_{1/3} = \{0, 1, 3, 5, 7, \ldots\}.$$

Puisque chaque représentation binaire (sans queue de 1) correspond à exactement un élément de J, f est bijective. Donc

$$\mathbb{R} \sim J \sim V := \{B \in \wp(\mathbb{N}) : B \text{ est infini}\}.$$

Si on peut prouver que

$$\wp(\mathbb{N}) \setminus V \text{ est dénombrable} \tag{$*$}$$

alors

$$\wp(\mathbb{N}) = V \cup (\wp(\mathbb{N}) \setminus V) \sim V \sim \mathbb{R}$$

et on aura fini. Démontrons $(*)$. Remarquez que $\wp(\mathbb{N}) \setminus V = \wp_{\text{fin}}(\mathbb{N})$, l'ensemble des parties finis de $\mathbb{N}$. On a

$$\wp_{\text{fin}}(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \wp(\{0, 1, 2, 3, \ldots, n\})$$

est chaque $\wp(\{0, 1, 2, 3, \ldots, n\})$ est fini (donc dénombrable). Donc $\wp_{\text{fin}}(\mathbb{N})$ est une réunion dénombrable des ensembles dénombrables et donc $\wp_{\text{fin}}(\mathbb{N})$ est dénombrable.

Ceci complète la démonstration du théorème 9.6.1.

Remarque 9.6.2. Puisque $\wp(\mathbb{N}) \sim \mathbb{R}$, l'Hypothèse de Continu peut être reformulée comme suit :

$$\textit{Il n'existe aucun ensemble } A \textit{ satisfaisant } \mathbb{N} \prec A \prec \wp(\mathbb{N}). \tag{HC}$$

Il existe aussi une *Hypothèse de Continu Généralisée*, qui s'énonce ainsi :

$$\begin{aligned}&\textit{Si } E \textit{ est un ensemble infini alors il n'existe aucun ensemble } A \textit{ satisfaisant}\\ &E \prec A \prec \wp(E).\end{aligned} \tag{HCG}$$

Exercices.

9.6.1. Soit A un ensemble infini et soient

$$\wp_{\text{fin}}(A) = \{X \subseteq A : X \text{ est fini}\},$$
$$\wp_{\text{inf}}(A) = \{X \subseteq A : X \text{ est infini}\}.$$

Démontrez que $\wp_{\text{fin}}(A) \preceq \wp_{\text{inf}}(A)$.

9.7 Les nombres indescriptibles

On va voir qu'il existe des nombres indescriptibles. Premièrement, il faut définir le terme "indescriptible".

Soit A un *alphabet* fini. Par exemple, A peut être l'ensemble de tous les caractères utilisés dans toutes les langues sur la Terre (humain, ordinateur, logique, et des autres). En fait, on peut avoir un alphabet dénombrable si on veut.

Définition 9.7.1. Une *description de longueur* k est un élément de $A^k = A \times \cdots \times A$, ou il y a k copies de A. L'ensemble de tous les descriptions est

$$D = \bigcup_{k \in \mathbb{N}_+} A^k.$$

Une *interpretation* I de D est une fonction $I \colon D \to \mathbb{R}$.

Bien sur, il existe des descriptions (en fait, la plupart des descriptions) qui ne correspondent pas au nombres réels. On peut attribuer un nombre réel arbitraire, comme 0, à toute description non numérique on non-sens.

Définition 9.7.2. Donné une interpretation I, on définit l'ensemble des *nombres descriptibles* d'être l'image $I(D) \subseteq \mathbb{R}$. Tout nombre qui n'est pas descriptible est *indescriptible*.

Par exemple, si A est l'alphabet universal décrit ci-dessus et I est l'interpretation habituelle de chaînes de caractères dans cet alphabet :

- tout nombre rationnel est descriptible comme "p/q",
- tout nombre algébrique est descriptible (par exemple, "la solution de $x^5 + 25x^2 - 7$ tel que..."),
- tout nombre donné par une formule fini (par exemple, $e = \sum_{n=0}^{\infty} \frac{1}{n!}$),
- tout nombre qui est le résultat de tout programme d'ordinateur fini est descriptible.

Théorème 9.7.3. *Pour un alphabet fixe A et une interpretation I, l'ensemble des nombres descriptibles est dénombrable. Ainsi, l'ensemble des nombres indescriptibles est non dénombrable. En particulier, la plupart des nombres réels sont indescriptibles.*

Preuve. Puisque notre alphabet A est dénombrable, le produit cartésien fini A^k est dénombrable. Puisque

$$D = \bigcup_{k \in \mathbb{N}^+} A^k$$

est une réunion dénombrable d'ensembles dénombrables, on sait que D est dénombrable. Donc l'image de I, qui est

$$I(D) = \{I(d) : d \in D\} = \bigcup_{d \in D} \{I(d)\},$$

est une réunion dénombrable d'ensembles dénombrables. Donc l'image de I (l'ensemble des nombre descriptibles) est dénombrable. Par conséquent, l'ensemble $\mathbb{R} \setminus I(D)$ des nombres indescriptibles est non dénombrable. □

Index

Bibliographie

[Dai] Daniel Daigle. La théorie ZFC des ensembles. Disponible à http://mysite.science.uottawa.ca/asavag2/mat2762/notes/Daigle-ZFC.pdf.

[Nes] Ali Nesin. Foundations of mathematics I : Set theory (only a draft). Disponible à http://mysite.science.uottawa.ca/asavag2/mat2762/notes/Nesin-SetTheoryLectureNotes.pdf.