Mathématiques discrètes

David Hébert
hebert.iut@gmail.com

2022

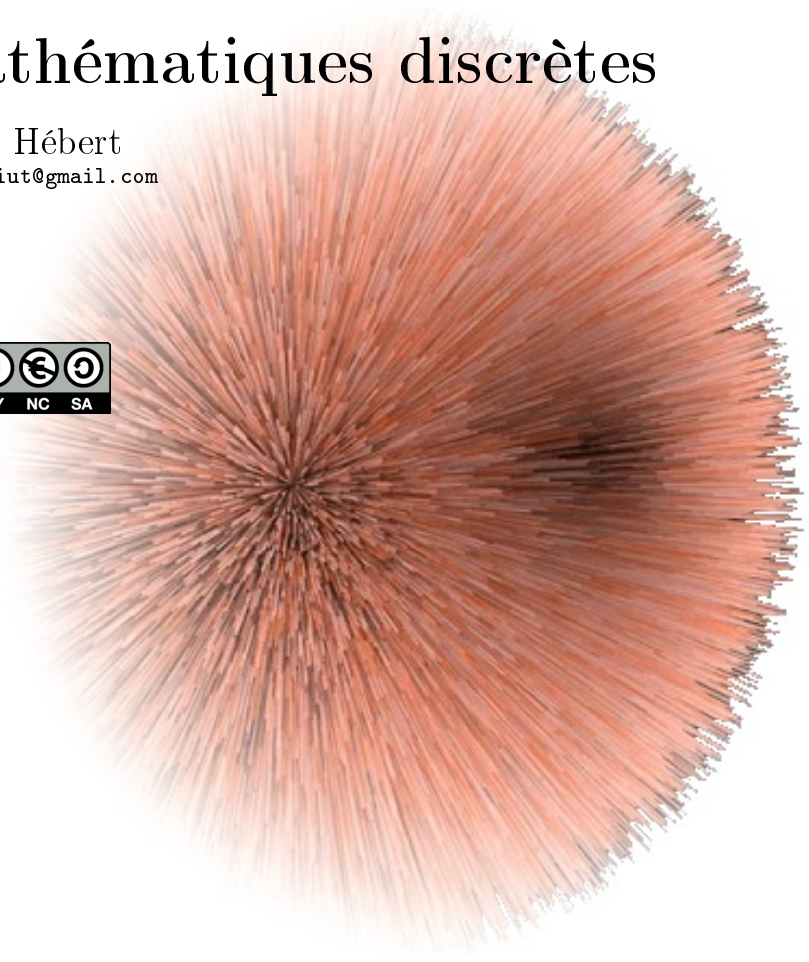


Table des matières

1. Logique propositionnelle

Proposition

Suis-je sûr de douter ?

Est-ce vrai ou est-ce faux ? Si je n'en doute pas c'est que je suis certain de douter. Si j'en doute c'est que j'envisage de ne pas douter.

Cette phrase n'est donc ni vraie ni fausse et vraie et fausse en même temps. Une sorte de phrase quantique !

Lorsqu'on va voir un mathématicien, plus précisément un logicien, pour lui demander de rendre des comptes sur ce phénomène, il répond calmement que cette phrase ne rentre pas dans le cadre des phrases étudiables. Lorsque l'on tombe sur ce genre de paradoxe, c'est qu'il y a un problème de cadrage. Alors cadrons un peu tout ça.

Définition

Une **proposition** est un énoncé dont on peut dire sans ambigüité qu'il est vrai ou qu'il est faux.

Ainsi la proposition $p =$"$2+2=4$" est une proposition vraie. De même $q =$"$2+2=5$" est une proposition fausse. Mais $r =$"Suis-je sûr de douter ?" n'est pas une proposition de sorte que la question de la valeur de vérité (vrai ou faux) ne se pose pas. Tout comme $s =$"$x+1>0$". C'est parfois vrai, parfois faux. Cela dépend de x. Il y a donc ambigüité, ce n'est donc pas une proposition.

Maintenant que le cadre est placé nous pouvons enrober de quelques définitions et outils.

Définition

- Une **tautologie** est un énoncé toujours vrai. On le note $\top$ (ou 1 ou $\mathcal{V}$).
- Une **contradiction** est un énoncé toujours faux. On le note $\bot$ (ou 0 ou $\mathcal{F}$).

Connecteurs logique et tables de vérité

Pour travailler avec les propositions et définir des outils de calculs, on utilise des *tables de vérité*. Il s'agit de table décrivant toutes les combinaisons de vérité possible d'une expression propositionnelle.

Définition

On définit le connecteur logique **OU** entre deux propositions p et q, noté $p \vee q$, la proposition définie par la table de vérité ci-contre.

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Définition

On définit le connecteur logique **ET** entre deux propositions p et q, noté $p \wedge q$, la proposition définie par la table de vérité ci-contre.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Définition

On définit le **NON**, la négation logique d'une proposition p, noté $\neg p$, par la table de vérité ci-contre.

p	$\neg p$
0	1
1	0

Le parenthésage est important. Dressons la table de vérité de l'expression (bien définie) suivante :

$$E = [p \vee (r \wedge \neg(q \wedge p))] \wedge (\neg r)$$

p	q	r	A $q \wedge p$	B $\neg A$	C $r \wedge B$	D $p \vee C$	$\neg r$	D $\wedge \neg r$ E
0	0	0	0	1	0	0	1	0
0	0	1	0	1	1	1	0	0
0	1	0	0	1	0	0	1	0
0	1	1	0	1	1	1	0	0
1	0	0	0	1	0	1	1	1
1	0	1	0	1	1	1	0	0
1	1	0	1	0	0	1	1	1
1	1	1	1	0	0	1	0	0

L'expression $E = p \vee q \wedge r$ n'est pas bien définie. Nous ne savons pas quel connecteur appliquer en premier ni même si cela à une incidence sur le résultat. Cette expression peut soit se comprendre comme $E_1 = p \vee (q \wedge r)$ ou $E_2 = (p \vee q) \wedge r$. Comparons leur table de vérité :

p	q	r	$q \wedge r$	E_1	$p \vee q$	E_2
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	1	0
0	1	1	1	1	1	1
1	0	0	0	1	1	0
1	0	1	0	1	1	1
1	1	0	0	1	1	0
1	1	1	1	1	1	1

Les tables de vérités de E_1 et E_2 sont différentes ce qui laisse à penser que ces expressions le sont aussi. Cela motive la définition suivante.

Définition

Deux propositions p et q sont égales si elles ont les mêmes tables de vérité. Dans ce cas on note $p = q$.

CANDIMATICA©

Passer par les tables de vérité peut s'avérer fastidieux. On observe en effet qu'une expression propositionnelle concernant trois propositions fait apparaitre une table de vérité à 8 lignes. On peut montrer qu'une expression impliquant n propositions donnera une table de vérité de 2^n lignes. C'est à dire que si dix propositions sont impliquées alors la table de vérité aura plus de mille lignes ! Vite, un théorème.

Théorème CANDIMATICA

Commutativité. $p \vee q = q \vee p$ et $p \wedge q = q \wedge p$.

Associativité. $p \vee (q \vee r) = (p \vee q) \vee r$ et $p \wedge (q \wedge r) = (p \wedge q)$etr.

Neutralité. $p \wedge \top = p$ et $p \vee \bot = p$.

Distributivité. $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ et $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$.

Idempotence. $p \vee p = p$ et $p \wedge p = p$.

Morgan. $\neg(p \vee q) = \neg p \wedge \neg q$ et $\neg(p \wedge q) = \neg p \vee \neg q$.

Absorption 1. $p \vee \top = \top$ et $p \wedge \bot = \bot$.

Tiers exclus. $p \vee \neg p = \top$.

Involution. $\neg(\neg p) = p$.

Contradiction. $p \wedge \neg p = \bot$.

Absoption 2. $p \vee (p \wedge q) = p$ et $p \wedge (p \vee q) = p$.

Le mot Candimatica est purement mnémotechnique. Il m'a été suggéré par Mahmoud.

Démonstration. Il s'agit de comparer les tables de vérité. Nous n'allons pas le faire pour tous. Détaillons une des deux égalités de Morgan [1] et une des deux propriétés d'absorption 2.

1. Auguste de Morgan (1806-1871), mathématicien et logicien britannique.

		A		B	C	
p	q	$p \wedge q$	$\neg A$	$\neg p$	$\neg q$	$B \vee C$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

On observe ainsi que $\neg(p \wedge q) = \neg p \vee \neg q$.

		A	
p	q	$p \wedge q$	$p \vee A$
0	1	0	0
0	1	0	0
1	0	0	1
1	1	1	1

On observe que $p \vee (p \wedge q) = p$

Il en va de même pour les autres propriétés. □

La propriété de l'associativité permet en entre autre de considérer des connections logique entre plus de deux propositions. Tant que le connecteur est le même la priorité des opérations n'est pas problématique. On se permettra alors d'écrire $p \vee q \vee r$ sous entendu qu'il s'agit de $(p \vee q) \vee r$ et qu'il appartient à chacun de déplacer les parenthèses à sa convenance.

Il est souvent plus facile de passer par ces règles que de revenir aux calculs sur les tables de vérité. Comme l'exemple suivant l'illustre.

$$\begin{aligned}
(p \wedge q) \wedge [(\neg p \wedge q) \vee (\neg p \wedge \neg q)] &= (p \wedge q) \wedge [\neg p \wedge (q \vee \neg q)] && \text{factorisation (distributivité)} \\
&= (p \wedge q) \wedge [\neg p \wedge \top] && \text{tiers exclus} \\
&= (p \wedge q) \wedge \neg p && \text{neutralité} \\
&= (p \wedge \neg p) \wedge q && \text{associativité et commutativité} \\
&= \bot \wedge q && \text{contradiction} \\
&= \bot && \text{absorption 1}
\end{aligned}$$

Implication

Il s'agit à présent de mesurer le *raisonnement*. C'est à dire la mesure que partant d'une proposition p, dont la véracité n'est pas à établir, on arrive à une proposition q. Ce que l'on cherche à mesurer est le raisonnement, la méthode utilisée. Il s'agit de l'implication.

Définition

On définit l'**implication** d'une proposition p vers une proposition q, notée $p \Rightarrow q$, par la table de vérité ci-contre.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Partant d'une proposition p vraie, par un raisonnement logique, c'est à dire sans digression et fausseté, on ne peut arriver qu'à démontrer une proposition vraie. De sorte que $1 \Rightarrow 1$ est vrai et $1 \Rightarrow 0$ est faux. Mais lorsque le point de départ du raisonnement est faux, on peut faire n'importe quoi et arriver à un énoncé qui peut-être vrai comme faux tout en suivant un raisonnement correct ; cela traduit que $0 \Rightarrow 0$ et $0 \Rightarrow 1$ sont tous deux vrais.

L'implication n'est pas vraiment un nouveau connecteur logique. D'une part, il a des propriétés très différentes du OU et du ET, ne serait-ce que la commutativité ($(p \Rightarrow q) \neq (q \Rightarrow p)$) mais d'autre part le théorème suivant permet de s'y ramener.

Théorème

$$(p \Rightarrow q) = \neg p \vee q$$

Démonstration.

p	q	A ¬p	A ∨ q
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

On observe que la table de $p \Rightarrow q$ et $\neg p \vee q$ sont identiques. □

Définition

- La **réciproque** de $p \Rightarrow q$ est $q \Rightarrow p$.
- La **contraposé** de $p \Rightarrow q$ est $\neg q \Rightarrow \neg p$.

Proposition 1.0.1

Une implication et sa contraposé ont la même valeur de vérité.

Démonstration. $(\neg q \Rightarrow \neg p) = (\neg(\neg q) \vee \neg p) = (q \vee \neg p) = (\neg p \vee q) = (p \Rightarrow q)$ par involution et commutativité. □

Considérons p="n^2 est impaire" et q="n est impaire". Tout d'abord ce ne sont pas des propositions car elles dépendent toutes les deux d'un paramètre n. Ce n'est pas loin d'être des propositions : dès que l'on donne une valeur à n on peut dire sans ambigüité leur valeur de vérité. Nous verrons très bientôt que nous pouvons nous permettre de telle considération (il s'agit de prédicat). Pour cet exemple, faisons comme s'il s'agissait de bien belle proposition.

Si nous souhaitons démontrer que tout nombre dont le carré est impaire est forcément impaire, il faut logiquement montrer que $p \Rightarrow q$. C'est un théorème difficile de prime abord. Mais le résultat précédent nous indique qu'il suffit de montrer sa contraposé $\neg q \Rightarrow \neg p$ c'est à dire que tout nombre paire a un carré paire ce qui est laissé au lecteur (et ben plus facile).

Un tel raisonnement s'appelle un *raisonnement par contraposé*[2].

Proposition

Si $(p \wedge \neg q) = \bot$ alors $(p \Rightarrow q) = \top$.

Démonstration. En effet, si $(p \wedge \neg q) = \bot$ alors en prenant la négation logique des deux cotés de cette égalité on a $\neg(p \wedge \neg q) = \top$. La propriété de Morgan et l'involution donne $\top = \neg p \vee \neg\neg q = \neg p \vee q = p \Rightarrow q$. □

Ce résultat permet de démontrer le *raisonnement par l'absurde*. Lorsque l'on souhaite démontrer que $p \Rightarrow q$ alors on montre que partant de p et $\neg q$ il y a une contradiction, c'est-à-dire $p \wedge \neg q = \bot$.

2. Original...

Equivalence

Pour finir le *si et seulement si*.

Définition

On définit l'**équivalence** entre deux propositions p et q, notée $p \Leftrightarrow q$, par la table de vérité ci-contre.

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Théorème

$$(p \Leftrightarrow q) = (p \Rightarrow q) \wedge (q \Rightarrow p)$$

Le précédent résultat sur l'implication permet par ailleurs d'écrire $(p \Leftrightarrow q) = (\neg p \vee q) \wedge (\neg q \vee p)$.

Démonstration. On laisse le soin au lecteur de comparer les tables de vérité. □

2. Ensembles de cardinalité finie

Axiomes

Un ensemble est une boite avec des trucs dedans. Telle est la version simpliste et suffisante d'un ensemble. Suffisante pendant un temps, et les mathématiciens faisaient à peu près n'importe quoi avec. Arriva un jour ou cette notion enfantine devint beaucoup trop problématique et on s'aperçut finalement que pour faire bien on ne pouvait pas faire n'importe quoi. Le célèbre *Paradoxe du barbier* de Bertran RUSSELL en est l'exemple emblématique :

> Dans une ville, un barbier rase (uniquement) tous les hommes qui ne se rasent pas eux-même.
> Qui rase le barbier ?

Pour formaliser la notion d'ensemble (et ainsi esquiver les paradoxes), plusieurs tentatives d'axiomatisation ont été proposées. La plus connue, celle que nous adopteront, est la théorie ZFC pour Zermelo, Frenkel avec l'axiome du Choix.

Définition

Un **ensemble** X est une collection d'**élément**. Un élément x appartenant à X est noté

$$x \in X$$

Les ensembles sont soumis aux axiomes suivants :

Axiome d'extentionnalité. Deux ensembles avec les même éléments sont égaux.

Axiome de l'ensemble vide. Il existe un ensemble sans élément appellé l'**ensemble vide** et généralement noté $\varnothing$.

Axiome de la paire. Si X et Y sont deux ensembles, il existe un ensemble avec ces deux ensembles comme élément. On le note $\{X, Y\}$.

Axiome de la réunion. On vera plus tard.

Axiome de l'ensemble des parties. On vera plus tard.

Axiome de l'infini. Il existe un ensemble X tel que $\varnothing \in X$ et tel que si $x \in X$ alors x et les éléments de x sont des éléments de X.

Schéma d'axiomes de compréhension. On vera plus tard.

Axiome du choix. Étant donné un ensemble X non vide d'ensemble non vide, il existe un ensemble, appelé ensemble de choix, contenant exactement un élément de chaque élément de X.

Plusieurs axiomes sont laissés pour plus tard. Nous les détaillerons dans la suite de ce cours. Mais la majorité de ces axiomes sont très naturels, dans le sens où ils ne sont pas contre nature à la logique classique.

L'axiome du choix est beaucoup plus problématique : dans une version simple il stipule qu'étant donné plein d'ensemble, on peut choisir un élément dans chaque ensemble. Ce qui est formellement facile lorsqu'on dispose d'un nombre fini d'ensemble mais est plus compliqué à imaginer avec une infinité. Cela donne naissance à des "paradoxes" qui n'en sont pas. Comme par exemple le paradoxe de Banach-Tarski qui utilise l'axiome du choix : il existe un moyen de découper une boule en 5 morceaux de tel manière qu'un réassemblement de ces morceaux permette d'obtenir deux boules strictement identique à la première. Ce résultat contre nature n'en reste pas moins un théorème c'est à dire un énoncé démontré par un raisonnement logique, donc indiscutablement vrai. Dans le cœur de la preuve il y a l'axiome du choix qui permet de choisir des éléments dans un ensemble sans forcement maitriser ces choix. Ainsi même si l'énoncé du paradoxe semble faire croire que l'axiome du choix est faux, un œil bienfaisant sur la démonstration permet de comprendre que c'est "mathématiquement" possible mais irréalisable dans la pratique. Cela suffit à certain pour considérer l'axiome du choix et donc la théorie ZFC. D'autre par contre ne vont pas l'admettre et travailler avec la théorie ZF...

Quoiqu'il en soit c'est avec ces axiomes et uniquement eux que l'on construit les ensembles classiques. Partons du commencement avec $\varnothing$, l'ensemble vide (qui ne contient aucun élément). En utilisant l'axiome de la paire, on construit alors l'ensemble $\{\varnothing\}$ qui est donc un ensemble composé d'un élément qui est l'ensemble

vide. En utilisant encore l'axiome de la paire on construit l'ensemble $\{\varnothing,\{\varnothing\}\}$. En continuant de la sorte jusqu'à l'infini, ce qui est possible d'après l'axiome de l'infini on construit un ensemble

$$\left\{\underbrace{\varnothing}_{0},\underbrace{\{\varnothing\}}_{1},\underbrace{\{\varnothing,\{\varnothing\}\}}_{2},\underbrace{\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}}_{3},\dots\right\}$$

Cet ensemble est communément noté $\mathbb{N}$. Ainsi le nombre 3 manipulé depuis toujours est en fait l'ensemble $\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$.

Dans la pratique que nous ferons de la théorie des ensembles nous considérons toujours un **référentiel**, c'est un dire un ensemble de base dont l'existence et la construction sont admises. On le notera dans la pratique $\mathcal{E}$. Toutes les définitions et notations seront relatives à ce référentiel. En particulier tous les ensembles que nous manipulerons seront des sous-ensembles de $\mathcal{E}$.

Définition

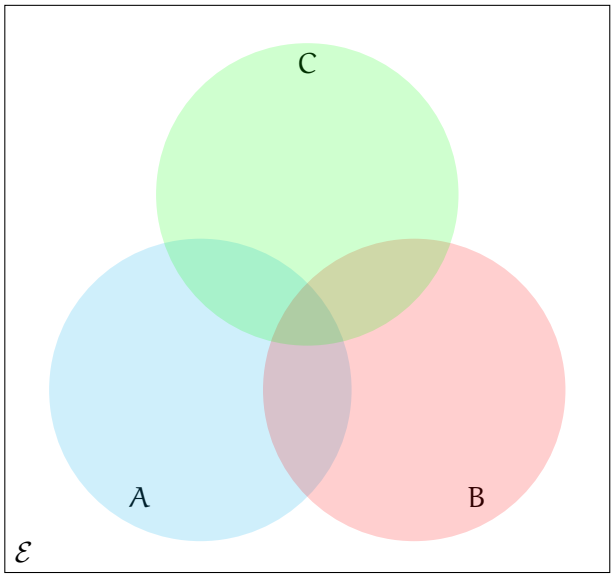
On dira que A est un **sous-ensemble** de B si tous les éléments de A sont des éléments de B. On note

$$A \subseteq B$$

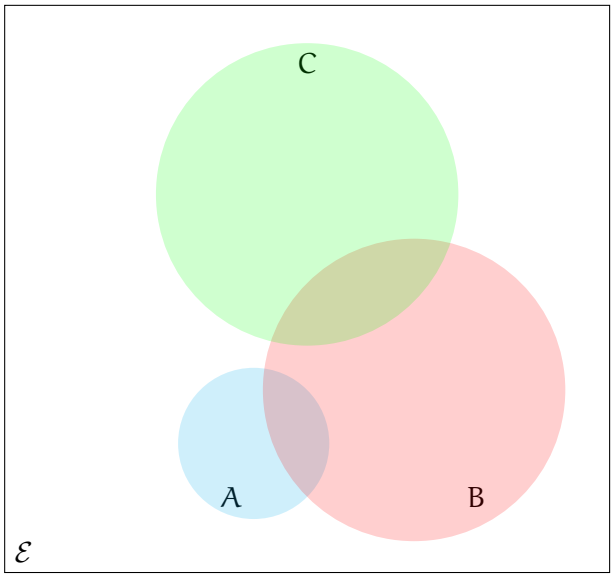
Par exemple $\mathbb{N}$ est un sous-ensemble de $\mathbb{Z}$, lui même un sous-ensemble de $\mathbb{Q}$, lui même un sous-ensemble de $\mathbb{R}$, lui même un sous-ensemble de $\mathbb{C}$, lui même un sous-ensemble de $\mathbb{H}$.

Représentation

L'outil de prédilection en théorie des ensembles est le diagramme de Venn[3]. Il consiste à placer les différents ensembles que l'on souhaite combiner comme des *patates*[4]. Il faut cependant faire attention, il faut, en générale, représenter tous les cas de figure possible.



Bon diagramme de Venn



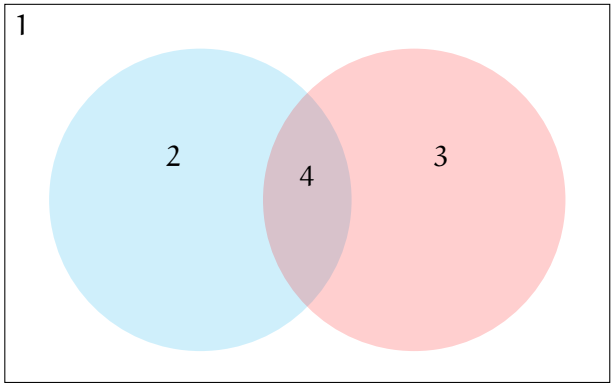
Mauvais diagramme de Venn

Proposition

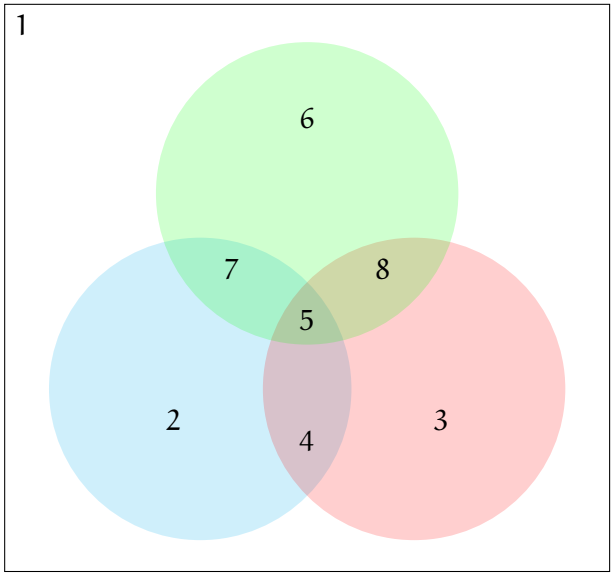
Un diagramme de Venn faisant intervenir n ensembles différents, découpe le référentiel en 2^n zone.

Démonstration. Ce résultat se démontre par récurrence sur n ce qui n'est pas le lieu ici. □

3. John Venn (1834-1923) est un mathématicien britannique.
4. On parle d'ailleurs de patatoïdes.



Deux ensembles partagent $\mathcal{E}$ en 4 zones



Trois ensembles partagent $\mathcal{E}$ en 8 zones

Peut-être que les curieux pourraient s'intéresser à Newroz...

Le calcul avec les diagrammes de Venn, permet assez souvent de représenter des configurations d'ensembles et d'observer des résultats. Il existe deux manières de définir/utiliser les ensembles :

en extension. Dans cette configuration, on décrit l'ensemble par les éléments qui le compose, entre accolade, comme dans l'exemple suivant :

$$A = \{a, 1, \text{"bonjour"}, \pi\}$$

Il y a deux règles a respecter dans ce cas :

1. L'ordre des éléments ne compte pas (c'est en fait l'axiome d'extentionnalité).

$$\{a, 1, \text{"bonjour"}, \pi\} = \{1, a, \text{"bonjour"}, \pi\}$$

2. On ne répète pas le même éléments.

$$\{a, 1, 1, 1, \text{"bonjour"}, \pi\} = \{a, 1, \text{"bonjour"}, \pi\}$$

en compréhension. Cela est une conséquence de l'axiome du schéma d'axiomes en compréhension. On défini un ensemble par la propriété qui le caractérise (qui permet de le *comprendre*).

$$B = \left\{ x \in \mathbb{R} \middle| x + 1 < 0 \right\}$$

Nous donnerons plus de détails sur les ensembles en compréhension dans le chapitre sur les prédicats.

Opérations

Il existe trois opérations élémentaires sur les ensembles. On peut en définir également d'autre mais elles se ramènes souvent à s'interpréter avec ces trois suivantes.

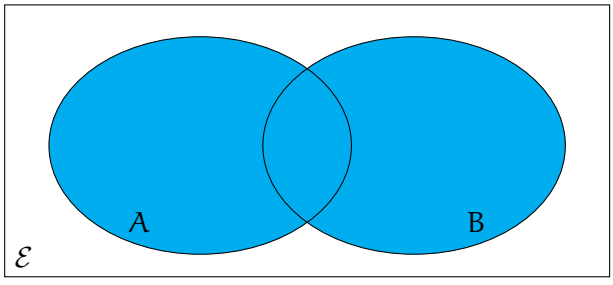
On fixe un référentiel $\mathcal{E}$. C'est entre autre l'axiome de la réunion qui justifie la première définition. Les autres découlent de celle-ci.

Définition

L'**union** de deux ensembles A et B, notée

$$A \cup B$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui appartiennent soit à A soit à B.

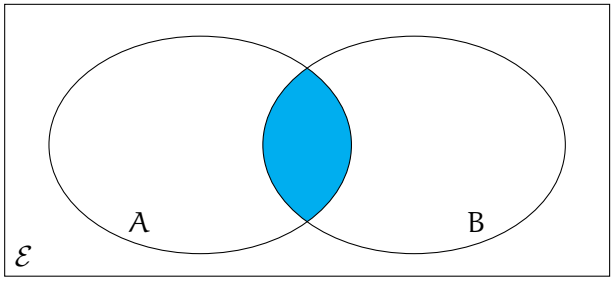


Définition

L'**intersection** de deux ensembles A et B, notée

$$A \cap B$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui appartiennent à la fois à A et à B.

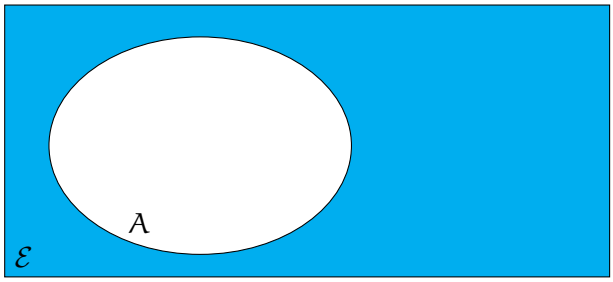


Définition

Le **complémentaire** de A, noté

$$\overline{A}$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui ne sont pas dans A.



Le complémentaire est toujours relatif au référentiel. Il est parfois nécessaire de le préciser. On note alors $\complement_{\mathcal{E}} A$ (nous pourrons nous passer de cette notation).

CANDIMATICA©

Il peut être parfois fastidieux de faire des diagrammes de Venn. Par exemple le diagramme de Venn à 5 ensembles est d'une part assez difficile à construire et d'autre part, un tel diagramme est assez peu élégant. On peut travailler avec les ensembles en s'appuyant sur des résultats bien connus, résumés dans l'acronyme *CANDIMATICA*. On fixe 3 trois ensembles A, B et C d'un même référentiel $\mathcal{E}$.

Théorème CANDIMATICA

Commutativité. $A \cup B = B \cup A$ et $A \cap B = B \cap A$.

Associativité. $(A \cup B) \cup C = A \cup (B \cup C)$ et $(A \cap B) \cap C = A \cap (B \cap C)$.

Neutralité. $A \cup \varnothing = A$ et $A \cap \mathcal{E} = A$.

Distributivité. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Idempotence. $A \cup A = A$ et $A \cap A = A$.

Morgan. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ et $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Absorption 1. $A \cup \mathcal{E} = \mathcal{E}$ et $A \cap \varnothing = \varnothing$.

Tiers exclus. $A \cup \overline{A} = \mathcal{E}$.

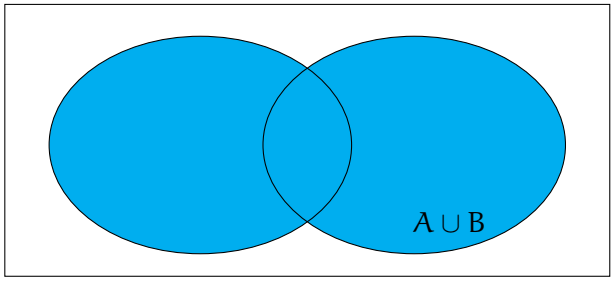
Involution. $\overline{\overline{A}} = A$.

Contradiction. $A \cap \overline{A} = \varnothing$.

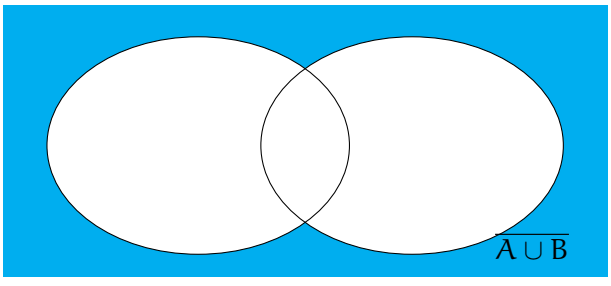
Absoption 2. $A \cup (A \cap B) = A$ et $A \cap (A \cup B) = A$.

Démonstration. On peut par exemple comparer les diagrammes de Venn et vérifier qu'ils couvrent les même zones. Vérifions une des propriétés de Morgan.

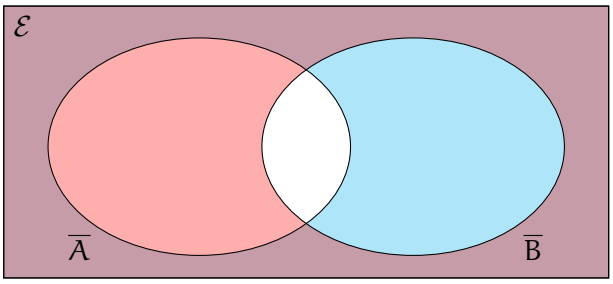
Voici le diagramme de $A \cup B$



Le complémentaire est donc



Colorons $\overline{A}$ (en bleue) et $\overline{B}$ (en rouge).



On observe alors que l'intersection de ces deux ensembles est bien $\overline{A \cup B}$.

□

Ensemble des parties

L'axiome de l'ensemble des parties justifie la définition suivante.

Définition

Pour un ensemble A, on note $\mathcal{P}(A)$ l'ensemble de tous les sous-ensembles de A.

$$\mathcal{P}(A) = \{X \subseteq A\}$$

Par exemple si $A = \{a, b\}$ alors

$$\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

Si $A = \{\alpha, \beta, \gamma\}$ alors

$$\mathcal{P}(A) = \{\varnothing, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\beta, \gamma\}, \{\alpha, \beta, \gamma\}\}$$

Cardinalité

Définition

La **cardinalité** d'un ensemble A, noté $\sharp A$ (ou parfois $|A|$ ou $\mathtt{Card}(A)$) est le nombre d'élément de A.

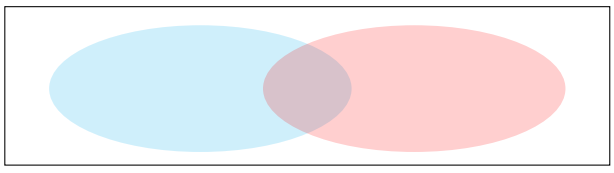
Ainsi, si $A = \{a, b, c\}$ alors $\sharp A = 3$.

Proposition

Soient A et B deux ensembles.

$$\sharp(A \cup B) = \sharp A + \sharp B - \sharp(A \cap B)$$

Démonstration.



Si on compte $\sharp A + \sharp B$ les éléments de $A \cap B$ on été compté deux fois (une fois dans A et une fois dans B) de sorte que $\sharp A + \sharp B - \sharp(A \cap B)$ compte le nombre d'élément de $A \cup B$.

□

Proposition

Soit A un ensemble.

$$\sharp\mathcal{P}(A) = 2^{\sharp A}$$

Démonstration. Il s'agit de raisonner par récurrence sur $\sharp A$. □

3. Ensembles en compréhension

Prédicats

L'énoncé "$x+1<0$" n'est pas une proposition, parce qu'il y a ambiguïté sur la valeur de vérité. Cependant lorsque l'on remplace x par n'importe quel nombre réel cela deviens une proposition. Cela motive la définition de prédicat.

Définition

Un **prédicat** sur un ensemble $\mathcal{E}$ est un énoncé $p(x)$ dépendant d'un paramètre x, de sorte qu'en remplaçant x par n'importe quelle valeurs $a \in \mathcal{E}$, $p(a)$ est une proposition

Ainsi $p(x) = "x+1<0"$ est un prédicat sur $\mathbb{R}$ de sorte que $p(1)$ est faux, comme $p(0)$ ou $p(-1)$ mais $p(-\pi)$ est vrai.

Définition

Soit p un prédicat sur un ensemble $\mathcal{E}$. La **classe** de p sur $\mathcal{E}$, noté $\mathtt{Cl}_{\mathcal{E}}(p)$ est l'ensemble des valeurs de $\mathcal{E}$ tel que le prédicat soit vrai.

$$\mathtt{Cl}_{\mathcal{E}}(p) = \left\{ x \in \mathcal{E} \middle| p(x) = \top \right\}$$

Avec notre exemple de $p(x) = "x+1<0"$, on observe que $\mathtt{Cl}_{\mathbb{R}}(p) =]-\infty;-1[$:

$$]-\infty;-1[= \left\{ x \in \mathbb{R} \middle| "x+1<0" = \top \right\}$$

Dans la pratique on ne note pas $\top$, il est sous-entendu qu'il n'y a que la valeur de vérité vraie qui nous intéresse, de sorte que l'on préfère la notation

$$]-\infty;-1[= \left\{ x \in \mathbb{R} \middle| x+1<0 \right\}$$

Une telle notation rentre dans le cadre du schéma d'axiome en compréhension de la théorie des ensembles. Ce schéma d'axiome dis en qu'une telle considération et possible et bien construite.

Pont entre proposition et ensemble

D'un coté nous avons la théorie des propositions avec sa batterie de propriétés (candimatica) et de l'autre la théorie des ensembles avec aussi ses propriété (candimatica). Les prédicats se trouvent à l'intersection de ces deux théories et le théorème suivant en forme en quelque sorte le pont

Théorème 3.0.1

Soient p et q deux prédicats définis sur un ensemble $\mathcal{E}$.

1. $\mathtt{Cl}_{\mathcal{E}}(p \vee q) = \mathtt{Cl}_{\mathcal{E}}(p) \cup \mathtt{Cl}_{\mathcal{E}}(q)$
2. $\mathtt{Cl}_{\mathcal{E}}(p \wedge q) = \mathtt{Cl}_{\mathcal{E}}(p) \cap \mathtt{Cl}_{\mathcal{E}}(q)$
3. $\mathtt{Cl}_{\mathcal{E}}(\neg p) = \overline{\mathtt{Cl}_{\mathcal{E}}(p)}$
4. $\mathtt{Cl}_{\mathcal{E}}(p \Rightarrow q) = \overline{\mathtt{Cl}_{\mathcal{E}}(p)} \cup \mathtt{Cl}_{\mathcal{E}}(q)$
5. $\mathtt{Cl}_{\mathcal{E}}(p \Leftrightarrow q) = \left(\overline{\mathtt{Cl}_{\mathcal{E}}(p)} \cup \mathtt{Cl}_{\mathcal{E}}(q)\right) \cap \left(\overline{\mathtt{Cl}_{\mathcal{E}}(q)} \cup \mathtt{Cl}_{\mathcal{E}}(p)\right)$

Démonstration. C'est une conséquence triviale des définitions et constructions □

Prenons pas exemple $p(x) = "x>0"$ et $q(x) = "x \leqslant 1"$. D'après ce théorème :

$$\begin{aligned}\mathtt{Cl}_{\mathbb{R}}(p \Rightarrow q) &= \overline{\mathtt{Cl}_{\mathbb{R}}(x > 0)} \cup \mathtt{Cl}_{\mathbb{R}}(x \leqslant 1)\\ &= \overline{]0;+\infty[} \cup]-\infty;1]\\ &=]-\infty;0] \cup]-\infty;1]\\ &=]-\infty;0]\end{aligned}$$

Cela signifie que pour tout les $x \in]-\infty;0]$ le prédicat "$x > 0$" $\Rightarrow$ "$w \leqslant 1$" est vrai. En particulier, si $x = -12$ (la première proposition de cette implication est fausse, donc l'implication est vrai).

Quantificateurs

Il existe un outil permettant de transformer les prédicats en propositions. Il s'agit des quantificateurs. Comme leur nom l'indique, ils vont *quantifier* les prédicats. Il s'agit donc de savoir si cette quantification est vraie ou fausse ; on a donc une proposition. Il existe deux quantificateurs : l'universel et l'existentiel.

Définition

Soit p un prédicat sur un ensemble $\mathcal{E}$. Le **quantificateur universel**, noté $\forall$ (prononcer *quelque soit* ou *pour tout*), transforme un prédicat $p(x)$ en proposition $\forall x, p(x)$. De plus

$$(\forall x, p(x)) = \top \qquad \Longleftrightarrow \qquad \mathtt{Cl}_{\mathcal{E}}(p) = \mathcal{E}$$

Ainsi la proposition $\forall x, p(x)$ est vrai si et seulement si la classe de p est le référentiel d'étude. Dans la pratique, le référentiel est sous-entendu, on ne le précise pas. Il peut arriver qu'il soit nécessaire de le préciser, on note alors $\forall x \in \mathcal{E},\ p(x)$. Considérons le prédicat $p(x) =$ "$x \geqslant 0$". La proposition $\forall x \in \mathbb{R},\ p(x)$ est fausse tandis que $\forall x \in \mathbb{N},\ p(x)$ est vraie.

Définition

Soit p un prédicat sur un ensemble $\mathcal{E}$. Le **quantificateur existentiel**, noté $\exists$ (prononcer *il existe*), transforme un prédicat $p(x)$ en proposition $\exists x, p(x)$. De plus

$$(\exists x, p(x)) = \top \qquad \Longleftrightarrow \qquad \mathtt{Cl}_{\mathcal{E}}(p) \neq \varnothing$$

Comme précédemment, si cela est nécessaire, on précise le référentiel d'étude.
Par exemple $\exists x \in \mathbb{R}, x^2 < 0$ est une proposition fausse tandis que $\exists x \in \mathbb{C}, x^2 < 0$ est vraie.
Le théorème suivant connecte ces deux quantificateurs et va justifier le *raisonnement par contre-exemple*.

Théorème 3.0.2

$$\neg\,(\forall x, p(x)) = (\exists x, \neg p(x)) \qquad\qquad \neg\,(\exists x, p(x)) = (\forall x, \neg p(x))$$

Démonstration.

Le second énoncé est la négation du premier (utilisé avec de l'involution). Démontrons alors le premier.

$$\begin{aligned}\neg\,(\forall x, p(x)) &= \neg\,(\mathtt{Cl}_{\mathcal{E}}(p) = \mathcal{E})\\ &= (\mathtt{Cl}_{\mathcal{E}}(p) \neq \mathcal{E})\\ &= \left(\overline{\mathtt{Cl}_{\mathcal{E}}(p)} \neq \varnothing\right)\\ &= (\mathtt{Cl}_{\mathcal{E}}(\neg p) \neq \varnothing)\\ &= (\exists x, \neg p(x))\end{aligned}$$

□

Ainsi lorsque l'on veut montrer que $\forall x, p(x)$ est faux, il suffit de montrer qu'il existe un x tel que $p(x)$ soit faux (c'est à dire $\exists x, \neg p(x)$).

4. Algèbre de Boole

Axiomes

Nous avons vu que les théories des ensembles et des propositions possédaient de nombreuses similitudes, notamment *CANDIMATIA*. L'idée ici est d'introduire une "méga" théorie qui regroupe toutes ces théories similaire. La difficulté consiste alors à bien la définir : qu'est-ce qui est axiomatique et qu'est-ce qui se démontre ? Voici une réponse.

Définition

Une *algèbre de Boole* $\mathbb{B}$ est la donnée de :

- Un ensemble, que l'on assimile à $\mathbb{B}$, avec au moins deux éléments distincts, notés 0 et 1.
- Trois opérations :

  Une addition entre deux éléments a et b de $\mathbb{B}$ notée $a+b$.

  Une multiplication entre deux éléments a et b de $\mathbb{B}$ notée $a \times b$ ou plus communément ab.

  La conjugaison d'un élément $a \in \mathbb{B}$ noté $\overline{a}$.

Ces données satisfont les axiomes de CADER :

Commutativité : $a+b=b+a$ et $ab=ba$

Associativité : $(a+b)+c=a+(b+c)$ et $(ab)c=a(bc)$

Distributivité : $a(b+c)=(ab)+(ac)$ et $a+(bc)=(a+b)(a+c)$

Eléments neutre : $a+0=0$ et $a1=a$

Relation 0-1 : $a+\overline{a}=1$ et $a\overline{a}=0$

Nous avons vus aux chapitre précédent qu'étant donnée un référentiel $\mathcal{E}$ fixé, $\mathcal{P}(\mathcal{E})$ muni de l'union, de l'intersection et du complémentaire est une algèbre de Boole où $0=\varnothing$ et $1=\mathcal{E}$.

L'idée est à présent de vérifier que ces axiomes et uniquement ces axiomes permettent d'obtenir toutes les propriétés CANDIMATICA

De CADER à CANDIMATICA

Proposition Idempotence

Soient a un élément de $\mathbb{B}$ une algèbre de Boole :

$$a+a=a, \qquad aa=a$$

Démonstration. Nous ne pouvons utiliser que les axiomes donnés dans la définition d'une algèbre de Boole.

$$\begin{aligned} a &\overset{E}{=} a+0 \\ &\overset{R}{=} a+a\overline{a} \\ &\overset{D}{=} (a+a)(a+\overline{a}) \\ &\overset{R}{=} (a+a)1 \\ &\overset{E}{=} a+a \end{aligned}$$

$$\begin{aligned} a &\overset{E}{=} a1 \\ &\overset{R}{=} a(a+\overline{a}) \\ &\overset{D}{=} (aa)+(a\overline{a}) \\ &\overset{R}{=} (aa)+0 \\ &\overset{E}{=} aa \end{aligned}$$

□

Proposition Absorption I

Soient a un élément de $\mathbb{B}$ une algèbre de Boole :

$$a + 1 = 1, \qquad a0 = 0$$

Démonstration. Nous ne pouvons utiliser que les axiomes donnés dans la définition d'une algèbre de Boole ainsi que la proposition d'idempotence.

$$\begin{aligned} a + 1 &\overset{R}{=} a + (a + \overline{a}) \\ &\overset{A}{=} (a + a) + \overline{a} \\ &\overset{I}{=} a + \overline{a} \\ &\overset{R}{=} 1 \end{aligned} \qquad \begin{aligned} a0 &\overset{R}{=} a(a\overline{a}) \\ &\overset{A}{=} (aa)\overline{a} \\ &\overset{I}{=} a\overline{a} \\ &\overset{R}{=} 0 \end{aligned}$$

□

Proposition Absorption II

Soient a et b des éléments de $\mathbb{B}$ une algèbre de Boole :

$$a + (ab) = a, \qquad a(a + b) = a$$

Démonstration. Nous ne pouvons utiliser que les axiomes donnés dans la définition d'une algèbre de Boole ainsi que les propositions d'idempotence et d'absoption I.

$$\begin{aligned} a + ab &\overset{E}{=} (a1) + (ab) \\ &\overset{D}{=} a(1 + b) \\ &\overset{A^I}{=} a1 \\ &\overset{E}{=} a \end{aligned} \qquad \begin{aligned} a(a + b) &\overset{E}{=} (a + 0)(a + b) \\ &\overset{D}{=} a + (0b) \\ &\overset{A^I}{=} a + 0 \\ &\overset{E}{=} a \end{aligned}$$

□

Unicité du conjugué

Il reste à montrer la propriété de Morgan et l'involution. La clef de la preuve de ces deux résultats est le résultat suivant.

Théorème Unicité du conjugué

Soient A et B des éléments d'une algèbre de Boole $\mathbb{B}$.

$$\overline{A} = B \iff \Big(\; A + B = 1 \quad \wedge \quad AB = 0 \; \Big)$$

Démonstration. Le sens $\Rightarrow$ est une reformulation de l'axiome des relations 0-1. Démontrons la réciproque. Nous disposons de deux hypothèses $H_+ : A + B = 1$ et $H_\times : AB = 0$. Montrons qu'avec ces deux

hypothèses, CADER, les absorptions et l'idempotence, $\overline{A} = B$.

$$\begin{aligned}
\overline{A} &\overset{E}{=} \overline{A} + 0 \\
&\overset{H_\times}{=} \overline{A} + AB \\
&\overset{D}{=} (\overline{A} + A)(\overline{A} + B) \\
&\overset{R}{=} 1(\overline{A} + B) \\
&\overset{E}{=} \overline{A} + B \\
&\overset{E}{=} (\overline{A}1) + B \\
&\overset{H_+}{=} (\overline{A}(A + B)) + B \\
&\overset{D}{=} (\overline{A}A) + (\overline{A}B) + B \\
&\overset{R}{=} 0 + (\overline{A}B) + B \\
&\overset{E}{=} (\overline{A}B) + B \\
&\overset{A^{II}}{=} B
\end{aligned}$$

□

Corollaire Involution

Soit a un élément de $\mathbb{B}$ une algèbre de Boole :

$$\overline{\overline{a}} = a$$

Démonstration. On cherche à appliquer le théorème d'unicité du conjugué avec $A = \overline{a}$ et $B = a$. Sa conclusion est bien la propriété de l'involution : $\overline{A} = B$ se traduit en effet $\overline{\overline{a}} = a$. Il s'agit donc de démontrer que les hypothèses de ce théorème sont satisfaits. Précisément que $\overline{a} + a = 1$ et $\overline{a}a = 0$ ce qui n'est que la reformulation de l'axiome des relation 0-1 (avec la commutativité). □

Corollaire Morgan

Soient a et b des éléments de $\mathbb{B}$ une algèbre de Boole :

$$\overline{a + b} = \overline{a}\overline{b}, \qquad \overline{ab} = \overline{a} + \overline{b}$$

Démonstration. La démonstration de ces deux égalités sont duales. Nous n'allons démontrer que $\overline{a + b} = \overline{a}\overline{b}$. Posons $A = a + b$ et $B = \overline{a}\overline{b}$.

$$\begin{aligned}
A + B &= a + b + (\overline{a}\overline{b}) \\
&\overset{D}{=} a + [(b + \overline{a})(b + \overline{b})] \\
&\overset{R}{=} a + [(b + \overline{a})1] \\
&\overset{E}{=} a + (b + \overline{a}) \\
&\overset{A+C}{=} b + (a + \overline{a}) \\
&\overset{R}{=} b + 1 \\
&\overset{A^I}{=} 1
\end{aligned}$$

$$\begin{aligned}
AB &= (a + b)(\overline{a}\overline{b}) \\
&\overset{D}{=} (a(\overline{a}\overline{b})) + (b(\overline{a}\overline{b})) \\
&\overset{A+C}{=} ((a\overline{a})\overline{b}) + (\overline{a}(b\overline{b})) \\
&\overset{R}{=} (0\overline{b}) + (\overline{a}0) \\
&\overset{A^I}{=} 0 + 0 \\
&\overset{E}{=} 0
\end{aligned}$$

Nous avons donc démontrer que $A+B=1$ et $AB=0$. D'après le théorème d'unicité du conjugué, $\overline{A}=B$ soit $\overline{a+b}=\overline{a}\overline{b}$. □

En conclusion uniquement à partir de CADER, nous arrivons à retrouver toutes les propriétés CANDIMATICA.

Corollaire

Soit $\mathbb{B}$ une algèbre de boole alors $\overline{0}=1$.

Bien que cet énoncé semble évident, il n'est ni démontré pour le moment, ni utilisé.

Démonstration. On a $0+1=1$ (soit par la neutralité de 0, soit par l'absorption I) et $01=0$ (soit par la neutralité du 1, soit par l'absorption I). D'après le théorème d'unicité du conjugué, $\overline{0}=1$. □

Un autre exemple

Soit D l'ensemble des diviseurs positif de 6. Sans plus de cérémonie on a $D=\{1,2,3,6\}$. On définit sur D les trois opérations suivantes :

- Pour a et b dans D on pose $a\times_D b=\mathrm{PGCD}(a,b)$.
- Pour a et b dans D on pose $a+_D b=\mathrm{PPCM}(a,b)$.
- Pour a dans D on pose $\overline{a}=\dfrac{6}{a}$.

Les règles de calcul arithmétiques donnes les tables de calculs suivantes.

$+_D$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\times_D$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

a	$\overline{a}$
1	6
2	3
3	2
6	1

En observant ces tableaux on aperçoit très facilement (par symétrie) que $a+_D b=b+_D a$ et $a\times_D b=b\times_D a$. De même, par des résultats bien connus de l'arithmétique, l'associativité et la distributivité sont vérifiées. Il reste à vérifier l'axiome des éléments neutres et des relations 0-1 pour montrer que cet ensemble et ces opérations définissent bien une algèbre de Boole.

On observe que la table d'addition que $a+_D 1=a$ de sorte que 1 semble être le bon candidat pour 0_D. De la même manière, puisque $a\times_D 6=a$, $1_D=6$. Il suffit alors de vérifier que ces éléments neutres vérifient les relations 0-1. Cela se fait au cas par cas et est trivialement observé (partie encadrée dans les tableaux).

5. Relations binaires

Nous avons vu que les ensembles, une fois l'axiomatique correctement posée, offraient un cadre de travail très confortable à beaucoup de calcul : tout est ensemble. La continuité canonique de l'étude est de mettre les ensembles en relation et d'étudier leurs dépendances ou indépendances, tout du moins de se donner des outils de mesure de tels phénomènes. Les *relations* donnent ce cadre de travail. Nous quitterons très rapidement le chemin tortueux de la généralité pour le confortable sentier de la relation qu'un ensemble peut avoir avec lui-même.

Produit cartésien

Définition

Soient X et Y des ensembles de référentiels fixés. On définit le **produit cartésien** de X et Y noté

$$X \times Y$$

prononcé *x croix y*, l'ensemble formé des **couples** (x, y) où $x \in X$ et $y \in Y$.

L'existence du produit cartésien est garantie par les axiomes de la théorie des ensembles ; notamment l'axiome de la paire.

On fera attention aux notations. On note $\{x, y\}$ l'ensemble à deux éléments x et y, tandis que l'on note (x, y) le couple de $X \times Y$[5].

En particulier, nous avions souligné que la notion en extension était assujettie à deux règles :

1. Ne pas répéter deux fois le même élément. C'est à dire que l'ensemble $\{x, x\}$ n'existe pas, ou plutôt se simplifie au singleton $\{x\}$. Alors que pour un produit cartésien l'élément $(x, x) \in X \times X$ peut exister.
2. L'ordre des éléments ne compte pas. C'est à dire que l'ensemble $\{x, y\}$ est le même ensemble que $\{y, x\}$. Alors que le couple $(x, y) \in X \times Y$ n'est pas, à priori, le même élément que le couple $(y, x) \in Y \times X$.

Soient $X = \{1, 2, 3\}$ et $Y = \{a, b\}$ alors $X \times Y = \left\{ \begin{array}{ll} (1, a), & (1, b), \\ (2, a), & (2, b), \\ (3, a), & (3, b) \end{array} \right\}$

Proposition

Soient X et Y deux ensembles de cardinalité finie alors

$$\sharp(X \times Y) = \sharp X \times \sharp Y$$

Définition

Soit X un ensemble. On note $X^2 = X \times X$. De manière générale, pour tout entier $n \in \mathbb{N}_{>0}$ on note $X^n = X \times X^{n-1}$ où $X^1 = X$. Les éléments de X^n sont appelé des n-uplet.

Si X est un ensemble alors par construction les éléments de X^2 sont des couples $(x_1, x_2) \in X \times X$ par construction. Observons les éléments X^3. Selon la définition précédente, il s'agit de $X \times X^2$, c'est à dire des couples de la forme $(x_1, (x_2, x_3))$. On peut monter que $X \times X^2 = X^2 \times X$ c'est à dire que le couple $(x_1, (x_2, x_3))$ s'identifie au couple $((x_1, x_2), x_3)$. Cette identification permet la notation (x_1, x_2, x_3). C'est pourquoi on parle de triplet (3-uplet).

Relation binaire

Nous nous intéressons aux relations entre ensembles de cardinalité finie.

5. En bref, il faut faire attention aux symboles utilisées : accolade pour des ensembles, parenthèses pour des couples

Définition

Soient X et Y deux ensembles. Une relation de X vers Y (ou X sur Y) est la donnée d'un sous ensemble $\mathcal{R} \subseteq X \times Y$. On note $x\mathcal{R}y$ pour $(x, y) \in \mathcal{R}$

Soient $X = \{1, 2, 3\}$, $Y = \{a, b\}$ et $\mathcal{R} = \{(2, a), (1, b), (2, b), (3, a)\}$. Ainsi 2 est en relation avec a, noté $2\mathcal{R}a$ mais 2 n'est pas en relation avec b.

Donnons nous un outil permettant de représenter et de travailler avec les relations. Le premier de ces outils est la représentation matricielle qui est dans la pratique la forme la plus utilisée parce qu'elle se programme facilement (par presque tous les langages de programmation).

Définition

Soit $\mathcal{R}$ une relation de X vers Y deux ensembles de cardinalité finies. La **matrice booléenne** de $\mathcal{R}$ est une matrice avec $\sharp X$ lignes et $\sharp Y$ colonnes définie par la règle

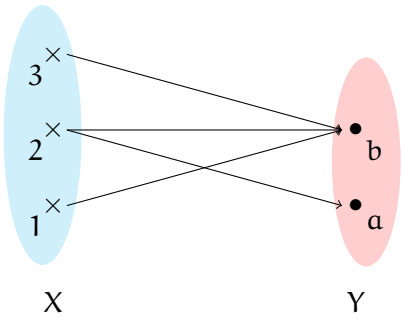
$$M_{i,j} = \begin{cases} 1 & \text{si } x_i \mathcal{R} y_j \\ 0 & \text{sinon} \end{cases}$$

La matrice booléenne de la relation précédente est

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Il existe une manière plus *humaine* pour représenter les relations. Il s'agit de la représentation sagittale bipartie. Sagittale = avec des flèches. Bipartie = entre deux paries. On utilise les diagrammes de Venn. On représente les deux ensembles par deux patatoïdes, en marquant les éléments qui les composent. On relie les éléments qui sont relation.

Sur l'exemple précédent la représentation sagittale bipartie est



Relation binaire interne

Un cas particulier, et souvent très pratique, est les relations d'un ensemble sur lui-même.

Définition

Un relation $\mathcal{R}$ d'un ensemble X sur lui-même est appelé une **relation binaire interne**. On dit simplement que $\mathcal{R}$ est une relation sur X.

Si par exemple $X = \{a, b, c\}$ alors

$$\mathcal{R} = \{(a, b), (b, a), (b, b), (c, a), (c, c)\}$$

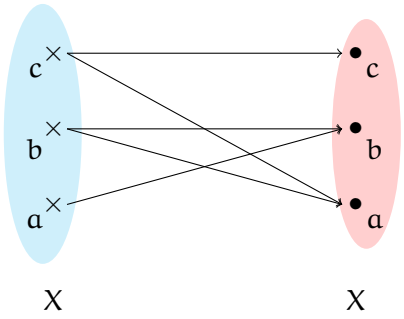
est une relation sur X. Pour cette relation $a\mathcal{R}b$ et $b\mathcal{R}a$ mais $c\mathcal{R}a$ sans que a en soit en relation avec c. L'ordre des éléments est important. Dans le cas particulier d'une relation binaire interne, il est donc possible qu'un élément soit en relation avec lui-même comme c'est la cas de l'exemple ou $b\mathcal{R}b$ et $c\mathcal{R}c$.

Dans ce cas, les matrices booléennes sont des matrice carrés (autant de ligne que de colonne). Dans cet exemple

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

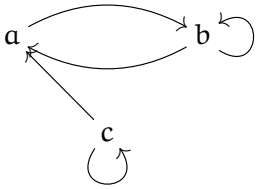
Approchons-nous de la théorie des graphes. En effet pour représenter les relations binaires internes pour un traitement *humain*, un peu plus interprétable que les matrices booléennes, on va partir des représentations sagittales biparties.

La représentation sagittale bi-partie de l'exemple précédent est



Dans une telle représentation, il n'est pas nécessaire de représenter deux fois l'ensemble X. Il suffit de le représenter une seule fois et de relier les éléments en relation, le sens de la flèches indiquant le sens de la relation.

Finalement une représentation sagittale est simplement



Propriétés STAR

Certaines relations ont des propriétés assez spéciales (qui permettent de les classer par exemple). Détaillons-en certaines.

Définition

Soit $\mathcal{R}$ une relation binaire sur un ensemble X.

Symétrique. On dira qu'une relation est symétrique si

$$\forall x, y \in X, \quad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x)$$

Transitive. On dira qu'une relation est transitive si

$$\forall x, y, z \in X, \qquad (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow (x\mathcal{R}z)$$

Antisymétrique. On dira qu'une relation est antisymétrique si

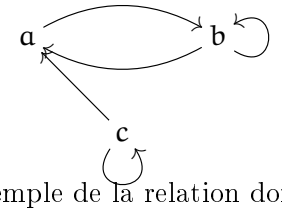
$$\forall x, y \in X, \quad (x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow (x = y)$$

Reflexive. On dira qu'une relation est réflexive si

$$\forall x \in X, \qquad x\mathcal{R}x$$

Attention à ne pas assimiler l'antisymétricité à la négation de la symétricité. En effet la négation d'être symétrique transforme le quantificateur $\forall$ en $\exists$ ce qui n'est pas la caractérisation d'être antisymétrique.

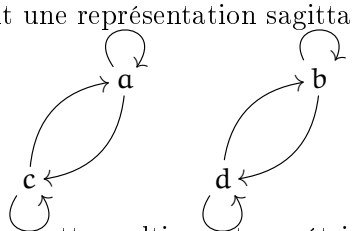
Reprenons l'exemple précédent avec la relation dont une représentation sagittale est



Cette relation n'est pas symétrique puisque $c\mathcal{R}a$ mais a n'est pas en relation avec c. De même cette relation n'est pas transitive car $c\mathcal{R}a$ et $a\mathcal{R}b$ mais c n'est pas en relation avec b. Elle n'est pas non plus antisymétrique puisque $a\mathcal{R}b$, $b\mathcal{R}a$ et pourtant $a \neq b$. Finalement cette relation n'est pas réflexive car a n'est pas en relation avec a.

En particulier cette relation n'est ni symétrique ni antisymétrique.

Prenons l'exemple de la relation dont une représentation sagittale est la suivante :



On laisse le soin au lecteur de vérifier que cette realtion est symétrique, réflexive et transitive.

Voici un petit outil (informatique) permettant de vérifier certaine de ces propriétés.

Théorème

Soient $\mathcal{R}$ une relation binaire sur une ensemble X et M la matrice booléenne de $\mathcal{R}$ (il s'agit donc d'une matrice carré).

- La relation $\mathcal{R}$ est réflexive si et seulement si

$$\forall i, \qquad M_{i,i} = 1$$

  Autrement : il n'y a que des 1 sur la diagonale principale de M.

- La relation $\mathcal{R}$ est symétrique si et seulement si

$$\forall i, j, \qquad M_{i,j} = M_{j,i}$$

  Autrement : la matrice est symétrique par rapport la la diagonale principale.

- La relation $\mathcal{R}$ est antisymétrique si et seulement si

$$\forall i \neq j, \qquad , M_{i,j} \times Mj, i = 0$$

  où le produit peut être assimiler à celui de $\mathbb{Z}$ (mais est en fait celui de l'algèbre booléenne standard). Autrement dit : aucun 1 n'est symétriquement opposé, par rapport à la diagonale principale, à un 1.

Démonstration.

- Dire que $x_i \mathcal{R} x_i$ est strictement équivalent à dire $M_{i,i} = 1$.
- La proposition $x_i \mathcal{R} x_j$ est soit vraie soit faux. Si elle est vraie elle implique, si la relation est réflexive, que $x_j \mathcal{R} x_i$. Donc $M_{i,j} = 1$ et $M_{j,i} = 1$ soit $M_{i,j} = M_{j,i}$. Si $x_i \mathcal{R} x_j$ est faux alors $M_{i,j} = 0$. Dans ce cas peut importe que $x_j \mathcal{R} x_i$ ou non, la proposition de symétricité sera vérifiée. Mais si $x_j \mathcal{R} x_i$ est vraie alors, puisque qu'il y a le quantificateur $\forall$, il faut, par le raisonnement précédent (en inversant i et j) que $x_i \mathcal{R} x_j$ ce que nous avons supposer faux. Donc nécessairement $x_j \mathcal{R} x_i$ est faux, c'est à dire $M_{i,j} = 0 = M_{j,i}$.
- On raisonne comme précédemment en raisonnant avec des 0 et 1 dans la matrice. Si $M_{i,j} = 0$ ou $M_{j,i} = 0$ alors $x_i \mathcal{R} x_j \wedge x_j \mathcal{R} x_i$ est faux et donc l'implication est vraie. Dans ce cas $M_{i,j} \times M_{j,i} = 0$.

□

Lorsque l'on combine certaine de ces propriétés on caractérise (classe) les relations.

Définition

Soit $\mathbb{R}$ une relation sur un ensemble X.

- Si $\mathcal{R}$ est réflexive, symétrique et transitive alors on dira que c'est une **relation d'équivalence**.
- Si $\mathcal{R}$ est réflexive, antisymétrique et transitive alors on dira que c'est une **relation d'ordre**.

Par exemple sur $\mathbb{N}$ la relation $=$ est une relation d'équvalence. De même la relation $\leqslant$ est une relation d'ordre.

Un jour je serais le meilleur dresseur.

7. Sommations finies

Indices

On rappel que pour tout $a \leqslant b$, on note $[\![a;b]\!]$ l'intervalle des nombres entiers entre a et b. Comme pour les nombres réels on adoptera les notations de bornes incluses ou non ($[\![a;b[\![$, $]\!]a;b]\!]$ et $]\!]a;b[\![$)

On rappel qu'une bijection de E sur F est la donnée d'une application $\varphi : E \to F$ tel qu'il existe $\psi : F \to E$ tel que pour

(i). $\forall e \in E, \psi(\varphi(e)) = e$.

(ii). $\forall f \in F, \varphi(\psi(f)) = f$.

On dit que ψ est la *bijection réciproque*.

Définition

Un sous-ensemble d'un référentiel quelconque qui peut être mis en bijection avec un sous-ensemble de $\mathbb{Z}$ est un **ensemble d'indice**

Par exemple $\{-1;7;9\}$ est un ensemble d'indice. Dans la pratique les ensembles d'indices sont les sous-ensembles de $\mathbb{Z}$ de la forme $[\![a;b]\!]$ ou $[\![a;b[\![$ lorsque $b = +\infty$.

Lemme : L'ensemble des entiers naturel $\mathbb{N}$ est un ensemble d'indice.

Démonstration. On montre que les deux applications suivantes sont des bijections réciproques l'une de l'autre :

$$\begin{array}{rccl} \varphi : \mathbb{N} & \longrightarrow & \mathbb{Z} & \\ n & \longmapsto & \begin{cases} -\dfrac{n}{2}, & \text{si } n \text{ est paire} \\ \dfrac{n+1}{2}, & \text{sinon} \end{cases} \end{array} \qquad \begin{array}{rccl} \psi : \mathbb{Z} & \longrightarrow & \mathbb{N} & \\ x & \longmapsto & \begin{cases} -2x, & \text{si } x \leqslant 0 \\ 2x-1, & \text{sinon} \end{cases} \end{array}$$

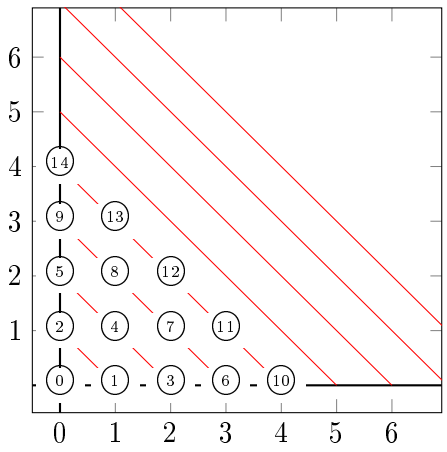
□

Proposition

L'union, l'intersection, le complémentaire et le produit cartésien (fini) d'ensembles d'indice est un ensemble d'indice.

Démonstration. L'union, l'intersection et le complémentaire de sous-ensembles de $\mathbb{Z}$ est un sous-ensemble de $\mathbb{Z}$, ce qui permet de construire des bijections aisément pour arriver à la définition.

D'après le lemme précédent, il suffit de montrer que $\mathbb{N} \times \mathbb{N}$ est un ensemble d'indice ce qui permettra de prouver que tout sous-ensemble de $\mathbb{N}\times\mathbb{N}$ est un ensemble d'indice donc tout sous-ensemble de $\mathbb{Z}\times\mathbb{Z}$ et *a fortiori* les sous-ensembles de la forme $I \times J$. Pour cela on numérote les éléments de $\mathbb{N} \times \mathbb{N}$ en diagonale ce qui permet d'associé à chaque point du réseau $\mathbb{N} \times \mathbb{N}$ une valeur entière et réciproquement.



□

Définition

Soit I un ensemble d'indice. Une **suite réelle** u indexée par I est la donnée d'une application de I sur $\mathbb{R}$.
Pour tout $i \in I$ on appel **i-ème terme** de u, noté u_i l'image de i par u.

En d'autre terme, à chaque indice on associe une valeur réelle.
Les suites indexées par $[\![0;+\infty[\![$ sont les *suites numériques* classiques.

Définition

Soit u une suite indexée par un ensemble d'indice I. On note

$$\sum_{i\in I} u_i$$

la **sommation** de tous les termes la suite u.

Par exemple si $I = [\![1;3]\!]$ et $u = (2,-7,\pi)$ alors $\sum_{i\in I} u_i = 2 + (-7) + \pi = -5 + \pi$.

Définition **Troncature**

Soient I un ensemble d'indice et $J \subseteq I$. On note $u_{|J}$ la **restriction** de u à J.

$$\forall j \in J,\ u_{|J}(j) = u(j)$$

Pour ne pas alourdir les notations et lorsqu'il n'y a pas d'ambiguïté on notera simplement u la restriction de u à J.
Si par exemple $I = [\![0;5]\!]$, $u = (9,6,1,0,1,7)$ et $J = \{0;2;4\}$ alors $u_{|J} = (9,1,1)$.

Remarque : La variable de sommation est dite *muette* : elle n'intervient pas dans le résultat de la sommation mais dans sa formulation. Ainsi $\sum_{i\in I} \alpha_i = \sum_{j\in I} \alpha_j = \sum_{k\in I} \alpha_k = \sum_{truc\in I} \alpha_{truc}$.

Propriétés de la sommation

A partir de maintenant et jusqu'à la fin du chapitre, les ensembles d'indices sont tous de cardinalité finie.

Proposition

Soient I et J des ensembles d'indices, α une suite de nombres réelles indexées par $I \cup J$.

(i). Si $I \cap J = \varnothing$, $\sum_{k\in I\cup J} \alpha_k = \sum_{i\in I} \alpha_i + \sum_{j\in J} \alpha_j$.

(ii). $\sum_{k\in I\cup J} \alpha_k = \sum_{i\in I} \alpha_i + \sum_{j\in J} \alpha_j - \sum_{l\in I\cap J} \alpha_l$.

Démonstration. Notons $I = \{i_1,\dots,i_N\}$ et $J = \{j_1,\dots,j_M\}$ alors $I \cup J = \{i_1,\dots,i_N,j_1,\dots,j_M\}$ dans ce cas

$$\sum_{k\in I\cup J} \alpha_k = \alpha_{i_1} + \cdots + \alpha_{i_N} + \alpha_{j_1} + \cdots + \alpha_{j_M} = \sum_{i\in I} \alpha_i + \sum_{j\in J} \alpha_j$$

Si $I \cap J \neq \varnothing$, notons $I \cap J = \{k_1, \dots, k_R\}$ alors $I = \{i_1, \dots, i_N, k_1, \dots, k_R\}$ et $J = \{j_1, \dots, j_M, k_1, \dots, k_R\}$. Nous avons alors :

$$\begin{aligned}
\sum_{i\in I} \alpha_i + \sum_{j\in J} \alpha_j - \sum_{l\in I\cap J} \alpha_l &= (\alpha_{i_1} + \cdots + \alpha_{i_N} + \alpha_{k_1} + \cdots + \alpha_{k_R}) \\
&\quad + (\alpha_{j_1} + \cdots + \alpha_{j_M} + \alpha_{k_1} + \cdots + \alpha_{k_R}) \\
&\quad - (\alpha_{k_1} + \cdots + \alpha_{k_R}) \\
&= (\alpha_{i_1} + \cdots + \alpha_{i_N}) + (\alpha_{j_1} + \cdots + \alpha_{j_M}) + (\alpha_{k_1} + \cdots + \alpha_{k_R}) \\
&= \sum_{l\in I\cup J} \alpha_l
\end{aligned}$$

□

Corollaire

Soit $(\alpha_i)_{i\in I}$ une suite de nombres réelles indexées par un ensemble d'indice I.

$$\sum_{i\in\varnothing} \alpha_i = 0$$

Démonstration. D'après le point (i) du précédent résultat nous avons :

$$\sum_{i\in I} \alpha_i = \sum_{i\in I\cup\varnothing} \alpha_i = \sum_{i\in I} \alpha_i + \sum_{i\in\varnothing} \alpha_i$$

d'où le résultat. □

Théorème Linéarité

Soient I un ensemble d'indice, α et β des suites de nombres réelles indexées par I et $\lambda \in \mathbb{R}$.

(i) - **Commutativité.** $\sum_{i\in I} (\alpha_i + \beta_i) = \sum_{i\in I} \alpha_i + \sum_{i\in I} \beta_i$.

(ii) - **Distributivité.** $\sum_{i\in I} \lambda\alpha_i = \lambda \sum_{i\in I} \alpha_i$.

Démonstration. Il s'agit d'un reformulation de la commutativité de l'addition ($a + b = b + a$) et de la distributivité dans $\mathbb{R}$ ($\lambda(a + b) = \lambda a + \lambda b$). □

Théorème Fubini

Soit α une suite de nombre réelles indexées par un ensemble de la forme $I \times J$ pour deux ensembles d'indices I et J.

(iii) - **Associativité.** $\sum_{(i,j)\in I\times J} \alpha_{(i,j)} = \sum_{i\in I} \left(\sum_{j\in J} \alpha_{(i,j)} \right) = \sum_{j\in J} \left(\sum_{i\in I} \alpha_{(i,j)} \right)$.

Démonstration. Il s'agit de la reformulation de l'associativité de la l'addition ($(a + b) + c = a + (b + c)$). □

Théorème Changement de variable

Soit $\varphi : J \to I$ une bijection entre deux ensembles d'indices et α une suite de nombres réelles

indexées par I.

$$\sum_{i\in I}\alpha_i=\sum_{j\in J}\alpha_{\varphi(j)}$$

Démonstration. Numérotons les éléments de I et de J à l'aide de φ. Précisément, notons $I=\{i_1,\dots,i_N\}$ et $J=\{j_1,\dots,j_N\}$ (ils sont nécessairement de même cardinalité N car en bijection) de telle sorte que $\varphi(j_k)=i_k$. Alors

$$\begin{aligned}\sum_{j\in J}\alpha_{\varphi(j)} &= \alpha_{\varphi(j_1)}+\cdots+\alpha_{\varphi(j_N)}\\ &= \alpha_{i_1}+\cdots+\alpha_{i_N}\\ &= \sum_{i\in I}\alpha_i\end{aligned}$$

□

Corollaire Formule du produit

Soient α et β deux suites de nombres réelles respectivement indexées par I et J des ensembles d'indices. Si $i\notin I$ on convient que $\alpha_i=0$. De même si $j\notin J$, $\beta_j=0$.

(iv). $\left(\sum_{i\in I}\alpha_i\right)\times\left(\sum_{j\in J}\beta_j\right)=\sum_{(i,j)\in I\times J}\gamma_{(i,j)}$ où $\gamma_{(i,j)}=\alpha_i\beta_j$.

(v). Dans le cas où $I=[\![a;n]\!]$ et $J=[\![b;m]\!]$ pour des entiers $a\leqslant n$ et $b\leqslant m$,

$$\left(\sum_{i=a}^{n}\alpha_i\right)\times\left(\sum_{j=b}^{m}\beta_j\right)=\sum_{k=a+b}^{n+m}\gamma_k$$

où $\gamma_k=\sum_{i=a}^{k-b}\alpha_i\beta_{k-i}=\sum_{j=b}^{k-a}\alpha_{k-j}\beta_j$.

Démonstration. La première égalité est la réécriture de la somme. Seul le dernier point nécessite quelques détails. On a $[\![a;n]\!]\times[\![b;m]\!]=X_{a+b}\cup X_{a+b+1}\cup X_{a+b+2}\cup\cdots X_{n+m}$, où $X_k=\{(i,j)\in[\![a;n]\!]\times[\![b;m]\!]\,|\,i+j=k\}$. Naturellement si $k\neq k'$ alors $X_k\cap X_{k'}=\varnothing$; il ne peut, en effet, exister de couple (i,j) tel que $i+j=k$ et $i+j=k'$ lorsque $k\neq k'$. Ainsi :

$$\begin{aligned}\left(\sum_{i=a}^{n}\alpha_i\right)\times\left(\sum_{j=b}^{m}\beta_j\right) &= \sum_{(i,j)\in[\![a;n]\!]\times[\![b;m]\!]}\alpha_i\beta_j\\ &= \sum_{(i,j)\in X_{a+b}}\alpha_i\beta_j+\sum_{(i,j)\in X_{a+b+1}}\alpha_i\beta_j+\cdots+\sum_{(i,j)\in X_{n+m}}\alpha_i\beta_j\\ &= \sum_{k=a+b}^{n+m}\sum_{(i,j)\in X_k}\alpha_i\beta_j\end{aligned}$$

Or $\varphi_k:[\![a;b-k]\!]\to X_k$, $i\mapsto(i,k-i)$ est une bijection de sorte qu'en appliquant ce changement de variable on a $\sum_{(i,j)\in X_k}\alpha_i\beta_j=\sum_{i\in[\![a;b-k]\!]}\alpha_i\beta_{k-i}$. De la même manière, la bijection $\psi:[\![b;k-a]\!]\to X_k$ prouve la seconde égalité. □

Sommations classiques

Proposition

Somme de Gauss. Soit $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

Somme quadratique de Gauss. Soit $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

Somme des termes d'une suite géométrique. Soient $q \in \mathbb{R} - \{1\}$ et $n \in \mathbb{N}$,

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

Binôme de Newton. Soient a et b des nombres réels et $n \in \mathbb{N}$.

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

où $C_n^k = \dfrac{n!}{k!(n-k)!}$ est le coefficient binomiale.

Démonstration. Ces résultats se démontrent par récurrence, ce que nous aborderons en TD. □

8. Récurrence

Avec les outils de logique propositionnelle que nous avons développé nous pouvons énoncer la récurrence comme suit :

Théorème Principe de récurrence

$$\Big(\forall n \in \mathbb{N}\ p(n)\Big) \iff \Big((p(0)) \wedge (\forall n \in \mathbb{N}\ (p(n) \Rightarrow p(n+1)))\Big)$$

Nous passerons la démonstration de ce principe qui s'enfonce profondément dans la théorie des ensembles.

L'idée de ce principe est que pour montrer qu'un prédicat $p(n)$ est vraie alors il suffit de montrer que $p(0)$ est vraie et que que la propriété de l'induction est vérifié, c'est à dire que **si** $p(n)$ est vraie **alors** $p(n+1)$ est aussi vraie... C'est étrange de supposer que ce l'on cherche à montrer $(p(n))$ est vraie mais c'est qu'est le principe de la récurrence.

Détaillons sur la somme de Gauss.

Dans cette exemple le prédicat $p(n)$ est

$$p(n) = \left(\sum_{k=0}^{n} k = \frac{n(n+1)}{2}\right)$$

Attention, la variable k est la variable de sommation. Une autre manière de reformuler ce prédicat est de dire que *la somme des entiers de* 0 *à* n *vaut* $\dfrac{n(n+1)}{2}$ (on voit bien ici qu'il n'y a pas de k).

Nous voulons démontrer que ce prédicat est vraie pour tout n.

Pour ce faire nous allons vérifier que $p(0)$ est vraie d'une part et que d'autre par $p(n) \Rightarrow p(n+1)$ (indépendamment de n).

Initialisation. Nous voulons donc vérifier que $p(0)$ est un prédicat vraie, c'est à dire que

$$p(0) = \left(\sum_{k=0}^{0} k = \frac{0(0+1)}{2}\right)$$

D'un coté $\displaystyle\sum_{k=0}^{0} k = 0$ et d'autre par $\dfrac{0(0+1)}{2} = 0$ et nous observons bien que $\displaystyle\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2}$ ce qui veut dire que la proposition $p(0)$ (qui demande si l'égalité est juste ou non) est vraie.

Hérédité. C'est la partie difficile du raisonnement par récurrence. On suppose que pour un $n \in \mathbb{N}$ quelconque $p(n)$ est vraie (sans chercher à donner une valeur à n). Partant de cette vérité, on cherche à vérifier que $p(n+1)$ est vraie.

L'erreur à ne pas commettre est de dire *ben je remplace le* n *par un* $n+1$ *et voila*[6]. L'idée est **en utilisant** l'hypothèse que $p(n)$ est vraie (on parle de l'hypothèse de récurrence) on arrive à montrer que $p(n+1)$. Dans notre exemple qu'est-ce que $p(n+1)$?

$$p(n+1) = \left(\sum_{k=0}^{n+1} k = \frac{(n+1)((n+1)+1)}{2}\right)$$

Soit en faisant une petite addition

$$p(n+1) = \left(\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}\right)$$

L'idée est de montrer que ce prédicat, précisément cette égalité, est bien vraie **sachant qu'à tout moment du raisonnement on peut utiliser l'hypothèse de récurrence** $(p(n))$ (en fait, si on utilise pas l'hypothèse de récurrence, ce n'est pas un raisonnement par récurrence. C'est d'ailleurs

6. Ça serait trop facile pour être mathématiques hein !

une aide dans le raisonnement : pour avoir une bonne idée, il faut que je m'arrange pour utiliser l'hypothèse de récurrence).

Et là... il faut une idée ! Voici de quoi s'en sortir (dans ce cas ; si nous changeons de prédicat p, l'idée à avoir est différente) : on veut calculer $\sum_{k=0}^{n+1} k = 0+1+2+\cdots+(n-1)+n+(n+1)$. On observe que la somme de tous les nombres entiers jusqu'à $n+1$, il faut faire la somme jusqu'à n puis ajouter $n+1$. De manière savante :

$$\begin{aligned}\sum_{k=0}^{n+1} k &= \underbrace{0+1+2+\cdots+(n-1)+n}+(n+1)\\ &= \left(\sum_{k=0}^{n} k\right)+(n+1)\end{aligned}$$

Ici nous utilisons l'hypothèse de récurrence $p(n)$ pour ce même n. Cette somme est égale à $\frac{n(n+1)}{2}$.

$$\begin{aligned}\sum_{k=0}^{n+1} k &= \underbrace{0+1+2+\cdots+(n-1)+n}+(n+1)\\ &= \left(\sum_{k=0}^{n} k\right)+(n+1)\\ &= \frac{n(n+1)}{2}+(n+1)\\ &= \frac{n(n+1)}{2}+\frac{2(n+1)}{2}\\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

Ce qui permet de conclure.

Conclusion de la récurrence. En conclusion, nous avons démontrer que pour tout $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$