Université de Rennes 1
UFR Mathématiques
2022-2023

Parcours d'Accès Spécifique Santé (PASS)
Option Informatique et option Mathématiques

Compléments maths PASS 1 (CMP1)

Algèbre - Raisonnement et vocabulaire ensembliste

Version provisoire du 3 janvier 2023

L'objet de ce cours est de faire une présentation rapide d'objets centraux en mathématiques comme les nombres, la logique, les ensembles et les applications.

Programme

Méthodologie mathématique Connecteurs logiques. Calcul propositionnel. Quantificateurs, variables. Démonstration : récurrence, contraposée, absurde.

Bases de la théorie des ensembles Éléments, parties, intersection, réunion, complémentaire, produit cartésien.

Introduction aux notions d'application, d'image, d'antécédent, d'injection, de surjection, de bijection, de composition, de restriction, de prolongement.

Manipulation des signes sommes, des indices.

1 Les nombres réels

Voici une courte présentation des nombres réels dans laquelle sont évoquées sans démonstration leurs principales propriétés ainsi que celles de réels particuliers comme les entiers naturels, les entiers relatifs et les rationnels.

1.1 Chiffres, nombres et écriture décimale

Idéogramme (d'après le dictionnaire de l'Académie française) "Signe graphique exprimant directement une idée, une notion, une unité de sens, et non pas un son isolé ou une syllabe. Les caractères chinois sont des idéogrammes. Les chiffres se lisent comme des idéogrammes."

Comme le dit l'Académie française, les chiffres de la base dix, 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9, sont des idéogrammes, c'est à dire des symboles qui représentent des notions. Les notions dont il s'agit sont des quantités particulières. Ces chiffres permettent aussi en les combinant de représenter avec peu de symboles des quantités finies arbitrairement grandes et appelées entiers naturels. C'est le principe de l'écriture décimale. La figure 1 donne à la fois tous les chiffres et des exemples d'entiers naturels, zéro, un, deux, trois, quatre, cinq, six, sept, huit, neuf, dix, onze et douze, représentés avec un ou deux chiffres.

Nombre (d'après le dictionnaire de l'Académie française) "Notion permettant d'indiquer la quantité d'éléments qui forment un ensemble d'êtres ou de choses, d'établir le rapport d'une quantité à une autre quantité de même nature, appelée unité et prise comme référence... (en mathématiques) Élément d'un ensemble défini par des propriétés opératoires, servant à compter, comparer, mesurer, calculer.

Cette définition suggère qu'il existe plusieurs notions de nombre. Dans cette partie cinq d'entre elles seront présentées en introduisant successivement les entiers naturels, les entiers relatifs, les décimaux les rationnels et les réels.

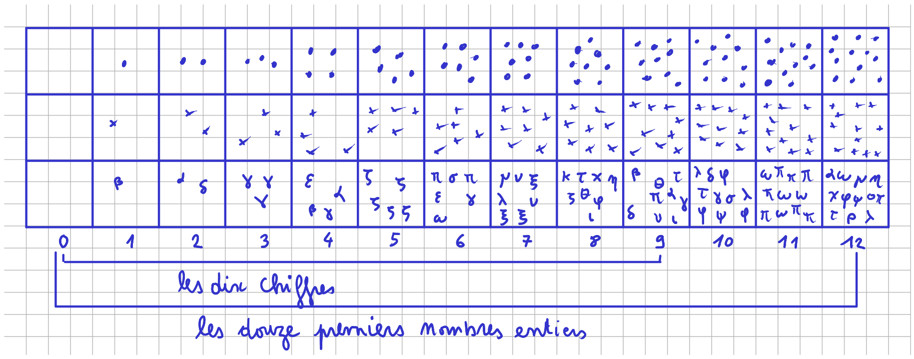

FIGURE 1 – Les chiffres de la base dix et quelques nombres

Écriture décimale Tous ces nombres dont il sera question admettent une écriture décimale dite aussi écriture en base dix. Il s'agit d'une écriture du type $\pm u_n ... u_i ... u_1, d_1 ... d_j ...$ où les u_i et les d_j sont des chiffres de la base dix et u_n est non nul sauf peut-être lorsque $n = 0$. Ainsi le rationnel $\frac{22}{7}$ admet comme début d'écriture $3,142857...$ avec $n = 1$, $u_1 = 3$, $d_1 = 1$, $d_2 = 4$, $d_3 = 2$, $d_4 = 8$, $d_5 = 4$, $d_6 = 7$,... Le signe $+$ peut être omis mais pas le signe $-$. Sauf les nombres qui peuvent être écrits avec un nombre fini de décimales (c'est à dire ceux qui sont tels que la suite des d_j se termine par une infinité de 0 qu'on omet d'écrire) et qui admettent exactement deux écritures, tout nombre admet une et une seule écriture en base dix : $\frac{1}{3}$ admet comme unique écriture en base dix, $0,333333...$, alors que 1 admet deux écritures, 1 et $0,999999...$ Signalons aussi qu'inversement à toute écriture décimale correspond un nombre.

1.2 Des entiers naturels aux réels

L'ensemble $\mathbf{N}$ des entiers naturels est formé des nombres de la comptine numérique : $0, 1, 2, 3, ..., 17, ..., 86, ..., 100, ..., 421, ..., 512, ...$. Ces nombres servent à compter le nombre d'éléments d'un ensemble et à comparer deux ensembles entre eux.

La figure 2 illustre, en prenant les exemples des nombres sept (7) et douze (12), comment reconnaître deux quantités représentée par le même entier naturel grâce à des traits couplant deux à deux des éléments des deux quantités.

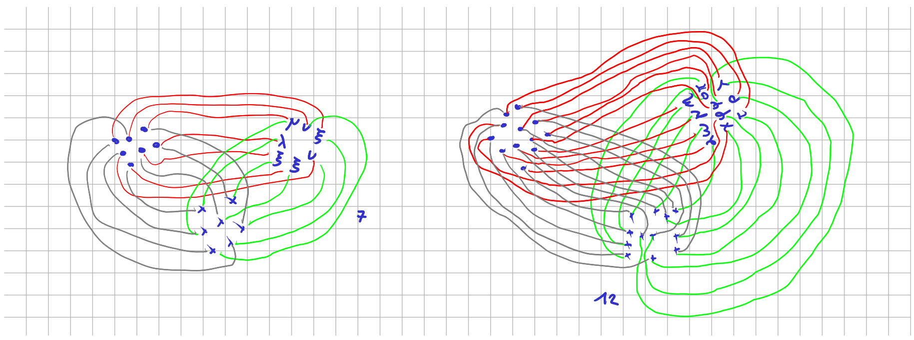

FIGURE 2 – Sept (7) et douze (12)

L'ensemble $\mathbf{Z}$ des entiers relatifs est formé des entiers naturels munis d'un signe $+$ ou $-$: $..., -314, ..., -56, ..., -21, ..., -3, -2, -1, 0, 1, 2, 3, ..., 17, ..., 86, ..., 421, ..., 512, ...$ Tout entier naturel est un entier relatif : $\mathbf{N} \subset \mathbf{Z}$.

L'ensemble $\mathbf{D}$ des décimaux est formé des nombres positifs ou négatifs dont l'écriture en base dix est finie : $-3,14$, 0 , 7 ou $1,602173634 \times 10^{-19}$ en sont des exemples. Tout entier relatif est un décimal : $\mathbf{Z} \subset \mathbf{D}$. Ce sont ceux qui admettent deux écritures dont l'une se termine en répétant 9 une infinité de fois.

L'ensemble $\mathbf{Q}$ des rationnels est formé des quotients de nombres relatifs par des entiers naturels non nuls : $-\frac{314}{271}$, $\frac{2}{3} = \frac{44}{66} = 0,666666666...$, 0 ou 1 en sont des exemples. Tout nombre décimal est un rationnel : $\mathbf{D} \subset \mathbf{Q}$.

Les rationnels sont caractérisés par leur écriture en base dix : d'une part l'écriture en base dix d'un rationnel se termine par la répétition infinie d'une séquence finie de chiffres et d'autre part toute écriture en base dix qui se termine par la répétition infinie d'une séquence finie de chiffres est l'écriture d'un rationnel.

L'ensemble $\mathbf{R}$ des réels est formé des nombres qui admettent une écriture en base dix quelconque. Tout rationnel est un réel : $\mathbf{Q} \subset \mathbf{R}$. Un réel qui n'est pas un rationnel est dit irrationnel.

Un réel non nul est dit strictement positif si son écriture débute par le signe $+$ et il est dit strictement négatif si son écriture débute par le signe $-$. Par exemple, les entiers naturels non nuls sont strictement positifs.

Certains réels ne sont pas des rationnels. C'est le cas du réel x strictement positif qui admet 0 comme unique chiffre à gauche de la virgule et dont toutes les décimales sont nulles sauf celles de rang 1, 2, 4,...,2^n,..., $n \in \mathbf{N}$ qui prennent la valeur 1 :

$$x = 0,110100010000000100000000000000001000...$$

L'écriture en base dix de ce réel n'est pas une écriture en base dix qui se termine par la répétition infinie d'une séquence finie de chiffres. Ce n'est donc pas un rationnel.

1.3 Les opérations sur les nombres

Ces cinq ensembles de nombres possèdent tous les nombres 0 et 1 et sont munis de deux opérations, des lois de composition interne en langage mathématique, l'addition et la multiplication, qui vérifient les propriétés suivantes.

Si x et y sont des nombres (entiers naturels, respectivement entiers relatifs, décimaux, rationnels, réels) alors les opérations d'addition et de multiplications leurs associent deux nombres (entiers naturels, respectivement entiers relatifs, décimaux, rationnels, réels) notés $(x + y)$ et $(x \times y)$ et appelés somme et produit de x et y. Quand il n'y a pas d'ambiguïté on peut omettre les parenthèses.

Le nombre 0 est le neutre pour l'addition : si x est un nombre alors $0 + x = x + 0 = x$.

Classiquement $\mathbf{N}^* = \mathbf{N} \setminus \{0\}$, $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$, $\mathbf{D}^* = \mathbf{D} \setminus \{0\}$, $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$, $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$.

Le nombre 1 est le neutre pour la multiplication : si x est un nombre alors $1 \times x = x \times 1 = x$.

Les opérations d'addition et de multiplication sont commutatives : si x et y sont des nombres alors $x + y = y + x$ et $x \times y = y \times x$.

Les opérations d'addition et de multiplication sont associatives : si x, y et z sont des nombres alors $x + (y + z) = (x + y) + z$ et $x \times (y \times z) = (x \times y) \times z$.

L'opération de multiplication est distributive par rapport à celle d'addition : si x, y et z sont des nombres alors $x \times (y + z) = (x \times y) + (x \times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$.

Tout nombre réel admet un opposé : si x est un nombre réel il existe un nombre noté $(-x)$ tel que $(-x) + x = x + (-x) = 0$. Si x est un relatif (respectivement, décimal, respectivement rationnel) alors $(-x)$ l'est aussi. En revanche si x est un entier naturel non nul alors $(-x)$ est un relatif mais n'est pas un entier naturel non nul.

L'opposé de la somme $x+y$ de deux réels est la somme des opposés : $(-(x+y)) = (-x)+(-y)$.

Tout nombre réel non nul admet un inverse (pour la multiplication) : si x est un nombre réel différent de 0 il existe un nombre noté (x^{-1}) ou $\left(\frac{1}{x}\right)$ tel que $(x^{-1}) \times x = x \times (x^{-1}) = 1$. Si x est rationnel non nul alors (x^{-1}) l'est aussi. En revanche si x est un décimal qui n'est pas une puissance de 10, c'est à dire dont l'écriture décimale ne contient qu'un chiffre non nul, 1, et qui n'apparaît qu'une seule fois, alors (x^{-1}) est un relatif mais n'est pas un décimal.

L'inverse du produit $x \times y$ de deux réels non nul est le produit des inverses : $\frac{1}{(x \times y)} = \left(\frac{1}{x}\right) \times \left(\frac{1}{y}\right)$.

On peut vérifier en utilisant l'associativité de l'addition et de la multiplication que l'opposé d'un nombre est unique et que si ce nombre est non nul son inverse est unique.

1.4 Les puissances entières et rationnelles

Soit x un réel. On pose $x^0 = 1$. Si n un entier naturel x^n désigne la multiplication n fois de x par lui-même. En particulier $x^0 = 1$ et $x^{n+1} = (x^n) \times x$. Si n est un entier relatif négatif strictement ($-n$ est alors un entier naturel) alors x^n est l'inverse de x^{-n} : $x^n = \frac{1}{x^{-n}}$. On a $x^n = \left(\frac{1}{x}\right)^n$. Le nombre x^n est appelé x puissance n.

Si $x, y \in \mathbf{R}$ et $n, m \in \mathbf{Z}$ alors $(xy)^n = (x^n) \times (y^n)$, $x^{n+m} = (x^n) \times (x^m)$ et $(x^n)^m = x^{n \times m}$.

Si x est un réel positif ou nul et si n est un entier naturel non nul alors il existe un unique réel positif ou nul y tel que $y^n = x$. On note $x^{\frac{1}{n}}$ ce réel. Le nombre $x^{\frac{1}{n}}$ est appelé racine n-ième de x. Notons que si x est rationnel positif le nombre $x^{\frac{1}{n}}$ n'est pas nécessairement rationnel.

Si x est un réel positif ou nul et $r = \frac{p}{q}$ est un rationnel avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}$ non nul alors on définit x puissance r comme étant le nombre $x^r = (x^p)^{\frac{1}{q}}$. Cette définition ne dépend pas du choix de p et q mais seulement de r.

Si $x, y > 0$ et $r, s \in \mathbf{Q}$ alors $(xy)^r = (x^r) \times (y^r)$, $x^{r+s} = (x^r) \times (x^s)$ et $(x^r)^s = x^{r \times s}$.

Remarquons que si x est un décimal dont l'écriture décimale est $\pm u_n ... u_i ... u_1, d_1 ... d_j ... d_m$ alors $x = \pm(u_1 10^0 + ... + u_n 10^{n-1} + d_1 10^{-1} + ... + d_m 10^{-m})$.

1.5 L'ordre sur les nombres

Un ensemble E est muni d'un relation d'ordre (ou simplement d'un ordre) qu'on notera $\leq$ si quels que soient x, y et z dans E alors
- $x \leq x$ (la relation d'ordre $\leq$ est dite réflexive),
- si $x \leq y$ et $y \leq x$ alors $x = y$ (la relation d'ordre $\leq$ est dite antisymétrique),
- si $x \leq y$ et $y \leq z$ alors $x \leq z$ (la relation d'ordre $\leq$ est dite transitive).

Les cinq ensembles de nombres $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{D}$, $\mathbf{Q}$ et $\mathbf{R}$ sont munis d'un ordre. Quand on prend deux nombres x et y, soit ils sont égaux ($x = y$), soit l'un est strictement supérieur à l'autre : $x < y$ si $(y - x)$ est strictement positif et $y < x$ si $(x - y)$ est strictement positif. Si y est strictement supérieur à x on dit aussi que x est strictement inférieur à y

Un réel x qui vérifie $0 < x$ ou $0 = x$ est dit positif ou nul : on écrit alors $0 \leq x$. Un réel x qui vérifie $x < 0$ ou $0 = x$ est dit négatif ou nul : on écrit alors $x \leq 0$.

Classiquement $\mathbf{Z}_+ = \{x \in \mathbf{Z}, x \geq 0\} = \mathbf{N}$, $\mathbf{Z}_+^* = \{x \in \mathbf{Z}, x > 0\} = \mathbf{N}^*$. De façon analogue $\mathbf{D}_+ = \{x \in \mathbf{D}, x \geq 0\}$, $\mathbf{D}_+^* = \{x \in \mathbf{D}, x > 0\}$, $\mathbf{Q}_+ = \{x \in \mathbf{Q}, x \geq 0\}$, $\mathbf{Q}_+^* = \{x \in \mathbf{Q}, x > 0\}$, $\mathbf{R}_+ = \{x \in \mathbf{R}, x \geq 0\}$, $\mathbf{R}_+^* = \{x \in \mathbf{R}, x > 0\}$.

Entre un entier naturel ou relatif n et l'entier $n + 1$ appelé successeur de n il n'y a aucun entier : un nombre z qui vérifie $n < z < n + 1$ n'est jamais entier. Par exemple l'entier naturel 315 est le successeur de l'entier naturel 314.

L'ensemble $\mathbf{N}$ des entiers naturels possède deux propriétés remarquables en lien avec l'ordre et cette notion de successeur. D'une part tout sous-ensemble non vide de $\mathbf{N}$ admet un plus petit élément. C'est un entier naturel appartenant au sous-ensemble et qui est inférieur à tous les autres entiers naturels de ce sous-ensemble. D'autre part tout sous-ensemble non vide de $\mathbf{N}$ pour lequel il existe un majorant, c'est à dire un entier naturel pas nécessaire dans ce sous-ensemble mais supérieur à tous les entiers naturels de cet ensemble, admet aussi un plus grand élément. C'est un entier naturel appartenant au sous-ensemble et qui est supérieur à tous les autres entiers naturels de ce sous-ensemble.

La propriété de successeur est vrai dans $\mathbf{Z}$. En revanche, dans $\mathbf{D}$, $\mathbf{Q}$ et $\mathbf{R}$ la notion de successeur n'a pas d'intérêt car si x et y sont deux réels (ou de rationnels ou deux décimaux) qui vérifient $x < y$ alors il existe un décimal z tel que $x < z < y$.

L'ordre sur $\mathbf{R}$ se comporte bien par rapport aux deux opérations. Si x, y et z sont des nombres et si $x < y$ alors $x + z = z + x < y + z = z + y$. Si x, y et z sont des nombres et si $x < y$ et $0 < z$ alors $x \times z = z \times x < y \times z = z \times y$.

Soit x un réel non nul. Si $0 < x$ alors $0 < (x^{-1})$ et $(-x) < 0$ et si $x < 0$ alors $(x^{-1}) < 0$ et $0 < (-x)$.

La partie entière $E(x)$ d'un réel x est définie de la façon suivante. Si x est strictement positif ou s'il est nul, c'est l'entier naturel dont l'écriture coïncide avec celle des termes qui apparaissent à gauche de la virgule dans l'écriture de x. Si x est strictement négatif, c'est l'entier relatif qui précède celui dont l'écriture coïncide à celles des termes qui, dans l'écriture de x, apparaissent à gauche de la virgule.

Si x est un nombre réel alors sa partie entière $E(x)$ est l'unique entier relatif qui vérifie la double inégalité $E(x) \leq x < E(x) + 1$.

L'existence de la division euclidienne, c'est à dire le fait que si a est entier relatif et si b est un entier naturel non alors il existe un unique couple (q, r) d'entiers relatifs tel que $a = bq + r$ avec $0 \leq r < b$, est une conséquence directe des propriétés précédentes.

La valeur absolue $|x|$ d'un réel x est le plus grand des deux nombres x et $-x$: si $0 \leq x$ alors $|x| = x$ et si $x \leq 0$ alors $|x| = -x$. Si x réel alors $-|x| \leq x \leq |x|$.

On peut vérifier que si x et y sont deux réels alors $||x| - |y|| \leq |x - y| \leq |x| + |y|$.

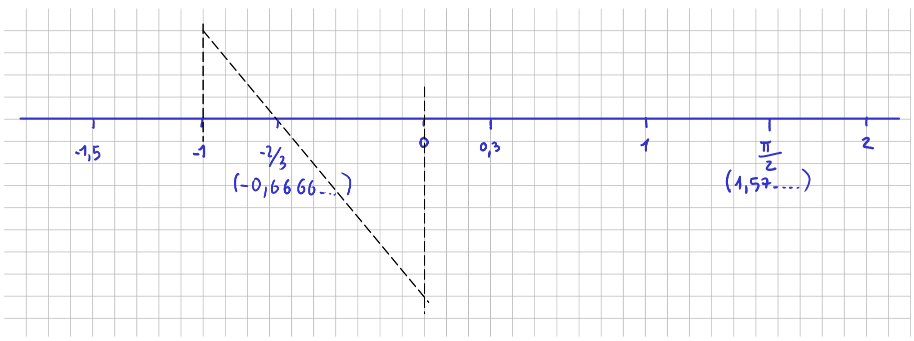

FIGURE 3 – Quelques réels

1.6 Retour sur l'écriture décimale

Si $x \in \mathbf{R}^+$ admet comme écriture décimale $u_n...u_i...u_1, d_1...d_j...$ avec les u_i et les d_j dans $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ alors pour tout $m \in \mathbf{N}$

$(u_1 10^0 + ... + u_n 10^{n-1} + d_1 10^{-1} + ... + d_m 10^{-m}) \leq x < (u_1 10^0 + ... + u_n 10^{n-1} + d_1 10^{-1} + ... + d_m 10^{-m}) + 10^{-m}$.

Le nombre $(u_1 10^0 + ... + u_n 10^{n-1} + d_1 10^{-1} + ... + d_m 10^{-m})$ qui est aussi noté

$$\left(\sum_{i=1}^{n} u_i \times 10^i + \sum_{j=1}^{m} d_j \frac{1}{10^j} \right)$$

est un décimal et $10^m \times (u_1 10^0 + ... + u_n 10^{n-1} + d_1 10^{-1} + ... + d_m 10^{-m})$, c'est à dire

$$10^m \times \left(\sum_{i=1}^{n} u_i \times 10^i + \sum_{j=1}^{m} d_j \frac{1}{10^j} \right),$$

est égal à la partie entière $E(10^m \times x)$ de $10^m \times x$.

L'ensemble **R** des réels possède une remarquable propriété en lien avec l'ordre. Considérons un sous-ensemble non vide de **R** et supposons qu'il existe un réel inférieur ou égal à tous les nombres ce sous-ensemble. Alors, parmi tous les réels inférieurs ou égaux à tous les nombres ce sous-ensemble, l'un est plus grand que tous les autres : il est appelé borne inférieure du sous-ensemble considéré. Par exemple le réel $\sqrt{2}$ qui n'est pas un rationnel est la borne inférieure du sous-ensemble formé des rationnels positifs et de carré supérieur ou égal à 2.

2 Logique

Raisonnement (d'après le dictionnaire de l'Académie française) "Manière dont l'esprit enchaîne les unes aux autres des propositions pour établir une vérité (par opposition à l'intuition, au sentiment, à la croyance) ; suite ordonnée de raisons, ensemble d'arguments qui s'enchaînent de façon à démontrer, à prouver, à convaincre. La logique est la science des règles formelles qui fondent le raisonnement..."

Dans les sciences expérimentales un principe essentiel qui guide le raisonnement et de partir des expériences pour tirer des conclusions générales. Lorsqu'on procède ainsi on parle d'un raisonnement inductif. Si ceci est bien adapté au cadre expérimental, ça l'est moins en mathématiques quand on veut démontrer. Par exemple, conclure que les entiers naturels premiers sont les nombres impairs différents de 1 parce que 3, 5 et 7 le sont illustre un usage inadapté du raisonnement inductif. En mathématiques on procède différemment. On part de propriétés générales pour en déduire des propriétés particulières. Pour y arriver on met en place un raisonnement déductif. Le raisonnement inductif sera utilisé pour poser des conjectures qui sont les questions que les mathématiques cherchent à résoudre.

Les mathématiques étudient des propositions (ou des propriétés, des assertions, des prédicats, des énoncés, des formules) et le raisonnement mathématique consiste, en partant de propositions connues pour vraies et en utilisant des règles de déduction, à démontrer une nouvelle proposition.

2.1 Connecteurs logiques

Un prédicat en mathématiques est l'équivalent d'une phrase dans une langue, c'est à dire un assemblage de mots qui obéit à certaines règles.

Pour réaliser ces assemblage on recourt à des connecteurs logiques qui servent à produire de nouveaux prédicats à partir de plus anciens. Voici cinq connecteurs fondamentaux. Le premier est un connecteur unaire. Il agit sur un prédicat. Les autres sont des connecteurs binaires. Ils agissent sur un couple de prédicats.

2.1.1 La négation

Si P est un prédicat alors lui est associée sa négation qui est notée $\neg P$ ou $\overline{P}$ ou encore non(P). Il est a noter que la négation de la négation d'un prédicat est le prédicat lui-même : $\neg\neg P = P$ ($\neg\neg P = P$, non(non(P) $= P$).

2.1.2 La conjonction

Si P et Q sont deux prédicats alors leur est associée leur conjonction qui est notée indifféremment $P \wedge Q$, $Q \wedge Q$, P et Q, Q et P.

2.1.3 La disjonction

Si P et Q sont deux prédicats alors leur est associée leur disjonction qui est notée indifféremment $P \vee Q$, $Q \vee Q$, P ou Q, Q ou P.

2.1.4 L'implication

Si P et Q sont deux prédicats alors leur est associée l'implication de Q par P notée indifféremment $P \Rightarrow Q$, P implique Q.

2.1.5 L'équivalence

Si P et Q sont deux prédicats alors leur est associée l'équivalence de P et Q notée indifféremment $P \Leftrightarrow Q$, $Q \Leftrightarrow P$, P est équivalent à Q, Q est équivalent à P, P et Q sont équivalents, Q et P sont équivalents.

2.2 Calcul propositionnel et tables de vérité

2.2.1 Enchaînement de connecteurs et de prédicats

Pour construire un prédicat à partir de prédicat on enchaîne connecteurs et prédicats. On utilise des parenthèses pour lever les ambiguïtés. Une parenthèse ouvrante est toujours associée à une parenthèse fermante qui la suit et si une parenthèse est comprises entre deux parenthèses associées la parenthèse qui lui est associée est aussi entre ces deux parenthèses. Par exemple $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow R)$ est un prédicat mais $(P \Rightarrow Q) \Rightarrow Q) \Rightarrow R($ n'est pas une écriture autorisée.

2.2.2 Calcul propositionnel

Un prédicat peut être soit vrai soit faux. Le calcul propositionnel consiste à construire grâce à l'usage de connecteurs logiques des prédicats à partir de prédicats initiaux connus pour être vrais (ou faux) et à ensuite déterminer si les prédicats produits sont vrais ou faux.

Les règles de déduction sont données par les tables suivantes dites tables de vérité. Dans ces tables V signifie que le prédicat est vrai et F qu'il est faux.

Table de la négation

P	$\neg P$
V	F
F	V

Ceci signifie que si un prédicat P est vraie alors sa négation $\neg P$ est fausse et s'il est faux sa négation $\neg P$ est vraie.

Table de la conjonction

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Ceci signifie que $P \wedge Q$ est vrai si P est vrai et Q est vrai et que sinon $P \wedge Q$ est faux.

Table de la disjonction

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Ceci signifie que $P \vee Q$ est faux si P est faux et Q est faux et que sinon $P \vee Q$ est vrai.

Table de l'implication

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Ceci signifie que $P \Rightarrow Q$ est vrai sauf si P est vrai et Q est faux.

Table de l'équivalence

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Ceci signifie que $P \Leftrightarrow Q$ est vrai lorsque P et Q sont simultanément vrais ou simultanément faux.

Table associée à des enchaînements de connecteurs et de prédicats

On peut calculer la table associée à un enchaînement de connecteurs. Par exemple la table associée au prédicat $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow R)$ est

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q) \Rightarrow (Q \Rightarrow R)$
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	V	V
V	F	F	F	V	V
F	V	V	V	V	V
F	V	F	V	F	F
F	F	V	V	V	V
F	F	F	V	V	V

.

Lorsque deux enchaînements de connecteurs donnent les mêmes tables on peut utiliser indifféremment l'un ou l'autre.

Ainsi la table de $\neg(\neg P \wedge \neg Q)$ ci-dessous est la même que celle de $P \vee Q$:

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$
V	V	F	F	F	V
V	F	F	V	F	V
F	V	V	F	F	V
F	F	V	V	V	F

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

.

De même la table de $\neg P \vee Q$ ci-dessous est la même que celle de $P \Rightarrow Q$:

P	Q	$\neg P$	$\neg P \vee Q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

.

Enfin, la table de $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ ci-dessous est la même que celle de $P \Leftrightarrow Q$:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

.

2.3 Le langage de la théorie des ensembles

Le langage de la théorie des ensembles repose sur les symboles suivants :
- les connecteurs logiques : $\wedge$ (et), $\neg$ (non), $\vee$ (ou), $\Rightarrow$ (implique) ;
- le quantificateur existentiel $\exists$ (il existe) et le quantificateur universel $\forall$ (pour tout) ;
- les parenthèses (et) ;
- des lettres appelées variables ;
- le symbole $=$ (est égal à) ;
- le symbole $\in$ (appartient à) qui est spécifique à la théorie des ensembles
- le symbole $|$ qui indique une substitution.

Ces symboles permettent d'écrire des formules ou prédicats en respectant quelques règles :
- si x et y sont deux variables alors $x = y$ et $x \in y$ sont des prédicats sans variable liée et dont les variables libres sont x et y ;
- si A est un prédicat alors $\neg A$ est un prédicat qui possède les mêmes variables liées et les mêmes variables libres que A ;
- si x est une variable libre du prédicat A alors $\exists x A$ et $\forall x A$ sont des prédicats dont les variables libres sont celles de A à l'exception de x et les variables liées sont celles de A auxquelles est ajoutée x ($\exists x$ se lit “il existe x tel que” et $\forall x$ se lit “pour tout x”) ;
- si A et B sont des prédicats tels que si une variable est libre pour l'un elle n'est pas liée pour l'autre alors $A \wedge B$, $A \vee B$ et $A \Rightarrow B$ sont des prédicats dont les variables libres et les variables liées sont celles de A et B ;
- si x est une variable libre du prédicat A et y n'est pas une variable liée de A alors $A(y|x)$ est le prédicat obtenu en substituant y à x dans A.

Les prédicats $\neg(x = y)$ et $\neg(x \in y)$ s'écrivent également $x \neq y$ et $x \notin y$.

Un prédicat A qui possède comme variables libres les variables $x_1, ..., x_n$ peut être noté $A(x_1, ..., x_n)$.

Un prédicat sans variable libre s'appelle une assertion.

Un prédicat est souvent formé de prédicats imbriqués. Il peut être utile d'utiliser des parenthèses pour faciliter la lecture et lever toute ambiguïté. En l'absence de parenthèses on suivra l'ordre de priorité suivant : $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \forall, \exists$. Ainsi $\neg A \wedge B \vee C \Rightarrow D$ est le même prédicat que $((\neg A) \wedge (B \vee C)) \Rightarrow D$. Lorsque le connecteur $\Rightarrow$ (ou le connecteur $\vee$ ou le connecteur $\wedge$) apparaît plusieurs fois sans parenthèse on associe à droite : ainsi $A \Rightarrow B \Rightarrow C \Rightarrow D$ est le même prédicat que $A \Rightarrow (B \Rightarrow (C \Rightarrow D))$.

2.4 Les principes de la démonstration

Faire une démonstration consiste, en appliquant certaines règles de déduction, à déterminer si un prédicat est vrai ou faux sous certaines hypothèses. Avec ce point de vue la vérité est relative. On part d'une famille de prédicats supposés vrais (hypothèse) et on espère qu'en appliquant certaine règles on pourra montrer qu'un prédicat donné est vrai (conclusion). Au cours d'une démonstration on peut être amené à rajouter puis à abandonner de nouvelles hypothèses dites hypothèses auxiliaires. Voici les treize règles qui généralisent les tables de vérité des connecteurs.

— **Le modus ponens** Si A est vrai et $A \Rightarrow B$ est vrai alors B est vrai.
— **L'abandon de l'hypothèse auxiliaire** Si en supposant A vrai (c'est à dire en considérant qu'on rajoute A comme une hypothèse supplémentaire) on démontre que B est vrai alors $A \Rightarrow B$ est vrai.
— **L'analyse** Si $A \wedge B$ est vrai alors A est vrai et B est vrai.
— **La synthèse** Si A est vrai et B est vrai alors $A \wedge B$ est vrai.
— **La disjonction des hypothèses** Si $A \Rightarrow C$ est vrai et $B \Rightarrow C$ est vrai alors $(A \vee B) \Rightarrow C$ est vrai.
— **L'affaiblissement d'une thèse** Si A est vrai alors $A \vee B$ est vrai et $B \vee A$ est vrai.
— **La réduction à l'absurde ou reductio ad absurdum** Si $A \Rightarrow (B \wedge \neg B)$ alors $\neg A$ est vrai.
— **La double négation** Si $\neg\neg A$ est vrai alors A est vrai.
— **La singularisation** Si $\forall x A(x)$ est vrai et si y n'est pas une variable liée de A alors $A(y|x)$ est vrai.
— **La généralisation** Si A est vrai, si $A \Rightarrow B(x)$ et si x n'est pas une variable libre de A alors $\forall x B(x)$ est vrai.
— **Preuve directe de l'existence** Si $A(x)$ est vrai alors $\exists x A(x)$ est vrai.
— **Conséquence de l'existence** Si $\exists x A(x)$ est vrai, si $A(x) \Rightarrow B$ est vrai et si x n'est pas une variable libre de B alors B est vrai.
— **Répétition** Si B est démontré sous l'hypothèse auxiliaire A on peut répéter B tant que A n'est pas abandonnée.

Ces règles de déduction sont celles de la logique classique, en particulier la règle de la double négation que n'acceptent pas certains logiciens dits intuitionnistes.

Une proposition est l'énoncé d'un prédicat vrai. Il prend souvent l'une des formes suivantes :

proposition $A \Rightarrow B$
proposition *Si A est vrai alors B est vrai.*
proposition *Si A alors B.*

où A est l'hypohèse et B la conclusion. Suivant l'intérêt qu'on porte à une proposition on l'appellera théorème (d'un intérêt théorique) ou lemme (d'un intérêt pratique pour démontrer des théorèmes ou des propositions).

En utilisant ces règles de déduction on démontre que si A B et C sont des prédicats alors

— **La contraposée ou modus tollens**

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

— **Le tiers exclu**

$$A \vee \neg A$$

— **La non contradiction**

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

— **Du faux découle ce que l'on veut ou ex falso sequitur quodlibet**

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

— **La transitivité de l'implication**

$$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$

— **La loi de Peirce**

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

— **Les lois de Morgan**

$$\begin{array}{rcl} (\neg A \wedge \neg B) & \Rightarrow & \neg(A \vee B) \\ (\neg A \vee \neg B) & \Rightarrow & \neg(A \wedge B) \\ \neg(A \vee B) & \Rightarrow & (\neg A \wedge \neg B) \\ \neg(A \wedge B) & \Rightarrow & (\neg A \vee \neg B) \end{array}$$

Ces propositions ne dépendent pas des prédicats A, B et C. C'est ce qu'on appelle des tautologies.

L'équivalence entre deux prédicats, notée $A \Leftrightarrow B$, peut être définie comme étant le prédicat $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Ceci est en cohérence avec la coïncidence des tables de vérité correspondante. Lorsque $A \Leftrightarrow B$ est vraie on dit A est équivalent à B.

Donnons un exemple de raisonnement en établissant que si A et B sont deux prédicats alors $A \Leftrightarrow B$ vrai si et seulement si A et B sont vrais ou si $\neg A$ et $\neg B$ sont vrais. Supposons donc $A \Leftrightarrow B$ vrai. D'après le principe du tiers exclu soit A est vrai soit $\neg A$ est vrai. Si A est vrai alors B est vrai d'après le modus ponens. Si $\neg A$ est vrai alors $\neg B$ est vrai d'après le modus tollens. Réciproquement si A et B sont vrais ou si $\neg A$ et $\neg B$ sont vrais alors $A \Leftrightarrow B$.

On a les tautologies suivantes. Soient A, B et C des prédicats.

— (commutativité, associativité et distributivité de $\wedge$ et $\vee$)

$$\begin{array}{rcl} (A \wedge B) & \Leftrightarrow & (B \wedge A) \\ (A \vee B) & \Leftrightarrow & (B \vee A) \\ ((A \wedge B) \wedge C) & \Leftrightarrow & (A \wedge (B \wedge C)) \\ ((A \vee B) \vee C) & \Leftrightarrow & (A \vee (B \vee C)) \\ ((A \vee B) \wedge C) & \Leftrightarrow & ((A \wedge C) \vee (B \wedge C)) \\ ((A \wedge B) \vee C) & \Leftrightarrow & ((A \vee C) \wedge (B \vee C)) \end{array}$$

—

$$\begin{array}{rcl} (A \wedge B) & \Leftrightarrow & \neg(\neg B \vee \neg A) \\ (A \vee B) & \Leftrightarrow & \neg(\neg B \wedge \neg A) \end{array}$$

Ainsi $\neg$ et $\wedge$ permettent d'exprimer $\vee$ et $\neg$ et $\vee$ permettent d'exprimer $\wedge$.

—

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$$

Ceci confirme ce qu'indiquaient les tables de vérité, à savoir que $\Rightarrow$ s'exprime à l'aide de $\neg$ et $\vee$.

Nous donnons maintenant une série de tautologies liées à $\forall$ et $\exists$. Le recours aux règles de singularisation, de généralisation, de preuve directe de l'existence et de conséquence de l'existence est nécessaire pour les établir.

Si A et B sont des prédicats alors

$$\begin{array}{rcll} (\exists x A) & \Leftrightarrow & \neg(\forall x \neg A) & \\ (\forall x A) & \Leftrightarrow & \neg(\exists x \neg A) & \\ (\exists x \exists y A) & \Leftrightarrow & (\exists y \exists x A) & \\ (\forall x \forall y A) & \Leftrightarrow & (\forall y \forall x A) & \\ (\forall x (A \wedge B)) & \Leftrightarrow & (A \wedge (\forall x B)) & \text{si } x \text{ n'est pas une variable libre de } A \\ (\forall x (A \vee B)) & \Leftrightarrow & (A \vee (\forall x B) & \text{si } x \text{ n'est pas une variable libre de } A \\ (\forall x \forall y (A \wedge B)) & \Leftrightarrow & ((\forall x A) \wedge (\forall y B)) & \text{si } x \text{ n'est pas une variable libre de } B \\ & & & \text{et } y \text{ n'est pas une variable libre de } A \\ (\forall x \forall y (A \vee B)) & \Leftrightarrow & ((\forall x A) \vee (\forall y B)) & \text{si } x \text{ n'est pas une variable libre de } B \\ & & & \text{et } y \text{ n'est pas une variable libre de } A. \end{array}$$

L'ordre entre quantificateur universel ($\forall$) et existentiel ($\exists$) est important. En général les prédicats $\exists x \forall y A$ et $\forall y \exists x A$ ne sont pas synonymes. En revanche $(\exists x \forall y A) \Rightarrow (\forall y \exists x A)$ est toujours vrai.

D'une certaine façon le travail mathématique consiste à déterminer la véracité de prédicats. Dans un texte mathématique on rencontre des assertions dont on sait qu'elles sont vraies, dans ce cas on ne l'indique généralement pas, et d'autres dont on essaie de savoir si elles le sont.

Dans la suite on aura pour règle d'éviter le plus possible de représenter les connecteurs logiques et les quantificateurs par les symboles $\wedge$, $\neg$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$ et $\forall$. On préférera les paraphraser par des mots du langage courant.

2.5 Raisonnement par récurrence

Le raisonnement par récurrence est un raisonnement qui permet d'établir que des propriétés P_n indexées par les entiers naturels supérieurs ou égaux à un entier naturel p donné sont toutes vraies. Il suffit de montrer que la propriété P_p est vraie (initialisation ou vérification au rang initial) et de montrer que si n est un entier naturel quelconque supérieur ou égal à p la véracité de la propriété P_n entraîne la véracité de la propriété P_{n+1} (hérédité). Il y a un point subtil dans ce raisonnement. Lorsqu'on le fait on ne sait pas si P_n est vraie, on ne fait que le supposer. Pour que le raisonnement soit complet il est indispensable de vérifier que P_p est vraie.

Le principe du raisonnement par récurrence repose sur le résultat suivant.

Considérons un sous-ensemble non vide E de $\mathbf{N}$ qui vérifie la propriété suivante : le successeur de tout élément de E est dans E, c'est à dire que pour tout entier naturel n, $n+1 \in E$ dès que $n \in E$. Alors il existe $p \in \mathbf{N}$ tel que $E = \{n \in \mathbf{N} | n \geq p\}$.

Prouvons ce résultat. Puisque E est un sous-ensemble non vide de $\mathbf{N}$, il possède un plus petit élément qu'on va noter p. Alors $p \in E$ et $E \subset \{n \in \mathbf{N} | n \geq p\}$. On raisonne par l'absurde en supposant que $E \neq \{n \in \mathbf{N} | n \geq p\}$ et en obtenant sous cette hypothèse une contradiction. L'hypothèse $E \neq \{n \in \mathbf{N} | n \geq p\}$ entraîne que $\{n \in \mathbf{N} | n \geq p\} \setminus E$ est un sous-ensemble non vide de $\mathbf{N}$. Il possède donc un plus petit élément qu'on va noter q. De $\{n \in \mathbf{N} | n \geq p\} \setminus E \subset \{n \in \mathbf{N} | n \geq p\}$ on déduit que $q \geq p$ et puisque $p \in E$ nécessairement $q > p$. Par conséquent $q - 1 \geq p$ et donc $q - 1 \in E$. Puisque le successeur de tout élément de E est dans E on en déduit que $q = (q-1)+1 \in E$ puisque c'est le successeur de $q-1$ qui est dans E. Ceci n'est pas possible. Par conséquent l'hypothèse $E \neq \{n \in \mathbf{N} | n \geq p\}$ est fausse et $E = \{n \in \mathbf{N} | n \geq p\}$.

Revenons au raisonnement par récurrence. L'ensemble $\{n \in \mathbf{N} | P_n \text{ est vraie}\}$ des entiers naturels n pour lesquels P_n est vraie est non vide car il contient comme plus petit élément p et il est tel que si n appartient à cet ensemble (i.e. si P_n est vraie) alors son successeur $n+1$ appartient aussi à cet ensemble (i.e. P_{n+1} est aussi vraie). L'ensemble $\{n \in \mathbf{N} | P_n \text{ est vraie}\}$ est donc l'ensemble E précédent. Il est donc égal à $\{n \in \mathbf{N} | n \geq p\}$. Ceci signifie que P_n est vraie pour tous les entiers n supérieurs ou égaux à p.

3 Ensembles

3.1 Les axiomes de la théorie des ensembles

La théorie des ensembles consiste à considérer une collection d'objets appelés ensembles et caractérisés par certaines propriétés qu'on va décrire : les axiomes de la théorie des ensembles. Ils fondent la théorie des ensembles. De ces axiomes on pourra déduire ensuite la véracité de prédicats : on établira des propositions qui préciseront des propriétés caractéristiques des ensembles et déduites des axiomes. La famille de ces propositions formera la connaissance que l'on a de la théorie des ensembles.

Voici maintenant les propriétés fondamentales (axiomes) qui décrivent les ensembles et leurs relations. Ces propriétés sont énoncées sous deux formes. D'abord à l'aide d'une phrase, ensuite à l'aide d'une assertion construite avec les règles syntaxiques exposées précédemment.
1 - Deux ensembles sont égaux si tout élément de l'un est élément de l'autre :

$$\forall x \forall y((x = y) \Leftrightarrow (\forall z((z \in x) \Leftrightarrow (z \in y))).$$

2 - Il existe un ensemble sans élément. Il est appelé ensemble vide et noté $\emptyset$:

$$\exists x \forall y(\neg(y \in x)).$$

3 - Étant donnés deux ensembles il existe un ensemble appelé paire dont les éléments sont exactement ces deux ensembles. Si les deux ensembles donnés sont égaux alors on parle de singleton associé à cet ensemble donné :

$$\forall x \forall y \exists z \forall t(((x \in z) \wedge (y \in z)) \wedge ((t \in z) \Rightarrow ((t = x) \vee (t = y)))).$$

4 - Étant donné un ensemble il existe un ensemble dont les éléments sont exactement les éléments des éléments de cet ensemble donné. C'est la réunion des ensembles qui sont éléments de l'ensemble donné :

$$\forall x \exists y \forall z((\exists t((z \in t) \wedge (t \in x))) \Leftrightarrow (z \in y)).$$

5 - Étant donné un ensemble et une prédicat $A(x)$ alors les éléments a de l'ensemble donné tels que $A(a)$ est vraie forment un ensemble. C'est le sous-ensemble de l'ensemble donné défini par compréhension à partir du prédicat $A(x)$:

$$\forall X \exists Y \forall x((x \in Y) \Leftrightarrow ((x \in X) \wedge (A(x)))).$$

Il est noté $\{x \in X : A(x)\}$.
6. Étant donné un ensemble il existe un ensemble dont les éléments sont exactement les ensembles dont les éléments sont également des éléments de l'ensemble donné. Cet ensemble est l'ensemble des parties ou des sous-ensembles de l'ensemble donné :

$$\forall x \exists y \forall z((\forall t((t \in z) \Rightarrow (t \in x))) \Leftrightarrow (z \in y)).$$

7 - Il existe un ensemble dont l'ensemble vide est un élément et tel que si un second ensemble est un élément quelconque de cet ensemble alors la réunion de ce second ensemble et du singleton associé à ce second ensemble est un élément de cet ensemble. Ceci signifie qu'il existe un ensemble infini :

$$\exists E \forall x \exists y \forall z((\emptyset \in E) \wedge ((x \in E) \Rightarrow ((z \in y) \Leftrightarrow ((z \in x) \vee (z = x))))).$$

8 - Étant donné un ensemble et un prédicat $A(x, y)$ tel que pour tout élément a de l'ensemble donné il existe au plus un ensemble b tel que $A(a, b)$ soit vraie alors les ensembles b ainsi obtenus quand a décrit l'ensemble donné forment un ensemble appelé image de l'ensemble donné par A :

$$\begin{gathered}(\forall x \forall y \forall y'((A(x, y) \wedge (A(x, y')) \Rightarrow (y = y'))) \\ \Downarrow \\ (\forall X \exists Y \forall y((\exists x((x \in X) \wedge A(x, y))) \Leftrightarrow (y \in Y))).\end{gathered}$$

9 - Étant donné un ensemble non vide il existe un élément qui appartient à cet ensemble et qui ne possède aucun élément en commun avec l'ensemble donné. En particulier un ensemble n'est jamais élément de lui-même :

$$\forall x \exists y \forall z((x = \emptyset) \vee ((y \in x) \wedge ((z \in y) \Rightarrow (\neg(z \in x))))).$$

Soit y un ensemble non vide et x le singleton $x = \{y\}$. D'après l'axiome 9 si z est un élément de y ($z \in y$) alors z n'est pas y qui est l'unique élément de x : $(\neg(z = y))$. En particulier $(\neg(y \in y))$: un ensemble n'est jamais élément de lui même.
10 - Étant donné un ensemble dont tous les éléments sont des ensembles non vides il existe un ensemble qui a en commun avec chaque élément de l'ensemble donné un et un seul élément :

$$\forall x \left((\emptyset \in x) \vee \left(\exists y \forall t \left((t \in x) \Rightarrow \left(\exists z \forall u \left(\begin{array}{c} ((z \in t) \wedge (z \in y)) \\ \wedge \\ (((u \in t) \wedge (u \in y)) \Rightarrow (u = z)) \end{array} \right) \right) \right) \right) \right).$$

On peut choisir simultanément un élément dans chaque ensemble d'une famille d'ensembles non vides.

Ces règles sont les 9 axiomes de la théorie des ensembles de Zermelo et Fraenkel auxquels on a ajouté l'axiome du choix. L'axiome 2 nous garantit l'existence d'au moins un ensemble, l'ensemble vide. Les autres axiomes nous garantissent l'existence de nombreux ensembles. Les six premiers axiomes permettent de donner un sens en termes d'ensembles aux notions de couple, de produit cartésien, d'intersection, de réunion, de différence, de projection sur un des facteurs d'un sous-ensemble d'un produit cartésien. L'axiome 7 assure l'existence d'un ensemble infini et permet de construire les entiers naturels. Les axiomes 8, 9 et 10 sont plus difficiles à saisir. Le dernier, appelé axiome du choix a une importance importante dans toutes les branches des mathématiques.

Gödel montre qu'il existe des assertions dont on ne peut dire si elles sont vraies ou fausses en utilisant les 10 axiomes précédents et le langage de la théorie des ensembles. Il montre également que pour montrer qu'il n'existe pas d'assertions contradictoires dans la théorie des ensembles il faut raisonner dans une théorie plus forte que la théorie des ensembles.

3.2 Définition par compréhension, inclusion, intersection, réunion, différence, complémentaire, couple, produit cartésien, projection

Si X est un ensemble et A un prédicat $(\forall x \in X \ A)$ est synonyme de $(\forall x((x \in X) \Rightarrow A))$ et $(\exists x \in X \ A)$ est synonyme de $(\exists x((x \in X) \wedge A))$. Le prédicat $(\forall x \in X \ A)$ se lit "pour tout x dans X on a A" ou "si x dans X alors A". Le prédicat $(\exists x \in X \ A)$ se lit "il existe x dans X tel que A".

L'ensemble des parties Si X est un ensemble, l'ensemble des parties de X donné par l'axiome 6 est noté $\mathcal{P}(X)$ ou 2^X.

Inclusion Soit X et Y deux ensembles. On dit que Y est inclus dans X et on écrit $Y \subset X$ ou $X \supset Y$ si l'assertion

$$\forall x((x \in Y) \Rightarrow (x \in X))$$

est vraie. D'après le premier axiome $X = Y$ si $Y \subset X$ et $X \subset Y$. On note $Y \not\subset X$ la négation $(\neg(Y \subset X))$.

Définition par compréhension Soit X un ensemble et $A(x)$ un prédicat qui possède une variable libre. Alors le sous-ensemble

$$Y = \{x \in X : A(x)\}$$

de X défini par compréhension à partir du prédicat $A(x)$ (voir axiome 5) est caractérisé de la façon suivante

$$\forall x((x \in Y) \Leftrightarrow ((x \in X) \wedge A(x))).$$

Réunion Si X et Y sont deux ensembles alors la réunion $X \cup Y$ vérifie

$$\forall x(((x \in X) \vee (x \in Y)) \Leftrightarrow (x \in X \cup Y)).$$

Si I est un ensemble et $(X_i)_{i\in I}$ est une famille d'ensembles indexée par I alors la réunion $X = \bigcup_{i\in I} X_i$ donnée par le quatrième axiome vérifie

$$\forall x((\exists i((i \in I) \wedge (x \in X_i))) \Leftrightarrow (x \in X)).$$

Intersection Si X et Y sont deux ensembles alors l'intersection $X \cap Y$ vérifie

$$\forall x(((x \in X) \wedge (x \in Y)) \Leftrightarrow (x \in X \cap Y))).$$

Si I est un ensemble non vide et $(X_i)_{i\in I}$ est une famille d'ensembles indexée par I alors l'intersection $X = \bigcap_{i\in I} X_i$ est l'ensemble

$$X = \{x \in X_{i_0} : \forall i((i \in I) \Rightarrow (x \in X_i))\}$$

où i_0 est un élément quelconque de I.

Différence et complémentaire Si X et Y sont deux ensembles alors la différence $X \setminus Y$ et le sous-ensemble de X défini par

$$X \setminus Y = \{x \in X : (\neg(x \in Y))\}.$$

Si $Y \subset X$ alors $X \setminus Y$ s'appelle le complémentaire de Y dans X.

Couple Soit x et y deux ensembles alors l'ensemble $\{x, \{x, y\}\}$ s'appelle le couple de premier terme x et de second terme y. Il est noté (x, y). Le couple (x, y) existe par l'axiome 3 : c'est la paire obtenue à partir de x et de la paire obtenue à partir de x et de y. Il est unique par l'axiome 1.

n-uplet Un n-uplet $(x_1, ..., x_n)$ peut être défini comme le couple formé du $n-1$-uplet $(x_1, ..., x_{n-1})$ et de x_n. Il s'agit là d'une définition par récurrence. On convient d'identifier à $(x_1, .., x_n)$ tous les couples de la forme $((x_1, ..., x_k), (x_{k+1}, ..., x_n))$ avec $k \in \{1, ..., n-1\}$.

Produit cartésien Soit X et Y deux ensembles. Le produit cartésien $X \times Y$ est le sous-ensemble de $\mathcal{P}(X \cup Y)$ défini par

$$X \times Y = \{z \in \mathcal{P}(X \cup Y) : (\exists x \exists y(((x \in X) \wedge (y \in Y)) \wedge (z = (x, y)))))\}.$$

C'est l'ensemble des couples (x, y) avec $x \in X$ et $y \in Y$.

Produit cartésien de plusieurs ensembles Si $X_1, ..., X_n$ sont des ensembles alors le produit $X_1 \times ... \times X_n$ aussi noté $\prod_{i=1}^{n}$ est le produit cartésien de $X_1 \times ... \times X_{n-1}$ avec X_n. Il s'agit là d'une définition par récurrence. On convient d'identifier à $X_1 \times X_n$ tous les produits cartésiens de la forme $(X_1 \times ... \times x_k), (X_{k+1} \times ... \times X_n))$ avec $k \in \{1, ..., n-1\}$. Les Le produit cartésien $X_1 \times ... \times X_n$ est l'ensemble des n-uplets $(x_1, ..., x_n)$ avec $x_k \in X_k$ pour chaque $k \in \{1, ..., n\}$.

Projection Soit X et Y deux ensembles et Z un sous-ensemble du produit cartésien $X \times Y$. Alors la projection de Z sur X parallèlement à Y est le sous-ensemble de $\pi_X(Z)$ défini par

$$\pi_X(Z) = \{x \in X : \exists y((x, y) \in Z\}.$$

C'est l'ensemble des éléments x de X pour les quels il existe au moins un $y \in Y$ tel que le couple (x, y) soit dans Z. On définit de façon analogue la projection de Z sur Y parallèlement à X en posant

$$\pi_Y(Z) = \{y \in Y : \exists x((x, y) \in Z\}.$$

Soit X, Y, Z et T quatre ensembles et A et B des prédicats avec une variable libre. Alors
- $(X \cap Y) \subset X$, $(X \cap Y) \subset Y$,

- $X \cap X = X$, $X \cap Y = Y \cap X$, $X \cap (Y \cap Z) = (X \cap Y) \cap Z$,
- $X \subset (X \cup Y)$, $Y \subset (X \cup Y)$,
- $X \cup X = X$, $X \cup Y = Y \cup X$, $X \cup (Y \cup Z) = (X \cup Y) \cup Z$,
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Y)$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Y)$,
- si $Z \subset Y$ et $Y \subset X$ alors $Z \subset X$,
- si $Y \subset X$ alors $X = Y \cup (X \setminus Y)$, $\emptyset = Y \cap (X \setminus Y)$, $Y = X \setminus (X \setminus Y)$,
- si $Y = \{x \in X : A(x)\}$ et $Z = \{x \in X : B(x)\}$ alors

$$\begin{array}{rcl} X \setminus Y &=& \{x \in X : (\neg A(x))\}, \\ Y \cap Z &=& \{x \in X : (A(x) \wedge B(x))\}, \\ Y \cup Z &=& \{x \in X : (A(x) \vee B(x))\}, \end{array}$$

- si Z et T sont des sous-ensembles de $X \times Y$ alors

$$\pi_X(Z \cup T) = \pi_X(Z) \cup \pi_X(T), \quad \pi_X(Z \cap T) \subset \pi_X(Z) \cap \pi_X(T)$$

et si de plus $Z \subset T$ alors $\pi_X(Z) \subset \pi_X(T)$.

Soit I un ensemble non vide, Y un ensemble et $(X_i)_{i \in I}$ une famille d'ensembles. Alors

$$\begin{array}{rcl} \left(\bigcup\limits_{i \in I} X_i\right) \cap Y &=& \bigcup\limits_{i \in I} (X_i \cap Y), \\ \left(\bigcap\limits_{i \in I} X_i\right) \cup Y &=& \bigcap\limits_{i \in I} (X_i \cup Y). \end{array}$$

Si $\left(\bigcup\limits_{i \in I} X_i\right) \subset Y$ alors

$$\begin{array}{rcl} Y \setminus \left(\bigcup\limits_{i \in I} X_i\right) &=& \bigcap\limits_{i \in I} (Y \setminus X_i), \\ Y \setminus \left(\bigcap\limits_{i \in I} X_i\right) &=& \bigcup\limits_{i \in I} (Y \setminus X_i). \end{array}$$

Soit Iet J des ensembles non vides, soit $(I_j)_{j \in J}$ une famille de sous-ensembles non vides de I dont la réunion est I et $(X_i)_{i \in I}$ une famille d'ensembles. Alors

$$\bigcup_{i \in I} X_i = \bigcup_{j \in J} \left(\bigcup_{i \in I_j} X_i\right) \text{ et } \bigcap_{i \in I} X_i = \bigcap_{j \in J} \left(\bigcap_{i \in I_j} X_i\right).$$

Soit X et Y des ensembles, I un ensemble non vide et $(Z_i)_{i \in I}$ une famille de sous-ensembles de $X \times Y$ alors

$$\pi_X \left(\bigcup_{i \in I} Z_i\right) = \left(\bigcup_{i \in I} \pi_X(Z_i)\right), \pi_X \left(\bigcap_{i \in I} Z_i\right) \subset \left(\bigcap_{i \in I} \pi_X(Z_i)\right)$$

et

$$\pi_Y \left(\bigcup_{i \in I} Z_i\right) = \left(\bigcup_{i \in I} \pi_Y(Z_i)\right), \pi_Y \left(\bigcap_{i \in I} Z_i\right) \subset \left(\bigcap_{i \in I} \pi_Y(Z_i)\right).$$

4 Applications

4.1 Fonctions, applications et graphes

4.1.1 Fonction

Une fonction est un triplet $f = (E, F, \mathcal{G})$ où E et F sont des ensembles et $\mathcal{G}$ un sous-ensemble de $E \times F$ tel que si $x \in E$ alors il existe au plus un $y \in F$ et noté $f(x)$ tel que $(x, y) \in \mathcal{G}$. La fonction f est souvent notée $f : E \to F$. L'ensemble $\mathcal{G}$ s'appelle le graphe de f.

4.1.2 Application

Une application est un triplet $f = (E, F, \mathcal{G})$ où E et F sont des ensembles et $\mathcal{G}$ un sous-ensemble de $E \times F$ tel que si $x \in E$ alors il existe un et un seul $y \in F$ et noté $f(x)$ tel que $(x, y) \in \mathcal{G}$. L'application f est souvent notée $f : E \to F$. L'ensemble E s'appelle le domaine ou l'ensemble de départ de f, l'ensemble F s'appelle l'ensemble d'arrivée et l'ensemble $\mathcal{G}$ s'appelle le graphe de f.

Soit $f : E \to F$ et $f' : E \to F$ deux applications. Si pour tout $x \in E$ on a $f(x) = f'(x)$ alors $f = f'$.

Si E et F sont deux ensembles, il existe un ensemble noté E^F dont les éléments sont les applications de E dans F.

Si F est un ensemble alors $\emptyset^F = \{(\emptyset, F, \emptyset)\}$. Si E est un ensemble non vide alors $E^\emptyset = \emptyset$.

4.1.3 Image, image réciproque, antécédent

Si $(x, y) \in \mathcal{G}$ alors y est appelée image de x par f ou valeur de f en x et x est appelé antécédent de y par f. Si $X \subset E$ Le sous-ensemble des éléments de F qui sont des images d'éléments de X par f s'appelle l'image de X par f et il est noté $f(X)$. L'ensemble $f(E)$ s'appelle ensemble des valeurs de f ou l'image de f. Si $Y \subset F$ le sous-ensemble des éléments de E qui sont les antécédents des éléments de Y par f s'appelle l'image réciproque de Y par f et il est noté $f^{-1}(Y)$.

4.1.4 Deux exemples : l'application identité et les applications constantes

Si E est un ensemble alors l'ensemble $\mathcal{I}_E = \{(x, x) : x \in E\}$ est le graphe d'une application de Id_E de E dans E appelée identité de E : si $x \in E$ alors $Id_E(x) = x$.

Soit E et F deux ensembles. Soit $y \in F$. On appelle application constante y l'application f de E dans F définie par $f(x) = y$ si $x \in E$. Son graphe est l'ensemble $\{(x, y) : x \in E\}$.

4.2 Restriction, prolongement, corestriction, coprolongement

Soit $E \subset E'$, $f : E \to F$ et $f' : E' \to F$. On dit que f est une restriction de f' à E ou que f' est un prolongement de f à E' si pour tout $x \in E$ on a $f(x) = f'(x)$.

Soit $E \subset E'$ et $f : E \to F$. Alors il existe un prolongement f' de f à E'.

Soit $E \subset E'$ et $f' : E' \to F$. Alors il existe une et une seule restriction de f' à f.

Soit $F \subset F'$, $f : E \to F$ et $f' : E \to F'$. On dit que f est une corestriction de f' à F ou que f' est un coprolongement de f à F' si pour tout $x \in E$ on a $f(x) = f'(x)$.

Soit $F \subset F'$ et $f : E \to F$. Alors il existe un et un seul coprolongement f' de f à F'. Les graphes de f et f' sont égaux et $f'(E) = f(E)$.

Soit $F \subset F'$ et $f' : E \to F'$ telle que $f'(E) \subset F$. Alors il existe une unique corestriction f de f' à F. Les graphes de f et f' sont égaux et $f'(E) = f(E)$.

4.3 Composition

Soit $f : E \to F$ et $g : F' \to H$ deux applications de graphes $\mathcal{F}$ et $\mathcal{G}$. Si $F \subset F'$ alors l'ensemble

$$\mathcal{H} = \{(x,z) \in E \times H : \exists y \in F \ (x,y) \in \mathcal{F} \text{ et } (y,z) \in \mathcal{G}\}$$

est le graphe d'une application h de domaine E et d'ensemble d'arrivée H. Si $x \in E$ alors $(x, g(f(x))) \in \mathcal{H}$. En d'autres termes, si $x \in E$, $h(x) = g(f(x))$.

Soit $f : E \to F$ et $g : F' \to H$ deux applications de graphes $\mathcal{F}$ et $\mathcal{G}$. Si $F \subset F'$ l'application dont le graphe est l'ensemble

$$\mathcal{H} = \{(x,z) \in E \times H : \exists y \in F \ (x,y) \in \mathcal{F} \text{ et } (y,z) \in \mathcal{G}\}$$

est appelée composée de f suivie de g et est notée $g \circ f$ (lire g rond f). On a $(g \circ f)(x) = g(f(x))$ si $x \in E$.

Si $f : E \to F$ alors $f = Id_F \circ f = f \circ Id_E$.

Soit E, F, F' et G quatre ensembles tels que $F \subset F'$. Alors l'ensemble

$$\mathcal{H} = \{(f,g,h) \in E^F \times {F'}^G \times E^G : \forall x \in E, h(x) = g(f(x))\}$$

est le graphe d'une application de $E^F \times {F'}^G$ dans E^G appelée composée. Si $(f,g,h) \in \mathcal{H}$ alors $h = g \circ f$.

Si $f : E \to F$, $g : F' \to H$, $h : H' \to K$ telles que $F \subset F'$ et $H \subset H'$ alors $h \circ (g \circ f) = (h \circ g) \circ f$.

4.4 Injection, surjection, bijection

Soit $f : E \to F$ une application. Elle est dite injective si deux éléments distincts quelconques de E ont toujours des images distinctes, c'est à dire si pour tout $y \in F$ l'ensemble $f^{-1}(\{y\})$ est vide ou un singleton. Elle est dite surjective si tout élément de F admet au moins un antécédent, c'est à dire si $f(E) = F$. Elle est dite bijective si elle est à la fois injective et surjective. Une injection est une application injective, une surjection est une application surjective et une bijection est une application bijective.

Soit F un ensemble. La seule application de $\emptyset$ dans F est $(\emptyset, F, \emptyset)$ qui est clairement injective. Elle est surjective donc bijective si et seulement si $F = \emptyset$.

Si E est un ensemble alors Id_E est une bijection.

La restriction, la corestriction ou le coprolongement d'une injection sont injectifs.

Si $E \subset F$ le coprolongement de Id_E à F est une injection appelée injection canonique ou inclusion de E dans F.

Soit $f : E \to F$ et $g : F \to G$ deux applications. Si f et g sont injectives alors $g \circ f$ est injective. Si f et g sont surjectives alors $g \circ f$ est surjective. Si $g \circ f$ est injective alors f est injective. Si $g \circ f$ est surjective alors g est surjective.

4.5 Réciproque ou inverse pour la composition

Soit $f : E \to F$ une application. Une application $g : F \to E$ est appelée réciproque de f ou inverse de f pour la composition si pour $x \in E$ et $y \in F$ on a $g(f(x)) = x$ et $f(g(y)) = y$.

Si g est une réciproque de f alors f est une réciproque de g.

Si $g : F \to E$ et $g' : F \to E$ sont deux réciproques d'une application $f : E \to F$ alors $g = g'$.

Une application $f : E \to F$ possède une réciproque si et seulement si f est bijective.

Si $f : E \to F$ admet une réciproque alors cette réciproque, qui est unique est noté f^{-1}.

La réciproque f^{-1} d'une bijection est également une bijection.

D'après ce qui précède, s'il existe une bijection d'un premier ensemble dans un second, il existe aussi une bijection du second dans le premier. C'est pourquoi on dit que deux ensembles sont en bijection s'il existe une bijection de l'un dans l'autre.

Soit $f : E \to F$ une bijection et $g : F \to E$. Si pour tout $x \in E$ on a $g(f(x)) = x$ alors g est la réciproque de f. Si pour tout $y \in F$ on a $f(g(y)) = y$ alors g est la réciproque de f.

Soit $f : E \to F$ une application et $\mathcal{G}$ son graphe. Alors E et $\mathcal{G}$ sont en bijection : l'application qui à $x \in E$ associe $(x, f(x)) \in \mathcal{G}$ est une bijection.

Soit $f : E \to F$ et $g, h : F \to E$ telles que si $x \in E$ et $y \in F$ alors $g(f(x)) = x$ et $f(h(y)) = y$. Alors f est bijective et $f^{-1} = g = h$.

Soit E un ensemble et $f \in E^E$. On dit que f est une involution si $f \circ f = Id_E$, c'est à dire si f est son propre inverse.

Soit E un ensemble et $a, b \in E$. La transposition de a et b est l'application σ_{ab}^E définie par $\sigma_{ab}^E(a) = b$, $\sigma_{ab}^E(b) = a$ et $\sigma_{ab}^E(x) = x$ si $x \in E \setminus \{a, b\}$.

Soit E un ensemble et $a, b \in E$. La transposition σ_{ab}^E est l'identité si et seulement si $a = b$.

Les transpositions sont des involutions.

Une transposition est une bijection puisque elle possède un inverse, elle même.

Soit $f : E \to F$. Si f est injective alors il existe une surjection $g : F \to E$ telle que si $x \in E$ alors $g(f(x)) = x$. Si f est surjective alors il existe une injection $g : F \to E$ telle que si $y \in F$ alors $f(g(y)) = y$.

Soit $f : E \to F$ de graphe $\mathcal{F}$ et $g : E \to G$ de graphe $\mathcal{G}$. Alors l'ensemble

$$\mathcal{H} = \{(x, y, z) \in E \times F \times G : (x, y) \in \mathcal{F}, (x, z) \in \mathcal{G}\}$$

est le graphe d'une application $h : E \to F \times G$ telle que si $x \in E$ alors $h(x) = (f(x), g(x))$.

Soit $f : E \to F$ de graphe $\mathcal{F}$ et $g : E \to G$ de graphe $\mathcal{G}$ deux applications définies sur le même ensemble de départ. Alors l'application de graphe

$$\mathcal{H} = \{(x, y, z) \in E \times F \times G : (x, y) \in \mathcal{F}, (x, z) \in \mathcal{G}\}$$

est notée (f, g). Si $x \in E$ alors $(f, g)(x) = (f(x), g(x))$.

Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications. Alors l'ensemble

$$\mathcal{H} = \{(x, x'), (y, y') \in (E \times E') \times (F \times F') : (x, y) \in \mathcal{F}, (x', y') \in \mathcal{F}\}$$

est le graphe d'une application $h : E \times E' \to F \times F'$ telle que si $(x, x') \in E \times E'$ $h(x, x') = (f(x), f'(x'))$.

Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications et soit $h : E \times E' \to F \times F'$ l'application de

$$\mathcal{H} = \{(x, x'), (y, y') \in (E \times E') \times (F \times F') : (x, y) \in \mathcal{F}, (x', y') \in \mathcal{F}\}.$$

L'application h est injective si et seulement si f et et f' le sont. Elle est surjective si et seulement f et f' le sont.

Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications. On suppose que $E \cap E' = \emptyset$. Alors $\mathcal{G} = \mathcal{F} \cup \mathcal{F}'$ est le graphe d'une application $g : E \cup E' \to F \cup F'$ telle que $g(x) = f(x)$ si $x \in E$ et $g(x) = f'(x')$. On a $g(E \cup E') = f(E) \cup f'(E')$. Si f et f' sont des bijections et $F \cap F' = \emptyset$ alors g est une bijection.

5 Indices

5.1 Famille indexée

Un famille indexée est la donnée d'un ensemble I appelé ensemble d'indices et d'une application ϕ de I dans un ensemble E qui permet d'indexer des éléments de E. On note x_i l'élément de E qui est l'image de i par l'application ϕ. On note $(x_i)_{i\in I}$ la famille de E indexée par I (via ϕ).

Souvent I est un sous-ensemble de $\mathbf{N}$ ou de $\mathbf{Z}$ ou encore de $\mathbf{N}^n$ ou de $\mathbf{Z}^n$.

5.2 Action d'une loi sur une famille indexée

On considère un ensemble E muni d'une loi de composition interne, c'est à dire d'une application $*$ de $E\times E$ dans E. On suppose que cette loi $*$ est associative, c'est à dire que si $x,y,z\in E$ alors $x*(y*z)=(x*y)*z$. Alors si $(x_i)_{i\in\mathbf{N}}$ est une famille indexée de E alors on définit par récurrence $\mathop{*}\limits_{i=1}^{n} x_i$ si $n\in\mathbf{N}^*$ de la façon suivante : $\mathop{*}\limits_{i=1}^{1} x_i = x_1$ et si $n>1$

$$\mathop{*}\limits_{i=1}^{n} x_i = \left(\mathop{*}\limits_{i=1}^{n-1} x_i\right) * x_n.$$

On suppose que $*$ est de plus commutative, c'est à dire que si $x,y\in E$ alors $x*y=y*x$. Alors l'ordre importe peu quand on fait agir $*$ et on peut définir de façon analogue $\mathop{*}\limits_{i\in I} x_i$ si $\mathcal{F}=(x_i)_{i\in I}$ est une famille d'éléments de E indexée par un ensemble fini et non vide I :

$$\mathop{*}\limits_{i\in I} x_i = \mathop{*}\limits_{k=1}^{n} x_{i_k}$$

où l'application $k\in\{1,...,n\}\mapsto i_k\in I$ est une bijection qui permet d'ordonner I (on indexe la famille d'indices I par les entiers $\{1,...,n\}$). Cette définition ne dépend pas de la façon d'ordonner I.

5.3 Les symboles $\sum$ et $\prod$

5.3.1 Le symbole $\sum$

Si la loi est notée $+$ et qu'elle est associative et commutative (comme l'addition dans $\mathbf{R}$) on pose $\mathop{+}\limits_{i\in I} x_i = \sum\limits_{i\in I} x_i$ et $\mathop{+}\limits_{i=1}^{n} x_i = \sum\limits_{i=1}^{n} x_i$.

Si l'ensemble d'indices I est de la forme $I=K\times L$ alors on a

$$\sum_{i\in I} x_i = \sum_{(k,l)\in K\times L} x_{kl} = \sum_{k\in K}\left(\sum_{l\in L} x_{kl}\right) = \sum_{l\in L}\left(\sum_{k\in K} x_{kl}\right).$$

On peut montrer par récurrence sur n

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \text{ et } \sum_{k=1}^{n} x^k = x\frac{1-x^n}{1-x} \text{ si } x\in\mathbf{R}\setminus\{1\}.$$

5.3.2 Le symbole $\prod$

Si la loi est notée $\times$ et qu'elle est associative et commutative (comme la multiplication dans $\mathbf{R}$) on pose $\mathop{\times}\limits_{i\in I} x_i = \prod\limits_{i\in I} x_i$ et $\mathop{\times}\limits_{i=1}^{n} x_i = \sum\limits_{i=1}^{n} x_i$.

Si l'ensemble d'indices I est de la forme $I = K \times L$ alors on a

$$\prod_{i \in I} x_i = \prod_{(k,l) \in K \times L} x_{kl} = \prod_{k \in K} \left(\prod_{l \in L} x_{kl} \right) = \prod_{l \in L} \left(\prod_{k \in K} x_{kl} \right).$$

5.3.3 Lorsque E est muni des deux lois $+$ et $\times$

On suppose que E est muni de deux lois $+$ et $\times$, toutes les deux associatives et commutatives. On suppose aussi que $\times$ est distributive par rapport à $+$. Ceci signifie que si $x, y, z \in E$ alors $x \times (y + z) = (x \times y) + (x \times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$.

Dans ce cas, si $(x_n)_{n \in \mathbf{N}^*}$ est une suite d'éléments de E alors :

$$\begin{array}{ll} \text{si } n = 1, & \displaystyle\sum_{i=1}^{1} x_i = x_1 \text{ et } \prod_{i=1}^{1} x_i = x_1; \\ \text{si } n \in \mathbf{N} \text{ et } n > 1, & \displaystyle\sum_{i=1}^{n+1} x_i = \left(\sum_{i=1}^{n} x_i \right) + x_{n+1} \text{ et } \prod_{i=1}^{n+1} x_i = \left(\prod_{i=1}^{n} x_i \right) \times x_{n+1}. \end{array}$$

Si $x \in E$ alors x^n désigne $\displaystyle\prod_{i=1}^{n} x$.

Si $x \in E$ et si $n \in \mathbf{N}^*$ alors $\displaystyle\prod_{i=1}^{n} x^i = x^{\frac{n(n+1)}{2}}$.

Table des matières