Éléments de mathématiques pour le XXI^{e} siècle, volume 1

Du même auteur

- Déjà paru :
  - Éléments de mathématiques pour le XXI[e] siècle, volume 2 : Fondements des mathématiques 2 (théorie des ensembles, mathématiques discrètes, structures algébriques de base)
- À paraître :
  - Éléments de mathématiques pour le XXI[e] siècle, volume 3 : Fondements des mathématiques 3
  - Éléments de mathématiques pour le XXI[e] siècle, volume 4 : Fondements des mathématiques 4

Éléments de mathématiques pour le XXI^{e} siècle, volume 1

Fondements des mathématiques 1
(logique des propositions et des prédicats, systèmes déductifs formels, arithmétique de Peano, structures algébriques de base)

Étienne Bonheur

https://www.paysmaths.net

ISBN : 978-2-9569666-0-9
Dépôt légal : Juillet 2019

Table des matières

Introduction

Ce livre est le premier volume d'une série qui doit, à terme, couvrir l'ensemble des notions du premier cycle universitaire en mathématiques, tout en débordant largement sur le deuxième cycle. Il sera donc utile aux étudiants en licence ou en classes préparatoires scientifiques, ainsi qu'aux étudiants en master, y compris ceux préparant le CAPES ou l'agrégation (dont les programmes sont également très largement couverts par cette série d'ouvrages) [1]. Les enseignants y trouveront aussi de nombreux éléments leur permettant de préparer leurs cours, ou de compléter leurs connaissances dans des domaines qui ne leur sont pas familiers.

De manière plus générale, cette série d'ouvrages pourra être utile à toute personne s'intéressant aux mathématiques actuelles (les *mathématiques du XXI^e siècle* auxquelles fait référence le titre [2]). Elle devrait, *en théorie*, être accessible même sans connaissance préalable. En effet, les mathématiques sont prises à leur début et les différents concepts progressivement construits, chaque définition, théorème et démonstration ne faisant appel qu'à ce qui a été défini précédemment. Ce principe général aura cependant quelques exceptions : je pourrai, pour des raisons didactiques (notamment dans les remarques et exemples), ou par volonté de synthèse, être parfois amené à faire référence à des notions postérieures. À noter aussi que je suivrai un ordre me permettant d'enchaîner logiquement les différentes notions, mais qui n'est pas nécessairement l'ordre que l'on pourrait trouver dans un cursus universitaire, c'est-à-dire, par exemple, que certains éléments apparaissant dans les premiers volumes peuvent être enseignés traditionnellement dans des classes de troisième année de licence, voire au-delà. Néanmoins les chapitres peuvent être largement indépendants, et la compréhension d'un chapitre donné n'est pas toujours nécessaire à la compréhension de ceux qui suivent. Par ailleurs, lorsque cela peut être utile, les prérequis principaux seront indiqués au début d'une section [3].

Chaque ouvrage se veut à la fois

- didactique, avec des preuves très détaillées, des explications informelles, et de nombreux exemples et contre-exemples ;
- complet, voire encyclopédique, avec un exposé de nombreuses notions, des théorèmes tous démontrés, et de nombreux détails historiques (notamment sur l'origine des notations et du vocabulaire mathématique) ;
- synthétique, avec en particulier la volonté de multiplier les points de vue ; par exemple, les sujets pourront être abordés de façon à la fois formelle et informelle, et il pourra arriver que je donne plusieurs définitions équivalentes d'un même concept, ou plusieurs preuves d'un même théorème.

J'ai décidé de ne pas inclure de bibliographie, qui ne serait qu'une très longue liste de documents, et dont l'intérêt serait limité, sachant que dans cet ouvrage, tous les termes sont définis, tous les théorèmes sont prouvés, et le lecteur peut ainsi vérifier par lui-même tous les résultats. Les affirmations non justifiées (par exemple les remarques historiques) et certaines démonstrations sont directement sourcées dans les notes de bas de page. Cependant, pour les remarques portant sur l'origine du vocabulaire et des notations, je n'indiquerai pas à chaque fois mes sources principales, qui sont

1. Ou des cursus équivalents, pour les lecteurs francophones non français.

2. Le début du titre faisant par ailleurs référence aux *Éléments* d'Euclide, et aux *Éléments de Mathématique* de Bourbaki, deux œuvres partageant avec la présente série la volonté d'exposition des savoirs selon un ordre logique précis, à partir d'axiomes donnés.

3. Les différents prérequis indiqués ne correspondent ni à un minimum, ni à un maximum à connaître pour comprendre la section en cours, mais doivent être pris comme une aide pour identifier, parmi les notions abordées précédemment, celles pouvant être utiles.

- Jeff MILLER. *Earliest Known Uses of Some of the Words of Mathematics*. URL : `http://jeff560.tripod.com/mathword.html`.
- Jeff MILLER. *Earliest use of various mathematical symbols*. URL : `http://jeff560.tripod.com/mathsym.html`.
- Florian CAJORI. *A history of mathematical notations*. The Open Court Publishing Co., 1928-1929.

Je précise que les sources indiquées ne sont pas nécessairement exhaustives (je peux par exemple donner uniquement une source simple d'accès, ce qui est le cas des précédentes), et que dans la mesure du possible, je vérifie et recoupe toutes les informations, y compris les références données par ces différentes sources. Par ailleurs, les citations issues de textes non francophones feront automatiquement l'objet d'une traduction personnelle, sans que je le signale non plus à chaque fois.

Je précise aussi que les remarques historiques sont nécessairement succinctes, et ne rendent pas forcément compte de la complexité de l'évolution des concepts étudiés. Il en est de même pour la présentation de ces concepts, sous la forme de définitions, axiomes ou théorèmes. Celle-ci peut parfois donner l'impression que les notions s'articulent entre elles de façon naturelle, mais encore une fois cela cache les multiples variantes et points de vue, les contributions des différents mathématiciens, ainsi que leurs interrogations et tâtonnements, qui ont permis de façonner les mathématiques contemporaines.

On notera enfin qu'aucun paragraphe ne commence par « exercice », ce qui ne veut pas dire que le lecteur ne dispose d'aucun matériel pour s'exercer : les exemples ainsi que les nombreux théorèmes peuvent être considérés comme autant d'exercices corrigés (beaucoup d'énoncés que l'on trouve fréquemment dans la littérature mathématique sous l'intitulé *exercice* se trouvent ici sous l'intitulé *théorème*). Ainsi, chaque théorème étant suivi d'une preuve complète, il n'y aura pas dans cette série d'ouvrages d'expressions comme « la preuve est laissée en exercice », « le lecteur prouvera lui-même que ... », et autres « on démontre facilement que ... ».

Les quatre premiers volumes traitent des fondements modernes des mathématiques. Je prends cette expression dans un sens un peu général : au-delà de son acception la plus usuelle (comprenant, pour faire simple, la logique [4] mathématique et la théorie des ensembles), j'inclus d'autres sujets comme la construction des ensembles classiques de nombres (ensemble $\mathbb{N}$ des entiers naturels, ensemble $\mathbb{R}$ des nombres réels, ...) ou l'étude de certaines structures algébriques de base (comme les groupes ou les anneaux).

Ce premier volume est essentiellement consacré à la notion de logique mathématique. On étudiera en particulier les sujets suivants :

- la logique des propositions (ou calcul des propositions) ;
- le calcul booléen (ou algèbre de Boole) ;
- la logique des prédicats (ou calcul des prédicats, ou logique du premier ordre) ;
- des systèmes formels utilisés dans la théorie de la démonstration : seront notamment détaillés un système déductif à la Hilbert et la déduction naturelle (pour la logique des propositions et la logique des prédicats) ;
- quelques exemples d'autres logiques formelles (logique du second ordre, logique intuitionniste ...).

On trouvera aussi divers sujets un peu moins liés aux mathématiques formelles :

- des éléments de logique traditionnelle (syllogismes et diagrammes logiques) ;
- des exemples de paralogismes [5] classiques.

Enfin, la présentation de la logique des prédicats sera aussi l'occasion d'aborder d'autres notions :

- une première approche de quelques structures algébriques de base (groupes, anneaux, ...) ;
- la théorie axiomatique de l'arithmétique de Peano, qui formalise les propriétés des nombres entiers et des opérations associées (addition, multiplication).

4. Logique : du grec *logikê*, dérivé de *logos*, signifiant à la fois raison, langage, et raisonnement.

5. Un paralogisme est un raisonnement incorrect qui peut sembler correct, l'erreur pouvant être commise de bonne foi ou dans l'intention de tromper (dans ce cas on utilise plutôt le terme *sophisme*).

Le deuxième volume sera principalement consacré à l'exposé de la théorie des ensembles de Zermelo-Fraenkel (qui est le fondement formel des mathématiques le plus classique) et à quelques applications immédiates : reprise et généralisation des structures algébriques de base vues dans le volume 1, introduction du concept de *morphisme* entre structures et de celui de *cardinal* (qui généralise le principe permettant de *dénombrer* un ensemble fini, c'est-à-dire de compter ses éléments) ; construction de l'ensemble $\mathbb{N}$ des entiers naturels et de l'ensemble $\mathbb{Z}$ des entiers relatifs ; présentation d'applications diverses dans le domaine de ce qu'on appelle les *mathématiques discrètes* : éléments de théorie des nombres (l'étude des propriétés des nombres entiers), et introduction à l'analyse combinatoire (l'étude du dénombrement d'ensembles finis).

Les troisième et quatrième volumes seront consacrés

- à des compléments de théorie des ensembles : étude du concept d'*ordinal*, qui généralise le principe permettant d'*ordonner* un ensemble fini (en numérotant ses éléments), et compléments sur les cardinaux ;
- à des exemples de théories alternatives des ensembles : théorie des classes de von Neumann-Bernays-Gödel (NBG) et de Morse-Kelley (MK), théorie NFU (*New Foundations with Urelements*) ;
- à l'*introduction* de différentes théories mathématiques plus avancées en rapport avec la logique et les fondements des mathématiques : théorie des modèles, théorie de la calculabilité, théorie des catégories et des topos (et théorie élémentaire de la catégorie des ensembles, autre théorie alternative des ensembles), théorie homotopique des types (permettant aussi un autre fondement formel alternatif des mathématiques) ;
- à l'étude d'autres éléments de mathématiques discrètes (compléments de théorie des nombres et d'analyse combinatoire, introduction à la théorie des graphes) ;
- à des compléments sur les différentes structures mathématiques, et à la construction des autres ensembles classiques de nombres (ensemble $\mathbb{Q}$ des rationnels, ensemble $\mathbb{R}$ des réels, …).

Vocabulaire et notations

On distingue traditionnellement, dans les ouvrages mathématiques, les *théorèmes*, les *propositions* ou *assertions* (théorèmes de moindre importance), les *lemmes* (résultats qui constituent une étape dans la démonstration d'un théorème), et les *corollaires* (conséquences immédiates d'un théorème). Ces distinctions étant purement subjectives, je ne les utiliserai pas comme intitulé : je garderai le sens habituel de *proposition* en logique (affirmation qui peut-être vraie, ou fausse) et je n'emploierai que le mot *théorème* ; c'est-à-dire qu'aucun paragraphe ne commencera par *lemme* ou *corollaire* (mais je pourrai toujours indiquer qu'un certain théorème est un lemme, ou un corollaire, d'un autre).

Je pourrai par contre employer le terme (tout aussi subjectif) *trivial*, que l'on rencontre en mathématiques, et qui peut désigner soit un énoncé dont la vérité est évidente, soit un objet mathématique dont l'existence va de soi et dont l'étude n'a pas grand intérêt (par exemple : en théorie des groupes, le *groupe trivial* formé du seul élément neutre, ou encore : la fonction nulle est une *solution triviale* de l'équation différentielle $y' = y$). Le terme *trivial* vient du latin *tri* (trois) et *via* (la voie, la route). *Trivia* est, pour les romains, un carrefour où se rejoignent trois voies. *Trivial* désigne jusqu'au XIX^{e} siècle une chose commune, banale, puis prend son sens moderne de grossier, vulgaire, qui existait déjà en latin. Le mot est aussi passé dans la langue anglaise avec le sens « insignifiant, banal ». On le trouve dans son acception mathématique, proche du sens anglais, dans un article du mathématicien britannique Arthur Cayley (1821-1895) [6].

Un autre élément de jargon mathématique que je pourrai employer est le terme *respectivement*, comme raccourci pour condenser plusieurs phrases en une : une expression comme

$$\dots [A] \text{ (respectivement } [A']) \dots [B] \text{ (respectivement } [B']) \dots$$

est un raccourci pour les deux phrases :

$$\dots [A] \dots [B] \dots$$
$$\dots [A'] \dots [B'] \dots$$

Par exemple : un triangle (respectivement carré) est une figure à trois (respectivement quatre) côtés.

En ce qui concerne l'égalité, qui a en mathématiques un sens parfois subtil, je ferai la distinction entre *égalité*, *égalité par définition*, et *affectation* :

- égalité :
$$A = B$$
(« A est égal à B »)
signifie : les objets A et B sont identiques.
- égalité par définition :
$$A \overset{\text{def}}{\equiv} B$$
(« A est égal, par définition, à B »)
signifie : on donne par définition, à l'objet B, le nom A.

6. Arthur CAYLEY. « Deuxième mémoire sur les fonctions doublement périodiques ». Dans : *Journal de Mathématiques Pures et Appliquées* 19 (1854), p. 193-208.

- affectation :

$$A :\equiv B$$

(« A prend la valeur B »)

signifie : la variable A prend la valeur B. Il s'agit en quelque sorte d'une affectation, dans le sens informatique du terme.

Les sens de $A \overset{\text{def}}{\equiv} B$ et de $A :\equiv B$ sont proches, l'affectation pouvant être considérée comme une définition, mais je réserverai en général le symbole $\overset{\text{def}}{\equiv}$ à des définitions de portée générale, et le symbole $:\equiv$ à des définitions de portée plus locale. Bien entendu, si $A \overset{\text{def}}{\equiv} B$, ou si $A :\equiv B$, on peut en déduire que $A = B$, mais les symboles $\overset{\text{def}}{\equiv}$ et $:\equiv$ apportent une information supplémentaire.

Les notations précédentes sont des variantes de symboles classiques : pour indiquer une définition, on trouve couramment $=_{\text{def}}$, notation introduite en 1894 par le mathématicien italien Cesare Burali-Forti (1861-1931) dans *Logica matematica*, ou sa variante $\overset{\text{def}}{=}$, ou encore l'un des symboles

$$\triangleq \qquad \equiv \qquad :=$$

Le signe d'égalité (=) a été utilisé pour la première fois en 1557 par le mathématicien et médecin anglais Robert Recorde (v. 1510-1558) dans *The Whetstone of Witte* [7], dans une version où les deux barres sont plus allongées que dans la version moderne. Il écrit :

> « Pour éviter la répétition fastidieuse de ces mots, *est égal à*, j'utiliserai (comme je le fais souvent dans mon travail) une paire de parallèles, ou lignes jumelles, de même longueur, comme ceci : ═══ , parce que deux choses ne peuvent pas être plus égales. »

Il faudra attendre 1618 pour que le symbole d'égalité apparaisse à nouveau dans un ouvrage imprimé, dans une annexe anonyme de la traduction par Edward Wright de *Descriptio* du mathématicien, physicien et astronome John Napier (ou Neper) (1550-1617), annexe probablement rédigée par le mathématicien et théologien anglais William Oughtred (1574-1660). Même s'il est largement répandu en Angleterre au XVII$^{\text{e}}$ siècle, ce n'est qu'au XVIII$^{\text{e}}$ siècle que le symbole de Recorde s'impose partout, car il était, surtout en Europe, en compétition avec $\propto$, le symbole d'égalité qu'utilise en 1637 le mathématicien, physicien et philosophe français René Descartes (1596-1650) dans *La Géométrie*, son ouvrage mathématique majeur.

Je précise enfin que j'énonce souvent les définitions en faisant appel au terme « lorsque », comme par exemple

> On dit que [A] *lorsque* [B].

signifiant qu'on donne par définition à B le nom A. Cette formulation permet d'éviter les classiques « si » ou « si et seulement si » que l'on trouve aussi dans cette situation, mais qui induisent une regrettable confusion entre une définition et un théorème exprimant une implication ou une équivalence entre deux propositions. Ici, « lorsque » est l'équivalent du symbole $\overset{\text{def}}{\equiv}$, et la phrase précédente doit se comprendre comme

$$A \overset{\text{def}}{\equiv} B$$

7. Un mathématicien inconnu de Bologne (Italie) a aussi utilisé à la même période, apparemment de façon indépendante, le symbole = dans ses manuscrits.

Chapitre 1

Fondements des mathématiques

1.1 Paradoxes de l'infini et des ensembles

Notre point de départ sera deux concepts qui peuvent sembler sans rapport mais qui sont pourtant liés : celui d'*ensemble* et celui d'*infini*. La notion d'*ensemble* est importante en mathématiques,

- parce qu'elle apparaît de façon naturelle pour classer différents objets (ensembles de nombres, ensembles de solutions d'une équation, ensembles de points du plan, ensembles de fonctions ...) ;
- parce que de nombreuses notions s'appuient sur elle (comme les structures de *groupe* et d'*espace vectoriel*, qui ont de multiples applications) ;
- parce qu'étudier en toute généralité les propriétés des ensembles, indépendamment de celles de leurs éléments (ce qui est l'objet de la théorie des ensembles), permet de bénéficier de méthodes communes pouvant s'appliquer à différents domaines, que l'on s'intéresse par exemple à l'ensemble $\mathbb{N}$ des entiers naturels, à l'ensemble $\mathbb{R}$ des nombres réels, à l'ensemble des points du plan, à l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, ... ;
- mais aussi parce que, comme nous le verrons, tous les concepts mathématiques usuels (les différents types de nombres, les structures algébriques, les fonctions, les structures géométriques, ...) peuvent même être *représentés* par des ensembles [1], ce qui fait de *la* [2] théorie des ensembles une candidate raisonnable aux fondements formels des autres branches des mathématiques. Je reviendrai sur ce sujet dans la section 1.3.

Les bases de la théorie des ensembles ont été posées à la fin du XIX^{e} siècle par le mathématicien allemand Georg Cantor (1845-1918), en collaboration avec un autre mathématicien allemand, Richard Dedekind (1831-1916). Cantor était motivé en particulier par le concept d'infini, sur lequel s'interrogent les mathématiciens depuis l'époque des philosophes grecs [3], et qui amène de nombreux paradoxes, dont voici quelques exemples classiques :

1. Ce qui ne signifie pas que ces différents objets mathématiques *sont* (intrinsèquement) des ensembles, mais juste qu'ils peuvent être *codés* par des ensembles, de la même façon qu'en informatique, différentes données peuvent être codées par une série de 0 et de 1.

2. Je fais un abus de langage courant en employant le singulier, car il y a plusieurs théories des ensembles, mais celle que je détaillerai dans le volume 2, la *théorie des ensembles de Zermelo-Fraenkel*, est la plus classique.

3. Sans entrer dans le détail de la genèse de la théorie, je précise que les interrogations de Cantor n'étaient pas d'ordre philosophique, mais en rapport avec les mathématiques. Il a été amené à s'interroger sur l'existence de différents types d'infini, et à développer une arithmétique sur les ensembles infinis, à partir de ses travaux sur les séries trigonométriques, qui l'ont conduit à construire des ensembles de nombres réels, par une sorte de *récurrence* pouvant se prolonger au-delà de l'ensemble infini des entiers naturels.

Exemple 1.1.1 (Paradoxes de Zénon)

Les paradoxes de Zénon sont une série de paradoxes attribués au philosophe grec Zénon d'Élée (v. 490 AEC-v. 430 AEC[4]). Il aurait créé une quarantaine de paradoxes, dont seuls une dizaine nous sont parvenus, de façon indirecte, en particulier dans la *Physique* du philosophe grec Aristote (384 AEC-322 AEC), et dans les écrits du philosophe grec Simplicius (fin Ve siècle-milieu VIe siècle), commentateur d'Aristote. Zénon d'Élée était un disciple du philosophe grec Parménide (VIe siècle AEC-Ve siècle AEC), qui rejetait la réalité du pluralisme et du changement. Pour lui, la réalité était une et indivisible, le changement n'existait pas, et les apparences du contraire n'étaient que des illusions. Les différents commentateurs historiques ne sont pas toujours d'accord sur les objectifs poursuivis par Zénon en présentant ses paradoxes, mais l'une des interprétations classiques est qu'il a voulu soutenir Parménide en montrant que le sens commun concernant la réalité de la pluralité et du changement conduisait à des paradoxes, et donc était absurde. Les quatre paradoxes les plus classiques et commentés sont des paradoxes du mouvement ; ce sont

- le paradoxe de la flèche ;
- le paradoxe du stade ;
- le paradoxe d'Achille et de la tortue ;
- le paradoxe de la dichotomie.

Selon les cas, Zénon suppose que les différentes grandeurs physiques (longueur, temps...) sont soit discrètes, soit continues. Des quantités sont *discrètes* quand elles sont formées d'assemblages de plusieurs choses séparées les unes des autres, et qu'un saut est nécessaire pour passer de l'une à l'autre (par exemple les cinq doigts de la main), et *continues* dans le cas contraire, quand il y a toujours un élément entre deux autres, et quand on peut diviser à l'infini. Les deux premiers paradoxes (le paradoxe de la flèche et le paradoxe du stade) s'adressent à ceux qui pensent que l'espace et le temps sont discrets, et les deux suivants (le paradoxe d'Achille et de la tortue, et le paradoxe de la dichotomie) s'adressent à ceux qui pensent que le temps et l'espace sont continus. Et dans tous les cas Zénon propose un raisonnement illustrant, selon lui, l'impossibilité du mouvement :

Le **paradoxe de la flèche** : on imagine une flèche qui se déplace. Si le temps est une succession d'instants, la flèche se trouve à chaque instant à une position donnée, mais pendant cet instant elle n'a pas le temps de bouger et reste immobile. Il en est de même pour chaque instant donc la flèche est toujours immobile, et le mouvement n'existe pas.

Le **paradoxe du stade** : dans un stade, des personnes sont alignées par rangs de trois : une rangée notée $A_1A_2A_3$, une rangée $B_1B_2B_3$, une rangée $C_1C_2C_3$. Dans chaque rangée, chaque personne se situe à la même distance de ses voisins immédiats. La rangée des A est immobile, celle des B se déplace vers la droite, celle des C se déplace vers la gauche, tout le monde à la même vitesse. On obtient la situation suivante entre deux instants :

Avant				
	A_1	A_2	A_3	
B_1	B_2	B_3	$\rightarrow$	
	$\leftarrow$	C_1	C_2	C_3

Après		
A_1	A_2	A_3
B_1	B_2	B_3
C_1	C_2	C_3

Entre ces deux moments, C_1 est passé devant deux B, mais uniquement devant un A, ce qui, pour Zénon, est paradoxal, le temps mis pour passer devant deux B devant être le double de celui mis

4. J'utilise l'abréviation AEC (avant l'ère commune), au lieu du plus classique av. J.-C. (avant Jésus-Christ), pour noter les dates correspondant aux années d'avant notre ère. Outre l'intérêt d'être culturellement neutre, et sans référence à une quelconque mythologie, cette notation est plus simple et plus esthétique.

pour passer devant un A puisque la longueur est double. Une autre interprétation du paradoxe est la suivante : en supposant l'espace et le temps discrets, on suppose que les différents objets A, B, et C sont, sur chaque ligne, séparés par la plus petite unité de longueur d, et qu'ils se déplacent pendant la plus petite unité de temps t. Alors C_1 et B_2 devraient se croiser à un moment qui n'existe pas, puisque cela devrait se produire après un temps $\frac{t}{2}$, ce qui est paradoxal puisque t est la plus petite unité de temps.

Le **paradoxe d'Achille et de la tortue** : le héros grec légendaire Achille dispute une course avec une tortue qui démarre avant lui. À tout moment, pour rattraper la tortue, il doit d'abord courir jusqu'au point où elle se trouve à ce moment-là. Mais le temps qu'il arrive à ce point, la tortue aura avancé jusqu'à un nouveau point. Et ainsi de suite, à chaque fois qu'Achille atteint l'ancienne position de la tortue, celle-ci aura avancé jusqu'à une nouvelle position. La conclusion de Zénon est qu'Achille ne peut jamais rattraper la tortue.

Le **paradoxe de la dichotomie** : un coureur se trouvant à une certaine distance de la ligne d'arrivée doit d'abord parcourir la moitié de la distance qui lui reste, puis à nouveau la moitié de la nouvelle distance qui lui reste (le quart de la distance précédente), et ainsi de suite. Quelle que soit la distance à laquelle se trouve le coureur, il aura toujours la moitié de la distance restante à parcourir, et il ne pourra donc jamais atteindre l'arrivée. Dans une autre version de ce paradoxe, on raisonne à l'envers pour conclure qu'il ne peut même pas démarrer : pour parcourir la distance qui le sépare de l'arrivée, le coureur doit avoir parcouru la moitié de cette distance, mais pour parcourir cette moitié il doit avoir parcouru la moitié de la moitié (le quart de la distance totale), et pour cela il doit avoir parcouru la moitié de ce quart, et ainsi de suite.

Je reprends les différents paradoxes, en donnant quelques résolutions classiques. On notera que celles-ci sont essentiellement mathématiques : nous n'aborderons pas le problème de l'adéquation du modèle mathématique à la réalité physique (par exemple, le fait de diviser indéfiniment une longueur a-t-il vraiment un sens ?), ni l'approche purement philosophique (certains peuvent penser que la solution mathématique ne répond pas au problème *philosophique* posé par Zénon …).

Le paradoxe de la flèche : le mouvement d'un objet à un instant t n'est pas une caractéristique de l'objet à cet instant. Un objet est en mouvement s'il occupe des positions différentes à des instants différents. Le mouvement et la vitesse d'un objet sont définis à partir des différentes positions qu'il occupe, donc il n'y a pas vraiment de paradoxe.

Le paradoxe du stade : dans la première interprétation, il y a une simple confusion entre vitesse et vitesse relative. Si d est la distance entre deux personnes, et si la vitesse de C (ou de B), par rapport à A qui est immobile, est v, alors la vitesse de C par rapport à B est $2v$, et le temps mis pour parcourir la distance $2d$ à la vitesse $2v$ est bien le même que celui mis pour parcourir la distance d à la vitesse v. La deuxième interprétation est plus subtile. Dans le cas d'un espace et d'un temps discrets, la question de savoir où se croisent B_2 et C_1 n'a pas de sens. B_2 passe d'une position à la suivante, de même pour C_1, et il n'y a pas vraiment de croisement (qui supposerait un chemin continu entre deux points, et pas un chemin discret).

Pour les deux paradoxes suivants, les longueurs et les temps sont continus, ce qui peut se modéliser mathématiquement par l'analyse réelle moderne, basée sur l'ensemble des nombres réels $\mathbb{R}$.

Ces pages ne sont pas incluses dans l'aperçu.

Le volume 1 des
Éléments de mathématiques pour le XXI^e siècle
(ISBN : 978-2-9569666-0-9) est disponible
en version papier et numérique.
Détails sur le site *Paysages Mathématiques* :
https://www.paysmaths.net/boutique

- Le deuxième théorème d'incomplétude de Gödel, toujours de manière informelle, stipule qu'aucune théorie suffisamment élaborée (vérifiant des hypothèses semblables à celles du théorème précédent) ne peut démontrer sa propre cohérence.

Les théorèmes d'incomplétude de Gödel ont ainsi montré que réaliser l'ensemble des objectifs de Hilbert était impossible. Néanmoins, des objectifs plus modestes ont pu être atteints, et la logique mathématique actuelle, qui s'appuie essentiellement sur les idées logicistes et surtout formalistes, peut être considérée comme la continuation naturelle du programme original de Hilbert. Ainsi, même si on ne peut pas formaliser *toutes* les mathématiques *possibles*, on peut le faire de façon à peu près satisfaisante pour l'ensemble des mathématiques *actuelles*. Tous les objets associés aux notions mathématiques usuelles (les différents types de nombres, les structures algébriques, les fonctions, les différents concepts géométriques, ...) peuvent être représentés par des ensembles ; c'est pourquoi les mathématiciens se sont employés à formaliser correctement la théorie naïve des ensembles de Cantor, en développant différentes théories.

Celle qui est la plus usuelle pour fonder les mathématiques est la **théorie des ensembles de Zermelo-Fraenkel** (je la détaillerai dans le volume 2). Élaborée par le mathématicien allemand Ernst Zermelo (1871-1953) en 1908 [22], elle a été complétée par le mathématicien allemand Abraham Fraenkel (1891-1965), le mathématicien et logicien norvégien Thoralf Skolem (1887-1963), et le mathématicien et physicien américano-hongrois John von Neumann (1903-1957). On la note souvent **ZF** (pour Zermelo-Fraenkel), et on inclut généralement un axiome plus controversé, l'axiome du choix, pour aboutir à la théorie ZF avec axiome du choix, ou **ZFC**. Cet axiome est controversé dans la mesure où il permet de définir un ensemble sans donner de construction effective de celui-ci, ce qui pose des problèmes aux mathématiciens proches du constructivisme ; par ailleurs, certaines de ses conséquences sont contre-intuitives, et peuvent sembler paradoxales. La théorie ZFC se formule dans le cadre formel de ce qu'on appelle la **logique des prédicats** (ou calcul des prédicats), ou **logique du premier ordre** (voir le chapitre 4). Les différentes façons de construire un ensemble sont données par les axiomes de la théorie, de telle sorte que les propriétés coïncident avec celles de la notion intuitive d'ensemble, mais que les paradoxes vus précédemment soient impossibles.

Comme fondements des mathématiques, d'autres théories (autres que ZFC), ou même d'autres systèmes formels (autres que la logique des prédicats), sont possibles. En particulier [23] :

1. Il existe des variantes de ZFC s'appuyant sur la logique intuitionniste, comme la théorie **IZF** (*Intuitionistic Zermelo–Fraenkel*) du mathématicien britannique John Myhill (1923-1987), ou la théorie **CZF** (*Constructive Zermelo-Fraenkel*) du mathématicien et logicien britannique Peter Aczel (1941-).
2. Un groupe de mathématiciens francophones, formé en 1935 sous le pseudonyme collectif de Nicolas Bourbaki, a commencé à publier à partir de 1939 un traité de mathématiques en plusieurs volumes (le projet est, à ce jour, inachevé), les ***Éléments de mathématique*** [24]. Cette œuvre se veut un exposé des mathématiques de l'époque, rédigé de façon rigoureuse. Le fondement choisi est une théorie des ensembles (correspondant à peu près à la théorie ZFC), exprimée dans un système formel très inspiré de Hilbert, proche (mais différent) de la logique des prédicats actuelle. Le groupe Bourbaki a eu une influence notable dans la communauté mathématique en général (introduction ou vulgarisation de plusieurs notations, termes, et notions), et aussi dans la recherche et l'enseignement des mathématiques en France. Mais le traité de Bourbaki fait aussi l'objet de plusieurs critiques, en particulier en ce qui concerne son approche de la logique et le système formel choisi comme fondement des mathématiques, qui était déjà obsolète lors de la parution (les avancées de la logique formelle, depuis Gödel, ne sont pas prises en compte) [25].

22. Ernst ZERMELO. « Untersuchungen über die Grundlagen der Mengenlehre *[Études sur les fondements de la théorie des ensembles]* ». Dans : *Mathematische Annalen* 65 (1908), p. 261-281.

23. Les deux premiers exemples sont donnés à titre indicatif, et je n'y reviendrai pas. Les trois suivants seront abordés (avec plus ou moins de détails) dans les prochains volumes.

24. Le singulier est volontaire, pour exprimer l'idée d'unité de la discipline.

25. Voir par exemple la critique du mathématicien Patrick Dehornoy, ou celle, féroce, du mathématicien Adrian Richard David Mathias :
- Patrick DEHORNOY. *La théorie des ensembles*. Calvage & Mounet, 2017, p. 606.

3. La **théorie des classes**, proposée dans les années 1920 par von Neumann, qui est dérivée de la théorie ZFC, et contient deux types d'objets fondamentaux, les ensembles et les classes. Cette théorie a ensuite été revue et simplifiée par le mathématicien suisse Paul Bernays (1888-1977), puis par Kurt Gödel au cours des années 1930 ; elle est aussi connue sous le nom de **théorie des ensembles de von Neumann-Bernays-Gödel**, ou **NBG** (voir le volume 3). Le vocabulaire des classes est aussi fréquemment utilisé dans la théorie ZFC, même si celle-ci ne permet pas de formaliser complètement cette notion (les classes y sont définies dans le métalangage comme étant des collections d'éléments vérifiant une propriété exprimée dans le langage de la théorie). NBG et ZFC sont très proches : on dit que NBG est une extension conservative de ZFC, c'est-à-dire que les énoncés qui ne font pas intervenir les classes sont équivalents dans les deux théories (un théorème de NBG est un théorème de ZFC, et réciproquement). Les nouveaux théorèmes que peut démontrer NBG sont les théorèmes utilisant les classes. Du fait qu'elle est une extension de ZFC, on pourrait penser que la théorie NBG aurait été la théorie choisie pour les ensembles, mais c'est ZFC la théorie usuelle de référence, peut-être en raison de deux avantages (outre celui de l'antériorité) :
   - La plupart des mathématiques usuelles ne nécessitent pas l'utilisation des classes, et ZFC est plus simple que NBG, puisqu'elle n'a qu'un objet d'étude (les ensembles), alors que NBG en a deux (les ensembles et les classes).
   - Les résultats théoriques de la théorie des modèles (voir le volume 3) sont techniquement plus faciles à établir avec ZFC, car ses modèles ont une structure plus simple que ceux de NBG.
4. La théorie **ETCS** (pour *Elementary Theory of the Category of Sets* [Théorie élémentaire de la catégorie des ensembles]), élaborée à la fin des années 1960 par le mathématicien William Lawvere (1937-). Elle s'appuie sur la **théorie des catégories**, élaborée dans les années 1940 par le mathématicien américain d'origine polonaise Samuel Eilenberg (1913-1998) et le mathématicien américain Saunders Mac Lane (1909-2005), et popularisée dans les années 1960 en France par le mathématicien français [26] Alexandre Grothendieck (1928-2014). On trouvera dans le volume 3 une introduction à la théorie des catégories, et à la théorie ETCS.
5. La **théorie des types** est une classe de systèmes formels ayant des applications en mathématiques, logique et informatique. Le principe des *types* a été élaboré par Bertrand Russell et Alfred North Whitehead, dans leur ouvrage *Principia Mathematica*, qui, bien que complexe et incomplet, est la première tentative de fondement des mathématiques. Elle reprend et complète le projet de Frege. L'idée de base de la théorie est d'introduire une hiérarchie entre les objets (contrairement à la logique des prédicats où il n'existe qu'un seul type d'objets). Ceux d'ordre 0 sont les individus. Les relations et fonctions entre individus sont les objets d'ordre 1. De manière générale, les objets d'ordre $n+1$ sont les fonctions et relations dont les variables sont les objets d'ordre inférieur ou égal à n. Je présenterai dans les prochains volumes deux théories particulières qui s'appuient sur le principe des types (mais qui sont néanmoins très différentes) :
   - La théorie ***New Foundations with Urelements*** [Nouveaux fondements avec uréléments], ou **NFU**, proposée par le mathématicien américain Ronald Jensen (1936-) en 1969 et popularisée par le mathématicien Randall Holmes, qui est une variante de la théorie ***New Foundations*** [Nouveaux Fondements], ou **NF**, élaborée en 1937 par le philosophe et logicien américain Willard Van Orman Quine (1908-2000). Ces théories s'inspirent de la théorie des types, mais peuvent s'exprimer dans le système formel de la logique des prédicats.
   - La **théorie intuitionniste des types**, du logicien, philosophe et mathématicien suédois Per Martin-Löf (1942-). Cette théorie est à la base de la **théorie homotopique des types**, théorie très récente puisqu'elle

- Adrian Richard David MATHIAS. « The ignorance of Bourbaki ». Dans : *The Mathematical Intelligencer* 14 (3 1992). URL : `https://www.dpmms.cam.ac.uk/~ardm/bourbaki.pdf`.
- Adrian Richard David MATHIAS. *Hilbert, Bourbaki and the scorning of logic*. 2012. URL : `https://www.dpmms.cam.ac.uk/~ardm/lbmkemily5.pdf`.

26. Né en Allemagne, arrivé en France avec ses parents en 1933, il reste apatride (par choix idéologique) jusqu'en 1972 où il est naturalisé français.

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 2

Logique des propositions

2.1 Introduction

C'est le philosophe grec Aristote (384 AEC-322 AEC [1]) qui est en général considéré comme le fondateur de la logique ; c'est en particulier à lui que l'on doit le concept de *syllogisme* (voir la section 5.17). Parmi les auteurs ayant considérablement influencé l'étude de cette logique dite *traditionnelle*, ou *aristotélicienne*, nous pouvons aussi citer le philosophe Chrysippe de Soles (v. 280 AEC-v. 206 AEC), l'un des fondateurs du stoïcisme, le philosophe et théologien français Pierre Abélard (1079-1142), le théologien britannique Guillaume d'Ockham (ou d'Occam) (v. 1285-1347) [2], le philosophe et mathématicien Gottfried Wilhelm Leibniz (1646-1716), et le mathématicien, logicien, philosophe et théologien autrichien Bernard Bolzano (1781-1848).

La logique des propositions (ou calcul des propositions), qui marque au XIX^e^ siècle le début de la formalisation moderne de la logique traditionnelle, traite des propositions, c'est-à-dire des expressions pouvant être soit vraies, soit fausses. Issue en grande partie des travaux des logiciens et mathématiciens britanniques George Boole (1815-1864) et Auguste De Morgan (1806-1871), elle peut être considérée comme une première étape dans la construction de la logique mathématique actuelle, qui sera suivie par l'invention de la logique des prédicats (voir le chapitre 4). Parmi les auteurs ayant contribué au développement de la logique des propositions, citons le mathématicien et logicien britannique John Venn (1834-1923), le philosophe américain Charles Peirce (1839-1914), le mathématicien américain Emil Leon Post (1897-1954), et le philosophe britannique d'origine autrichienne [3] Ludwig Wittgenstein (1889-1951). [4]

La logique des propositions fait intervenir plusieurs éléments :

- Des **propositions atomiques**, ou **variables propositionnelles**, qui peuvent prendre deux *valeurs de vérité* : *vrai*, ou *faux* (on note aussi souvent V pour *vrai* et F pour *faux* ; ou encore 1 pour *vrai*, 0 pour *faux*).
- Des **connecteurs** (*et*, *ou*, *implication*,...), permettant de connecter les propositions atomiques. On utilise aussi le terme **opérateur** à la place de *connecteur*, car le fait de connecter deux propositions atomiques revient à effectuer une opération. Par exemple, dans le calcul booléen, qui est une façon d'« algébriser » la logique (voir la section 3.1), le connecteur *et* correspond à une multiplication, et le connecteur *ou* correspond à une addition : à deux éléments a et b, qui représentent chacun une proposition atomique (et prenant la valeur 1 pour *vrai* et 0 pour *faux*), on associe un troisième élément que l'on note soit $a \times b$ (il représente alors la formule « *a et b* »), soit $a + b$ (il représente alors la formule « *a ou b* »), et qui prend aussi les valeurs 1 ou 0 (selon les valeurs de a et de b).

1. Voir la note 4, p. 8.
2. Guillaume d'Ockham a donné son nom au *rasoir d'Ockham* (même si ce principe était connu avant lui), l'un des principes heuristiques fondamentaux en sciences qui, en termes modernes, peut se formuler ainsi : les hypothèses suffisantes les plus simples sont les plus vraisemblables.
3. Né en Autriche en 1889, il acquiert la nationalité britannique en 1939.
4. Source des deux derniers paragraphes : Patrick J. HURLEY. *A Concise Introduction to Logic*. 12^e^ éd. Cengage Learning, 2015.

- Des **propositions**, ou **formules propositionnelles** (ou juste **formules**), obtenues à l'aide des propositions atomiques et des connecteurs. Les propositions prennent aussi les deux valeurs de vérité *vrai* ou *faux*, selon les valeurs de vérité des propositions atomiques qui les constituent. On utilise souvent les lettres P, Q, R pour désigner des propositions (le mathématicien et logicien britannique Bertrand Russell (1872-1970) a popularisé cet usage en 1903 dans *The Principles of Mathematics*).

Exemple 2.1.1 (Exemples et contre-exemples de propositions atomiques [5])
Exemples de propositions atomiques vraies :

- $1 + 1 = 2$
- 6 est un nombre pair.
- La France est un pays.

Exemples de propositions atomiques fausses :

- $2 + 2 = 3$
- 5 est un nombre pair.
- La France se situe en Amérique.

Exemples de propositions atomiques dont la valeur de vérité dépend du contexte :

- $x + y = z$
- x est un nombre pair.
- Il pleut.

Exemples d'expressions qui ne sont pas des propositions atomiques :

- 3
- $1 + 1$
- Ici
- Viens ici !
- Quelle heure est-il ?

Pour les cinq derniers exemples, il n'y a pas de « valeur de vérité » naturelle affectée à ces expressions.

Remarque 2.1.2 : On peut remarquer que, selon le contexte, une proposition peut être considérée comme automatiquement vraie : par exemple, dans un texte mathématique

- $1 + 1 = 2$ peut s'interpréter comme : « $1 + 1 = 2$ » est *vrai*.
- P, donc Q peut s'interpréter comme : la proposition P est vraie ; on en déduit que la proposition Q est vraie.

Exemple 2.1.3 (Paradoxe du menteur)
Il existe de nombreuses variantes de ce paradoxe, par exemple :

1. La phrase suivante elle-elle vraie ? :

   « Cette phrase est fausse. »

5. Ce qui suit doit se comprendre en interprétant chacune des expressions de façon « naturelle ».

Si elle est vraie, alors elle est fausse, si elle est fausse, alors elle est vraie. Il y a un paradoxe. Il existe d'autres expressions du même genre :

- « La phrase suivante est fausse. La phrase précédente est vraie. »
- « Je mens. »

2. Le paradoxe du menteur est attribué au philosophe grec Eubulide (IV^e siècle AEC [6]), qui passe pour être l'inventeur de plusieurs paradoxes, dont celui-ci :

   « Celui qui dit qu'il ment est-il un menteur ? »

3. Une autre variante classique fait dire au Crétois Épiménide (vers le VI^e siècle AEC), dans un poème :

   « Tous les Crétois sont des menteurs. »

   Mais cette version n'est pas réellement paradoxale : la négation de « Tous les Crétois sont des menteurs » est « Il existe au moins un Crétois qui n'est pas un menteur ». Le terme menteur lui-même est ambigu :

   - On peut le comprendre comme *dire parfois des mensonges*. Dans ce cas, la négation de « Tous les Crétois sont des menteurs » est « Il existe au moins un Crétois qui dit toujours la vérité ». La phrase « Tous les Crétois sont des menteurs » peut alors être vraie ou fausse, il n'y a pas de paradoxe : si elle est vraie, tous les Crétois disent parfois des mensonges (ce qui est le cas du Crétois Épiménide, il dit parfois des mensonges, mais pas dans cette phrase). Si elle est fausse, il existe au moins un Crétois qui dit toujours la vérité (mais ce n'est pas Épiménide, puisque la phrase qu'il vient de prononcer est fausse).
   - On peut comprendre le terme *menteur* comme *dire toujours des mensonges*. Dans ce cas, la négation de « Tous les Crétois sont des menteurs » est « Il existe au moins un Crétois qui dit parfois la vérité ». Si la phrase « Tous les Crétois sont des menteurs » est vraie, alors, puisque celui qui la prononce est Crétois, cette phrase devrait être fausse. Si la phrase est fausse, il existe au moins un Crétois qui dit parfois la vérité, et on ne peut rien en déduire d'autre. Il n'y a pas de paradoxe (on peut juste dire que la phrase est fausse).

Dans le cadre de la logique des propositions, puisqu'il n'est pas possible de définir une valeur de vérité naturelle pour une expression de la forme « Cette phrase est fausse », ce n'est pas une proposition atomique. On pourrait dire, d'une certaine manière, que se demander si l'expression « Cette phrase est fausse » est vraie ou fausse, n'a pas plus de sens que de se demander si l'expression « Quelle heure est-il ? » est vraie ou fausse.

2.2 Connecteurs

Les connecteurs agissent sur une ou plusieurs propositions, et permettent d'en obtenir une autre dont la valeur de vérité dépend des valeurs de vérité des propositions qui la constituent. Il existe cinq connecteurs classiques :

- la négation ;
- la conjonction (*et*) ;
- la disjonction (*ou*) ;
- l'implication ;
- l'équivalence.

6. Voir la note 4, p. 8.

Négation

Définition 2.2.1 (Négation)
La *négation* de P, notée en général $\neg P$ (lire : *non P*), est un connecteur *unaire*, c'est-à-dire qu'il n'a qu'un argument (il n'agit que sur une proposition). $\neg P$ prend la valeur de vérité contraire de celle de P :

$$\neg P \text{ est } \begin{cases} \textit{vrai} & \text{si } P \text{ est } \textit{faux} \\ \textit{faux} & \text{si } P \text{ est } \textit{vrai} \end{cases}$$

Ce qui peut se traduire par le tableau suivant, dit *table de vérité* :

P	$\neg P$
F	V
V	F

TABLE 2.1 – Table de vérité de la négation.

Remarque 2.2.2 (Origine des notations) : Le symbole ¬ a été introduit en 1930 par le mathématicien et logicien néerlandais Arend Heyting (1898-1980) dans son article « Die formalen Regeln der intuitionistischen Logik *[Les règles formelles de la logique intuitionniste]* » [7].

Remarque 2.2.3 (Notations) : On trouve aussi pour la négation de P les notations $\bar{P}$ et $\sim P$.

Remarque 2.2.4 (Remarque historique [8]) : C'est le philosophe britannique d'origine autrichienne [9] Ludwig Wittgenstein (1889-1951) qui est le plus souvent crédité de l'invention du principe des *tables de vérité* (dans *Tractatus logico-philosophicus* en 1921). Néanmoins, ce principe apparaît aussi en 1920 dans la thèse du mathématicien américain Emil Leon Post (1897-1954) [10], repris dans un article en 1921 [11]. Ces deux auteurs utilisent l'expression « table de vérité » (*wahrheitstafel* pour Wittgenstein, *truth table* pour Post). Par ailleurs, on trouve des tables de vérité dans des notes ajoutées par Wittgenstein sur un manuscrit de Russell (les deux hommes ont travaillé ensemble), datant de 1912 environ. Des notes manuscrites du poète, dramaturge et critique littéraire britannique d'origine américaine [12] T.S. Eliot (1888-1965), prises lors d'une conférence de Russell de 1914, font aussi référence aux tables de vérité. On ne sait pas si Russell et Wittgenstein ont élaboré cet outil ensemble, ou si l'un des deux l'a exposé à l'autre. Enfin, on trouve des tables de vérité dans des manuscrits du mathématicien, logicien, et philosophe américain Charles Peirce (1839-1914), en particulier un daté de 1902. Ce qui fait dire à l'historien des mathématiques Irving Anellis :

> « La découverte par Zellweger du manuscrit de Peirce de 1902 nous permet de déclarer sans équivoque, avec certitude, que *la première table de vérité attestée, vérifiable, convaincante, attribuable et complète est attachée à Peirce*, plutôt qu'aux notes de Wittgenstein de 1912 ou celles d'Eliot sur les conférences à Harvard de Russell en 1914. » [13]

7. Arend HEYTING. « Die formalen Regeln der intuitionistischen Logik *[Les règles formelles de la logique intuitionniste]* ». Dans : *Sitzungsberichte der preußischen Akademie der Wissenschaften* (1930), p. 43.
8. Source supplémentaire : Irving ANELLIS. « The Genesis of the Truth-Table Device ». Dans : *Russell: the journal of Bertrand Russell Studies* 24 (2004), p. 55-70.
9. Né en Autriche en 1889, il acquiert la nationalité britannique en 1939.
10. Emil Leon POST. « Introduction to a General Theory of Elementary Propositions ». Thèse. Columbia University, 1920.
11. Emil Leon POST. « Introduction to a General Theory of Elementary Propositions ». Dans : *American Journal of Mathematics* 43 (1921), p. 163-185.
12. Né aux États-Unis, il est naturalisé britannique en 1927.
13. ANELLIS. Ibid, p.66.

Remarque 2.2.5 : Si on utilise les valeurs 0 et 1 à la place respectivement de F et V, la table de vérité s'écrit :

P	$\neg P$
0	1
1	0

On peut alors remarquer que la valeur de la négation de P correspond à l'écart entre la valeur de P et 1. En notant $v(P)$ la valeur de P :

$$v(\neg P) = 1 - v(P)$$

Exemple 2.2.6
Si p représente la proposition atomique « Il pleut à Paris », alors $\neg p$ représente la proposition « Il ne pleut pas à Paris ». On notera que la logique des propositions ne dit pas si ces propositions sont vraies ou fausses, mais permet de déterminer leur valeur de vérité les unes par rapport aux autres. Par exemple, si on sait que « Il pleut à Paris » est *vrai*, alors on en déduit que « Il ne pleut pas à Paris » est *faux*.

Exemple 2.2.7
1. Sachant que « 5 est un nombre pair » est *faux* (dans l'interprétation naturelle de cette phrase), on en déduit que ¬ « 5 est un nombre pair » est une proposition vraie (de la forme $\neg P$, avec P *faux*), que l'on peut traduire par : « 5 n'est pas un nombre pair ».
2. $\neg(1 + 1 = 2)$, que l'on écrit aussi $1 + 1 \neq 2$, est une proposition fausse (de la forme $\neg P$, avec P *vrai*).

Exemple 2.2.8
Comme dans l'exemple précédent, la négation de certaines relations mathématiques se formule en général avec un raccourci faisant intervenir un nouveau symbole. Par exemple

$$\begin{aligned} \neg(a = b) &\quad \text{s'écrit plutôt} \quad a \neq b \\ \neg(x \in E) &\quad \text{s'écrit plutôt} \quad x \notin E \\ \neg(A \subseteq B) &\quad \text{s'écrit plutôt} \quad A \not\subseteq B \end{aligned}$$

Conjonction

Définition 2.2.9 (Conjonction)
La *conjonction* (*et*), notée en général $\wedge$, est un connecteur binaire, c'est-à-dire qu'il a deux arguments. $P \wedge Q$ ne prend la valeur *vrai* que si P et Q prennent simultanément la valeur *vrai*, autrement dit si P *et* Q sont des propositions vraies (et donc prend la valeur *faux* lorsqu'au moins l'une des deux propositions prend la valeur *faux*) :

$$P \wedge Q \text{ est } \begin{cases} \textit{vrai} & \text{si } P \text{ est } \textit{vrai} \text{ et } Q \text{ est } \textit{vrai} \\ \textit{faux} & \text{sinon} \end{cases}$$

Ce qui peut se traduire par la table de vérité suivante :

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

TABLE 2.2 – Table de vérité de la conjonction.

Remarque 2.2.10 (Origine des notations) : Le symbole $\wedge$ a été introduit en 1930 par le mathématicien et logicien néerlandais Arend Heyting (1898-1980) dans son article « Die formalen Regeln der intuitionistischen Logik *[Les règles formelles de la logique intuitionniste]* » [14].

Remarque 2.2.11 (Notations) : $\wedge$ est le symbole classique pour représenter la conjonction, mais dans un texte mathématique (hors logique pure) il est fréquent de noter directement « et ». Je pourrai utiliser indifféremment les deux, sachant qu'il n'y a de toute façon pas d'ambiguïté : dans une formule, « et » représente le symbole de conjonction $\wedge$, et pas le terme « et » du métalangage. De façon générale, j'emploierai le plus souvent $\wedge$ dans un cadre de logique pure (pour ce volume essentiellement), mais « et » dans les autres cas.

Remarque 2.2.12 : La conjonction est *commutative*, c'est-à-dire que la valeur de vérité de $P \wedge Q$ ne change pas si on permute P avec Q.

Remarque 2.2.13 : Si on utilise les valeurs 0 et 1 à la place respectivement de F et V, la table de vérité s'écrit :

P	Q	$P \wedge Q$ (P et Q)
0	0	0
0	1	0
1	0	0
1	1	1

On peut alors remarquer que la valeur de $P \wedge Q$ est le produit des valeurs de P et de Q (pour la multiplication usuelle de deux nombres entiers). On peut également remarquer que cette valeur est aussi la plus petite des valeurs de P et de Q, que l'on note $\min(v(P), v(Q))$:

$$\begin{aligned} v(P \wedge Q) &= \min(v(P), v(Q)) \\ &= v(P) \times v(Q) \end{aligned}$$

Exemple 2.2.14
On considère les propositions atomiques p et q suivantes :

- p : « Il pleut à Paris. »
- q : « Il neige à Londres. »

La logique des propositions ne nous dit pas si p et q sont des propositions vraies ou fausses, mais si

14. Arend HEYTING. « Die formalen Regeln der intuitionistischen Logik *[Les règles formelles de la logique intuitionniste]* ». Dans : *Sitzungsberichte der preußischen Akademie der Wissenschaften* (1930).

Ces pages ne sont pas incluses dans l’aperçu.

2.4 Syntaxe de la logique des propositions

Revenons à la syntaxe de la logique des propositions. Les symboles servant à construire des formules sont

- des symboles pour les propositions atomiques, que l'on prend dans un ensemble infini dénombrable, c'est-à-dire dont les éléments peuvent être indexés par l'ensemble des entiers naturels ; on pourra par exemple les désigner par p_1, p_2, p_3, … ;
- les symboles de connecteurs :
$$\neg \quad \wedge \quad \vee \quad \Longrightarrow \quad \Longleftrightarrow$$
- des symboles de ponctuation, comme des parenthèses, pour lever les ambiguïtés et préciser l'ordre des opérations.

Remarque 2.4.1 : Dans la théorie formelle, les symboles peuvent avoir n'importe quelle forme, et être représentés par n'importe quel « objet ». Par exemple, dans certaines variantes de la logique des propositions, ces symboles sont codés par des nombres entiers. Mais quelle que soit l'option choisie, il y a une condition qui doit être toujours vérifiée : afin de pouvoir reconnaître de façon non ambiguë une succession de symboles, ils doivent être non seulement distincts les uns des autres (par exemple si $\wedge$ est le symbole pour la conjonction, il ne doit pas faire partie des symboles pour les propositions atomiques), mais aussi aucun symbole ne peut être une suite finie d'autres symboles. Par exemple, si $*$ est un symbole, et si $**$ est un autre symbole de la théorie alors l'expression « $**$ » est ambiguë, car elle peut représenter soit un unique symbole, soit la succession de deux symboles « $*$ ».

Définition 2.4.2 (Proposition, formule propositionnelle)
L'ensemble des *propositions*, ou *formules propositionnelles* (ou juste *formules*), est le plus petit ensemble tel que :

- Toute proposition atomique est une formule.
- Si P est une formule, alors
$$\neg P$$
est une formule.
- Si P et Q sont des formules, alors
$$(P \wedge Q) \quad (P \vee Q) \quad (P \Longrightarrow Q) \quad (P \Longleftrightarrow Q)$$
sont des formules.

Remarque 2.4.3 : Par convention, pour éviter de surcharger les propositions avec des parenthèses, on ne note en général pas les parenthèses extérieures d'une formule. Par exemple
$$(P \wedge Q) \Longrightarrow (P \vee Q) \quad \text{signifie} \quad ((P \wedge Q) \Longrightarrow (P \vee Q))$$
De plus, le connecteur $\neg$ est prioritaire sur les connecteurs $\wedge$ et $\vee$, qui sont eux-mêmes prioritaires sur les connecteurs $\Longrightarrow$ et $\Longleftrightarrow$. Par exemple
$$\neg P \wedge Q \Longrightarrow R \vee S \quad \text{signifie} \quad (\neg P \wedge Q) \Longrightarrow (R \vee S)$$
Il existe d'autres conventions classiques, mais que je n'emploierai pas : dans l'une d'elles, la conjonction est prioritaire sur la disjonction. Par exemple
$$P \wedge Q \vee R \quad \text{signifie alors} \quad (P \wedge Q) \vee R$$

Remarque 2.4.4 : Dans ce qui précède, les lettres P et Q ne sont pas des symboles appartenant à la syntaxe de la logique des propositions (comme les symboles de propositions atomiques $p_1, p_2, \dots$, ou les symboles de connecteurs $\neg$, $\Longrightarrow$, $\dots$), mais sont des symboles du métalangage (représentant des formules). Par exemple

$$p_1 \Longrightarrow p_2$$

est une formule de la logique des propositions, formée à partir des symboles « p_1 », « p_2 », et « $\Longrightarrow$ », mais si je désigne cette formule par la lettre P, en écrivant par exemple

$$P :\equiv p_1 \Longrightarrow p_2$$

le symbole P ne fait pas partie des symboles de la syntaxe de la logique des propositions, mais est un symbole du métalangage.

Remarque 2.4.5 : Cette définition permet de caractériser les formules qui ont un sens dans la logique des propositions (par opposition à une succession de symboles quelconques, par exemple « $p_1 \wedge$ »), qu'on appelle aussi des *formules bien formées*. Certains auteurs font une distinction entre *formule* (qui peut être une suite de symboles quelconques) et *formule bien formée*. Je ne ferai pas cette distinction, et dans la suite, toute formule sera considérée comme étant *bien formée*.

Exemple 2.4.6
À partir des propositions atomiques p_1 et p_2 uniquement, on peut construire les formules suivantes :

$$p_1 \qquad p_2$$

d'après la première règle. Donc par application de la deuxième règle on obtient les deux formules

$$\neg p_1 \qquad \neg p_2$$

et par application des règles du troisième type on obtient les formules

$$p_1 \wedge p_2 \quad p_2 \wedge p_1 \quad p_1 \vee p_2 \quad p_2 \vee p_1 \quad p_1 \Longrightarrow p_2 \quad p_2 \Longrightarrow p_1 \quad p_1 \Longleftrightarrow p_2 \quad p_2 \Longleftrightarrow p_1$$

On peut ensuite construire de nouvelles formules à partir des propositions déjà obtenues, par exemple

$$\neg(p_1 \wedge p_2) \qquad (p_1 \wedge p_2) \Longrightarrow p_1 \qquad (p_2 \Longrightarrow p_1) \vee (p_2 \vee p_1)$$

et ainsi de suite. On notera qu'on ne fait ici que construire des formules qui ont un sens en logique des propositions, mais pour l'instant il n'y a aucune valeur de vérité associée.

Exemple 2.4.7
Voici quelques autres exemples de formules, si p_1 et p_2 sont des propositions atomiques, et si P, Q, R, sont des formules :

$$(p_1 \wedge p_2) \vee P \qquad P \Longrightarrow (Q \Longrightarrow R) \qquad (\neg(P \wedge R) \vee Q) \wedge R$$

Par contre, les expressions suivantes ne sont pas des formules :

$$\neg \qquad P \wedge \qquad PQR \qquad \vee p_1$$

Ces pages ne sont pas incluses dans l’aperçu.

Définition 2.5.1 (Valuation)
On appelle *valuation* toute fonction v de l'ensemble des propositions atomiques dans $\{0, 1\}$, que l'on prolonge ensuite à l'ensemble des formules, de la façon suivante :

$$\begin{aligned} v(\neg P) &= 1 - v(P) \\ v(P \wedge Q) &= \min(v(P), v(Q)) \\ v(P \vee Q) &= \max(v(P), v(Q)) \\ v(P \implies Q) &= \begin{cases} 0 & \text{si } v(P) = 1 \text{ et } v(Q) = 0 \\ 1 & \text{sinon} \end{cases} \\ v(P \iff Q) &= \begin{cases} 0 & \text{si } v(P) \neq v(Q) \\ 1 & \text{si } v(P) = v(Q) \end{cases} \end{aligned}$$

Remarque 2.5.2 (Vocabulaire) : À la place de *valuation*, on trouve aussi les termes *évaluation*, ou *assignation*, ou *distribution des valeurs de vérité*, ou *interprétation*.

Remarque 2.5.3 : On retrouve les définitions déjà données dans la section 2.2. L'utilisation des valeurs de vérité 0 et 1 permet d'exprimer facilement le comportement des différents connecteurs, mais il serait équivalent de définir la valuation comme une fonction à valeurs dans $\{\mathrm{F}, \mathrm{V}\}$, et de donner les différentes définitions à partir de tous les cas possibles (par exemple à l'aide des tables de vérité). Je pourrai d'ailleurs, pour désigner les deux valeurs de vérité possibles, employer indifféremment 0/1, F/V, ou *faux/vrai*.

Remarque 2.5.4 : Du fait qu'une valuation ne peut prendre que deux valeurs possibles, il est aussi équivalent de définir les différents cas de la façon suivante :

$$\begin{aligned} v(\neg P) &= 1 \text{ si et seulement si } v(P) = 0 \\ v(P \wedge Q) &= 1 \text{ si et seulement si } v(P) = v(Q) = 1 \\ v(P \vee Q) &= 0 \text{ si et seulement si } v(P) = v(Q) = 0 \\ v(P \implies Q) &= 0 \text{ si et seulement si } v(P) = 1 \text{ et } v(Q) = 0 \\ v(P \iff Q) &= 1 \text{ si et seulement si } v(P) = v(Q) \end{aligned}$$

ce qui est la traduction de

- $\neg P$ est *vrai* si et seulement si P est *faux*.
- $P \wedge Q$ est *vrai* si et seulement si P est *vrai* et Q est *vrai*.
- $P \vee Q$ est *faux* si et seulement si P est *faux* et Q est *faux*.
- $P \implies Q$ est *faux* si et seulement si P est *vrai* et Q est *faux*.
- $P \iff Q$ est *vrai* si et seulement si P et Q ont la même valeur de vérité (ces propositions sont soit vraies toutes les deux, soit fausses tous les deux).

Si on souhaite harmoniser cette définition en ne caractérisant que les valeurs 1, on peut aussi modifier la définition des valeurs de vérité associées à « $\vee$ » et « $\implies$ » ainsi :

$$\begin{aligned} v(P \vee Q) &= 1 \text{ si et seulement si } v(P) = 1 \text{ ou } v(Q) = 1 \\ v(P \implies Q) &= 1 \text{ si et seulement si } v(P) = 0 \text{ ou } v(Q) = 1 \end{aligned}$$

ce qui est la traduction de

Ces pages ne sont pas incluses dans l’aperçu.

Exemple 2.6.22 (Double négation)
Vérifions la propriété de double négation, ou involutivité du connecteur ¬ : la négation de la négation équivaut à la formule de départ. Vérifions donc

$$\neg(\neg P) \equiv P$$

C'est immédiat, puisque la négation inverse les valeurs de vérité, ce qui peut se voir sur la table de vérité suivante :

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

Exemple 2.6.23 (Lois d'absorption)
Vérifions les lois dites d'absorption :

$$P \wedge (P \vee Q) \equiv P$$
$$P \vee (P \wedge Q) \equiv P$$

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

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

Métathéorème 2.6.24 (Conservation de l'équivalence par les connecteurs)
Les connecteurs conservent la relation d'équivalence, c'est-à-dire que si $P \equiv P'$ et $Q \equiv Q'$, alors

$$\neg P \equiv \neg P'$$
$$P \wedge Q \equiv P' \wedge Q'$$
$$P \vee Q \equiv P' \vee Q'$$
$$P \implies Q \equiv P' \implies Q'$$
$$P \iff Q \equiv P' \iff Q'$$

Preuve
On fait l'hypothèse $P \equiv P'$ et $Q \equiv Q'$.

- Pour toute valuation v, on a les équivalences suivantes :

$$\begin{aligned} v(\neg P') &= 1 && \\ v(P') &= 0 && \text{par définition de } \neg \\ v(P) &= 0 && \text{car } P \equiv P' \\ v(\neg P) &= 1 && \text{par définition de } \neg \end{aligned}$$

  donc $\neg P \equiv \neg P'$.
- Pour toute valuation v, on a les équivalences suivantes :

$$v(P' \wedge Q') = 1$$

$v(P') = v(Q') = 1$ par définition de $\wedge$
$v(P) = v(Q) = 1$ car $P \equiv P'$ et $Q \equiv Q'$
$v(P \wedge Q) = 1$ par définition de $\wedge$

- On prouve de la même manière les autres cas ($P \vee Q$, $P \implies Q$, $P \iff Q$).

Métathéorème 2.6.25 (Remplacement d'une sous-formule par une formule équivalente)
Si on remplace dans une proposition P, une sous-formule par une formule équivalente, le résultat obtenu est une proposition équivalente à P.

Preuve
On démontre le résultat par induction structurelle :

- Si P est une proposition atomique, sa seule sous-formule est P, donc si on la remplace par une sous-formule équivalente le résultat obtenu est équivalent à P.
- On fait l'hypothèse que la propriété à démontrer est vraie pour la formule P, et on veut prouver qu'elle est vraie pour la formule $\neg P$. On remplace une sous-formule F de $\neg P$ par une formule équivalente F'. Si F est la formule $\neg P$, le résultat est immédiat. Sinon F est une sous-formule de P, donc par hypothèse d'induction on obtient une formule P' équivalente à P. Et alors d'après le métathéorème précédent, $\neg P' \equiv \neg P$.
- On fait l'hypothèse que la propriété à démontrer est vraie pour les formules P et Q, et on veut prouver qu'elle est vraie pour la formule $P \wedge Q$ (le raisonnement est le même pour $P \vee Q$, $P \implies Q$, $P \iff Q$). On remplace une sous-formule F de $P \wedge Q$ par une formule équivalente F'. Si F est la formule $P \wedge Q$, le résultat est immédiat. Sinon, F est une sous-formule de P ou de Q. On considère par exemple que c'est une sous-formule de P (le raisonnement est identique si c'est une sous-formule de Q). Par hypothèse d'induction, on obtient une formule P' équivalente à P. Et alors d'après le métathéorème précédent, $P' \wedge Q \equiv P \wedge Q$.

Exemple 2.6.26
Puisque $\neg(\neg P) \equiv P$, on en déduit par exemple, en remplaçant P par la formule équivalente $\neg(\neg P)$,

$$P \implies Q \equiv \neg(\neg P) \implies Q$$

Voyons d'autres exemples de propriétés classiques des connecteurs.

Exemple 2.6.27 (Lois de De Morgan)
On appelle lois de De Morgan les deux propriétés suivantes

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$
$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

Vérifions la première de ces propriétés :

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

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

On pouvait aussi noter directement que $\neg(P \wedge Q)$ est *faux* si et seulement si $P \wedge Q$ est *vrai*, autrement

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 3

Introduction au calcul booléen (algèbre de Boole)

3.1 Définitions et propriétés élémentaires

Introduction

Le *calcul booléen*, ou *algèbre de Boole* (ou encore *algèbre de Boole logique*, pour la différencier de la structure algébrique du même nom, dont le calcul booléen est un cas particulier, et que nous verrons dans la section 8.7), a été créé par George Boole (1815-1864), logicien, mathématicien et philosophe britannique, qui l'expose en 1847 dans *The Mathematical Analysis of Logic*. Il utilise des techniques algébriques pour étudier la logique des propositions. Le calcul booléen a de nombreuses applications en électronique et en informatique : en 1937, l'ingénieur, électricien et mathématicien américain Claude Shannon (1916-2001), étudiant au Massachusetts Institute of Technology (MIT) montre dans sa thèse (*A Symbolic Analysis of Relay and Switching Circuits*) que le calcul booléen peut être utilisé pour simplifier les arrangements des relais électromécaniques utilisés dans les commutateurs téléphoniques de l'époque. C'est son travail qui fonde le principe de l'électronique numérique et des circuits capables d'effectuer des opérations logiques et arithmétiques, base de la conception des ordinateurs modernes.

Opérateurs de base

On considère l'ensemble $\mathbb{B}$ à deux éléments 0 et 1. Sur cet ensemble, on définit un *opérateur unaire* (c'est-à-dire une fonction de $\mathbb{B}$ dans $\mathbb{B}$), l'opérateur **complémentaire** (dit aussi *contraire*, ou *inversion*), noté $^-$ et deux *opérateurs binaires* (c'est-à-dire des fonctions qui à un couple d'éléments de $\mathbb{B}$ associent un élément de $\mathbb{B}$), l'**addition**, noté $+$, et la **multiplication**, noté $\times$ ou $\cdot$:

Définition 3.1.1 (Définition des opérations dans $\mathbb{B}$)

a	$\bar{a}$
0	1
1	0

a	b	$a+b$
0	0	0
0	1	1
1	0	1
1	1	1

a	b	$a \times b$ ou $a \cdot b$
0	0	0
0	1	0
1	0	0
1	1	1

Remarque 3.1.2 (Notations) : Pour désigner le complémentaire de a, on trouve aussi la notation a'.

Remarque 3.1.3 : Du point de vue algébrique, l'addition et la multiplication se comportent « presque » de la même façon que l'addition et la multiplication usuelles de deux nombres entiers, à la différence que $1+1=1$.

Remarque 3.1.4 : On peut reconnaître les tables de vérité de la logique des propositions : les deux valeurs 0 et 1 correspondent respectivement aux valeurs de vérité *faux* et *vrai*, et

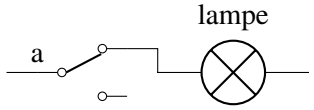
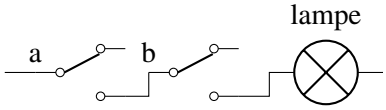
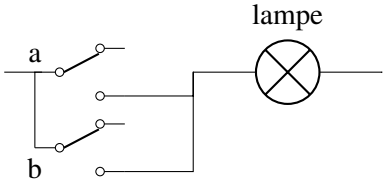
$$\bar{a} = 1 - a$$
$$a + b = \max(a, b)$$
$$a \times b = \min(a, b)$$

Donc du point de vue logique, l'opérateur complémentaire se comporte comme le connecteur négation $\neg$, l'addition se comporte comme le connecteur disjonction $\vee$, la multiplication se comporte comme l'opérateur conjonction $\wedge$. De plus, la constante 0 correspond à la proposition $\bot$ (contradiction) et la constante 1 à la proposition $\top$ (tautologie).

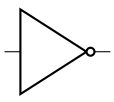
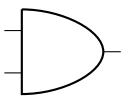
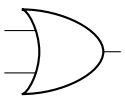
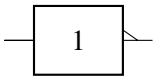
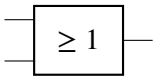
Remarque 3.1.5 (Notations) : Pour éviter de multiplier les symboles, on peut adopter les conventions usuelles des opérations classiques sur les entiers : le symbole de la multiplication peut être omis entre deux variables ou deux parenthèses, et la multiplication est prioritaire sur l'addition. Par exemple

$$a(b + cd) \quad \text{signifie} \quad a \times (b + (c \times d))$$

On peut réaliser physiquement ces opérations en utilisant par exemple les propriétés des interrupteurs électriques. Dans ce qui suit, chaque interrupteur est associé à une variable, et n'est actionné que lorsque cette variable est égale à 1. La lampe visualise le résultat de l'opérateur : elle est allumée lorsque le résultat est 1, éteinte sinon.

Opérateur $^-$ (complémentaire)	Opérateur $\times$ ($\wedge$)	Opérateur $+$ ($\vee$)
		
La lampe s'allume quand on n'appuie pas sur l'interrupteur a.	La lampe s'allume quand on appuie sur l'interrupteur a **et** sur le b.	La lampe s'allume quand on appuie sur l'interrupteur a **ou** sur le b.

En électronique numérique, ces opérateurs sont mis en œuvre par ce qu'on appelle des *portes logiques*, construites à l'aide de transistors. Il existe deux séries de symboles classiques pour les noter, dits *américains* pour les uns, et *européens* pour les autres.

	Opérateur $^-$ (complémentaire)	Opérateur $\times$ ($\wedge$)	Opérateur $+$ ($\vee$)
Symbole américain			
Symbole européen			

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 4

Logique des prédicats (logique du premier ordre)

Prérequis
Le chapitre 2 sur la logique des propositions. En particulier : les définitions des connecteurs (section 2.2), la définition d'une logique formelle, la double approche syntaxique et sémantique, le principe de construction d'un ensemble par induction (sections 2.3 à 2.7), et la section 2.9 dans laquelle on trouve les propriétés classiques (et d'autres moins classiques) des connecteurs.

4.1 Introduction

Pour formaliser les raisonnements mathématiques, le pouvoir expressif de la logique des propositions est trop limité. Par exemple, on peut toujours considérer une proposition exprimant la propriété

« 2 est un nombre pair »

mais c'est insuffisant pour étudier les propriétés des nombres entiers. En effet, on ne peut pas par exemple, définir de proposition

« être un nombre pair »

à partir de laquelle on pourrait exprimer la propriété « 2 est un nombre pair », ou « il existe un nombre pair », ou « tous les nombres ne sont pas pairs ». Nous ne pouvons pas non plus, en nous plaçant dans l'ensemble des nombres réels, exprimer la propriété

Tout nombre positif est le carré d'un autre nombre

que l'on pourrait aussi écrire ainsi :

Pour tout nombre x, si $x \geqslant 0$, alors il existe un nombre y tel que $x = y^2$

Pour cela, nous avons besoin de *prédicats*, c'est-à-dire de propriétés vérifiées par un objet (comme par exemple le fait d'être pair), ou par plusieurs objets, indiquant ainsi une relation entre eux (comme par exemple le prédicat « être supérieur ou égal à », entre deux nombres). Nous avons aussi besoin de *variables* comme x et y, et aussi de *quantificateurs* : dans le deuxième exemple, pour signifier que la propriété est vraie pour tout x, on utilisera ce qu'on appelle le quantificateur universel $\forall$, et pour signifier qu'il existe (au moins) un nombre

y on utilisera ce qu'on appelle le quantificateur existentiel $\exists$. La propriété du deuxième exemple pourra alors s'écrire

$$\overbrace{\forall x}^{\text{pour tout } x}\ ,(\ \underbrace{x \geqslant 0 \Longrightarrow}_{\text{si } x \text{ est positif alors}}\ \overbrace{\exists y}^{\text{il existe } y \text{ tel que}}\ , x = y^2)$$

La **logique des prédicats** (ou calcul des prédicats), ou **logique du premier ordre** (ou encore *calcul des prédicats du premier ordre*) [1], peut être considérée comme la base de la logique mathématique. Elle a été élaborée vers la fin du XIX^{e} siècle et le début du XX^{e} siècle par plusieurs logiciens et mathématiciens, avec la volonté de donner une fondation axiomatique aux mathématiques. On peut citer entre autres le mathématicien et linguiste italien Giuseppe Peano (1858-1932), le mathématicien allemand David Hilbert (1862-1943), les mathématiciens britanniques Alfred North Whitehead (1861-1947) et Bertrand Russell (1872-1970), le mathématicien, logicien, et philosophe américain Charles Peirce (1839-1914), et le mathématicien, logicien et philosophe allemand Gottlob Frege (1848-1925), dont le *Begriffsschrift* [l'Idéographie], en 1879, est parfois considéré comme la naissance de la logique des prédicats.

Cette logique étend celle des propositions en introduisant des éléments supplémentaires. Je vais, dans les sections qui suivent, préciser sa syntaxe, ainsi qu'une première approche informelle de sa sémantique, sur laquelle je reviendrai dans la section 4.8. Le deuxième aspect de la syntaxe, les règles d'inférence (ou règles de déduction), sera traité séparément dans le chapitre 5.

La syntaxe de la logique des prédicats consiste en la donnée de ce qu'on appelle un **langage du premier ordre** L, sous la forme d'une série de symboles. Ce langage n'est pas unique, il y en a une infinité, pouvant s'adapter à différentes théories mathématiques. Il existe des symboles communs à tous les langages du premier ordre (voir plus loin pour les détails) :

- symboles de ponctuations : les parenthèses ( ) ;
- symboles de connecteurs logiques : $\neg$ $\wedge$ $\vee$ $\Longrightarrow$ $\Longleftrightarrow$;
- symboles de variables, comme x ou y ;
- symboles de quantificateurs : $\forall$ et $\exists$;

et des symboles spécifiques à chaque langage, formant ce qu'on appelle sa signature :

- symboles de constantes, comme 0 et 1 représentant les entiers zéro et un ;
- symboles de prédicats, comme l'égalité ($=$) ou la relation d'ordre ($\leqslant$) ;
- symboles d'opérations, comme $+$ (pour l'addition) ou $\times$ (pour la multiplication).

Les symboles de la seconde catégorie (ceux permettant de définir la signature d'un langage) sont parfois appelés des *symboles non logiques*, par opposition à ceux de la première catégorie appelés *symboles logiques*.

D'un point de vue sémantique, ces symboles peuvent ensuite être interprétés dans ce que l'on appelle une ***L*-structure**. C'est-à-dire que l'on choisit un ensemble Ω non vide que l'on appelle **univers** (ou *domaine*, ou *ensemble de base*), dont les éléments seront les objets que l'on peut manipuler. Le terme *objet* désigne ici ce que l'on veut étudier (par exemple un nombre entier, un nombre réel, un ensemble, une figure géométrique, une fonction, …). Il est à noter qu'en logique des prédicats, on ne travaille que dans un univers, c'est-à-dire sur un seul type d'objets, et les quantificateurs ($\forall$ et $\exists$) ne portent que sur ces objets. C'est en ce sens qu'il s'agit d'une logique du *premier ordre* : il existe une logique du *second ordre* où on peut aussi utiliser des quantificateurs sur des ensembles d'objets, une logique du *troisième ordre* où on peut aussi utiliser des quantificateurs sur des ensembles d'ensembles d'objets, etc.

1. Il semble que l'expression *calcul des prédicats* soit la plus répandue pour les auteurs francophones, et *logique du premier ordre* pour les auteurs anglophones (*first order logic*). J'emploierai *logique des prédicats* plutôt que *calcul des prédicats* pour les mêmes raisons qui me font employer *logique des propositions* plutôt que *calcul des propositions* (quand le terme *calcul* ne désigne qu'une partie de la logique, cela permet de mieux distinguer les approches syntaxique et sémantique).

Ces pages ne sont pas incluses dans l’aperçu.

4.5 Formules

Pour définir une formule d'un langage du premier ordre donné, la première étape est de définir des relations que peuvent vérifier les différents termes.

Définition 4.5.1 (Formule atomique)
On appelle *formule atomique* toute expression de la forme $R(t_1, t_2, \dots, t_n)$, où $t_1, t_2, \dots, t_n$ sont des termes et R un prédicat d'arité n.

Remarque 4.5.2 : Comme pour les termes, les parenthèses et virgules ne sont pas nécessaires, et on peut définir de manière non ambiguë une formule atomique associée à un prédicat R d'arité n comme

$$Rt_1 \dots t_n$$

Remarque 4.5.3 : Il est possible dans la définition d'ajouter à l'ensemble des formules atomiques le symbole

$$\bot$$

que l'on nomme *absurde*, ou *contradiction*, et qui, de manière informelle, désigne une formule toujours fausse. Cet ajout n'est pas indispensable, mais peut être pratique pour définir certains systèmes d'inférence (voir la section 5.5 sur la déduction naturelle).

Exemple 4.5.4 (Exemples de formules atomiques)
Voici quelques exemples de formules atomiques, construites à partir de l'opération binaire $+$, des prédicats binaires $=$ et $\leqslant$, du prédicat unaire R, et des variables x, y, z :

$$y = z \qquad x + x = (y + z) + z \qquad x \leqslant y \qquad y + z \leqslant x \qquad R(x + y)$$

Dans ce qui précède, les prédicats $=, \leqslant, R$ ont été utilisés avec les termes suivants :

$$x \quad y \quad z \quad x + x \quad (y + z) + z \quad y + z \quad x + y$$

Remarque 4.5.5 : Comme précédemment, j'utilise la notation préfixée pour le cas général, par exemple

$$R(x + y)$$

qui désigne l'application du prédicat R au terme $x + y$, et la notation infixée pour les symboles usuels de prédicat binaire, par exemple

$$x \leqslant y$$

qui désigne l'application du prédicat binaire $\leqslant$ au couple (x, y), ce qui pourrait aussi s'écrire en notation préfixée

$$\leqslant xy$$

Nous pouvons maintenant définir les formules, par induction, en utilisant les connecteurs logiques et les deux quantificateurs.

Ces pages ne sont pas incluses dans l’aperçu.

Pour introduire une formule $\mathscr{F}$ dont toutes les variables libres sont à prendre parmi $x_1, \dots, x_n$, je noterai

$$\mathscr{F}[x_1, \dots, x_n]$$

et j'utiliserai alors le raccourci suivant, pour tous les termes $t_1, \dots, t_n$:

$$\mathscr{F}(t_1, \dots, t_n) \stackrel{\text{def}}{\equiv} \mathscr{F}(t_1, \dots, t_n/x_1, \dots, x_n)$$

Je pourrai aussi ne lister que les premières variables, c'est-à-dire que pour tout entier $k \leqslant n$:

$$\mathscr{F}(t_1, \dots, t_k) \stackrel{\text{def}}{\equiv} \mathscr{F}(t_1, \dots, t_k/x_1, \dots, x_k)$$

Par exemple, si on considère une formule $\mathscr{F}[x, y, \vec{a}]$ (autrement dit $\mathscr{F}[x, y, a_1, \dots, a_n]$).

$$\mathscr{F}(z, t) \stackrel{\text{def}}{\equiv} \mathscr{F}(z, t/x, y)$$
$$\mathscr{F}(z) \stackrel{\text{def}}{\equiv} \mathscr{F}(z/x)$$

4.8 Sémantique de la logique des prédicats

Je reprends ici l'aspect sémantique de la logique des prédicats parfois abordé de façon informelle dans les sections précédentes, mais en formalisant davantage.

Pour définir la valeur de vérité d'une formule (*vrai* ou *faux*), la première étape est d'interpréter le langage logique :

Définition 4.8.1 (L-structure, interprétation)
Pour tout langage du premier ordre L, on appelle *réalisation* de L, ou *L-structure*, la donnée $\mathscr{M}$ formée

- d'un ensemble *non vide* M (qu'on appelle *univers*, ou *domaine*, ou *ensemble de base*) ;
- d'un élément $c_{\mathscr{M}}$ de M pour chaque constante c (qu'on appelle *interprétation* de c) ;
- d'une fonction $f_{\mathscr{M}}$ de M^n dans M, pour chaque opérateur f d'arité n (qu'on appelle *interprétation* de f) ;
- d'une relation n-aire $R_{\mathscr{M}}$ (c'est-à-dire un sous-ensemble de l'ensemble M^n de tous les n-uplets $(x_1, \dots, x_n)$ d'éléments de M) pour chaque symbole R de prédicat d'arité n (qu'on appelle *interprétation* de R).

Remarque 4.8.2 (Notations) : Par convention, et sauf avis contraire, si je désigne une structure par une lettre majuscule dans une police d'écriture scripte ($\mathscr{M}, \mathscr{N}, \mathscr{A}, \dots$), alors la lettre correspondante dans une police ordinaire ($M, N, A, \dots$) désignera l'univers associé.

Remarque 4.8.3 (Notations) : S'il n'y a pas d'ambiguïté, il peut arriver qu'on fasse la confusion, dans la notation, entre la L-structure et l'univers associé, par exemple noter c_M, f_M, R_M pour $c_{\mathscr{M}}, f_{\mathscr{M}}, R_{\mathscr{M}}$. De la même façon il peut arriver qu'on fasse la confusion entre les symboles du langage et leur interprétation, en notant par exemple c, f, R au lieu de $c_{\mathscr{M}}, f_{\mathscr{M}}, R_{\mathscr{M}}$.

Remarque 4.8.4 : L'interprétation du prédicat binaire particulier correspondant à l'égalité ($=$) est imposée : c'est toujours le sous-ensemble

$$\{(x, x) \mid x \in M\}$$

C'est-à-dire que le symbole d'égalité du langage est interprété comme l'égalité (de la métathéorie) dans l'ensemble M.

Ces pages ne sont pas incluses dans l’aperçu.

4.10 Propriétés des quantificateurs

Métathéorème 4.10.1

1. Pour toute formule $\mathscr{F}$, si la variable x n'est pas libre dans $\mathscr{F}$

$$\forall x\mathscr{F} \equiv \exists x\mathscr{F} \equiv \mathscr{F}$$

2. Pour toute formule $\mathscr{F}$

$$\forall x\mathscr{F} \vDash \exists x\mathscr{F}$$

Preuve

1. Puisque x n'est pas libre dans $\mathscr{F}$, si A' est une x-variante de l'assignation A, alors A et A' coïncident sur les variables libres de $\mathscr{F}$, donc

$$v_A(\mathscr{F}) = v_{A'}(\mathscr{F})$$

On en déduit

$$v_A(\forall x\mathscr{F}) = v_A(\exists x\mathscr{F}) = v_A(\mathscr{F})$$

2. Si une assignation A est telle que

$$\mathscr{M} \vDash_A \forall x\mathscr{F}$$

alors puisque l'ensemble de base M n'est pas vide (par convention), il existe un élément a dans M et la x-variante A' de A telle que $A'(x) = a$ vérifie

$$\mathscr{M} \vDash_{A'} \mathscr{F}$$

Par conséquent

$$\mathscr{M} \vDash_A \exists x\mathscr{F}$$

Remarque 4.10.2 : De manière informelle, la première propriété signifie que si la variable x n'apparaît pas dans la formule $\mathscr{F}$, alors, si on ajoute un quantificateur portant sur cette variable, on obtient une formule équivalente.

Remarque 4.10.3 : La deuxième propriété est vraie car le domaine d'une structure est toujours supposé non vide ; elle ne s'étend pas à ce qu'on peut appeler des quantificateurs bornés, comme par exemple en théorie des ensembles : de

$$\forall x \in E, \mathscr{F}$$

on ne peut pas déduire

$$\exists x \in E, \mathscr{F}$$

car l'ensemble E peut être vide.

Métathéorème 4.10.4 (Négation d'une formule avec quantificateurs)
Pour toute formule $\mathscr{F}$:

1. La négation de $\forall x\mathscr{F}$ est équivalente à $\exists x\neg\mathscr{F}$:

$$\neg(\forall x\mathscr{F}) \equiv \exists x, \neg\mathscr{F}$$

2. La négation de $\exists x\mathscr{F}$ est équivalente à $\forall x\neg\mathscr{F}$:

$$\neg(\exists x\mathscr{F}) \equiv \forall x, \neg\mathscr{F}$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 5

Systèmes de déduction

Prérequis
La syntaxe de la logique des propositions (section 2.4) et de la logique des prédicats (sections 4.2 à 4.7).

5.1 Introduction

Un *système de déduction* (ou *système déductif*, ou *système d'inférence*, ou encore un *calcul*) comprend un ensemble de formules prises comme point de départ (des *axiomes*), et un ensemble de règles (qu'on appelle règles d'inférence) qui permettent de *déduire* (ou *prouver*) des formules, à partir d'un ensemble de formules Γ. Une formule prouvable à partir de Γ s'appelle un *théorème* de Γ ; on peut aussi dire que c'est une *conséquence* (ou *conséquence syntaxique*, l'équivalent de la notion de *conséquence sémantique*) de Γ. Parmi les systèmes déductifs les plus classiques, on trouve la **méthode des tableaux sémantiques**, la **résolution**, les **systèmes à la Hilbert**, la **déduction naturelle**, et le **calcul des séquents** :

1. La méthode des tableaux a été inventée en 1955 par le philosophe et logicien hollandais Evert Willhem Beth (1908-1964), et la résolution est en grande partie due au mathématicien et informaticien John Alan Robinson (1930-2016). Ces deux systèmes sont parfois appelés systèmes de *réfutation* (plutôt que de *déduction*), car leur principe général consiste à prouver une formule $\mathscr{F}$ en justifiant que la formule $\neg\mathscr{F}$ (la réfutation de $\mathscr{F}$) conduit à une contradiction.
2. Les systèmes à la Hilbert (il y a de nombreuses variantes) sont des systèmes de déduction qui suivent un modèle proposé par le mathématicien allemand David Hilbert (1862-1943).
3. La déduction naturelle est un système proposé par le mathématicien et logicien allemand Gerhard Gentzen (1909-1945) en 1934, proche de la manière de raisonner des mathématiciens.
4. Le calcul des séquents a été créé par Gerhard Gentzen à partir de son système de déduction naturelle, pour des raisons techniques en rapport avec la métathéorie des systèmes déductifs (son calcul des séquents lui permettait de démontrer des propriétés intéressantes du système déductif, qu'il ne pouvait justifier avec le système de déduction naturelle).

Les systèmes de déduction précédents sont tous équivalents, dans la mesure où ils permettent de démontrer exactement les mêmes théorèmes (de logique classique). Dans la suite de ce chapitre, je présenterai la méthode des tableaux sémantiques (dans les section 5.2, pour la logique des propositions, et 5.10, pour la logique des prédicats), la résolution (dans la section 5.3, pour la logique des propositions [1]), les systèmes de déduction

1. J'aborde brièvement et de manière informelle la résolution dans le cadre de la logique des propositions, mais je ne traite pas le cas de la logique des prédicats, qui est plus complexe, et ne me servira pas pour la suite.

à la Hilbert (dans les sections 5.4, pour la logique des propositions, et 5.11, pour la logique des prédicats), la déduction naturelle (dans les sections 5.5, pour la logique des propositions, et 5.12, pour la logique des prédicats), et le calcul des séquents (dans les sections 5.9 pour la logique des propositions et 5.13 pour la logique des prédicats). Mais ce sont essentiellement les systèmes à la Hilbert et la déduction naturelle que je détaillerai le plus (leur équivalence sera par ailleurs prouvée dans la section 5.15) :

- Avec peu d'axiomes et de règles, les systèmes à la Hilbert sont des systèmes simples, permettant aussi de justifier rapidement certaines propriétés de la logique. Leur principal défaut est le fait de ne pas pouvoir poser d'hypothèse, ce qui peut alourdir les démonstrations. Les axiomes sont aussi artificiels et peu intuitifs (voir l'exemple 5.4.16).
- La déduction naturelle est le système formel le plus proche du raisonnement naturel des mathématiciens. Il corrige certains défauts des systèmes à la Hilbert, en permettant en particulier de poser des hypothèses. Les règles de déduction reposent sur un principe de symétrie : chaque connecteur (implication $\Longrightarrow$, conjonction $\wedge$, ...) et chaque quantificateur ($\forall$, $\exists$) est associé à une paire de règles duales, l'*introduction*, qui indique comment prouver une formule qui fait intervenir le symbole, et l'*élimination*, qui indique comment utiliser une formule avec ce symbole.

Les autres systèmes sont principalement utilisés en logique pure ou en informatique (en particulier pour des techniques de démonstration automatique).

C'est aussi dans le cadre de la déduction naturelle que seront présentées quelques propriétés de la notion de *contradiction* d'un ensemble de formules, l'équivalent de la notion sémantique d'*inconsistance*, ainsi que la plupart des raisonnements usuels en mathématiques (raisonnement par modus ponens, par contraposition, par l'absurde ...). Ces différents raisonnements peuvent aussi être présents dans d'autres sections (en particulier celles consacrées aux systèmes à la Hilbert), mais c'est dans les sections traitant de la déduction naturelle qu'ils seront le plus approfondis. On trouvera par ailleurs dans la section 5.16 une synthèse sur les raisonnements mathématiques classiques.

Pour signifier que l'on peut déduire la formule $\mathscr{F}$ de l'ensemble de formules Γ (qui est donc l'ensemble des hypothèses, qu'on appelle aussi *l'environnement*, ou le *contexte*), on note en général (quel que soit le système d'inférence choisi)

$$\Gamma \vdash \mathscr{F}$$

Dans le cas où Γ est vide, c'est-à-dire quand on peut prouver la formule $\mathscr{F}$ sans aucune hypothèse (autre que les axiomes et les règles de déduction), on note

$$\vdash \mathscr{F}$$

et si Γ et Γ' sont deux ensembles de formules, on peut aussi noter

$$\Gamma \vdash \Gamma'$$

pour signifier que l'on peut déduire toutes les formules de Γ' à partir de Γ (autrement dit lorsque pour toute formule $\mathscr{F}$ de Γ', on a $\Gamma \vdash \mathscr{F}$).

L'ensemble des formules de Γ auquel on ajoute l'ensemble des formules de Γ', se note en utilisant le symbole de réunion $\cup$ de deux ensembles

$$\Gamma \cup \Gamma'$$

ou juste

$$\Gamma, \Gamma' \qquad \text{ou encore} \qquad \Gamma; \Gamma'$$

On pourra noter $\{\mathscr{F}_1, \ldots, \mathscr{F}_n\}$ l'ensemble constitué des formules $\mathscr{F}_1, \ldots, \mathscr{F}_n$ ou, par abus de notation, juste $\mathscr{F}_1, \ldots, \mathscr{F}_n$. Par exemple, si $\mathscr{F}, \mathscr{G}, \mathscr{H}$ sont des formules et Γ un ensemble de formules

$$\{\mathscr{F}, \mathscr{G}\} \vdash \mathscr{H} \qquad \text{ou} \qquad \mathscr{F}, \mathscr{G} \vdash \mathscr{H}$$

Ces pages ne sont pas incluses dans l’aperçu.

Remarque 5.4.5 : On déduit également de la monotonie et de la réflexivité la propriété que j'appellerai *répétition* : de $\Gamma \cup \{P\}$, on peut déduire P :

$$\Gamma, P \vdash P$$

puisque

$$\begin{cases} P \vdash P \\ \{P\} \subseteq \Gamma \cup \{P\} \end{cases}$$

Cette propriété peut aussi s'exprimer ainsi : si P appartient à Γ, alors

$$\Gamma \vdash P$$

Remarque 5.4.6 : On déduit du métathéorème précédent quelques propriétés des relations $\equiv$ et $\equiv_\Gamma$ (nous en verrons d'autres plus loin) : si $P \equiv Q$, alors $P \equiv_\Gamma Q$ par monotonie (si $P \vdash Q$, alors $\Gamma \cup \{P\} \vdash Q$), et les relations $\equiv$ et $\equiv_\Gamma$ sont des relations d'équivalence (elles sont réflexives, symétriques et transitives) : la symétrie de $\equiv_\Gamma$ est une conséquence immédiate de la définition (on peut permuter P et Q), la réflexivité est une conséquence de la monotonie et de la réflexivité de la logique ($\Gamma \cup \{P\} \vdash P$), et la transitivité est une conséquence de la monotonie et de la transitivité de la logique (si $\Gamma \cup \{P\} \vdash Q$, et si $\Gamma \cup \{Q\} \vdash R$, alors $\Gamma \cup \{P, Q\} \vdash R$ par monotonie et $\Gamma \cup \{P\} \vdash R$ par transitivité).

Un exemple de système de déduction à la Hilbert pour la logique des propositions est le système suivant, pour lequel la seule règle d'inférence est le modus ponens :

Règle d'inférence 5.4.7 (Règle du modus ponens)

$$\text{si} \begin{cases} P \\ P \Longrightarrow Q \end{cases}$$
$$\text{alors } Q$$

et qui utilise les axiomes suivants (deux pour l'implication, un pour la négation) :

Axiome 5.4.8 (Axiomes de Hilbert)

1. $AI_1 : P \Longrightarrow (Q \Longrightarrow P)$
2. $AI_2 : (P \Longrightarrow (Q \Longrightarrow R)) \Longrightarrow ((P \Longrightarrow Q) \Longrightarrow (P \Longrightarrow R))$
3. $AN : (\neg P \Longrightarrow \neg Q) \Longrightarrow ((\neg P \Longrightarrow Q) \Longrightarrow P)$

Remarque 5.4.9 : Dans d'autres variantes (équivalentes) des axiomes de Hilbert, l'axiome *AN* est remplacé par :

$$AN' : (\neg P \Longrightarrow Q) \Longrightarrow ((\neg P \Longrightarrow \neg Q) \Longrightarrow P)$$

ou par

$$AN'' : (\neg Q \Longrightarrow \neg P) \Longrightarrow (P \Longrightarrow Q)$$

On pourra trouver une justification de l'équivalence des trois variantes dans la remarque 5.4.26 (p. 223) et le métathéorème 5.4.32 (p. 226).

Ces pages ne sont pas incluses dans l’aperçu.

6	$(P \implies Q) \implies (P \implies R)$	Modus ponens à partir de 1 et 5
7	$P \implies R$	Modus ponens à partir de 4 et 6

En appliquant cette propriété en permutant P et Q, on obtient

$$Q \implies (P \implies R) \vdash P \implies (Q \implies R)$$

ce qui prouve aussi l'équivalence

$$P \implies (Q \implies R) \equiv Q \implies (P \implies R)$$

Remarque 5.4.26 : On déduit aussi du principe de permutation, en remplaçant P par « $\neg P \implies \neg Q$ », Q par « $\neg P \implies Q$ », et R par P, l'équivalence des deux axiomes pour la négation :

$$AN : (\neg P \implies \neg Q) \implies ((\neg P \implies Q) \implies P)$$
$$AN' : (\neg P \implies Q) \implies ((\neg P \implies \neg Q) \implies P)$$

Exemple 5.4.27 (Démonstration de l'équivalence entre P et $\neg\neg P$)

1. Démontrons

$$\vdash \neg\neg P \implies P$$

1	$(\neg P \implies \neg\neg P) \implies ((\neg P \implies \neg P) \implies P)$	Axiome AN en remplaçant Q par $\neg P$
2	$(\neg P \implies \neg P) \implies ((\neg P \implies \neg\neg P) \implies P)$	Par permutation (exemple précédent)
3	$\neg P \implies \neg P$	Répétition (en remplaçant P par $\neg P$)
4	$(\neg P \implies \neg\neg P) \implies P$	Modus ponens à partir de 3 et 2
5	$\neg\neg P \implies (\neg P \implies \neg\neg P)$	Axiome AI_1 en remplaçant P par $\neg\neg P$ et Q par $\neg P$
6	$\neg\neg P \implies P$	Transitivité de l'implication, à partir de 5 et 4

2. Démontrons

$$\vdash P \implies \neg\neg P$$

1	$((\neg\neg\neg P \implies \neg P) \implies ((\neg\neg\neg P \implies P) \implies \neg\neg P))$	Axiome AN en remplaçant P par $\neg\neg P$ et Q par P
2	$\neg\neg\neg P \implies \neg P$	Résultat du point précédent en remplaçant P par $\neg P$
3	$(\neg\neg\neg P \implies P) \implies \neg\neg P$	Modus ponens à partir de 2 et 1
4	$P \implies (\neg\neg\neg P \implies P)$	Axiome AI_1 en remplaçant Q par $\neg\neg\neg P$
5	$P \implies \neg\neg P$	Transitivité de l'implication à partir de 4 et 3

En appliquant le théorème de déduction à ce qui précède, on obtient

$$\begin{cases} \neg\neg P \vdash P \\ P \vdash \neg\neg P \end{cases}$$

autrement dit on a l'équivalence

$$\neg\neg P \equiv P$$

Ces pages ne sont pas incluses dans l’aperçu.

Réciproquement, prouvons

$$\neg\neg\neg P \vdash \neg P$$

1	$P \vdash \neg\neg P$	D'après ce qui précède (principe de non-contradiction)
2	$\neg\neg\neg P, P \vdash \neg\neg\neg P$	Répétition
3	$\neg\neg\neg P \vdash \neg P$	Règle d'introduction de $\neg$ à partir de 1 et 2

On en déduit

$$\neg P \equiv \neg\neg\neg P$$

Métathéorème 5.5.78 (Règle du modus tollens)
De $P \implies Q$ et $\neg Q$, on peut déduire $\neg P$:

$$\text{si} \quad \begin{cases} \Gamma & \vdash \neg Q \\ \Gamma' & \vdash P \implies Q \end{cases}$$
$$\text{alors} \quad \Gamma, \Gamma' \vdash \neg P$$

Preuve

1	$\Gamma, P \vdash \neg Q$	Hypothèse (et affaiblissement)
2	$\Gamma' \vdash P \implies Q$	Hypothèse
3	$P \vdash P$	Répétition
4	$\Gamma', P \vdash Q$	Modus ponens à partir de 2 et 3
5	$\Gamma, \Gamma' \vdash \neg P$	Règle d'introduction de $\neg$ à partir de 1 et 4

Remarque 5.5.79 : Dans le cas où les deux ensembles de formules sont identiques, on peut aussi écrire

$$\text{si} \quad \begin{cases} \Gamma & \vdash \neg Q \\ \Gamma & \vdash P \implies Q \end{cases}$$
$$\text{alors} \quad \Gamma \vdash \neg P$$

cette règle étant équivalente à la précédente (même raisonnement que pour la règle d'élimination de l'implication).

Théorème 5.5.80 (Corollaire : raisonnement par contraposition)
On peut déduire d'une implication $P \implies Q$ sa contraposée $\neg Q \implies \neg P$:

$$P \implies Q \vdash \neg Q \implies \neg P$$

ce qui équivaut, d'après le théorème de déduction, à

$$\vdash (P \implies Q) \implies (\neg Q \implies \neg P)$$

et à

$$P \implies Q, \neg Q \vdash \neg P$$

Ces pages ne sont pas incluses dans l’aperçu.

$\sqrt{2}^{\sqrt{2}}$ est rationnel ou irrationnel. Néanmoins, ce résultat est donné par le théorème de Gelfond-Schneider, démontré indépendamment en 1934 par le mathématicien russe Alexandre Gelfond (1906-1968), et le mathématicien allemand Theodor Schneider (1911-1988) :

> Si a est un nombre algébrique (un nombre qui est racine d'un polynôme non nul à coefficients rationnels) différent de 0 et de 1, et si b est un nombre algébrique irrationnel, alors a^b est un nombre transcendant (c'est-à-dire non algébrique).

Or $\sqrt{2}$ est un nombre algébrique irrationnel, et par conséquent $\sqrt{2}^{\sqrt{2}}$ est un nombre transcendant, donc irrationnel.

Théorème 5.5.115 (Lois de De Morgan)
Lois de De Morgan :

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$
$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

ce qui équivaut aussi à

$$\vdash \neg(P \vee Q) \iff (\neg P \wedge \neg Q)$$
$$\vdash \neg(P \wedge Q) \iff (\neg P \vee \neg Q)$$

Preuve

- Prouvons

$$\neg(P \vee Q) \vdash \neg P \wedge \neg Q$$

1	$\neg(P \vee Q) \vdash \neg(P \vee Q)$	Répétition
2	$P \vdash P \vee Q$	Règle d'introduction de la disjonction
3	$\neg(P \vee Q), P \vdash \bot$	Règle d'élimination de la négation à partir de 1 et 2
4	$\neg(P \vee Q) \vdash \neg P$	Règle d'introduction de la négation
5	$Q \vdash P \vee Q$	Règle d'introduction de la disjonction
6	$\neg(P \vee Q), Q \vdash \bot$	Règle d'élimination de la négation à partir de 1 et 5
7	$\neg(P \vee Q) \vdash \neg Q$	Règle d'introduction de la négation
8	$\neg(P \vee Q) \vdash \neg P \wedge \neg Q$	Règle d'introduction de la conjonction à partir de 4 et 7

- Prouvons

$$\neg P \wedge \neg Q \vdash \neg(P \vee Q)$$

1	$\neg P \wedge \neg Q, P \vee Q \vdash P \vee Q$	Répétition
2	$\neg P \wedge \neg Q, P \vee Q, P \vdash P$	Répétition
3	$\neg P \wedge \neg Q, P \vee Q, P \vdash \neg P$	Règle d'élimination de la conjonction
4	$\neg P \wedge \neg Q, P \vee Q, P \vdash \bot$	Règle d'élimination de la négation à partir de 2 et 3
5	$\neg P \wedge \neg Q, P \vee Q, Q \vdash Q$	Répétition
6	$\neg P \wedge \neg Q, P \vee Q, Q \vdash \neg Q$	Règle d'élimination de la conjonction
7	$\neg P \wedge \neg Q, P \vee Q, Q \vdash \bot$	Règle d'élimination de la négation à partir de 5 et 6
8	$\neg P \wedge \neg Q, P \vee Q \vdash \bot$	Par disjonction des cas, à partir de 1, 4, 7
9	$\neg P \wedge \neg Q \vdash \neg(P \vee Q)$	Par introduction de la négation

On en déduit

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 6

Sophismes et paralogismes

6.1 Introduction

Un *paralogisme* est un raisonnement incorrect (étymologiquement, un « raisonnement à côté »). Ce terme est en général employé quand l'erreur est involontaire, faite de bonne foi, ce qui le distingue du *sophisme*, qui est un paralogisme fallacieux, c'est-à-dire prononcé dans l'intention de tromper. Étymologiquement, les sophismes sont les arguments employés par les *sophistes*, qui étaient des orateurs de la Grèce antique, utilisant des techniques dont le seul objectif était la persuasion de leur auditoire. Ils n'hésitaient donc pas à employer des raisonnements incorrects, mais qui, par leur éloquence, pouvaient passer pour corrects. [1]

On distingue en général les paralogismes formels, que l'on peut identifier en étudiant uniquement la structure de l'argument, des paralogismes informels, qui dépendent du contenu. La section qui suit cette introduction sera consacrée aux premiers, et les autres sections aux paralogismes informels, que je classerai en trois catégories :

- Ceux en rapport avec le raisonnement déductif, c'est-à-dire dans lequel la conclusion se déduit de façon certaine des prémisses (c'est le type de raisonnement que l'on trouve en logique formelle, donc dans les mathématiques).
- Ceux en rapport avec le raisonnement inductif, dans lequel l'étude des prémisses montre que la conclusion est uniquement probable. Ce type de raisonnement ne se trouve pas en logique formelle, mais est employé en sciences. Il consiste par exemple à chercher des lois générales à partir de l'observation de faits particuliers. Il est important de ne pas confondre le raisonnement inductif avec le principe d'induction que nous avons vu. Le même terme est utilisé mais ces deux cas n'ont rien à voir. Comme toutes les autres règles mathématiques, l'induction fait partie des raisonnements de type déductif. Par ailleurs, même si le raisonnement inductif n'est pas utilisé dans une preuve mathématique formelle, une erreur en rapport avec ce type de raisonnement reste possible dans une démonstration « humaine » (par exemple la généralisation abusive d'une propriété).
- Les autres, que je désignerai par le terme *irrationnel* (dans le sens où l'erreur commise n'est plus directement liée à un raisonnement de type déductif ou inductif).

Je précise enfin que l'objectif de cette classification n'est pas de réaliser une étude épistémologique savante, et que ce chapitre me permet juste de présenter une liste (non exhaustive) de paralogismes classiques, que l'on peut rencontrer dans différents domaines (je ne me limite pas aux mathématiques). [2]

1. Les définitions peuvent varier selon les auteurs. Je préfère considérer le sophisme comme une sous-catégorie de paralogisme, ce qui est plus simple que d'employer le terme *paralogisme* uniquement quand l'erreur est involontaire. Sinon il n'existe pas de mot pour désigner l'erreur de raisonnement elle-même, indépendamment de l'intention du locuteur (ce que les anglophones nomment *fallacy*).

2. Les différents types de paralogismes et les exemples présentés dans ce chapitre s'appuient notamment sur les sources suivantes :

6.2 Paralogismes formels

Paralogisme 6.2.1 (Confusion entre implication et implication réciproque)
Cette erreur consiste à confondre une implication $P \implies Q$ et sa réciproque ($Q \implies P$), ce qui revient à confondre implication et équivalence, et peut aussi conduire à deux autres erreurs :

- l'*affirmation du conséquent*, où l'on déduit P de $P \implies Q$ et Q, ce qui est correct étant de déduire P de $Q \implies P$ et Q (modus ponens) ;
- la *négation de l'antécédent*, où l'on déduit $\neg Q$ de $P \implies Q$ et $\neg P$, ce qui est correct étant de déduire $\neg Q$ de $Q \implies P$ et $\neg P$ (modus tollens).

Exemple 6.2.2 (Exemples d'implications mathématiques vraies dont la réciproque est fausse)

- Tous les carrés sont des parallélogrammes, mais tous les parallélogrammes ne sont pas des carrés.
- Tous les nombres premiers sont supérieurs ou égaux à 2, mais tous les entiers supérieurs ou égaux à 2 ne sont pas premiers.
- Toutes les fonctions dérivables sont continues, mais toutes les fonctions continues ne sont pas dérivables.

Exemple 6.2.3
Exemples d'affirmation du conséquent et de négation de l'antécédent, pour lesquels les prémisses sont vraies, mais la conclusion absurde, ce qui illustre la non-validité de ce type de raisonnement :

- Exemple d'affirmation du conséquent :
  Tous les chiens ont quatre pattes.
  Un chat a quatre pattes.
  Donc un chat est un chien.
- Exemple de négation de l'antécédent :
  Tous les chiens ont quatre pattes.
  Un chat n'est pas un chien.
  Donc un chat n'a pas quatre pattes.
- Exemple d'affirmation du conséquent :
  Si vous habitez à Paris, alors vous vivez en France.
  Vous vivez en France.
  Donc vous habitez à Paris.
- Exemple de négation de l'antécédent :
  Si vous habitez à Paris, alors vous vivez en France.
  Vous n'habitez pas à Paris.
  Donc vous ne vivez pas en France.

- Normand BAILLARGEON. *Petit cours d'autodéfense intellectuelle*. Lux Éditeur, 2006.
- Patrick J. HURLEY. *A Concise Introduction to Logic*. 12e éd. Cengage Learning, 2015.
- Encyclopédie Wikipedia (anglophone et francophone).

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 7

Propriétés de la logique des propositions et de la logique des prédicats

7.1 Correction et complétude de la logique des propositions

Prérequis
Le chapitre 2 sur la logique des propositions (au moins les sections 2.4 à 2.7 et 2.9), les systèmes de déduction à la Hilbert (section 5.4), et les propriétés des ensembles non contradictoires de formules (section 5.7).

Nous avons vu que la double approche de la logique, sémantique et syntaxique, amène deux notions de conséquence :

- La formule P est une conséquence sémantique de l'ensemble de formules Γ lorsque P est vraie dans tout modèle de Γ, ce que l'on note
$$\Gamma \models P$$
- La formule P est une conséquence syntaxique de l'ensemble de formules Γ lorsqu'on peut déduire P de Γ, ce que l'on note
$$\Gamma \vdash P$$

Nous allons prouver que ces deux notions coïncident, c'est-à-dire que les symboles $\vdash$ et $\models$ sont interchangeables. Nous utiliserons comme système de déduction le système à la Hilbert décrit dans la section 5.4 (mais d'après les résultats de la section 5.15, il serait équivalent d'utiliser le système de déduction naturelle).

La première partie du théorème principal de ce chapitre est ce qu'on appelle la correction (ou adéquation) de la logique des propositions :

Métathéorème 7.1.1 (Théorème de correction de la logique des propositions)
Les deux versions suivantes de ce théorème sont équivalentes :

1. Si P est une conséquence syntaxique de Γ, alors P est une conséquence sémantique de Γ :
$$\text{si } \Gamma \vdash P$$
$$\text{alors } \Gamma \models P$$
2. Si Γ admet un modèle, alors Γ est non contradictoire.

Ces pages ne sont pas incluses dans l’aperçu.

— soit $\mathcal{T} \nvdash \mathcal{F}$ et alors par hypothèse $\mathcal{T} \vdash \neg\mathcal{F}$, donc $\mathcal{T} \vdash \mathcal{G}$.

On en déduit : $\mathcal{T} \vdash \mathcal{F}$ ou $\mathcal{T} \vdash \mathcal{G}$.

- La réciproque est toujours vérifiée (que la théorie soit complète ou pas) : on fait l'hypothèse que $\mathcal{T} \vdash \mathcal{F}$ ou $\mathcal{T} \vdash \mathcal{G}$.

— Si $\mathcal{T} \vdash \mathcal{F}$, alors $\mathcal{T} \vdash \mathcal{F} \vee \mathcal{G}$.

— Si $\mathcal{T} \vdash \mathcal{G}$, alors $\mathcal{T} \vdash \mathcal{F} \vee \mathcal{G}$.

Donc $\mathcal{T} \vdash \mathcal{F} \vee \mathcal{G}$.

3. On fait l'hypothèse que pour toute formule close $\mathcal{F}$ et $\mathcal{G}$

$$\mathcal{T} \vdash \mathcal{F} \vee \mathcal{G} \quad \text{si et seulement si} \quad \mathcal{T} \vdash \mathcal{F} \text{ ou } \mathcal{T} \vdash \mathcal{G}$$

Pour toute formule close $\mathcal{F}$, on a par tiers exclu

$$\mathcal{T} \vdash \mathcal{F} \vee \neg\mathcal{F}$$

Donc par hypothèse

$$\mathcal{T} \vdash \mathcal{F} \text{ ou } \mathcal{T} \vdash \neg\mathcal{F}$$

7.3 Correction et complétude de la logique des prédicats

Prérequis
Le chapitre 4 sur la logique des prédicats (en particulier les propriétés sémantiques des sections 4.8 à 4.10), les systèmes de déduction à la Hilbert (sections 5.4 et 5.11), et la complétude d'une théorie (section 7.2).

Dans la logique des prédicats, comme dans la logique des propositions, les deux notions de conséquence (sémantique et syntaxique) coïncident, c'est-à-dire que les symboles $\vdash$ et $\models$ sont interchangeables. Nous utiliserons dans ce qui suit le système à la Hilbert décrit dans la section 5.11.

Métathéorème 7.3.1 (Théorème de correction de la logique des prédicats)
Les deux versions suivantes de ce théorème sont équivalentes :

1. Si la formule $\mathcal{F}$ est une conséquence syntaxique de la théorie Γ, alors $\mathcal{F}$ est une conséquence sémantique de Γ :

$$\text{si } \Gamma \vdash \mathcal{F}$$
$$\text{alors } \Gamma \models \mathcal{F}$$

2. Si la théorie Γ admet un modèle, alors Γ est non contradictoire.

Preuve 1 (preuve de l'équivalence uniquement)
Vérifions l'équivalence des deux versions :

- On suppose la version 1 vérifiée. Démontrons la contraposée de la version 2 : si Γ est une théorie contradictoire, alors pour toute formule $\mathcal{F}$, on a $\Gamma \vdash \mathcal{F}$, donc d'après la version 1 du théorème, $\Gamma \models \mathcal{F}$. On en déduit que Γ n'a pas de modèle.
- On suppose la version 2 vérifiée, et on considère Γ et $\mathcal{F}$ tels que $\Gamma \vdash \mathcal{F}$. Puisque Γ est une théorie (donc sans variables libres), la clôture universelle $\mathcal{F}'$ de $\mathcal{F}$ est aussi telle que $\Gamma \vdash \mathcal{F}'$. Donc $\Gamma \cup \{\neg\mathcal{F}'\}$ est une théorie contradictoire. On en déduit d'après la version 2 du théorème (et par contraposition), que $\Gamma \cup \{\neg\mathcal{F}'\}$ n'admet pas de modèle, donc $\Gamma \models \mathcal{F}'$. Par conséquent, $\Gamma \models \mathcal{F}$.

Preuve 2 (preuve du théorème)
Démontrons la première version du théorème, par récurrence forte sur la taille des preuves, autrement dit démontrons que pour tout entier non nul n, s'il existe une preuve $\mathscr{P}_1, \ldots, \mathscr{P}_n$ de la formule $\mathscr{F}$ à partir de la théorie Γ, alors $\Gamma \vDash \mathscr{F}$.

- Au rang $n = 1$:

— Si $\mathscr{F}$ appartient à Γ, alors $\Gamma \vDash \mathscr{F}$.

— Si $\mathscr{F}$ est un axiome associé à un connecteur, $\mathscr{F}$ est une tautologie donc est universellement valide : $\vDash \mathscr{F}$ (et par conséquent $\Gamma \vDash \mathscr{F}$).

— Si $\mathscr{F}$ est l'axiome AU_1 : prouvons que pour tout terme t

$$\forall x \mathscr{F} \vDash \mathscr{F}(t/x)$$

On considère une structure $\mathscr{M}$ et une assignation A telles que $\mathscr{M} \vDash_A \forall x \mathscr{F}$. Par définition de $\forall$, la x-variante A' de A telle que $A'(x) = V_A(t)$ est telle que

$$\mathscr{M} \vDash_{A'} \mathscr{F}$$

et on a vu (métathéorème 4.8.27, p. 163) que cela équivaut à

$$\mathscr{M} \vDash_A \mathscr{F}(t/x)$$

On en déduit

$$\forall x \mathscr{F} \vDash \mathscr{F}(t/x)$$

et d'après le théorème de déduction

$$\vDash \forall x \mathscr{F} \Longrightarrow \mathscr{F}(t/x)$$

— Si $\mathscr{F}$ est l'axiome AU_2 : nous avons déjà vu (métathéorème 4.10.17, p. 197) que si x est libre dans $\mathscr{F}$

$$\forall x, (\mathscr{F} \Longrightarrow \mathscr{G}) \equiv \mathscr{F} \Longrightarrow (\forall x \mathscr{G})$$

donc a fortiori

$$\forall x, (\mathscr{F} \Longrightarrow \mathscr{G}) \vDash \mathscr{F} \Longrightarrow (\forall x \mathscr{G})$$

ce qui équivaut à

$$\vDash \forall x, (\mathscr{F} \Longrightarrow \mathscr{G}) \Longrightarrow (\mathscr{F} \Longrightarrow \forall x \mathscr{G})$$

— Si $\mathscr{F}$ est l'axiome AE_1 : prouvons

$$\mathscr{F}(t/x) \vDash \exists x \mathscr{F}$$

On considère une structure $\mathscr{M}$ et une assignation A telle que $\mathscr{M} \vDash_A \mathscr{F}(t/x)$. On a vu que la x-variante A' de A telle que $A'(x) = V_A(t)$ est telle que

$$\mathscr{M} \vDash_{A'} \mathscr{F}$$

Donc par définition de $\exists$

$$\mathscr{M} \vDash_A \exists x \mathscr{F}$$

On en déduit

$$\mathscr{F}(t/x) \vDash \exists x \mathscr{F}$$

et d'après le théorème de déduction

$$\vDash \mathscr{F}(t/x) \Longrightarrow \exists x \mathscr{F}$$

— Si $\mathscr{F}$ est l'axiome AE_2 : nous avons déjà vu que si x est libre dans $\mathscr{F}$

$$\forall x, (\mathscr{G} \Longrightarrow \mathscr{F}) \equiv \exists x \mathscr{G} \Longrightarrow \mathscr{F}$$

donc a fortiori

$$\forall x, (\mathscr{G} \Longrightarrow \mathscr{F}) \vDash \exists x \mathscr{G} \Longrightarrow \mathscr{F}$$

ce qui équivaut à

$$\vDash \forall x, (\mathscr{G} \Longrightarrow \mathscr{F}) \Longrightarrow (\exists x \mathscr{G} \Longrightarrow \mathscr{F})$$

— Si $\mathscr{F}$ est l'axiome AEg_1 : prouvons

$$\vDash \forall x, x = x$$

On considère une structure $\mathscr{M}$ et une assignation A quelconque. On a

$$V_A(x) = V_A(x)$$

(égalité dans la métathéorie) donc

$$\vDash_A x = x$$

On en déduit

$$\vDash x = x$$

et par généralisation

$$\vDash \forall x, x = x$$

Ces pages ne sont pas incluses dans l’aperçu.

Chapitre 8

Exemples de théories axiomatiques en logique des prédicats

8.1 Relations d'ordre

Définition 8.1.1 (Relation d'ordre)
On appelle *relation d'ordre* toute relation binaire $\leqslant$ vérifiant les axiomes suivants :

1. Réflexivité : pour tout x
$$x \leqslant x$$
2. Antisymétrie : pour tout x, y
$$(x \leqslant y \text{ et } y \leqslant x) \implies x = y$$
3. Transitivité : pour tout x, y, z
$$(x \leqslant y \text{ et } y \leqslant z) \implies x \leqslant z$$

On appelle *ensemble ordonné* tout modèle E des axiomes précédents, dans le langage de signature $\{\leqslant\}$. On peut le noter $(E, \leqslant)$, ou uniquement E s'il n'y a pas ambiguïté. On note aussi

$$x \not\leqslant y \stackrel{\text{def}}{\equiv} \neg(x \leqslant y)$$
$$x \leqslant y \leqslant z \stackrel{\text{def}}{\equiv} x \leqslant y \text{ et } y \leqslant z$$

Définition 8.1.2 (Ordre total)
On appelle relation d'*ordre total* toute relation d'ordre telle que tous les éléments soient *comparables*, c'est-à-dire que l'on ajoute l'axiome suivant : pour tout x et y

$$x \leqslant y \text{ ou } y \leqslant x$$

ce qui équivaut aussi à

$$x \not\leqslant y \implies y \leqslant x$$

Définition 8.1.3 (Relation de préordre)
On appelle *relation de préordre* toute relation binaire $\leqslant$ vérifiant les axiomes suivants :

1. Réflexivité : pour tout x
$$x \leqslant x$$
2. Transitivité : pour tout x, y, z
$$(x \leqslant y \text{ et } y \leqslant z) \implies x \leqslant z$$

On appelle *ensemble préordonné* tout modèle E des axiomes précédents, dans le langage de signature $\{\leqslant\}$.

Remarque 8.1.4 : Une relation d'ordre est donc une relation de préordre antisymétrique.

Remarque 8.1.5 (Notations) : Je rappelle que je peux utiliser indifféremment « et » et $\wedge$ pour noter le symbole de conjonction (de même, je peux utiliser « ou » et $\vee$ pour noter le symbole de disjonction). Dans ce chapitre qui ne traite pas de logique pure mais qui est une application à l'expression formelle de théories mathématiques, ce sont plutôt les termes « et » et « ou » qui seront privilégiés.

Remarque 8.1.6 : J'introduis les axiomes précédents par des expressions comme « pour tout x, y, z » pour signifier que l'on prend la clôture universelle des trois formules, c'est-à-dire qu'on rajoute devant chacune des formules un quantificateur universel pour chaque variable libre. Autrement dit, la forme complète des trois axiomes pour une relation d'ordre, sans variable libre, est

$$\begin{cases} \forall x, x \leqslant x \\ \forall x\ y, ((x \leqslant y \text{ et } y \leqslant x) \implies x = y) \\ \forall x\ y\ z, ((x \leqslant y \text{ et } y \leqslant z) \implies x \leqslant z) \end{cases}$$

Je pourrai dans la suite procéder de la même façon sans plus de précision.

Remarque 8.1.7 (Vocabulaire) : Lorsque $x \leqslant y$, on peut dire que x est *plus petit* que y, ou que y est *plus grand* que x, ou que x est *inférieur* (ou *inférieur ou égal*) à y, ou que y est *supérieur* (ou *supérieur ou égal*) à x. On trouve aussi, pour décrire cette situation, les expressions « x minore y » et « y majore x », mais ces termes sont ambigus, car on dit aussi que x *minore* l'ensemble A quand x est inférieur à tous les éléments de A, et que x *majore* l'ensemble A quand x est supérieur à tous les éléments de A.

Remarque 8.1.8 (Vocabulaire) : On trouve aussi le terme *ordre linéaire* à la place de *ordre total*.

Remarque 8.1.9 (Vocabulaire) : On appelle parfois *relation d'ordre partiel* une relation d'ordre qui n'est pas une relation d'ordre total. Mais ce vocabulaire peut être source de confusion, sachant qu'en anglais, on appelle généralement *partial order* (relation d'ordre partiel) toute relation d'ordre, et *partially ordered set* (ensemble partiellement ordonné) ou *poset*, tout ensemble muni d'une relation d'ordre (qui peut être un ordre total ou pas). Il semble que certains francophones utilisent l'anglicisme *poset* ; cet usage est très minoritaire, mais curieusement il a existé pendant longtemps une page Wikipédia (en français) dénommée *poset*, au lieu du beaucoup plus classique *ensemble ordonné* [1].

Remarque 8.1.10 : On peut remarquer qu'une relation binaire vérifiant la formule

$$\forall x\ y, (x \leqslant y \text{ ou } y \leqslant x)$$

1. Cette page, créée en 2008, a été renommée *ensemble partiellement ordonné* en 2018, ce qui est un peu mieux, mais n'est pas encore complètement cohérent (à partir du moment où l'on munit un ensemble d'une *relation d'ordre*, il est plus logique de le dénommer *ensemble ordonné* que *ensemble partiellement ordonné*).

Ces pages ne sont pas incluses dans l’aperçu.

Remarque 8.1.47 : $(\mathbb{Q}, <)$ et $(\mathbb{R}, <)$ sont des modèles de cette théorie. Puisqu'elle est complète, cela signifie en particulier qu'ils satisfont les mêmes énoncés. Autrement dit, toute formule close de la logique des prédicats sur la signature $\{<\}$ est vraie dans $\mathbb{Q}$ si et seulement si elle est vraie dans $\mathbb{R}$. Les propriétés de $<$ qui sont différentes dans $\mathbb{Q}$ et dans $\mathbb{R}$ ne sont donc pas exprimables par une formule du premier ordre, portant sur les éléments des ensembles (par exemple, le fait que toute partie non vide majorée de $\mathbb{R}$ possède une borne supérieure, qui est une propriété faisant intervenir des sous-ensembles de $\mathbb{R}$).

8.2 Monoïdes et groupes

Définition 8.2.1 (Commutativité, associativité)
On considère un langage disposant d'une opération binaire $*$.

1. On dit que les éléments x et y *commutent* lorsque
$$x * y = y * x$$
2. On dit que l'opération est *commutative* lorsque tous les éléments commutent, c'est-à-dire lorsque pour tout x et y
$$x * y = y * x$$
3. On dit que l'opération est *associative* lorsque pour tout x, y, z
$$(x * y) * z = x * (y * z)$$

Définition 8.2.2 (Monoïde)
On appelle *monoïde* tout modèle des axiomes suivants, dans le langage de signature $\{*, e\}$:

1. Associativité de $*$: pour tout x, y, z
$$(x * y) * z = x * (y * z)$$
2. e est élément neutre : pour tout x
$$x * e = e * x = x$$

Définition 8.2.3 (Monoïde commutatif)
On appelle *monoïde commutatif* tout monoïde dont la loi est commutative, autrement dit tel que pour tout x et y
$$x * y = y * x$$

Remarque 8.2.4 : L'élément neutre d'un monoïde est unique : en effet, si deux éléments e et e' vérifient la définition de l'élément neutre, alors

$$\begin{aligned} e &= e * e' && \text{(car } e' \text{ est élément neutre)} \\ &= e' && \text{(car } e \text{ est élément neutre)} \end{aligned}$$

Remarque 8.2.5 (Notations) : Dans un monoïde, puisque l'opération * est associative, on peut écrire sans ambiguïté

$$x * y * z$$

qui représente indifféremment $(x * y) * z$, ou $x * (y * z)$. De manière générale, si l'opération binaire $*$ est associative, une expression de la forme

$$x_1 * x_2 * \cdots * x_n$$

ne dépend pas de la façon dont sont placées les parenthèses. Par exemple

$$\begin{aligned}(x_1 * x_2) * (x_3 * x_4) &= x_1 * (x_2 * (x_3 * x_4)) \\ &= x_1 * ((x_2 * x_3) * x_4)\end{aligned}$$

et de même

$$\begin{aligned}(x_1 * x_2) * (x_3 * x_4) &= ((x_1 * x_2) * x_3) * x_4 \\ &= (x_1 * (x_2 * x_3)) * x_4\end{aligned}$$

Donc

$$(x_1 * x_2) * (x_3 * x_4) = x_1 * (x_2 * x_3 * x_4) = (x_1 * x_2 * x_3) * x_4 = x_1 * (x_2 * x_3) * x_4$$

Justifions le cas général (de manière informelle) par récurrence forte (dans la métathéorie) sur n :

- Si $n = 3$, les deux façons de placer les parenthèses sont

  $$(x_1 * x_2) * x_3 \qquad \text{et} \qquad x_1 * (x_2 * x_3)$$

  et on a par associativité

  $$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$$

- On fait l'hypothèse de récurrence que pour tout $p \leqslant n$ (avec $p \geqslant 3$) une expression de la forme « $x_1 * \cdots * x_p$ » ne dépend pas de la façon dont sont placées les parenthèses. Dans une expression de la forme

  $$(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n * x_{n+1})$$

  le calcul de chacune des deux parenthèses ne dépend pas de la façon dont sont placées les autres parenthèses (par hypothèse de récurrence). Il reste à justifier que le résultat ne dépend pas de k : en effet en utilisant l'associativité et l'hypothèse de récurrence

  $$\begin{aligned}&(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n * x_{n+1}) \\ &= (x_1 * \cdots * x_k) * ((x_{k+1} * \cdots * x_n) * x_{n+1}) && \text{par hypothèse de récurrence} \\ &= ((x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n)) * x_{n+1} && \text{par associativité} \\ &= (x_1 * \cdots * x_n) * x_{n+1} && \text{par hypothèse de récurrence}\end{aligned}$$

Remarque 8.2.6 (Notations) : Un monoïde est caractérisé par un ensemble de base E, une opération binaire $*$ et un élément particulier e, ce que l'on peut noter par le triplet $(E, *, e)$. Mais on peut aussi, par abus de notation, et selon le contexte, le noter uniquement $(E, *)$, voire juste E, s'il n'y a pas d'ambiguïté.

Remarque 8.2.7 (Vocabulaire et notations) :

1. Quand on utilise le symbole $\times$ à la place de $*$, l'opération binaire s'appelle une *multiplication* et le résultat de la multiplication un *produit*. L'élément neutre se note alors souvent 1.

2. Quand on utilise le symbole + à la place de $*$, l'opération binaire s'appelle une *addition* et le résultat de l'addition une *somme*. L'élément neutre se note alors souvent 0. La notation additive (+) est en général réservée au cas où l'opération est commutative.

L'origine de ces deux symboles particuliers est traitée dans la section 8.4.

Remarque 8.2.8 (Notations) : Si l'opération n'est pas additive, et s'il n'y a pas d'ambiguïté, on peut la noter par un point ($x \cdot y$) ou même sans aucun symbole par simple juxtaposition des termes : on note alors xy pour $x * y$. C'est cette convention que j'emploierai le plus souvent.

Exemple 8.2.9 (Ensembles de nombres usuels)

1. L'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des entiers relatifs $\mathbb{Z}$, l'ensemble des rationnels $\mathbb{Q}$, l'ensemble des réels $\mathbb{R}$, l'ensemble des complexes $\mathbb{C}$, munis de leur addition usuelle, sont des monoïdes commutatifs, d'élément neutre 0.
2. L'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des entiers relatifs $\mathbb{Z}$, l'ensemble des rationnels $\mathbb{Q}$, l'ensemble des réels $\mathbb{R}$, l'ensemble des complexes $\mathbb{C}$, munis de leur multiplication usuelle, sont des monoïdes commutatifs, d'élément neutre 1.
3. L'ensemble $\mathbb{Z}$ des entiers relatifs muni de la soustraction ne peut pas être un monoïde, puisque cette opération n'est pas associative : en général
$$x - (y - z) \neq (x - y) - z$$
Cette opération n'est pas non plus commutative puisqu'en général
$$x - y \neq y - x$$
4. L'ensemble des entiers naturels $\mathbb{N}$ muni de l'opération
$$x * y = x^y$$
ne peut pas être un monoïde, puisque cette opération n'est pas associative : par exemple
$$2^{(2^3)} = 2^8 = 256$$
mais
$$(2^2)^3 = 4^3 = 64$$
5. L'ensemble $\{-1, 1\}$, muni de la multiplication usuelle sur $\mathbb{Z}$, est un monoïde commutatif d'élément neutre 1.
6. L'ensemble $\mathbb{U}$ des nombres complexes de module 1, muni de la multiplication, est un monoïde commutatif d'élément neutre 1.
7. L'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité (nombres complexes z tels que $z^n = 1$), muni de la multiplication, est un monoïde commutatif d'élément neutre 1.
8. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n munis de l'addition (avec $n > 1$), est un monoïde commutatif d'élément neutre 0.
9. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n munis de la multiplication (avec $n > 1$), est un monoïde commutatif d'élément neutre 1.

Exemple 8.2.10 (Ensembles de fonctions)

1. L'ensemble des fonctions d'un ensemble E dans lui-même, muni de la composition des fonctions $\circ$, est un monoïde non commutatif, d'élément neutre la fonction identité ($x \mapsto x$).
2. L'ensemble des permutations d'un ensemble E (les bijections de E dans E), muni de la composition des fonctions $\circ$, est un monoïde non commutatif, d'élément neutre la fonction identité ($x \mapsto x$).

Exemple 8.2.11 (Ensembles d'ensembles)

On peut munir $\mathscr{P}(E)$, ensemble des sous-ensembles de E, de différentes opérations :

1. $\mathscr{P}(E)$ muni de la réunion $\cup$, est un monoïde commutatif, d'élément neutre $\varnothing$.
2. $\mathscr{P}(E)$ muni de l'intersection $\cap$, est un monoïde commutatif, d'élément neutre E.
3. $\mathscr{P}(E)$ muni de la différence symétrique Δ :

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

est un monoïde commutatif, d'élément neutre $\varnothing$.

Exemple 8.2.12 (Géométrie)

1.

L'ensemble des isométries du plan (les transformations qui conservent les longueurs) laissant invariant un triangle équilatéral ABC, muni de la composition $\circ$, est un monoïde non commutatif, d'élément neutre l'identité. Les 6 éléments de ce monoïde sont (en notant O le centre du triangle)

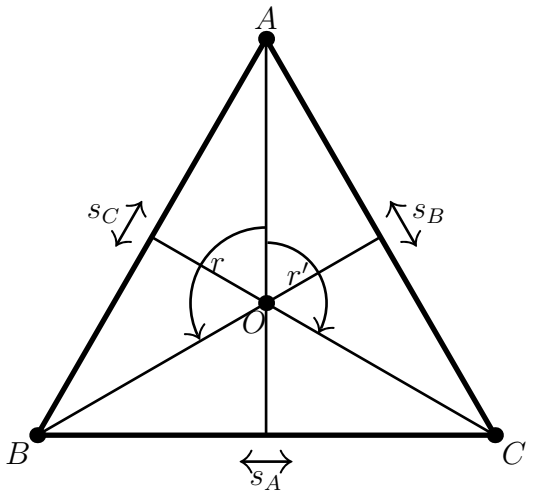


FIGURE 8.1 – Isométries du plan laissant invariant un triangle équilatéral.

- L'identité id.
- La rotation r de centre O et d'angle 120° dans le sens inverse des aiguilles d'une montre (sens trigonométrique).
- La rotation r' de centre O et d'angle 120° dans le sens des aiguilles d'une montre.
- La symétrie orthogonale (ou réflexion) s_A par rapport à la médiatrice du segment $[BC]$.
- La symétrie orthogonale (ou réflexion) s_B par rapport à la médiatrice du segment $[AC]$.
- La symétrie orthogonale (ou réflexion) s_C par rapport à la médiatrice du segment $[AB]$.

Ces pages ne sont pas incluses dans l’aperçu.

8.4 Anneaux et corps

Définition 8.4.1 (Anneau)
On appelle *anneau* tout ensemble A, muni d'une addition $+$ et d'une constante 0 telles que $(A, +, 0)$ soit un groupe commutatif, muni d'une multiplication $\times$ et d'une constante 1 telles que $(A, \times, 1)$ soit un monoïde, et tel que la multiplication soit distributive sur l'addition. Un anneau est donc un modèle des axiomes suivants, dans le langage de signature $\{+, \times, 0, 1\}$:

1. Associativité de l'addition et de la multiplication : pour tout x, y, z

$$(x + y) + z = x + (y + z)$$
$$(x \times y) \times z = x \times (y \times z)$$

2. Commutativité de l'addition : pour tout x, y

$$x + y = y + x$$

3. Distributivité de la multiplication sur l'addition : pour tout x, y, z

$$x \times (y + z) = x \times y + x \times z$$
$$(y + z) \times x = y \times x + z \times x$$

4. Élément neutre pour l'addition et la multiplication : pour tout x

$$x + 0 = 0 + x = x$$
$$x \times 1 = 1 \times x = x$$

5. Tout élément admet un opposé (un symétrique pour l'addition) :

$$\forall x \exists x', x' + x = x + x' = 0$$

De plus l'opposé de x est unique (propriété d'un monoïde) ; on le note $-x$.

Définition 8.4.2 (Anneau commutatif)
On appelle *anneau commutatif* tout anneau dans lequel la multiplication est commutative.

Remarque 8.4.3 : Puisque dans un anneau tout élément admet un opposé, on peut aussi définir de façon équivalente un anneau dans le langage de signature $(+, \times, -, 0, 1)$, en remplaçant l'axiome 5 (pour l'opposé) par :

$-x$ est l'opposé de x : pour tout x

$$(-x) + x = x + (-x) = 0$$

Remarque 8.4.4 (Notations) : Dans un anneau, comme précédemment dans un monoïde, la multiplication peut aussi souvent se noter $x \cdot y$ à la place de $x \times y$, ou directement sans symbole (xy). Ce raccourci n'est par contre pas employé avec le symbole $+$.

Remarque 8.4.5 (Notations) : Dans les axiomes précédents, les symboles 0 et 1 représentent respectivement l'élément neutre pour l'addition, et l'élément neutre pour la multiplication, dans un anneau A, et pas nécessairement les entiers naturels 0 et 1. En cas d'ambiguïté, on peut les noter respectivement 0_A et 1_A. Par exemple, si A est l'anneau des matrices réelles 2×2, 0_A représente la matrice $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, et 1_A représente la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. De même, d'autres symboles que $\times$ et $+$ peuvent être employés (voir plus loin les exemples d'anneaux).

Remarque 8.4.6 (Vocabulaire) : Pour certains auteurs, l'élément neutre pour la multiplication n'est pas inclus dans la définition d'un anneau, et on peut faire alors la distinction avec ce qu'on appelle un *anneau unitaire* ou *anneau unifère*, dans lequel il existe un tel élément.

Remarque 8.4.7 (Origine des notations) : L'origine du symbole $+$ serait une abréviation du mot latin *et* ; celle du symbole $-$ est plus incertaine, de nombreuses explications ayant été avancées, mais sans preuve. On trouve le symbole $+$ comme abréviation de *et* dans un manuscrit de *Algorismus proportionum*, du mathématicien Nicole (ou Nicolas) Oresme (v. 1320-1382), qui daterait du XIV^{e} siècle, mais il est possible que ce soit l'œuvre d'un copiste. L'abréviation $+$ pour le mot *et* est par ailleurs avérée dans un manuscrit latin de 1417. La première apparition dans un ouvrage imprimé des symboles $+$ et $-$ se produit en 1489, dans *Mercantile Arithmetic or Behende und hüpsche Rechenung auff allen Kauffmanschafft*, du mathématicien allemand Johannes Widmann (v. 1460-v. 1500). Dans cet ouvrage, ils ne désignent pas les opérations arithmétiques, mais des bénéfices ou des déficits dans des problèmes commerciaux, et sont aussi utilisés pour d'autres usages ($+$ à la place de *et*, $-$ comme séparateur). Il est probable que Widmann ait emprunté ces notations à des manuscrits datant des années 1480, dans lesquels elles apparaissent comme symboles d'opérations. On retrouve ensuite les symboles $+$ et $-$, toujours dans leur sens moderne (comme symboles d'opérations), dans *Een sonderlinghe boeck in dye edel conste Arithmetica* publié en 1514 par Giel Vander Hoecke, et dans *Ayn new Kunstlich Buech* publié en 1518 par Henricus Grammateus.

Vers la même époque (à la fin du XV^{e} siècle) ont aussi été introduits les symboles concurrents $\bar{p}$ (pour plus) et $\tilde{m}$ (pour moins), originaires d'Italie. Les symboles actuels $+$ et $-$ ont été progressivement utilisés par la communauté mathématique, en particulier après leur adoption en 1557 en Angleterre par le mathématicien et médecin Robert Recorde (v. 1510-1558), et en France par le logicien et philosophe Pierre de la Ramée (v. 1515-1572) et le mathématicien François Viète (1540-1603).

Remarque 8.4.8 (Origine des notations) : Le symbole $\times$ pour noter la multiplication apparaît en 1631 dans *Clavis Mathematicae* [La clé des mathématiques], du mathématicien et théologien anglais William Oughtred (1574-1660), et en 1618 dans une annexe anonyme de la traduction par Edward Wright de *Descriptio*, du mathématicien, physicien et astronome John Napier (ou Neper) (1550-1617), annexe probablement rédigée par Oughtred. Auparavant, le symbole $\times$ était utilisé dans des textes mathématiques, mais avec d'autres sens.

Le point comme symbole de multiplication a été introduit par le philosophe et mathématicien Gottfried Wilhelm Leibniz (1646-1716). Il écrit le 29 juillet 1698 au mathématicien suisse Jean Bernoulli (1667-1748) :

> « Je n'aime pas $\times$ comme symbole pour la multiplication, car on peut le confondre facilement avec x [...] je relie souvent simplement deux quantités par un point intercalaire et j'indique une multiplication par $ZC \cdot LM$. »[11]

On peut aussi trouver le symbole du point dans des ouvrages antérieurs, *Analyticae Praxis ad Aequationes Algebraicas Resolvendas* du mathématicien et astronome anglais Thomas Harriot (1560-1621), publié à titre posthume en 1631, et *Syntaxis mathematica* de Thomas Gibson, en 1655, mais il n'est pas sûr qu'ils l'utilisaient véritablement comme symbole de multiplication (plutôt comme séparateur après un coefficient). L'adoption en Europe du point comme symbole de multiplication est due en grande partie au philosophe

11. Cité par : Florian CAJORI. *A history of mathematical notations*. The Open Court Publishing Co., 1928-1929 (vol 1, p267).

Ces pages ne sont pas incluses dans l’aperçu.

La théorie de l'arithmétique de Peano du premier ordre, que l'on note PA, utilise le langage du premier ordre L_{PA} , de signature $\{0, S, +, \times\}$, avec S symbole d'opération unaire (opération *successeur*), et avec les axiomes suivants :

Axiome 9.2.1 (Axiomes de la théorie de l'arithmétique de Peano)

1. 0 n'est pas successeur : pour tout x
$$Sx \neq 0$$
2. S est injective : pour tout x et y
$$Sx = Sy \implies x = y$$
ce qui équivaut aussi, par contraposition, à
$$x \neq y \implies Sx \neq Sy$$
3. Schéma d'axiomes de récurrence du premier ordre. Soit $\mathscr{P}[x, \vec{a}]$ une formule. Pour tout $\vec{a}$
$$\text{si} \quad \begin{cases} \mathscr{P}(0) \\ \forall x, (\mathscr{P}(x) \implies \mathscr{P}(Sx)) \end{cases}$$
$$\text{alors} \quad \forall x \mathscr{P}(x)$$
4. Définition de l'addition (1) : pour tout x
$$x + 0 = x$$
5. Définition de l'addition (2) : pour tout x et y
$$x + Sy = S(x + y)$$
6. Définition de la multiplication (1) : pour tout x
$$x \times 0 = 0$$
7. Définition de la multiplication (2) : pour tout x et y
$$x \times Sy = (x \times y) + x$$

Remarque 9.2.2 (Notations) : La multiplication peut aussi se noter $x \cdot y$ à la place de $x \times y$, ou encore directement sans symbole (xy).

Remarque 9.2.3 (Notations) : Par convention, la multiplication est prioritaire sur l'addition. Par exemple,
$$x + y \times z \quad \text{signifie} \quad x + (y \times z)$$

Remarque 9.2.4 (Origine du vocabulaire) : *Arithmétique* vient du grec *arithmos* (nombre), qui a donné *arithmétiké* en grec et *arithmetica* en latin, la science du nombre. L'arithmétique désigne traditionnellement la branche des mathématiques qui consiste en l'étude des propriétés des opérations usuelles entre nombres (addition, soustraction, multiplication, division). Elle peut être considérée comme une partie élémentaire de la *théorie des nombres*, théorie qui consiste essentiellement en l'étude des nombres entiers (entiers naturels et entiers relatifs), comme par exemple l'étude des nombres premiers ou des équations diophantiennes. Les

Ces pages ne sont pas incluses dans l’aperçu.

- Prouvons $\mathscr{P}(0)$: d'après les axiomes 4 et 6

$$\begin{cases} (y+z)\times 0 = 0 \\ y\times 0 + z\times 0 = 0+0 = 0 \end{cases} \qquad \text{donc} \qquad (y+z)\times 0 = y\times 0 + z\times 0$$

- On fait l'hypothèse de récurrence $\mathscr{P}(x)$.

$$\begin{aligned} (y+z)\times Sx &= (y+z)\times x + (y+z) && \text{d'après l'axiome 7} \\ &= (y\times x + z\times x) + (y+z) && \text{par hypothèse de récurrence} \\ &= (y\times x + y) + (z\times x + z) && \text{par commutativité et associativité de l'addition} \\ &= y\times Sx + z\times Sx && \text{d'après l'axiome 7} \end{aligned}$$

On en déduit par récurrence

$$\forall x\ y\ z, (y+z)\times x = y\times x + z\times x$$

Théorème 9.2.12 (Monoïde commutatif pour la multiplication)
Tout modèle de l'arithmétique de Peano est un monoïde commutatif pour la multiplication, d'élément neutre 1, et tel que 0 soit élément absorbant, autrement dit les propriétés suivantes sont vérifiées :

1. Associativité : pour tout x, y, z
$$(x\times y)\times z = x\times(y\times z)$$
2. 1 est élément neutre : pour tout x
$$x\times 1 = 1\times x = x$$
3. 0 est élément absorbant : pour tout x
$$x\times 0 = 0\times x = 0$$
4. Commutativité : pour tout x, y
$$x\times y = y\times x$$

Preuve

1. Associativité : vérifions par récurrence sur z la formule

$$\mathscr{P}[z,x,y] :\equiv (x\times y)\times z = x\times(y\times z)$$

- Prouvons $\mathscr{P}(0)$: d'après l'axiome 6

$$\begin{cases} (x\times y)\times 0 &= 0 \\ x\times(y\times 0) &= x\times 0 = 0 \end{cases} \qquad \text{donc} \qquad (x\times y)\times 0 = x\times(y\times 0)$$

- On fait l'hypothèse de récurrence $\mathscr{P}(z)$.

$$\begin{aligned} (x\times y)\times Sz &= (x\times y)\times z + x\times y && \text{d'après l'axiome 7} \\ &= x\times(y\times z) + x\times y && \text{par hypothèse de récurrence} \\ &= x\times((y\times z)+y) && \text{par distributivité de la multiplication sur l'addition} \\ &= x\times(y\times Sz) && \text{d'après l'axiome 7} \end{aligned}$$

On en déduit par récurrence

$$\forall x\ y\ z, (x\times y)\times z = x\times(y\times z)$$

2. Élément neutre :

$$x\times 1 = x\times S0 \qquad \text{par définition de 1}$$

Ces pages ne sont pas incluses dans l’aperçu.

Théorème 9.3.9 (Relation d'ordre et successeur)

1. Pour tout x et y

$$x \leqslant y \iff Sx \leqslant Sy$$
$$x < y \iff Sx < Sy$$

2. Pour tout x

$$x < Sx$$

Plus précisément :

- Sx est le plus petit des éléments strictement supérieurs à x : pour tout x et y

$$x < y \iff Sx \leqslant y$$

- x est le plus grand des éléments strictement inférieurs à Sx : pour tout x et y

$$y < Sx \iff y \leqslant x$$

Preuve

1.

- Si $x \leqslant y$, il existe z tel que $y = x + z$ donc

$$y + 1 = x + 1 + z$$
$$Sy = Sx + z$$
$$Sx \leqslant Sy$$

Réciproquement, si $Sx \leqslant Sy$, alors il existe z tel que

$$y + 1 = x + 1 + z$$

donc par régularité de l'addition,

$$y = x + z$$
$$x \leqslant y$$

- On a

$$x < y \equiv (x \leqslant y \text{ et } x \neq y) \equiv (Sx \leqslant Sy \text{ et } x \neq y)$$

Et puisque

$$x \neq y \iff Sx \neq Sy$$

On en déduit

$$x < y \iff Sx < Sy$$

2. Nous avons vu que

$$x < y \iff \exists z, (y = x + z \text{ et } z \neq 0)$$

donc $x < Sx$, puisque $Sx = x + 1$ et $1 \neq 0$.

- Si $Sx \leqslant y$, il existe z tel que

$$y = Sx + z = x + 1 + z = x + (z + 1)$$

avec $z + 1 \neq 0$, donc $x < y$. Réciproquement, si $x < y$, alors il existe z tel que

$$y = x + Sz = x + (z + 1) = (x + 1) + z = Sx + z$$

donc $Sx \leqslant y$.

- Si $y \leqslant x$ alors puisque $x < Sx$ on en déduit

$$y < Sx$$

Ces pages ne sont pas incluses dans l’aperçu.

Liste des figures

Liste des tableaux

Liste des symboles

$=$	Égalité logique entre deux objets identiques, page 5
$\overset{\text{def}}{=}$	Égalité par définition, page 5
$:\equiv$	Égalité par affectation, page 6
$\equiv$	Équivalence sémantique (logique des propositions), page 65
$\equiv_\Gamma$	Équivalence sémantique dans le contexte Γ (logique des propositions), page 77
$\equiv$	Équivalence sémantique (logique des prédicats), page 172
$\equiv_\Gamma$	Équivalence sémantique dans le contexte Γ (logique des prédicats), page 183
$\equiv$	Équivalence syntaxique, page 209
$\equiv_\Gamma$	Équivalence syntaxique dans le contexte Γ, page 209
$\neg$	Connecteur logique pour la négation, page 32
$\wedge$	Connecteur logique pour la conjonction (*et*), page 33
$\vee$	Connecteur logique pour la disjonction (*ou*), page 35
$\Longrightarrow$	Connecteur logique pour l'implication, page 37
$\Longleftrightarrow$	Connecteur logique pour l'équivalence, page 39
$\uparrow$	Connecteur logique NON-ET, ou NAND, négation du connecteur logique conjonction (et), page 40
$\downarrow$	Connecteur logique NON-OU, ou NOR, négation du connecteur disjonction (ou), page 41
$\oplus$	Connecteur logique ou exclusif (OUX, ou XOR), négation du connecteur logique équivalence, page 41
$>$	Connecteur logique non-implication (inhibition), négation du connecteur logique implication, page 41
$\bot$	Contradiction : proposition toujours fausse quelles que soient les valeurs de vérité prises par les propositions atomiques intervenant dans sa construction, page 62
$\top$	Tautologie : proposition toujours vraie quelles que soient les valeurs de vérité prises par les propositions atomiques intervenant dans sa construction, page 62
$\forall$	Quantificateur universel : quel que soit, page 134
$\exists$	Quantificateur existentiel : il existe, page 134
$\exists!x$	Il existe un unique x tel que …, page 312

$\models P$	P est une tautologie (logique des propositions), page 61
$\models \mathscr{F}$	$\mathscr{F}$ est une formule valide (logique des prédicats), page 166
$v \models \Gamma$	La valuation v est un modèle de Γ (logique des propositions), page 72
$\mathscr{M} \models \Gamma$	La L-structure $\mathscr{M}$ est un modèle de Γ (logique des prédicats), page 174
$\Gamma \models P$	P est une conséquence sémantique de Γ (logique des propositions), page 73
$\Gamma \models \mathscr{F}$	$\mathscr{F}$ est une conséquence sémantique de Γ (logique des prédicats), page 174
$\Gamma \vdash \mathscr{F}$	$\mathscr{F}$ est une conséquence syntaxique de Γ, Γ prouve $\mathscr{F}$ (logique des propositions et des prédicats), page 206
$\mathscr{F}(t/x)$	Formule $\mathscr{F}$ dans laquelle le terme t remplace la variable x, page 154
$\mathscr{F}[x_1, \ldots, x_n]$	Formule $\mathscr{F}$ dont les variables libres sont à prendre parmi $x_1, \ldots, x_n$, page 156
$\vec{x}$	Liste de variables $x_1, \ldots, x_n$, pour un entier n indéterminé, page 135
$\mathbb{B}$	Ensemble à deux éléments : $\mathbb{B} = \{0, 1\}$, page 111
$\lvert x \rvert$	Valeur absolue de x (dans un anneau totalement ordonné) : $\lvert x \rvert \stackrel{\text{def}}{=} \max(x, -x)$, page 448

Index des notions

Index des noms propres