République Algérienne Populaire et Démocratique
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
Université Mustapha Ben Boulaid - BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

Polycopié de cours et des exercices corrigées

LOGIQUE MATHÉMATIQUES

Support destiné aux étudiants de $2^{ème}$ année Licence Mathématiqes
Réalisé le : 11/02/2023

Dr. BENZEGHLI Brahim
Enseignant chercheur au département de mathématiques - Université BATNA 2

Année universitaire 2022 – 2023

Dédicace …

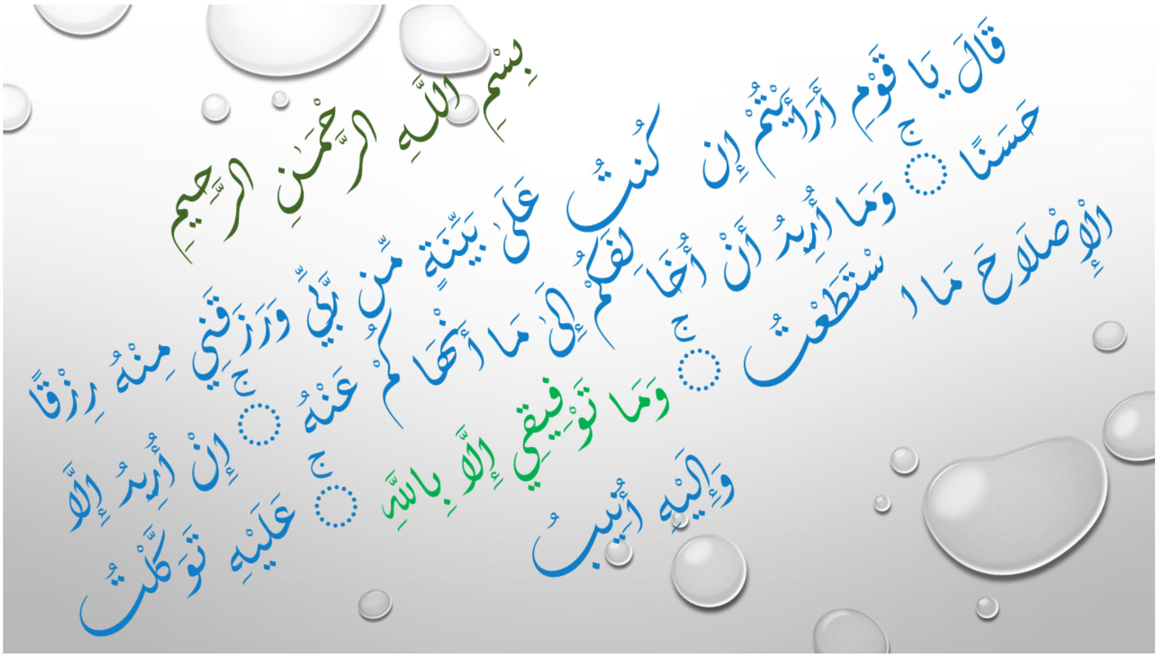

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ
قَالَ يَا قَوْمِ أَرَأَيْتُمْ إِن كُنتُ عَلَىٰ بَيِّنَةٍ مِّن رَّبِّي وَرَزَقَنِي مِنْهُ رِزْقًا حَسَنًا ۚ وَمَا أُرِيدُ أَنْ أُخَالِفَكُمْ إِلَىٰ مَا أَنْهَاكُمْ عَنْهُ ۚ إِنْ أُرِيدُ إِلَّا الْإِصْلَاحَ مَا اسْتَطَعْتُ ۚ وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ ۚ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ

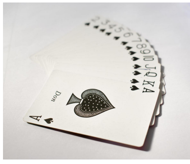
Table des matières

Table des figures

Liste des tableaux

Introduction

Une langue vivante est souvent ambigüe.



Prenons l'exemple de la conjonction "*ou*" ; au cafétéria, dire : « *café ou thé* » signifie l'un ou l'autre mais pas les deux. Par contre si dans un jeu de carte on cherche « *les as ou les piques* » alors il ne faut pas exclure l'as de pique.

Autre exemple : que répondre à la question «*As-tu* 100 *dinars en poche ?*» si l'on dispose de 2500 dinars ? Pour cette raison, il est important d'avoir un langage rigoureux.

Aussi, il y a des notions difficiles à expliquer avec des mots, par exemple : la continuité d'une fonction est souvent expliquée par «*on trace le graphe sans lever la main*». Il est clair que c'est une définition peu satisfaisante. Voici la définition mathématique de la continuité d'une fonction $f : I \to \mathbb{R}$ en un point $x_0 \in I$:

$$\forall \varepsilon > 0, \ \exists \delta > 0, \ \forall x \in I : \ \ (|x - x_0| < \delta \ \ \Rightarrow \ \ |f(x) - f(x_0)| < \varepsilon).$$

C'est le but de ce cours de rendre cette ligne plus claire ! C'est la logique mathématiques.

Historiquement ...

La logique mathématique est née à la fin du $19^{ième}$ siècle au sens philosophique du terme ; elle est devenue l'une des pistes les plus explorées par les mathématiciens de cette époque, afin de résoudre la crise des fondements provoquée par la complexité des mathématiques et la réapparition des paradoxes. Ses débuts sont bien marqués par la rencontre des deux visions nouvelles :

— La fondation axiomiques des mathématiques par *Frege*, *Russell*, *Peano* et *Hilbert* ;

— Le calcul propositionel par les deux valeurs de vérité "**vraie** ou **faux**" par *George Boole* qu'il a utilisé la notion des structures algébriques.

Mais avant ça, il a eu des tentatives de traitement formel des mathématiques, dues à *Leibniz* et *Lambert* entre la fin du $16^{ième}$ siècle et le début du $17^{ième}$ siècle. *Leibniz* a en particulier introduit une grande partie de la notation mathématiques moderne comme *les quantificateurs logiques* et *le symbole d'intégration* "$\int$" et beaucoup d'autres notations.

Le vrai départ de la logique mathématique était à partir du milieu du $19^{ième}$ siècle par les travaux de *George Boole* et ceux d'*Auguste De Morgan* qui ont introduit le calcul de vérité où les combinaisons logiques tels que **la conjonction**,

la disjonction et **l'implication** seront traiter comme des opérations semblable à l'addition et à la multiplication des entiers, mais portant sur les deux valeurs de vérité "**vrai** ou 1" et "**faux** ou 0", ces opérations booléennes se définissent au moyen de tables de vérité.

Le calcul de Boole véhiculait l'idée apparemment paradoxale, mais qui devait s'avérer spectaculaires fructueuse, que le langage logique pouvait se définir mathématiquement et devenir un objet d'étude pour les mathématiciens. Toutefois il ne permettait pas encore de résoudre les problèmes de fondements. Dès lors, nombre de mathématiciens ont cherché à l'étendre au cadre général du raisonnement mathématique et on a vu apparaître les systèmes logiques formalisés ; l'un des premiers est dû à *Frege* au tournant du $20^{ième}$ siècle.

En 1900 au cours d'une très célèbre conférence au congrès international des mathématiciens à Paris, *David Hilbert* a proposé une liste des 23 problèmes [3] non résolus les plus importants des mathématiques de l'époque. Le deuxième était celui de la cohérence de l'arithmétique, c'est-à-dire de démontrer par des moyens fini (et non à l'infini) la non-contradiction des axiomes de l'arithmétique.

Le programme de *Hilbert* a suscité de nombreux travaux en logique dans le premier quart du siècle, notamment le développement de systèmes d'axiomes pour les mathématiques : *les axiomes de Peano* pour l'arithmétique, ceux de *Zermelo* complétés par *Skolem* et *Fraenkel* pour la théorie des ensembles et le développement par *Whitehead* et *Russell* d'un programme de formalisation des mathématiques. C'est également la période où apparaissent les principes fondateurs de la théorie des modèles :

Notion de modèle d'une théorie et théorème de Löwenheim-Skolem.

En 1929 *Kurt Gödel* montre dans sa thèse de doctorat son théorème de complétude qui énonce le succès de l'entreprise de formalisation des mathématiques :

Tout raisonnement mathématique peut en principe être formalisé dans le calcul des prédicats.

Ce théorème a été accueilli comme une avancée notable vers la résolution du programme de *Hilbert*, mais un an plus tard, *Gödel* démontrait le *théorème d'incomplétude* [1] qui montrait irréfutablement l'impossibilité de réaliser ce programme.

Ce résultat négatif n'a toutefois pas arrêté l'essor de la logique mathématique. Les années 1930 ont vu arriver une nouvelle génération de logiciens anglais et américains, notamment *Alonzo Church*, *Alan Turing*, *Stephen Kleene*, *Haskell Curry et Emil Post*, qui ont grandement contribué à la définition de la notion d'algorithme et au développement de la théorie de la complexité algorithmique (théorie de la calculabilité, théorie de la complexité des algorithmes). La théorie de la démonstration de *Hilbert* a également continué à se développer avec les travaux de

1. publié en 1931

Gerhard Gentzen qui a produit la première démonstration de cohérence relative et a initié ainsi un programme de classification des théories axiomatiques.

Le résultat le plus spectaculaire de l'après-guerre est dû à *Paul Cohen* qui démontre en utilisant la méthode du forcing, l'indépendance de l'hypothèse du continu en théorie des ensembles, résolvant ainsi le premier problème de *Hilbert*. Mais la logique mathématique subit également une révolution due à l'apparition de l'informatique ; la découverte de la correspondance de *Curry-Howard*, qui relie les preuves formelles au *lambda-calcul* de *Church* et donne un contenu calculatoire aux démonstrations, va déclencher un vaste programme de recherche.

La logique classique est la première formalisation du langage et du raisonnement mathématique développée à partir de la fin du $19^{ième}$ siècle en logique mathématique. Appelée simplement logique à ses débuts, c'est l'apparition d'autres systèmes logiques formels, notamment pour la logique intuitionniste, qui a suscité l'adjonction de l'adjectif classique au terme logique.

La logique classique est caractérisée par des postulats qui la fondent et la différencient de la logique intuitionniste, exprimés dans le formalisme du calcul des propositions ou du calcul des prédicats. La logique est utilisée en informatique pour modéliser de manière formelle des "objets" rencontrés par les informaticiens ; par exemple : Bases de données, Bases de connaissances, Pré-post conditions d'une procédure, ... etc. l'informaticien doit être capable de se servir du modèle et raisonner sur celui-ci, comme la validation d'un modèle de données, prise de décision à partir des faits et d'une base de connaissances, preuve de correction d'une procédure ou d'un programme. La logique est à la base de l'étude des raisonnements, c'est-à-dire des déductions que l'on peut faire sur les modèles formels.

Le but de ce cours est d'étudier en détail les fondements de la logique classique et de donner aux étudiants une formation suffisante pour qu'ils puissent se familiariser avec d'autres logiques (*intuitionniste* ou *floue*) qu'ils peuvent rencontrer plus tard. Et également les sensibiliser au fait que la logique peut être très utile pour automatiser ou semi-automatiser les tâches de raisonnement rencontrées lors de la construction ou l'analyse de modèles et de programmes.

Les références principales utilisées pour la réalisation de ce cours sont [1], [2], [3], [4], [6], [5] et [7].

Chapitre 1

Les paradoxes (Antinomies)

Ce premier chapitre est donné aux étudiants sous forme de mini projet à faire en binômes et à rendre avant les examens.

1 Le paradoxe de Russel

Le paradoxe de Russell, ou *antinomie de Russell*, est un paradoxe très simple de la théorie des ensembles (*Russell* lui-même parle de théorie des classes, en un sens équivalent), qui a joué un rôle important dans la formalisation de celle-ci. Il fut découvert par *Bertrand Russell* vers 1901 et publié en 1903. Il était en fait déjà connu à *Göttingen*, où il avait été découvert indépendamment par *Ernst Zermelo*, à la même époque, mais ce dernier ne l'a pas publié.

1.1 Biographie de Bertrand Russell

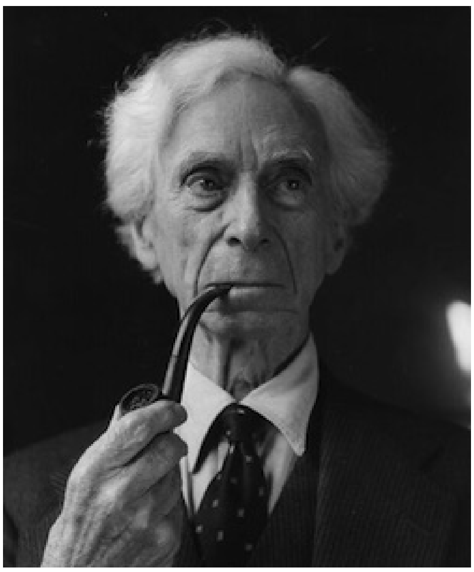


Figure 1.1 – Bertrand Russell

"Tout le problème de ce monde, c'est que les idiots et les fanatiques sont toujours si sûrs d'eux, tandis que les sages sont tellement pleins de doutes."

Né au Pays de Galles, petit fils de premier ministre (*John Russell*), *Bertrand Russell* est considéré comme le fondateur de la logique moderne. Après avoir perdu très tôt ses parents, il trouve dans les mathématiques le moyen de satisfaire ses besoins de certitude.

Avant tout logicien, *Bertrand Russell* conçoit avec *Alfred North Whitehead* un système de logique mathématique s'appuyant sur une analyse abstraite de la pensée (1913). Ses combats pour le pacifisme et pour l'objection de conscience l'obligent à quitter son poste d'enseignant au *Trinity College* et le conduisent en prison à plusieurs reprises.

Puis *Bertrand Russell* se consacre à la philosophie de la connaissance, en étant influencé par *David Hume* et *George Edward Moore*. Il bâtit son propre "*atomisme logique*" qui est une méthode d'analyse des propositions complexes en les ramenant à un système (*atomiste*) de propositions élémentaires. Après avoir tenté sans succès de fonder une école à *Beacon Hill* selon ses convictions sur l'éducation, il gagne sa vie comme écrivain, journaliste et conférencier.

Entre 1938 et 1944, *Bertrand Russell* enseigne aux Etats-Unis avant d'y être interdit d'enseignement en raison de ses positions contre la religion, pour la défense de la liberté sexuelle et pour son anticonformisme.

De retour en Angleterre, *Bertrand Russell* s'oppose farouchement à l'utilisation de l'énergie nucléaire à des fins militaires. Son prix Nobel de littérature en 1950 ne l'empêche pas de continuer ses combats (contre la guerre du Vietnam, "tribunal international" contre les crimes de guerre avec *Jean-Paul Sartre*). Il est même arrêté à l'âge de 89 ans lors d'une manifestation contre la bombe atomique.

Doué de multiples talents, *Bertrand Russell* est également un philosophe, un épistémologiste, un moraliste et un polémiste. Sur le plan politique, il est un militant de gauche, engagé en faveur du pacifisme, de l'humanisme et de la libre pensée, mais anticommuniste depuis son voyage en URSS en 1920, avec des convictions de socialiste libertaire proches de l'anarchisme.

1.2 Enoncé du paradoxe

On peut formuler le paradoxe ainsi : l'ensemble des ensembles n'appartenant pas à eux-mêmes appartient-il à lui-même ? Si on répond oui, alors, comme par définition les membres de cet ensemble n'appartiennent pas à eux-mêmes, il n'appartient pas à lui-même : contradiction. Mais si on répond non, alors, il a la propriété requise pour appartenir à lui-même : contradiction de nouveau. On a donc une contradiction dans les deux cas, ce qui rend l'existence d'un tel ensemble paradoxal. Réécrit plus formellement, si l'on pose :

$$Y = \{X \mid X \notin X\}.$$

On a immédiatement que $Y \in Y \Leftrightarrow Y \notin Y$, donc chacune des deux possibilités, $Y \in Y$ et $Y \notin Y$, mène a une contradiction.

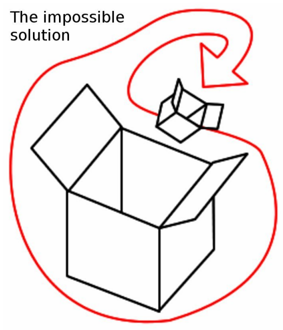


Figure 1.2 – Figure explicative du paradox de Rusell

Le paradoxe utilise très peu des propriétés de l'appartenance, une relation binaire suffit, ce qui a permis à *Bertrand Russell* de l'illustrer sous la forme plus imagée, mais qui a la même structure, du paradoxe du barbier. Un barbier se propose de raser tous les hommes qui ne se rasent pas eux-mêmes, et seulement ceux-là. Le barbier doit-il se raser lui même ? L'étude des deux possibilités conduit de nouveau à une contradiction. On résout le problème en affirmant qu'un tel barbier ne peut exister (ou, en jouant sur les mots, qu'il n'est pas un homme), ce qui ne surprendra personne : il n'y a pas vraiment de paradoxe. Plus exactement la démonstration qui précède constitue justement une démonstration de la non-existence d'un tel barbier.

Pourquoi les choses ne sont-elles pas aussi simples en théorie des ensembles ? Un principe qui semble assez naturel est de considérer que toute propriété, plus précisément tout prédicat du langage, définit un ensemble : celui des objets qui vérifient cette propriété. Mais si l'on utilise ce principe, dit principe de compréhension sans restriction, on doit admettre l'existence de l'ensemble paradoxal, défini par le prédicat « ne pas appartenir à soi-même » : c'est ce que l'on a fait justement en « définissant » l'ensemble $Y = \{X \mid X \notin X\}$. Plus simplement (l'existence d'un tel ensemble suffit, l'unicité est indifférente), on a utilisé le cas particulier suivant du principe de compréhension non restreint :

$$\exists Y \ \ \forall X \ \ (X \in Y \Leftrightarrow X \notin X).$$

La théorie qui contient ce seul axiome, et donc a fortiori toutes les instances du principe de compréhension non restreint, est contradictoire, la démonstration est la même que celle donnée ci-dessus.

Russell décrivit ce paradoxe dans une lettre adressée en 1902 à *Gottlob Frege*, où il montrait à ce dernier que l'une des règles introduite dans ses *Grundgesetze der Arithmetik*, la compréhension non restreinte, rendait la théorie de *Frege* contradictoire. Le paradoxe est alors bel et bien une antinomie : une contradiction interne à la théorie. *Frege* souhaitait dans cet ouvrage fonder les mathématiques sur des bases purement logiques, tâche à laquelle devait également s'atteler Russell, avec les *Principia Mathematica*. Il fait paraître ce paradoxe, (et d'autres) dans son ouvrage *The Principles of Mathematics* publié en 1903, tandis que, la même année, *Frege* adjoint au second volume de *Grundgesetze der Arithmetik* un appendice où il l'expose en en faisant précéder l'analyse de cet aveu d'une honnêteté confondante : « Pour un écrivain scientifique, il est peu d'infortunes pires que de voir l'une des fondations de son travail s'effondrer alors que celui-ci s'achève. C'est dans cette situation inconfortable que m'a mis une lettre de *M. Bertrand Russell*, alors que le présent volume allait paraître ».

La théorie des ensembles de *George Cantor* était également concernée par le paradoxe de *Russell*. Contrairement à la théorie de *Frege*, la théorie des ensembles de *Cantor*, est une théorie mathématique, et ne s'attaque pas à la formalisation de la logique elle-même (qui est le véritable succès de *Frege*). Cependant la théorie n'était pas formalisée, ce qui la rend d'ailleurs potentiellement sujette aux paradoxes qui font intervenir le langage, comme le paradoxe de Richard ou le paradoxe de *Berry*. *Le paradoxe de Russell* montrait que l'ensemble paradoxal en jeu ne peut exister, et laissait craindre que la théorie soit contradictoire. Mais *le paradoxe de Russell* n'était pas le premier paradoxe à apparaître dans la théorie des ensembles de *Cantor*. Le paradoxe de *Burali-Forti*, découvert par ce dernier en 1897, est très clairement interprété par *George Cantor* dans une lettre de 1899 à *Richard Dedekind* montrant que l'« ensemble » paradoxal en jeu, que nous appelons aujourd'hui la classe de tous les ordinaux, n'est pas un ensemble, plus exactement est de nature différente. De même pour le paradoxe de *Cantor* (1899) sur le plus grand cardinal. Il n'y a donc aucun doute, qu'à cette époque, *Cantor* ne pense pas que tout prédicat définisse un ensemble, même s'il ne donne pas de définition précise de la différence entre ce que nous appelons aujourd'hui « ensemble » et « classe propre », et qu'il évoque sous les termes de « multiplicité consistante et inconsistante ». Mais la solution de *Cantor* aux paradoxes ensemblistes, trop peu formelle, n'a pas vraiment réussi à convaincre *Richard Dedekind*, l'un des premiers à utiliser la notion d'ensemble, et qui reste très ébranlé par la découverte des paradoxes.

Par ailleurs, le paradoxe de Russell a l'avantage d'être particulièrement simple : nul besoin des notions de bon ordre, d'ordinal ou de cardinal en jeu dans les paradoxes de *Burali-Forti* et de *Cantor*. Il posa de façon encore plus cruciale la nécessité d'une formalisation de la théorie des ensembles (qui bien sûr doit éviter les paradoxes connus), et il joua un rôle important dans les débats autour de la mise au point de celle-ci.

1.3 Origines du paradoxe

La démonstration du paradoxe de *Russell* repose sur un argument diagonal, elle est très semblable à la démonstration du théorème de *Cantor* : le cardinal de l'ensemble des parties d'un ensemble (infini) E est strictement plus grand que celui de cet ensemble. Rappelons que pour démontrer ce théorème, on montre qu'une fonction f de E dans $\mathcal{P}(E)$, l'ensemble des parties de E, ne peut être surjective.

En effet $B = \{X \in E \mid X \notin f(X)\}$ n'appartient pas à l'image de f : sinon pour un certain Y, $B = f(Y)$, et $Y \in f(Y) \Leftrightarrow Y \notin f(Y)$, ce qui mène à une contradiction.

Cela rend impossible l'existence d'un plus grand cardinal. Or le cardinal de l'« ensemble » de tous les ensembles ne peut être que le plus grand cardinal. Plus précisément, l'« ensemble » de tous les ensembles contiendrait son ensemble des parties, et donc serait de cardinal supérieur ou égal à celui-ci.

Russell a déclaré qu'il était arrivé au paradoxe qui porte son nom en analysant soigneusement le paradoxe de *Cantor*. D'ailleurs, il peut paraître naturel pour un ensemble de ne pas appartenir à lui même. Si l'on introduit un axiome qui interdit à un ensemble de s'appartenir à lui même (comme l'axiome de fondation), cela ne résout pas le paradoxe : si une théorie est contradictoire, toute théorie obtenue en ajoutant des axiomes le sera également. On peut toujours définir l'ensemble $\{X \mid X \notin X\}$ des ensembles qui n'appartiennent pas à eux-mêmes, qui dans ce cas devient l'ensemble de tous les ensembles.

1.4 Les solutions du paradoxe

Les principales solutions apportées pour éluder ce paradoxe furent :

La restriction du principe de compréhension, due à *Zermelo* (1908) : un prédicat ne définit pas un ensemble mais sépare, dans un ensemble déjà donné, les objets qui ont une certaine propriété. Il est possible d'écrire le prédicat "$X \notin X$", mais celui-ci ne définit plus un ensemble. Il peut définir un sous-ensemble d'un ensemble donné, mais cela ne conduit pas à un paradoxe. Il est nécessaire, pour développer les mathématiques, d'introduire un certain nombre d'autres instances du principe de compréhension général comme axiomes particuliers (paire, réunion, ensemble des parties, ...). Plus tard *Abraham Fraenkel* et *Thoralf Skolem* introduisirent (indépendamment) le schéma d'axiomes de remplacement, qui est toujours une restriction du principe de compréhension général, mais étend encore le schéma d'axiomes de compréhension introduit par *Zermelo*. Ils précisèrent également la notion de prédicat, et, en particulier *Skolem*, le contexte logique (le calcul des prédicats du premier ordre).

La théorie des types de *Russell*, esquissée en appendice de l'ouvrage déjà cité de 1903. *Russell* la développe véritablement dans un article de 1908. Il poursuit, en compagnie de *Whitehead*, avec *les Principia Mathematica* parus en 1910. Selon cette théorie, les ensembles sont de types hiérarchisés. À un ensemble ne peuvent appartenir que des objets, qui peuvent être des ensembles, mais sont de types strictement inférieurs au type de l'ensemble initial, de sorte qu'on ne peut tout simplement plus écrire l'énoncé paradoxal (on ne peut plus écrire le prédicat d'auto-appartenance "$X \in X$", a fortiori sa négation). *Russell* n'a pas immédiatement développé la théorie des types après 1903. Il a d'abord pensé à des solutions alternatives, comme la théorie « pas de classe », qu'il tente d'esquisser dans son article de 1906. Dans ce même article, *Russell* ne cite d'ailleurs même pas la théorie des types parmi les solutions qu'il a explorées.

1.5 Versions positives du paradoxe

Le paradoxe de *Russell* repose sur un énoncé démontrable, ou encore universellement valide, du calcul des prédicats du premier ordre avec un symbole de relation binaire, soit $\mathcal{R}$, à savoir :

$$\neg \exists Y \, \forall X \, (X\mathcal{R}Y \Leftrightarrow \neg X\mathcal{R}X)$$

puisque l'existence d'un tel Y mène à une contradiction. C'est ce que l'on a déjà remarqué à propos du paradoxe du barbier. On a ainsi une version très épurée d'une certaine forme d'argument diagonal. On peut remarquer que, si la démonstration donnée ci-dessus repose sur le principe du tiers exclu, il n'est pas très difficile de la réaliser en logique intuitionniste.

Dans la théorie des ensembles de *Zermelo*, en fait dans toute théorie qui admet le schéma d'axiomes de compréhension, on montre, en réinterprétant le paradoxe, que pour tout ensemble A, il existe un ensemble Y qui n'appartient pas à A, à savoir :

$$Y = \{X \in A \mid X \notin X\}$$

On montre ainsi qu'il ne peut y avoir d'ensemble de tous les ensembles.

2 Le paradoxe du coiffeur

En 1901, le philosophe et mathématicien *Bertrand Russell* (1872 – 1970) découvre un éventuel paradoxe ou une contradiction apparente qui le conduit à modifier la théorie des ensembles. L'une des versions du paradoxe de *Russell*, connue sous le nom de « *Paradoxe du barbier* », met en scène un village dont, chaque jour, le barbier rase uniquement ceux qui ne se rasent pas eux-mêmes, et seulement ceux-ci. Par conséquent, le barbier se rase-t-il lui-même ?

Le scénario semble impliquer que le barbier se rase lui-même si et seulement s'il ne se rase pas lui-même. Comme l'écrit *Helen Joyce*, « *le paradoxe laisse entrevoir une perspective effrayante, selon laquelle l'ensemble des mathématiques repose sur des fondements instables et qu'aucune preuve n'est digne de confiance* ».

FIGURE 1.3 – Le paradoxe du coiffeur

Le paradoxe de *Russel*, dans sa forme d'origine, implique l'ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes. La plupart des ensembles R ne sont pas éléments d'eux-mêmes : par exemple, l'ensemble des cubes n'est pas un cube. Les exemples d'ensembles T qui se contiennent eux-mêmes comme éléments sont l'ensemble de tous les ensembles ou l'ensemble de tous les objets, à l'exception de cubes. Il semblerait que chaque ensemble doive être de type R

ou de type T, mais non des deux types. Cependant, *Russel* s'est interrogé sur l'ensemble S de tous les ensembles qui ne sont pas éléments d'eux-mêmes. D'une manière ou d'une autre, S n'est ni un élément de lui-même, ni un non-élément de lui-même. *Bertrand Russell* a compris qu'il devait modifier la théorie des ensembles pour éviter de telles confusions et de possibles contradictions.

L'une des réfutations possibles du paradoxe du barbier pourrait être simplement de répondre qu'un tel barbier n'existe pas. Néanmoins, le paradoxe de *Russell* a conduit à une version plus claire de la théorie des ensembles. Le mathématicien allemand *Kurt Gödel* a eu recours à des observations similaires pour formuler son théorème d'incomplétude. Le mathématicien britannique *Alan Turing* s'est également inspiré du travail de *Russell* quand il a étudié l'indécidabilité du problème de l'arrêt : étant donné un programme informatique, parviendra-t-il à s'arrêter en un nombre fini d'étapes ?

3 Le paradoxe du menteur

3.1 Enoncé

Le paradoxe du Menteur (*Euboulide*, siècle −4) consiste à dire « je mens » ou, sous une forme plus précise : « la présente phrase est fausse ». Si cette phrase est vraie, alors elle est fausse (puisque c'est ce qu'elle dit) ; et si elle est fausse, comme c'est précisément ce qu'elle dit, elle est vraie ! On ne peut pas lui attribuer une valeur de vérité (« **vraie** » ou « **fausse** ») de façon cohérente.

C'est là un paradoxe (l'argument est apparemment valable et pourtant sa conclusion heurte le sens commun), mais ce n'est pas encore une contradiction. En effet, que montre-t-il ? On dit qu'une phrase est une proposition (au sens des logiciens) si elle possède une valeur de vérité : on vient donc de montrer, par l'absurde, que « la présente phrase est fausse » n'est pas une proposition. On pourrait penser que ce n'est pas bien grave : après tout, dira-t-on, beaucoup de phrases ne sont pas des propositions au sens des logiciens (par exemple les phrases impératives comme « Essayons ! » ou interrogatives comme « Comment ? » ne sont ni vraies ni fausses). Mais une légère re-formulation montre qu'il y a ici un réel problème. Considérons la phrase : « la présente phrase est fausse ou dénuée de valeur de vérité ». Elle ne peut pas être vraie (puisqu'alors elle ne serait ni fausse ni dénuée de valeur de vérité, contrairement à ce qu'elle dit) ; et elle ne peut pas être fausse ou dénuée de valeur de vérité (car alors elle serait vraie puisque c'est ce qu'elle dit). Cette phrase n'est donc ni vraie, ni fausse, ni dénuée de valeur de vérité.

On pourrait chercher une issue en supposant l'existence d'autres valeurs de vérité que le vrai et le faux : la phrase aurait l'une de ces valeurs de vérité. Mais cela n'éliminerait pas le problème. En effet, considérons cette variante (qui englobe les précédentes) :

$$\textit{La présente phrase n'est pas vraie.} \tag{3.1.1}$$

Si elle est vraie, alors elle n'est pas vraie (puisque c'est ce qu'elle dit) ; et si elle n'est pas vraie, comme c'est précisément ce qu'elle dit, elle est vraie ! Il faut pourtant bien qu'elle soit vraie ou qu'elle ne le soit pas ; or chacune de ces options implique l'autre, donc elle est vraie et elle ne l'est pas : voilà une belle contradiction ! (Dans la suite, quand on parlera de paradoxes, il s'agira en fait de vraies contradictions.)

On pourrait encore tenter une échappatoire et dire : « la présente phrase » ? Mais quelle phrase ? Elle renvoie à elle-même, qui renvoie à elle-même et ainsi de suite : cette régression à l'infini ne renvoie finalement à rien, cette phrase tourne à vide, elle est dénuée de sens. Nous reviendrons sur cette question de l'auto-référence mais on peut déjà voir que cette objection ne résout pas le problème. Dans la phrase (3.1.1) ci-dessus, la locution « la présente phrase » renvoie clairement à la phrase (3.1.1), qui existe bien : elle est écrite, on l'a sous les yeux, elle est grammaticalement correcte et intelligible. Le fait est peut-être encore plus flagrant avec la version de *Lukasiewicz*, rapportée par *Tarski* : à la page 276, ligne 29 d'un [4] on lit

La proposition imprimée dans cet article à la page 276, *ligne* 29, *n'est pas vraie.*

Le livre existe réellement, la phrase qui s'y trouve imprimée à la page 276, ligne 29, parle d'elle-même, telle qu'elle existe matériellement : on ne peut pas plaider qu'elle ne renvoie à rien. Et la contradiction est toujours là.

3.2 La contradiction

L'existence d'une contradiction ne peut être prise à la légère. On pourrait même craindre qu'elle contamine tout le langage. En effet, selon les règles de la logique classique, d'une contradiction on peut déduire n'importe quelle proposition et donc aussi sa négation : il y aurait ainsi des contradictions partout ! Mais sur quoi repose ce principe de contamination ? Supposons qu'une proposition A soit vraie ainsi que sa négation $\neg A$. Soit B une proposition quelconque. De A on déduit $A \vee B$; mais de $\neg A$ et $A \vee B$ on déduit B. C'est tout ! La signification intuitive du syllogisme disjonctif est que si on a A ou B (ce que signifie la proposition $A \wedge B$) et qu'on n'a pas A (ce que signifie la proposition $\neg A$) alors on a B ; mais on voit que cela repose sur le fait que la proposition $\neg A$ implique qu'on n'a pas A, c'est-à-dire sur le principe de non-contradiction qui dit qu'on ne peut pas avoir à la fois A et $\neg A$.

Ainsi, les règles de déduction de la logique classique ont été formulées en vue d'une logique sans contradictions ; et quand on les applique pour montrer qu'une éventuelle contradiction contaminerait toutes les propositions, on oublie que leur justification intuitive n'est plus valable dans ce cas : on fait tourner un formalisme en ayant oublié sa justification intuitive ! Le fait qu'une contradiction contamine toutes les propositions est donc vrai dans la logique classique, à cause de son syllogisme disjonctif ; mais là où il y a des contradictions la logique classique n'est pas adaptée : le syllogisme disjonctif n'est plus justifié et il n'est pas vrai qu'une contradiction doive contaminer tout le langage. Dans la vraie logique du langage quotidien (où il y a des contradictions, comme celle du Menteur), de A et $\neg A$ on peut déduire des propositions comme $A \vee B$ ou $\neg A \vee B$ mais, faute du syllogisme disjonctif, on ne peut pas en extraire B ; la seule façon d'éliminer la disjonction est de revenir aux données A et $\neg A$: ainsi, loin d'être contagieuses, les contradictions sont stériles dans la logique du langage quotidien.

3.3 Remarque importante - Syllogisme disjonctif et implication

En logique classique, $(\neg A) \vee B$ coïncide avec $A \to B$ (c'est la définition du connecteur $\to$). Dans la logique du langage quotidien, ce n'est plus vrai si on donne à $A \to B$ son interprétation intuitive (« quand on a A on a B »). En effet, on vient de voir que si on a une contradiction, disons A et $\neg A$, alors on a A et on a $(\neg A) \vee B$ mais on ne peut pas en tirer B ; donc $(\neg A) \vee B$ ne signifie pas qu'avec A on a B.

Si on se limite à une partie du langage dans laquelle on a de bonnes raisons de penser qu'il n'y a pas de contradictions, on peut y appliquer les règles de la logique classique. Mais d'abord, comment trouver une partie du langage dans laquelle le paradoxe du menteur ne puisse être formé ? D'où est venu, au fond, ce paradoxe ?

3.4 Proposition d'une solution

Si une phrase A dit d'une autre phrase B qu'elle n'est pas vraie, il n'y a pas de contradiction : A est vraie si et seulement si B ne l'est pas. La contradiction surgit quand on prend $B \equiv A$ (« la présente phrase n'est pas vraie ») : alors A est vraie si et seulement si elle ne l'est pas. Le problème vient donc de ce que cette phrase particulière s'applique à elle-même. On dit cette phrase particulière car en général, quand une phrase se réfère à elle-même, cela ne pose pas de problème logique.

Exemples :

— La présente phrase est écrite en français.

— La présente phrase se termine par un point.

— La présente phrase contient six mots.

Ou ce joli pangramme auto-descriptif de *Gilles Esposito-Farèse* :

Cette phrase auto-descriptive contient exactement dix a, un b, huit c, dix d, trente-trois e, un f, cinq g, six h, vingt-sept i, un j, un k, deux l, deux m, vingt-cinq n, dix o, huit p, six q, treize r, quinze s, trente-deux t, vingt-deux u, six v, un w, quatorze x, un y, quatre z, six traits d'union, une apostrophe, trente virgules, soixante-huit espaces, et un point.

Chacune de ces phrases énonce sur elle-même un fait testable (et vrai). Certes, contrairement à la phrase du menteur, elles parlent de leur forme et non de leur vérité ; mais considérons alors la phrase :

La présente phrase est vraie ou ne l'est pas.

Elle parle de sa vérité et de rien d'autre, comme la phrase du menteur, et pourtant elle n'a rien de paradoxal : elle est tout simplement vraie.

L'auto-référence ne produit donc pas que des paradoxes. Mais elle semble quand même jouer un rôle crucial dans la construction du paradoxe du menteur. En effet, voyons si on peut le modifier de façon à supprimer l'auto-référence tout en maintenant la contradiction. Une tentative bien connue consiste à la remplacer par ce diptyque contradictoire :

La phrase ci-dessous n'est pas vraie.
La phrase ci-dessus est vraie.

Aucune des deux phrases ne se réfère directement à elle-même. Mais chacune se réfère à l'autre et donc indirectement à elle-même : on peut parler d'auto-référence indirecte, ou de cercle vicieux.

Le cercle vicieux peut être plus caché, comme dans cette version de *Yablo (*1993*)*, qui présente une liste infinie de phrases dont chacune affirme que les suivantes sont fausses :

$$\begin{array}{rcl} S_1 & = & \text{« } \textit{pour tout } k > 1 \textit{ la phrase } S_k \textit{ est fausse} \text{ »} \\ S_2 & = & \text{« } \textit{pour tout } k > 2 \textit{ la phrase } S_k \textit{ est fausse} \text{ »} \\ S_3 & = & \text{« } \textit{pour tout } k > 3 \textit{ la phrase } S_k \textit{ est fausse} \text{ »} \\ \text{etc.} & & \end{array}$$

Si S_n est vraie, alors S_{n+1} est fausse et toutes les suivantes aussi, mais ce dernier point signifie que S_{n+1} est vraie et donc S_n est fausse : contradiction ! Cela montre qu'aucune des phrases de la suite ne peut être vraie. Mais si elles sont toutes fausses, chacune est vraie (puisque ses suivantes sont bien fausses) : paradoxe ! Pourtant, là, on pourrait croire qu'il n'y a pas de cercle vicieux (et c'est ce que prétend *Yablo*) : apparemment aucune des phrases ne parle d'elle-même. Quoique ... Chacune parle de celles qui la suivent, donc elle fait allusion à sa propre place dans la suite, et par-là elle parle d'elle-même. D'ailleurs, la suite (S_n) est censée être définie par

$$S_n \overset{\text{déf}}{=} \text{« } \textit{pour tout } k > n \textit{ la phrase } S_k \textit{ est fausse.} \text{ »}$$

Mais cette « définition » présuppose l'existence de la suite. Il y a donc bien un cercle vicieux.

Conclusion :
On conclut de tout cela que le paradoxe du menteur et ses semblables dépendent d'une forme ou d'une autre d'auto-référence (ou de cercle vicieux).

Ce qui va nous donner une piste pour les éviter quand ce sera nécessaire, et c'est ce qu'on va voir maintenant.

4 Le paradoxe de Cantor

Le paradoxe de Cantor, ou paradoxe du plus grand cardinal, est un paradoxe de la théorie des ensembles dont l'argument a été découvert par *George Cantor* dans les années 1890. On le trouve dans sa lettre adressée à *David Hilbert*, datée de 1897. Il est appelé ainsi par *Bertrand Russell* dans ses *Principles of Mathematics* de 1903. Le paradoxe énonce que l'existence d'un plus grand cardinal conduit à une contradiction.

Dans une théorie des ensembles trop naïve, qui considèrerait que toute propriété définit un ensemble, ce paradoxe est bel et bien une antinomie, une contradiction déduite de la théorie, puisque le cardinal de la classe de tous les ensembles serait alors le plus grand cardinal. Mais ce n'en est pas une pour *Cantor*, qui n'a d'ailleurs jamais parlé de paradoxe. Pour lui, cela montre que le plus grand cardinal, s'il peut d'une certaine façon se définir, n'est pas un ensemble : reformulé en termes modernes et dans une théorie des ensembles axiomatique que ne connaissait pas *Cantor*, la classe des cardinaux n'est pas un ensemble.

4.1 Énoncé du paradoxe

On peut déduire le paradoxe de deux façons. Pour toutes deux on utilise que tout ensemble a un cardinal et donc, implicitement, l'*axiome du choix*.

1. On montre que la classe des cardinaux est équipotente à la classe des ordinaux, et donc le paradoxe de *Cantor* se ramène au paradoxe de *Burali-Forti*, il faut pour cela une forme du schéma d'axiomes de remplacement.
2. On utilise *le théorème de Cantor* sur la cardinalité de l'ensemble des parties : si le plus grand cardinal est un ensemble, il a donc un ensemble des parties, qui a alors un cardinal strictement supérieur à ce plus grand cardinal.

4.2 Paradoxe de *Cantor* et paradoxe de *Russell*

Pour *Cantor* tout ensemble pouvait être bien ordonné et avait un cardinal. Mais on peut éliminer tout appel à la notion de cardinal, et donc à l'axiome du choix dans le second raisonnement. Soit V la classe de tous les ensembles (dont le cardinal serait naturellement le plus grand cardinal). Si V est un ensemble, son ensemble des parties $\mathcal{P}(V)$ également. Donc $\mathcal{P}(V) \subset V$, l'identité définit une injection de $\mathcal{P}(V)$ dans V et contredit le théorème de *Cantor*. On a en fait montré que la classe de tous les ensembles n'est pas un ensemble.

Sous cette forme, il est très proche du paradoxe de *Russell*, et celui-ci a d'ailleurs déclaré qu'il était arrivé à son paradoxe en analysant la preuve du théorème de *Cantor*. En adaptant la démonstration du théorème de *Cantor* à ce cas particulier, on construit une réciproque à gauche f de l'identité de $\mathcal{P}(V)$ dans V, et on considère l'ensemble $\{x \in V \mid x \notin f(x)\}$, dont l'intersection avec $\mathcal{P}(V)$ est $\{x \in \mathcal{P}(V) \mid x \notin x\}$.

Le paradoxe de *Russell* a l'avantage d'être plus simple et de ne pas faire appel à l'ensemble des parties d'un ensemble, la seule propriété ensembliste est la compréhension non restreinte, qu'il utilise une seule fois, et qui est exactement la raison du paradoxe. Le paradoxe de *Cantor* utilise aussi la compréhension non restreinte, d'une façon analogue au paradoxe de *Russell* qui n'est pas correcte dans les théories des ensembles usuelles à la ZFC [1], mais aussi quand il affirme que l'ensemble des parties d'un ensemble est un ensemble, ce qui y est par contre licite (c'est l'axiome de l'ensemble des parties).

4.3 Version positive du paradoxe

On peut interpréter le paradoxe de Cantor dans la théorie des ensembles usuelle, pour montrer suivant les versions que la classe des cardinaux n'est pas un ensemble, ou que la classe V de tous les ensembles n'est pas un ensemble. Ceci est compatible avec l'analyse de *Cantor*.

5 Le paradoxe de Richard

Avant d'exposer *le paradoxe de Richard*, rappelons comment l'argument diagonal de *Cantor* permet de prouver que $\mathbb{R}$ n'est pas dénombrable (c'est-à-dire qu'on ne peut pas former une suite de réels qui les contienne tous). Donnons-nous une suite de réels écrits en base 10 (par exemple) :

$$\begin{array}{ccl} x_1 & = & e_1, c_{11}c_{12}c_{13}c_{14}\cdots \\ x_2 & = & e_2, c_{21}c_{22}c_{23}c_{24}\cdots \\ x_3 & = & e_3, c_{31}c_{32}c_{33}c_{34}\cdots \\ x_4 & = & e_4, c_{41}c_{42}c_{43}c_{44}\cdots \\ \vdots & \vdots & \qquad \vdots \end{array}$$

(les entiers e_i sont les parties entières ; les c_{ij} sont des chiffres ; pour les nombres décimaux, on choisit le développement qui se termine par des chiffres 0). Formons le réel

$$x \quad = \quad 0, c_1c_2c_3c_4\cdots \qquad \text{où} \quad \begin{cases} c_i = 1 & si \quad c_{ii} \neq 1 \\ c_i = 0 & si \quad c_{ii} = 1 \end{cases}$$

on a donc $c_i \neq c_{ii}$ pour tout i et par conséquent $x \neq x_i$ pour tout i. Cela montre qu'aucune suite de réels ne contient tous les réels.

5.1 Énoncé du paradoxe de Richard

Le paradoxe de *Jules Richard* utilise le même argument sur une autre suite. Appelons longueur d'un texte (fini) en une langue vivante le nombre de lettres et autres signes (chiffres, ponctuation, espaces,...) qu'il contient. Énumérons tous les textes par longueur croissante et, pour une longueur donnée, selon l'ordre

1. Théorie de *Zermelo-Fraenkel* avec axiome du choix.

lexicographique (on munit l'alphabet de son ordre usuel, qu'on prolonge comme on le veut aux autres signes). Certains de ces textes définissent un nombre réel (par exemple : « *la racine carrée positive de* 2 » ou « *le plus petit nombre premier qui s'écrive avec au moins cent chiffres en base 10* ») : conservons-les et supprimons tous les autres. Dans l'énumération restante, le premier texte définit un nombre x_1, le deuxième un nombre $x_2, \ldots$ etc. Chacun de ces nombres possède un développement décimal (unique, si on choisit pour les nombres décimaux le développement qui se termine par des chiffres 0). Appliquons l'argument diagonal comme ci-dessus :

$$\begin{cases} c_i = 1 & si \quad c_{ii} \neq 1 \\ c_i = 0 & si \quad c_{ii} = 1 \end{cases} \quad ; \quad \forall i \in \mathbb{N}^*$$

Cela définit, par la suite de ses chiffres décimaux, un nombre x de $[0,1[$ bien déterminé, qui n'est aucun des x_i : donc il ne peut pas être défini par un texte, mais c'est pourtant ce qu'on vient de faire.

5.2 Explication et solution

L'explication proposée par *Richard* est la suivante :

Quand on examine un à un les textes en une langue vivante pour décider s'ils définissent un réel, on arrive à un certain moment au texte ci-dessus, censé définir x.

Doit-on l'accepter ou le rejeter ?

La définition de x est valide si la suite $x_1, x_2, \cdots$ est bien définie. Or, dit *Richard*, elle ne l'est pas encore puisqu'on est en train de la constituer (il reste une infinité de textes à examiner). On définit x à partir de la suite (x_i) alors que la définition de x fait partie des textes à examiner pour définir cette suite : il y a là un cercle vicieux, les définitions de x et de la suite (x_i) se présupposant l'une l'autre.

Cela signifie que la notion de « réel définissable par un texte en français » est mal définie : elle dépend du contexte.

En effet, passons en revue une première fois tous les textes possibles : celui qui est censé définir x (ci-dessus) doit être rejeté car la liste (x_i) qu'il présuppose n'existe pas encore (et donc ce texte ne définit pas un nombre).

Après avoir terminé l'examen de tous les textes, on a une liste (x_i). Si alors on recommence depuis le début l'examen de tous les textes, cette fois le texte censé définir x doit être accepté puisque la liste (x_i) requise existe. Après avoir terminé ce second examen exhaustif, on a une nouvelle liste dont x fait partie, mais il n'y a plus de paradoxe : car le paradoxe était

le nombre x n'est pas sur la liste et il est sur la liste !

Et maintenant on a

le nombre x n'est pas sur la première liste et il est sur la deuxième.

Si on passe en revue une troisième fois tous les textes, le texte censé définir x définit un nouveau nombre, différent du précédent (car hors de la deuxième liste) ! Ainsi, dans ce processus, le même texte ne définit d'abord pas un nombre, puis il en définit un, puis il en définit un autre, ... etc. Chaque nouvelle vérification modifie le nombre défini par le même texte ! La notion de « définition » d'un nombre par un texte donné change d'une vérification à l'autre et le paradoxe surgit quand on veut appliquer la même notion à x et aux x_i.

Pour préciser tout cela on peut formaliser :
les textes énumérés sont alors les formules d'un langage formel $\mathcal{L}$; la définition de x est écrite dans un métalangage de $\mathcal{L}$, donc x n'a aucune raison de figurer dans la liste des nombres qui sont définis (en un sens précis, cette fois) par une formule de $\mathcal{L}$; et le paradoxe devient une preuve par l'absurde qu'en effet il n'y figure pas.

6 Le paradoxe de Grelling

Le paradoxe de Grelling-Nelson, occasionnellement appelé *paradoxe de Grelling* ou de façon erronée *paradoxe de Weyl*, est un paradoxe sémantique formulé en 1908 par *Kurt Grelling* et *Leonard Nelson*, et parfois attribué par erreur au philosophe et mathématicien allemand *Hermann Weyl*.

Le paradoxe repose sur la définition du terme **hétérologique** (du grec ancien **hétéro**, différent, et **logos**, langage) qui s'applique à un mot qui ne se décrit pas lui-même. Par exemple : « *long* » est un adjectif hétérologique en ceci que le mot n'est pas long puisque composé de seulement quatre lettres. De même, le mot « *illisible* » peut parfaitement être lu, il est donc hétérologique lui aussi. À l'inverse, le mot « *français* » est dit **autologique** car il correspond à sa définition, français est bien un mot du dictionnaire français.

Selon la définition ci-dessus, le paradoxe de *Grelling-Nelson* vient du fait que l'adjectif « **hétérologique** » est lui-même hétérologique si et seulement s'il ne l'est pas.

Ce paradoxe est semblable à d'autres paradoxes logiques comme ceux du menteur (ou paradoxe d'*Épiménide*) ou *du barbier* (ou *paradoxe de Russell*) en cela qu'il repose sur la négation d'une autoréférence.

Ce paradoxe est beaucoup plus résistant que beaucoup de paradoxes logiques : on ne peut l'éliminer, comme le paradoxe des catalogues, en disant que l'objet n'existe pas (l'adjectif hétérologique figure dans plusieurs dictionnaires), ni en arguant des effets pervers de l'infini, le nombre d'adjectifs d'une langue étant fini. Il ne peut être évacué qu'en interdisant à un adjectif de se qualifier lui-même, mais cet effet, comme l'a décrit *Noam Chomsky*, est une des bases du langage.

Toute classification binaire par un discriminateur donné crée automatiquement quatre classes dont quelques-unes peuvent être vides :
— le discriminateur répond positivement ("*court*" est autologique) ;
— le discriminateur répond négativement ("*long*" n'est pas autologique) ;

— le discriminateur ne peut répondre parce qu'on est en dehors de son domaine de définition (un substantif ou un verbe ne sera ni autologique, ni hétérologique, sauf cas particulier comme le mot "*existe*", qui existe) ;
— le discriminateur ne peut répondre pour certains opérandes, pour des raisons cette fois-ci sémantiques et non syntaxiques. Ceux-ci sont donc à exclure de son domaine de définition (comme le 0 en dénominateur pour l'opération de division). On peut rétablir le paradoxe en décrétant que les adjectifs qui ne peuvent décrire des adjectifs sont classés parmi les hétérologiques.

7 Le paradoxe Skolem

En *logique mathématique* et en *philosophie analytique*, le *paradoxe de Skolem* est une conséquence troublante du *théorème de Löwenheim-Skolem* en théorie des ensembles. Il affirme qu'une théorie des ensembles, comme ZFC, si elle a un modèle, a un modèle dénombrable, bien que l'on puisse par ailleurs définir une formule qui exprime l'existence d'ensembles non dénombrables. C'est un paradoxe au sens premier de ce terme : il va contre le sens commun, mais ce n'est pas une antinomie, une contradiction que l'on pourrait déduire dans la théorie.

7.1 Enoncé du paradoxe

Le théorème de Löwenheim-Skolem connait plusieurs variantes. Prenons la suivante :

en calcul des prédicats égalitaire du premier ordre, construit sur une signature (symboles primitifs non logiques) au plus dénombrable, tout modèle infini contient un sous-modèle dénombrable élémentairement équivalent, c'est-à-dire qu'il satisfait exactement les mêmes énoncés.

En particulier la théorie des ensembles ZFC, utilise comme seul symbole non logique celui de la relation d'appartenance. Donc, si ZFC est cohérente, elle a un modèle, nécessairement infini à cause des axiomes, et ce modèle possède une sous-structure dénombrable qui satisfait exactement les mêmes énoncés, en particulier les axiomes de ZFC. Les « points » de cette structure, qui sont des ensembles, sont, en tant qu'ensembles, inclus dans la classe de tous les ensembles, le support de la structure.

Or, l'un des premiers résultats de la théorie des ensembles est la démonstration de l'existence d'un ensemble non dénombrable. C'est une conséquence immédiate du théorème de *Cantor*. Comment un ensemble non dénombrable pourrait-il être inclus dans une sous-structure dénombrable ?

7.2 Résolution du paradoxe

Comme souligné par *Skolem*, le problème réside dans la relativité de ce qu'on appelle ici dénombrable. En théorie des ensembles, un ensemble est dénombrable s'il est en bijection avec $\mathbb{N}$, l'ensemble des entiers naturels. Mais nous avons utilisé cette notion en deux sens différents :

1. Les ensembles dénombrables au sens du modèle de ZFC ;
2. les ensembles dénombrables au sens de la théorie intuitive dans laquelle nous avons énoncé le théorème de *Löwenheim-Skolem*.

On peut tout à fait formaliser ce théorème en théorie des ensembles, mais on ne peut faire coïncider le modèle de ZFC dans lequel on a effectué cette formalisation, et celui auquel on applique le théorème. Dans le modèle dénombrable de ZFC obtenu par *Löwenheim-Skolem*, il existe bien une collection (un ensemble de l'univers de la formalisation) de couples qui établit une bijection entre les ensembles $\mathbb{N}$ et $\mathbb{R}$ du modèle, mais comme $\mathbb{R}$, l'ensemble des réels, n'est pas dénombrable, cette collection n'est pas représentée par un ensemble de ce modèle. Ce n'est même pas une classe. Il n'y a aucun moyen d'en parler dans ce modèle. L'ensemble $\mathbb{R}$ est bien non dénombrable au sens du modèle.

Le paradoxe repose sur une interprétation trop « *intuitive* » de la théorie axiomatique des ensembles, qui est une théorie formelle de l'appartenance au premier ordre, et sur une confusion entre *méta-théorie* et théorie, réminiscence des paradoxes des théories des ensembles insuffisamment formalisées comme ceux de *Richard* et de *Berry*.

Supposons que $\varphi(x)$ soit une formule du premier ordre sur le langage de la théorie des ensembles qui correspond exactement à la formalisation de « x est non-dénombrable ». Le problème réside dans le fait que l'on peut avoir :

1. avoir M satisfait $\varphi(x)$ sans que l'interprétation de x soit un ensemble non-dénombrable ;
2. avoir M satisfait $x \in y$ sans que l'interprétation de x appartienne à l'interprétation de y. D'ailleurs les interprétations de x et y ne sont peut-être pas des ensembles, mais « des chiens ou des chats ».

L'existence, pour tout modèle de ZFC, d'une sous-structure dénombrable élémentairement équivalente, est en fait un résultat utile de théorie des ensembles.

Chapitre 2

Le calcul propsitionnel

1 Vocabulaire usuel

1.1 Axiome

Définition 1.1. *Un axiome est un énoncé supposé vrai à priori et que l'on ne cherche pas à démontrer.*

Exemple 1.1.

— *Euclide a énoncé cinq axiomes "les cinq postulats d'Euclide", qu'il a renoncé à démontrer et qui devaient être la base de la géométrie (euclidienne).*
  Le cinquième de ces axiomes a pour énoncé : « par un point extérieur à une droite, il passe une et une seule droite parallèle à cette droite ».

— *Les (cinq) axiomes de Peano qui définissent l'ensemble des entiers naturels.*
  Le cinquième axiome affirme que : « si P est une partie de $\mathbb{N}$ contenant 0 et telle que le successeur de chaque élément de P est dans P (le successeur de n est $(n+1)$), alors $P = \mathbb{N}$ ». Cet axiome est appelé « l'axiome d'induction » ou encore « l'axiome de récurrence ».

Ces énoncés ont en commun d'être « évidents » pour tout le monde.

1.2 Proposition (Assertion ou Affirmation)

Définition 1.2. *Une proposition est un énoncé pouvant être vrai ou faux.*

Exemple 1.2.

— *Tout nombre premier est impair.*
  On peut facilement démontrer que cette proposition est fausse par un simple contre exemple " $p = 2$ est un nombre premier qui n'est pas impair".

— *Tout carré de réel est un réel positif.*
  c'est une proposition vraie.

Le mot proposition est clair : on propose quelque chose, mais cela reste à démontrer !

1.3 Théorème

Définition 1.3. *Un théorème est une proposition vraie (et en tout cas démontrée comme telle).*

Par abus de langage, le mot proposition désigne souvent, dans la pratique des cours de mathématiques, un théorème intermédiaire ou de moindre importance, et même on a tendance à appeler proposition la plupart des théorèmes pour réserver le mot théorème aux plus grands d'entre eux (Théorème de Pythagore, Théorème du point fixe, ...).

C'est d'ailleurs ce dernier point de vue que nous adopterons dans les chapitres ultérieurs (mais pas dans ce premier chapitre où le mot « proposition » aurait alors deux significations différentes).

Exemple 1.3.

— *L'énoncé* $\overline{\mathbb{R}} = \mathbb{C}$ *" Le corps des réels est algébriquement clôs dans le corps des complexes" s'appel le Théorème fondamental de l'algèbre.*
— *il n'existe pas des entiers strictement positifs* x, y *et* z *vérifiant* $x^n + y^n = z^n$ *pour* n *plus grand ou égale à* 3 *! c'est le Grand Théorème de Fermat.*

1.4 Corollaire

Définition 1.4. *Un corollaire à un théorème est un théorème qui est conséquence de ce théorème.*

Exemple 1.4.

Dans le chapitre « Continuité », le théorème des valeurs intermédiaires dit que l'image d'un intervalle de $\mathbb{R}$ *par une fonction continue à valeurs réelles, est un intervalle de* $\mathbb{R}$.

Un corollaire de ce théorème affirme alors que si une fonction définie et continue sur un intervalle de $\mathbb{R}$ *à valeurs réelles, prend au moins une valeur positive et au moins une valeur négative alors cette fonction s'annule au moins une fois dans cet intervalle.*

1.5 Lemme

Définition 1.5. *Un lemme est un théorème préparatoire à l'établissement d'un théorème de plus grande importance.*

Exemple 1.5.

— *L'énoncé du* ***lemme de Zorne*** *est*
"Tout ensemble ordonné dans lequel toute partie non vide, totalement ordonnée, est majorée, possède au moins un élément maximal"
Le théorème d'Hausdorf *est*
Tout ensemble ordonné possède une partie totalement ordonnée maximale
— *Dans la théorie de la mesure et de l'intégration, on rencontre le* ***lemme de Fatou*** *!*

1.6 Conjecture

Définition 1.6. *Une conjecture est une proposition que l'on suppose vraie sans parvenir à la démontrer.*

Les conjectures sont le moteur du progrès des mathématiques. Tel ou tel mathématicien a eu l'impression que tel ou tel résultat important était vrai et l'a énoncé sans pouvoir le démontrer, laissant à l'ensemble de la communauté mathématique le soin de le confirmer par une démonstration convaincante ou de l'infirmer.

Exemple 1.6.

— *Conjecture de Ferma : Si n est un entier supérieur ou égal à 3, il n'existe pas d'entiers naturels tous non nuls x, y et z tels que $x^n + y^n = z^n$ (cette conjecture date du $XVII^e$ siècle et il a été démontré récemment que ce résultat était vrai).*
— *conjecture de Bertrand énoncée en 1845 : Pour tout entier naturel non nul n, il existe un nombre premier p tel que $n < p < 2n$ (dans un premier temps, on ne sût pas si cette affirmation était vraie ou fausse et le problème resta ouvert pendant 5 ans jusqu'à ce que Chebychev en démontre la véracité en 1850).*
— *En arithmétique toujours, une conjecture très célèbre est la suivante : pour un réel $x \geq 2$, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x (par exemple, $\pi(3,2) = 2$ et $\pi(10) = 4$) et $Li(x)$ le nombre $\int_2^x \frac{1}{\ln t} dt$ ($Li(x)$ s'appelle le logarithme intégral de x). On a découvert avec le temps que ces deux expressions sont « proches » l'une de l'autre quand x est « grand ».*
On s'est alors intéressé à la différence $\pi(x) - Li(x)$. A partir d'un grand nombre de calculs numériques, on a conjecturé que pour tout réel $x \geq 2$, on avait $\pi(x) < Li(x)$. On a longtemps pensé que ce résultat était vrai, mais un mathématicien du nom de Skewes a démontré un jour que ce résultat était faux pour au moins un réel x inférieur à $e^{e^{e^{e^{7,5}}}}$ (nombre de Skewes). Puis on a découvert que le résultat était faux pour une infinité de valeurs de x.

Les considérations précédentes sont au-dessus du niveau d'une première année d'études supérieures. Si on les a citées, c'est pour fournir un exemple de résultat que l'on pensait « intuitivement » vrai et qui s'est pourtant avéré faux. Dans l'histoire, on trouve de très nombreux exemples de problèmes où l'intuition des mathématiciens a été mise en défaut.

1.7 Définition

Définition 1.7. *Une définition est un énoncé dans lequel on décrit les particularités d'un objet.*

On doit avoir conscience que le mot « axiome » est quelquefois synonyme de « définition ». Par exemple, quand vous lirez « *définition d'un espace vectoriel* », vous pourrez tout autant lire « *axiomes de la structure d'espace vectoriel* » et vice-versa.

1.8 Sémantique d'un langage propositionnel

L'étude sémantique d'un langage pour le calcul des propositions a pour but de donner une valeur de vérité aux formules du langage. Elle est aussi appelée la théorie des modèles.

La sémantique associe une fonction de valuation unique à chacun des connecteurs logiques

$$\begin{array}{rcl} \mathcal{V}: \ \mathcal{V}ar\mathcal{P}rop & \to & \{0,1\} \\ P & \mapsto & \mathcal{V}(P) = \begin{cases} 1 & si\ P\ est\ vraie \\ 0 & si\ P\ est\ fausse \end{cases} \end{array}$$

où $\mathcal{V}ar\mathcal{P}rop$ est l'ensemble des variables propositionnelles.

Cette fonction est décrite par un graphe appelé table de vérité (ou tableau de vérité). A chaque formule α à n variables propositionnelles correspond une fonction de vérité unique. Le graphe de cette fonction est défini par une table de vérité à 2^n lignes représentant la valeur de vérité de α correspondant à chaque combinaison de valeur de vérité des n variables (appelées aussi distribution de valeurs de vérité des variables).

2 Les connecteurs logiques

2.1 Négation d'une proposition

Définition 2.1. *Soit P une proposition. On définit sa négation, notée $\neg P$ (ou aussi non$P$), de la manière suivante :*

$$\mathcal{V}(\neg P) := \begin{cases} 1 & si \quad \mathcal{V}(P) = 0 \\ 0 & si \quad \mathcal{V}(P) = 1 \end{cases} \tag{2.1.1}$$

La table de vérité de la négation est la suivante :

P	$\neg P$
V	F
F	V

$\Leftrightarrow$

P	$\neg P$
1	0
0	1

Table 2.1 – Table de vérité de $\neg P$

Remarque 2.1. *Cette simple table contient en germe un très grand nombre d'erreurs de raisonnement à venir et ceci dans à peu près tous les chapitres.*

Exemple 2.1.

1. *On doit déjà avoir conscience que la négation de « ce chat est blanc » est, non pas « ce chat est noir », mais tout simplement « ce chat n'est pas blanc »*
2. *Le contraire de la phrase « f est la fonction nulle » est, non pas « f ne s'annule pas », mais « f n'est pas la fonction nulle » ou encore « f ne s'annule pas en au moins un point ».*

3. *Enfin, le contraire de la phrase « $x \geq 0$ » est « $x < 0$ », et non pas « $x \leq 0$ ».*

Théorème 2.1. *Soit P une proposition logique, alors*

$$\neg(\neg P) \Leftrightarrow P.$$

Démonstration. Dans la table de vérité suivante

P	$\neg P$	$\neg(\neg P)$
1	0	1
0	1	0

Table 2.2 – Démonstration du théorème 2.1

on peut voir que P et $\neg(\neg P)$ ont les mêmes valeurs de vérité. □

2.2 Les connecteurs logiques conjonction "$\wedge$" et disjonction "$\vee$"

Définition 2.2. *Soient P et Q deux propositions logiques.*

— *On définit la conjonction de P et Q q'on note par $P \wedge Q$, et qu'on lit « P et Q », par*

$$\mathcal{V}(P \wedge Q) := \begin{cases} 1 & si \quad \mathcal{V}(P) = 1 \quad et \quad \mathcal{V}(Q) = 1 \\ 0 & sinon \quad ! \end{cases} \tag{2.2.1}$$

— *On définit la disjonction de P et Q q'on note par $P \vee Q$, et qu'on lit « P ou Q », par*

$$\mathcal{V}(P \vee Q) := \begin{cases} 0 & si \quad \mathcal{V}(P) = 0 \quad et \quad \mathcal{V}(Q) = 0 \\ 1 & sinon \quad ! \end{cases} \tag{2.2.2}$$

Les tables de vérité de la conjonction et de la disjonction sont :

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

$\Leftrightarrow$

P	Q	$P \vee Q$	$P \wedge Q$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Table 2.3 – Tables de vérité de $\wedge$ et $\vee$

Remarque 2.2.

— *$P \vee Q$ est fausse si et seulement si P et Q sont sémultanément fausses.*
— *$P \wedge Q$ est vraie si et seulement si P et Q sont sémultanément vraies.*
— *Il existe en langage courant deux significations du mot « ou ».*
- *Il y a le « ou exclusif » qui signifie «soit l'un, soit l'autre, mais pas les deux».*
- *le «ou inclusif » qui signifie « soit l'un, soit l'autre, soit les deux».*

$\vee$ est le «ou inclusif».

Théorème 2.2. *Soit P une proposition, alors*

$$P \vee P \Leftrightarrow P \quad \text{et} \quad P \wedge P \Leftrightarrow P.$$

Démonstration. Dans la table de vérité suivante

P	$P \wedge P$	$P \vee P$
1	1	1
0	0	0

TABLE 2.4 – Démonstration du théorème 2.2

On peut voir que P, $P \wedge P$ et $P \vee P$ ont les mêmes valeurs de vérité, ce qui montre bien le théorème.

□

Théorème 2.3 (Lois de Morgan).
Soient P et Q deux propositions logiques, alors :

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q \quad \text{et} \quad \neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q. \tag{2.2.3}$$

Démonstration. Dans la table de vérité suivante

P	$\neg P$	Q	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
1	0	1	0	1	0	0	1	0	0
1	0	0	1	1	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1
0	1	0	1	0	1	1	0	1	1

TABLE 2.5 – Démonstration du théorème 2.3

On peut voir que la les colonnes en rouge sont identiques, ce qui montre que

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q.$$

Aussi les colonnes en bleu sont idntiques, donc

$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q.$$

□

A partir de ces résultats, on peut se convaincre que tout énoncé peut s'écrire en utilisant uniquement la conjonction $\wedge$ et la négation $\neg$ ou par la disjonction $\vee$ et la négation $\neg$, (par exemple, au paragraphe suivant, on verra que la proposition $P \Leftrightarrow Q$ est identique a la proposition $\{\neg(P \wedge \neg Q) \wedge \neg(Q \wedge \neg P)\}$). Ce résultat a une importance en électronique et en informatique.

Théorème 2.4. *Soient P, Q et R trois propositions logiques, alors*

1. *La conjonction et la disjonction sont commutatives, autrement dit*
$$P \wedge Q \Leftrightarrow Q \wedge P \quad \text{et} \quad P \vee Q \Leftrightarrow Q \vee P.$$
2. *La conjonction et la disjonction sont associatives, autrement dit*
$$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R) \quad \text{et} \quad (P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R).$$
3. *La conjonction est distributive sur la disjonction, et l'inverse aussi, autrement dit :*
$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R) \quad \text{et} \quad P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R).$$

Démonstration.

1. La commutativité est évidente.
2. Dans la table de vérité suivante

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

Table 2.6 – La commutativité de la conjonction "$\wedge$"

On peut constater que les colonnes en rouge sont identiques, donc
$$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R).$$
Donc, la disjonction est commutative. Et dans la table de vérité

P	Q	R	$P \vee Q$	$(P \vee Q) \vee R$	$Q \vee R$	$P \vee (Q \vee R)$
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	1	1	1
1	0	0	1	1	0	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	0	1	1	1
0	0	0	0	0	0	0

Table 2.7 – La commutativité de la disjonction "$\vee$"

On peut constater aussi que les colonnes en rouge sont identiques, donc
$$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R).$$
Donc, la conjonction est commutative.

3. Dans la table de vérité suivante

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Table 2.8 – La distributivité de la conjonction "$\wedge$" sur la disjonction "$\vee$"

On peut voir que les colonnes en rougs sont identiques, donc

$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R).$$

Et dans la table de vérité

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	0	1
1	0	1	1	1	0	0	1
1	0	0	0	1	0	0	1
0	1	1	0	0	0	1	0
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

Table 2.9 – La distributivité de la disjonction "$\vee$" sur la conjonction "$\wedge$"

On peut voir aussi que les colonnes rouges sont identiques, donc

$$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R).$$

□

2.3 Implication logique

Définition 2.3. *Soient P et Q deux propositions logiques, on définit l'implication logique : $P \Rightarrow Q$ par*

$$\mathcal{V}(P \Rightarrow Q) := \begin{cases} 0 & si \quad \mathcal{V}(P) = 1 \ et \ \mathcal{V}(Q) = 0 \\ 1 & sinon \quad ! \end{cases}$$

La table de vérité de l'implication logique est donnée par

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

$\Leftrightarrow$

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

TABLE 2.10 – La table de Vérité de l'implication logique "$\Rightarrow$"

Théorème 2.5. *Soient P et Q deux propositions, on a :*

$$\mathcal{V}((P \Rightarrow Q) = \mathcal{V}(\neg P \vee Q).$$

Ce théorème nous montre qu'on peut définir l'implication logique $P \Rightarrow Q$ par $\neg P \vee Q$.

Démonstration. La table de vérité suivante

P	$\neg P$	Q	$\neg P \vee Q$	$P \Rightarrow Q$
1	0	1	1	1
1	0	1	0	0
0	1	1	1	1
0	1	0	1	1

TABLE 2.11 – Démonstration du théorème 2.5

Montre bien le théorème. □

Théorème 2.6 (Transitivité de l''implication). *Soient P, Q et R trois propositions logiques, on a :*

$$\alpha : ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R).$$

Démonstration. La table de vérité suivante

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q) \wedge (Q \Rightarrow R)$	$P \Rightarrow R$	α
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	0	0	0	1	1
1	0	0	0	1	1	0	1
0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	1
0	0	1	1	0	0	1	1
0	0	0	1	1	1	1	1

TABLE 2.12 – Démonstration du théorème 2.6

Montre bien le théorème. □

Théorème 2.7 (Propositions équivalentes). *Soient P et Q deux propositions logiques, on a :*

$$\beta : (P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P)).$$

Ce théorème nous montre que l'équivalence entre deux propositions logiques peut être définit comme conjonction de deux implications dans les deux sens.

Démonstration. La table de vérité suivante

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$	β
1	1	1	1	1	1	1
1	0	0	1	0	0	1
0	1	1	0	0	0	1
0	0	1	1	1	1	1

Table 2.13 – Démonstration du théorème 2.7

Montre bien le théorème. □

Remarque 2.3. *Une équivalence signifie deux implications, l'une de gauche à droite et l'autre de droite à gauche.*

Quand on écrit $P \Leftrightarrow Q$, on doit être convaincu que la proposition de gauche P entraîne la proposition de droite Q et aussi que la proposition de droite Q entraîne la proposition de gauche P.

Occupons nous maintenant d'analyser la table de vérité de l'implication. Les deux dernières lignes de cette table de vérité peuvent paraître surprenantes (comment peut-il être vrai qu'une phrase fausse implique une phrase fausse ou aussi une phrase vraie ?)

L'exemple suivant fera comprendre « (Faux $\Rightarrow$ Faux) est vraie ».

Exemple 2.2.

1. *Vérifions que,*

$$\alpha : \left\{ \forall n \in \mathbb{N},\ (10^n + 1 \textit{ est divisible par } 9) \ \Rightarrow\ (10^{n+1} + 1 \textit{ est aussi divisible par } 9. \right\}$$

En effet ;
Soit $n \in \mathbb{N}$. La condition « $10^n + 1$ divisible par 9 » fournit un entier naturel k tel que $10^n + 1 = 9k$. Et on a donc :

$$\begin{aligned} 10^{n+1} + 1 &= 10 \times 10^n + 1 \\ &= 10 \times 10^n + 10 - 10 + 1 \\ &= 10 \times (10^n + 1) - 10 + 1 \\ &= 10 \times (10^n + 1) - 9 \\ &= 10 \times 9k - 9 \\ &= 9(10k - 1) \\ &= 9k' \quad \textit{où} \quad k' = (10k - 1) \in \mathbb{N}. \end{aligned}$$

on a obtenu comme conséquence de l'hypothèse initiale le fait que l'entier $10^{n+1} + 1$ est divisible par 9.

Conclusion :

L'implication proposée est totalement exacte et pourtant, aucune des deux phrases encadrant cette implication ne sont vraies (puisque les nombres 2, 11, 101, 1001*... ne sont à l'évidence pas divisibles par* 9*).*

D'ailleurs, en écrivant cette implication, nous ne nous sommes jamais demandé si la première phrase écrite était vraie. Il est important de le comprendre pour être capable le moment venu de gérer correctement le raisonnement par récurrence.

2. *Pour comprendre « (Faux $\Rightarrow$ Vrai) est vraie », on se contentera de l'exemple suivant :*

$$\alpha : \{(2 = 3 \ \ et \ \ 2 = 1) \ \ \Rightarrow (2 + 2 = 3 + 1) \ \ \Rightarrow \ \ (4 = 4) \ \}$$

L'affirmation de départ est fausse et on en déduit (tout à fait par hasard mais par un raisonnement tout à fait juste) une affirmation vraie. L'affirmation finale est vraie, mais ce ne sont pas les implications écrites qui la démontrent.

Une conséquence pratique de cette étude est que, si notre hypothèse de départ est fausse bien que par la suite nous tenions des raisonnements entièrement justes, nous n'avons aucune idée en fin de raisonnement de la véracité ou de la fausseté des conclusions auxquelles nous sommes parvenu.

2.4 Equivalence logique

Définition 2.4. *Deux propositions équivalentes P et Q sont deux propositions simultanément vraies et simultanément fausses, et on écrit $P \Leftrightarrow Q$.*

Autrement dit

$$\mathcal{V}(P \Leftrightarrow Q) := \begin{cases} 1 & si \quad \mathcal{V}(P) = \mathcal{V}(Q) \\ 0 & si \quad \mathcal{V}(P) \neq \mathcal{V}(Q) \end{cases}$$

On dira donc que deux propositions équivalentes sont deux propositions ayant les mêmes valeurs de vérité.

Cette phrase peut se visualiser dans un tableau appelé table de vérité dans lequel on fait apparaître les différentes valeurs de vérité possibles pour le couple (P, Q) (Vrai et Vrai, Vrai et Faux, ...) et, en correspondance, les valeurs de vérité de la proposition $P \Leftrightarrow Q$. Ainsi, la table de vérité de l'équivalence logique $P \Leftrightarrow Q$ est :

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

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Table 2.14 – Table de vérité de $P \Leftrightarrow Q$

On doit lire dans ce tableau que si les propositions P et Q ont la même valeur de vérité, la proposition $P \Leftrightarrow Q$ est vraie, et si P et Q ont des valeurs de vérité opposées, alors $P \Leftrightarrow Q$ est fausse.

Remarque 2.4. *On peut constater que l'équivalence logique joue pour les propositions, le rôle que joue l'égalité pour les nombres.*

Exemple 2.3.

— *Les expressions* $3+2$ *et* 5 *ne sont pas identiques et pourtant on écrit* $3+2=5$. *De même, les propositions* $(x^2=1)$ *et* $(x=1 \text{ ou } x=-1)$ *ne sont pas identiques et pourtant on écrit* $(x^2=1) \Leftrightarrow (x=1 \text{ ou } x=-1)$.

— *Les expressions « Le triangle ABC est rectangle » et « Le triangle ABC vérifiant* $AB^2+BC^2=AC^2$ *» ne sont pas identique et pourtant il y a une equivalence entres elles assurée par le théorème et le théorème inverse de Pythagore.*

2.5 C.N.S. , ssi , il faut et il suffit

Les expressions « **Condition nécessaire et suffisante (C.N.S.)** », « **si et seulement si (ssi)** », « **il faut et il suffit** » signifient toutes « **logiquement équivalent** » ou encore « $\Leftrightarrow$ ». Mais plus précisément, dans chacune de ces expressions, quel morceau correspond à « $\Rightarrow$ » et quel autre morceau correspond à « $\Leftarrow$ »? La réponse est fournie par le tableau suivant :

$\Rightarrow$	$\Leftarrow$
condition nécessaire il faut seulement si	condition suffisante il suffit si

Table 2.15 – Signification de l'implication directe "$\Rightarrow$" et l'implication inverse "$\Leftarrow$"

Exemple 2.4.

1. *Considérons par exemple l'implication vraie :*

$$\alpha : \{(n \geq 3 \text{ et } n \text{ premier }) \Rightarrow (n \text{ impair})\}$$

Si on cherche à l'énoncer dans le langage courant, on dira : pour que n soit un nombre premier supérieur ou égal à 3, il est nécessaire, il est obligatoire, il faut que n soit impair, mais on peut dire aussi que n peut être un nombre premier supérieur ou égal à 3 seulement si n est impair.

Mais si l'on considère l'implication contraire (qui est fausse) à savoir : n impair $\Rightarrow$ *(n* ≥ 3 *et n premier), on dira que pour que n soit un nombre premier supérieur ou égal à 3, il n'est pas suffisant, il ne suffit pas que n soit impair ou encore, si n est impair, n n'est pas nécessairement un nombre premier supérieur ou égal à 3.*

2. *Considérons encore l'implication vraie :*

$$(x+1)^2 = 9 \Leftarrow x+1 = 3$$

Pour que $(x+1)^2$ *soit égal à 9, il suffit, il est suffisant que* $x+1$ *soit égal à 3, ou encore* $(x+1)^2$ *vaut 9 si* $x+1$ *vaut 3. Mais, pour que* $(x+1)^2$ *soit égal à 9, il* *n'est pas nécessaire, il n'est pas obligatoire que $x+1$ soit égal 3 (car $x+1$ peut aussi être égal à -3) ou encore l'égalité $(x+1)^2 = 9$ ne se produit pas seulement si $x+1$ vaut 3 (l'implication $(x+1)^2 = 9 \Rightarrow x+1 = 3$ est fausse).*

2.6 Négation, Contraposée et Réciproque d'une implication

Définition 2.5. *Soient P et Q deux propositions et $P \Rightarrow Q$ l'implication logique de P vers Q.* ***La négation*** *de l'implication $P \Rightarrow Q$ notée $\neg(P \Rightarrow Q)$ est la donnée par :*

$$\mathcal{V}(\neg(P \Rightarrow Q)) := \begin{cases} 1 & si \quad \mathcal{V}(P \Rightarrow Q) = 0 \\ 0 & si \quad \mathcal{V}(P \Rightarrow Q) = 1 \end{cases}$$

Théorème 2.8. *Soient P et Q deux propositions. on a*

$$\alpha : \{\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q\}$$

est toujours vraie.

Démonstration. La table de vérité suivante

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$\neg Q$	$P \wedge \neg Q$	α
1	1	1	0	0	0	1
1	0	0	1	1	1	1
0	1	1	0	0	0	1
0	0	1	0	1	0	1

Table 2.16 – Démonstration du théorème 2.8

Montre bien le théorème. □

Ce théorème peut être démontrer aussi par une deuxième méthode on appliquant les théorèmes 2.3 et 2.5.

En effet ; on a

$$\begin{aligned} \neg(P \Rightarrow Q) &\Leftrightarrow \neg(\neg P \vee Q) \\ &\Leftrightarrow \neg(\neg P) \wedge \neg Q \\ &\Leftrightarrow P \wedge \neg Q \end{aligned}$$

□

Théorème 2.9. *Soient P et Q deux propositions. On a*

$$\alpha : \{(\neg Q \Rightarrow \neg P) \Leftrightarrow (P \Rightarrow Q)\}$$

est toujours vraie.

Démonstration. La table de vérité suivante

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	α
1	1	0	0	1	1	1
1	0	0	1	0	0	1
0	1	1	0	1	1	1
0	0	1	1	1	1	1

Table 2.17 – Démonstration du théorème 2.9

Montre bien le théorème. □

Définition 2.6 (Contraposée d'une implication). *Soient P et Q deux propositions. L'implication $\neg Q \Rightarrow \neg P$ s'appelle* ***la contraposée*** *(ou* ***l'implication contraposée****) de l'implication $P \Rightarrow Q$.*

La contraposée d'une implication est équivalente à celle-ci (voir théorème 2.9). Ceci fournira plus loin un type de raisonnement usuel : le raisonnement par contraposition.

Définition 2.7 (Réciproque d'une implication). *Soient P et Q deux propositions. L'implication $Q \Rightarrow P$ s'appelle la réciproque (ou l'implication réciproque) de l'implication $P \Rightarrow Q$.*

Le tableau suivant résume les trois dernières notions logiques et leurs significations :

Notion logique	Signification logique
La négation de $P \Rightarrow Q$	$P \wedge \neg Q$
La contraposée de $P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
La réciproque de $P \Rightarrow Q$	$Q \Rightarrow P$

Table 2.18 – Table signéficative de la négation, contraposé et réciproque d'une implication.

Exemple 2.5. *L'implication*

$$\forall n \geq 2 \quad (n \text{ premier et } n \neq 2) \Rightarrow n \quad \text{impaire} \tag{2.6.1}$$

La proposition (2.6.1) *est vraie.*

- *La contraposée de l'implication* (2.6.1) *est : (n pair) $\Rightarrow$ ($n = 2$ ou n non premier) et est (obligatoirement) vraie.*
- *La réciproque de l'implication* (2.6.1) *est : (n impair) $\Rightarrow$ (n premier et $n \neq 2$) et est fausse (puisque 9 n'est pas premier).*
- *Enfin, la négation de l'implication* (2.6.1) *est : (n premier et $n \neq 2$ et n est pair) et est (obligatoirement) fausse.*

D'une manière générale, la contraposée de $P \Rightarrow Q$ à savoir $\neg Q \Rightarrow \neg P$ est équivalente à $P \Rightarrow Q$ et a donc même valeurs de vérité, la négation de $P \Rightarrow Q$ à savoir $P \wedge \neg Q$ a des valeurs de vérité contraires. La véracité de la réciproque de $P \Rightarrow Q$ à savoir $Q \Rightarrow P$ n'a quant à elle aucun rapport avec celle de $P \Rightarrow Q$. Ces deux implications sont vraies ou fausses de manière totalement indépendantes.

3 Les quantificateurs universel "$\forall$" et existentiel "$\exists$"

3.1 Définition des quantificateurs

On se donne un ensemble E et une proposition $P(x)$ dont les valeurs de vérité sont fonction des éléments x de E. [2] [7]

Par exemple, considérons la proposition "$x^2 = 1$" dépendant d'un réel x. On ne peut pas dire que la phrase $x^2 = 1$ est vraie ou fausse tant qu'on ne sait pas ce que vaut x. Une telle proposition, dont les valeurs de vérité sont fonction d'une (ou plusieurs) variable(s) s'appelle *un prédicat*. Nous n'utiliserons plus ce terme par la suite. Cette proposition est vraie quand $x = 1$ ou quand $x = -1$ et est fausse dans les autres cas ou encore, la proposition "$x^2 = 1 \Leftrightarrow (x = 1 ou x = -1)$" est vraie pour tout choix du réel x.

D'une manière générale, on a la défintion :

Définition 3.1.

— *La proposition : « Pour tous les éléments x de E, la proposition $P(x)$ est vraie » s'écrit en abrégé :*

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

— *La proposition : « il existe au moins un élément x de E tel que la proposition $P(x)$ est vraie » s'écrit en abrégé :*

$$\exists x \in E / \quad P(x)$$

ou aussi

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

— *La proposition : « il existe un et un seul élément x de E tel que la proposition $P(x)$ est vraie » s'écrit en abrégé :*

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

Remarque 3.1.

Dans "$\exists x \in E / \quad P(x)$" ou "$\exists x \in E, \quad P(x)$", le "/" ou la virgule "," se lisent donc « tel que ».

Définition 3.2.

— *$\forall$ s'appelle le quantificateur universel ;*
— *$\exists$ s'appelle le quantificateur existentiel.*

Exercice

Exercice 3.1. *Ecrire avec des quantificateurs les propositions suivantes :*

1. *f est la fonction nulle (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
2. *Le dénominateur D de f s'annule au moins une fois sur $\mathbb{R}$.*
3. *f est l'identité de $\mathbb{R}$ (c'est-à-dire la fonction qui, à chaque réel, associe lui-même).*
4. *Le graphe de f coupe la droite d'équation $y = x$.*

5. *f est croissante sur $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
6. *L'équation $\sin x = x$ a une et une seule solution dans $\mathbb{R}$.*
7. *Pour tout point M du plan $\mathcal{P}$, M est sur le cercle $\mathcal{C}$ de centre Ω et de rayon ρ si et seulement si la distance de M à Ω vaut ρ.*

Corrigé de l'exercice 3.1.

1. $$\forall x \in \mathbb{R}, \quad f(x) = 0.$$
2. $$\exists x \in \mathbb{R} / \ \ D(x) = 0.$$
3. $$\forall x \in \mathbb{R}, \quad f(x) = x.$$
4. $$\exists x \in \mathbb{R} / \ \ f(x) = x.$$
5. *Ici on a plusieurs méthodes possibles*
   (a) *Première méthode :*
   $$\forall x, y \in \mathbb{R}, \ \ (x \leq y \Rightarrow f(x) \leq f(y))$$
   (b) *Deuxième méthode :*
   $$\forall x \in \mathbb{R}, \ \ \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \geq 0.$$
   (c) *Troixième méthode :*
   $$\forall x \in \mathbb{R}, \ \ f'(x) \geq 0 \quad f' \text{ est la dirivé de } f.$$
6. $$\exists ! x \in \mathbb{R}, \ \ \sin x = x.$$
7. $$\forall M \in \mathcal{P} \ \ (M \in \mathcal{C} \Leftrightarrow M\Omega = \rho).$$

Remarque 3.2.

1. *Dans la solution de l'exercice 3.1, en 5), il ne faut pas lire que pour tout x, y des réels, on a $x \leq y$ ou encore, il ne faut pas lire*
   $$(\forall x, y \in \mathbb{R}, x \leq y) \Rightarrow f(x) \leq f(y).$$
   Mais, il faut lire que pour tout x et y des réels, l'implication
   $$(x \leq y \Rightarrow f(x) \leq f(y)) \quad \text{est vraie.}$$

2. *De la même façon, en 7), il ne faut pas lire que tout point du plan est sur le cercle ou encore il ne faut pas lire*

$$(\forall M \in \mathcal{P}\ ,\ M \in \mathcal{C}) \Leftrightarrow (M\Omega = \rho)$$

mais il faut lire que pour tout point du plan, il est équivalent de dire que M est sur le cercle et que $M\Omega = \rho$. Dans cette phrase, le point M a la possibilité de ne pas être sur le cercle.

Exercice

Exercice 3.2. *Montrer que :*

$$\exists x \in \mathbb{R}/ \quad \sin(x) = x.$$

Corrigé de l'exercice 3.2. *On sait bien que* $\sin 0 = 0$ *et que* $0 \in \mathbb{R}$ *donc*

$$\exists x \in \mathbb{R}/ \quad \sin(x) = x.$$

Ici x est dit point fixe local au voisinage de 0.

Montrer qu'il existe un élément x de E vérifiant une certaine propriété, c'est fournir explicitement un tel élément.

Pour montrer la phrase ou la proposition

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

la plupart du temps, on fournit explicitement un élément précis x_0 de E vérifiant la propriété désirée.

Il est certain que, dans l'ensemble du cours de mathématiques, Nous aurons à disposition un petit nombre de théorèmes qui affirment l'existence d'un objet sans le fournir explicitement.

Exemple 3.1.

1. *Le théorème exposé au lycée : « **toute suite réelle croissante et majorée converge** » affirme qu'il existe une limite sans pour autant la fournir.*
2. *Le théorème fondamental de l'algèbre exposé en L2 : « **toute équation polynômiale de degré supérieur ou égal à** 1 **à coefficients dans** $\mathbb{C}$ **admet au moins une solution dans** $\mathbb{C}$ ». Ce théorème affirme l'existence d'une solution sans pour autant fournir cette solution.*
3. *Le corollaire du théorème des valeurs intermédiaires qui affirme que « **si** f **est une fonction continue sur un intervalle** I **de** $\mathbb{R}$ **à valeurs dans** $\mathbb{R}$ **qui prend une valeur positive en un réel** a **de** I **et une valeur négative en un réel** b **de** I**, alors l'équation** $f(x) = 0$ **admet au moins une solution dans** I ».*

3.2 Propriétés des quantificateurs avec une variable

Théorème 3.1. *Soient E un ensemble et $P(x)$ une proposition dont les valeurs de vérité sont fonction des éléments x de E.*

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

Dans le théorème 3.1, on constate que le contraire de $\forall$ est $\exists$ et le contraire de $\exists$ est $\forall$.

Exemple 3.2. *Dans la définition d'une fonction f continue en un réel x_0, on écrit :*

$$\{f \text{ est continue en } x_0\} \;\Leftrightarrow\; \{\forall \varepsilon > 0, \exists \eta > 0 \,/\, \forall x \in D_f, \, (|x - x_0| < \eta \;\Rightarrow\; |f(x) - f(x_0)| < \varepsilon\}.$$

Le théorème 3.1 permettra de fournir mécaniquement la définition de : « f n'est pas continue en x_0 », en niant la proposition précédente.

$$\{f \text{ n'est pas continue en } x_0\} \;\Leftrightarrow\; \{\exists \varepsilon > 0 \,/\, \forall \eta > 0, \exists x \in D_f, \,/\, (|x - x_0| < \eta \text{ et } |f(x) - f(x_0)| \geq \varepsilon\}.$$

Remarque 3.3. *On rappelle ici que*

1. *La négation de "$P \Rightarrow Q$" est "$P \wedge \neg Q$".*
2. *La négation de "$<$" est "$\geq$".*
3. *La négation de "$\forall \varepsilon > 0, \cdots$" est "$\exists \varepsilon > 0 \,/\, \cdots$" et non pas "$\exists \varepsilon \leq 0 \,/\, \cdots$".*

D'une manière générale :
La négation de $\forall x \in E, \cdots$ est $\exists x \in E \,/\, \cdots$.

Exercice

Exercice 3.3. *Soit $f : \mathbb{R} \to \mathbb{R}$. Ecrire avec des quantificateurs les propositions suivantes :*

1. *f n'est pas nulle .*
2. *Le dénominateur D de la fraction ne s'annule pas sur $\mathbb{R}$.*
3. *f n'est pas l'identité de $\mathbb{R}$.*
4. *f n'est pas croissante sur $\mathbb{R}$.*

Corrigé de l'exercice 3.3.

1. $$\exists x \in \mathbb{R} \ / \ f(x) \neq 0.$$

2. $$\forall x \in \mathbb{R}$$

   Ici, on constate que les phrases « le dénominateur ne s'annule pas » et « le dénominateur n'est pas nul » n'ont pas du tout la même signification.

3. $$\exists x \in \mathbb{R} \ / \ f(x) \neq x.$$

4. $$\exists (x_0, y_0) \in \mathbb{R}^2 \ / \ (x \leq y \ \wedge \ f(x) > f(y))$$

   Ici, il a fallu nier l'implication

   $$x \leq y \Rightarrow f(x) \leq f(y).$$

Exercice 3.4.

1. *Montrer que la fonction* sin *n'est pas nulle.*
2. *Montrer que la fonction valeur absolue n'est pas dérivable sur* $\mathbb{R}$.

Corrigé de l'exercice 3.4.

1. *Il suffit de donner un contre exemple, par exemple pour* $x = \frac{\pi}{2}$ *on a* $\sin \frac{\pi}{2} = 1$. *Donc, la fonction* sin *n'est pas nulle.*
2. *La fonction valeur absolue n'est pas dérivable en* 0 *En effet ;*

   $$\lim_{h \to 0} \frac{|h|}{h} = \begin{cases} 1 & si \quad h \to 0^+ \\ -1 & si \quad h \to 0^- \end{cases}$$

   Donc n'est pas dérivable sur $\mathbb{R}$.

Remarque 3.4.

1. *Dire qu'une fonction* f *est la fonction nulle équivaut à dire :*

   $$\forall x \in \mathbb{R}, \quad f(x) = 0.$$

   Dire que f *n'est pas la fonction nulle (ou tout simplement n'est pas nulle) équivaut donc à dire :*

   $$\neg(\forall x \in \mathbb{R}, \quad f(x) = 0) \quad \Leftrightarrow \quad \exists x \in \mathbb{R} \ / \ f(x) \neq 0.$$

2. *Dire qu'une fonction* f *est dérivable sur* $\mathbb{R}$ *équivaut à dire :* $\forall x \in \mathbb{R}$, f *est dérivable en* x.
   Dire que f *n'est pas dérivable sur* $\mathbb{R}$ *équivaut donc à dire :*

   $$\neg \ (\forall x \in \mathbb{R}, f \text{ est dérivable en } x) \Leftrightarrow \exists x \in \mathbb{R} \ / \ f \text{ n'est pas dérivable en } x.$$

Comme nous l'avons dit plus haut, pour montrer une phrase du type :

$$\exists x \in \mathbb{R} / \cdots$$

on fournit explicitement un réel x tel que $\cdots$.

En 1., nous avons fourni le réel $\frac{\pi}{2}$ et en 2., le réel 0.

Théorème 3.2. *Soient E un ensemble et $P(x)$ une proposition dont les valeurs de vérité sont fonction des éléments x de E.*

1. $(\forall x \in E, P(x) \wedge Q(x)) \Leftrightarrow ((\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x)))$.
2. $(\forall x \in E, P(x) \vee Q(x)) \Leftarrow ((\forall x \in E, P(x)) \vee (\forall x \in E, Q(x)))$.
3. $(\exists x \in E, P(x) \wedge Q(x)) \Rightarrow ((\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x)))$.
4. $(\exists x \in E, P(x) \vee Q(x)) \Leftrightarrow ((\exists x \in E, P(x)) \vee (\exists x \in E, Q(x)))$.

Dans (2.) et (3.), on ne trouve pas d'équivalence mais seulement une implication. Pour le comprendre, commençons par analyser le langage courant. La phrase « dans la classe, il existe une personne qui est un garçon et une autre personne qui est une fille » est vraie mais une même personne ne peut jouer les deux rôles à la fois ou encore la phrase « il existe un élève qui est un garçon et une fille » est fausse. De même, la phrase « dans la classe, tout élève est un garçon ou une fille » est vraie mais la phrase « dans la classe, tout élève est un garçon ou tout éléve est une fille » est fausse.

Exemple 3.3.

1. *Considérons les deux propositions*

$$(\exists x \in \mathbb{R} \;/\; \cos x = 0) \quad \textit{et} \quad (\exists x \in \mathbb{R} \;/\; \sin x = 0)$$

et

$$(\exists x \in \mathbb{R} \;/\; \cos x = 0 \quad \textit{et} \quad \sin x = 0)$$

La première proposition est vraie car 0 est un réel x tel que $\sin x = 0$ et $\frac{\pi}{2}$ est un réel x tel que $\cos x = 0$. Ainsi, dans les deux affirmations $(\exists x \in \mathbb{R} \;/\; \cos x = 0)$ et $(\exists x \in \mathbb{R} \;/\; \sin x = 0)$, la lettre x utilisée deux fois ne désigne pas forcément un même nombre. La deuxième proposition est clairement fausse

$$(\textit{ car par exemple : } \quad \forall x \in \mathbb{R},\; \cos^2 x + \sin^2 x = 1 \neq 0.)$$

2. *On rappelle qu'une fonction f de $\mathbb{R}$ dans $\mathbb{R}$ est monotone si et seulement si elle est croissante ou décroissante sur $\mathbb{R}$.*
Ceci s'écrit avec des quantificateurs :

$$(\forall (x,y) \in \mathbb{R}^2,\; (x \leq y \Rightarrow f(x) \leq f(y))) \;\; \textit{ou} \;\; (\forall (x,y) \in \mathbb{R}^2,\; (x \leq y \Rightarrow f(x) \geq f(y))),$$

et ne s'écrit sûrement pas

$$\forall (x,y) \in \mathbb{R}^2,\; (x \leq y \Rightarrow f(x) \leq f(y) \;\; \textit{ou} \;\; f(x) \geq f(y)),$$

cette deuxième phrase étant, elle, vérifiée par toute fonction de $\mathbb{R}$ dans $\mathbb{R}$.

3. *On considère deux fonctions f et g de $\mathbb{R}$ dans $\mathbb{R}$. On suppose que $f \times g = 0$.*

Peut-on affirmer que l'on a $f = 0$ ou $g = 0$?

La réponse est non. Il suffit de considérer deux fonctions non nulles f et g telles que, à chaque fois que f ne s'annule pas, ce soit g qui s'annule. Par exemple, sur I un sous ensemble non vide de $\mathbb{R}$, on pose :

$$f : \begin{array}{ccl} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} 1 & si \quad x \in I \\ 0 & si \quad x \in \mathbb{R} - I \end{cases} \end{array} \qquad et \qquad g : \begin{array}{ccl} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} 0 & si \quad x \in I \\ 1 & si \quad x \in \mathbb{R} - I \end{cases} \end{array}$$

Pour ces fonctions f et g,
— *Si x est un réel élément de I , $f(x)g(x) = x \times 0 = 0$.*
— *Si x est un réel élément de $\mathbb{R} - I$, $f(x)g(x) = 0 \times x = 0$.*
Revenons à des fonctions quelconques f et g et exprimons ce qui précède avec des quantificateurs.

$$fg = 0 \Leftrightarrow \forall x \in \mathbb{R},\ f(x)g(x) = 0 \Leftrightarrow \forall x \in \mathbb{R},\ (f(x) = 0 \ \ ou \ \ g(x) = 0) \quad (3.2.1)$$

alors que

$$f = 0 \quad ou \quad g = 0 \Leftrightarrow (\forall x \in \mathbb{R},\ f(x) = 0) \ \ ou \ \ (\forall x \in \mathbb{R},\ g(x) = 0) \qquad (3.2.2)$$

Remarque 3.5.

1. *Les propositions* (3.2.1) *et* (3.2.2) *ne sont pas les mêmes et encore une fois, on ne peut donc pas distribuer $\forall$ sur le mot **ou**.*
2. *Dans la phrase* (3.2.1), *« le mot **ou** est une fonction de x » et en faisant varier x, c'est tantôt $f(x)$ qui peut être nul et tantôt $g(x)$. Ce n'est pas le cas dans la phrase* (3.2.2).
3. *On peut distribuer "$\forall$" sur "$\wedge$" et "$\exists$" sur "$\vee$".*
4. *On ne peut pas distribuer "$\forall$" sur "$\vee$" et "$\exists$" sur "$\wedge$".*

Exercice

Exercice 3.5. *Ecrire avec des quantificateurs les propositions suivantes :*

1. (a) *Tout entier naturel est pair ou impair.*
   (b) *Tout entier naturel est pair ou tout entier naturel est impair.*
2. (a) *f est strictement monotone sur $\mathbb{R}$.*
   (b) *f n'est pas strictement monotone sur $\mathbb{R}$.*

Corrigé de l'exercice 3.5.

1. *(a)*

$$\forall n \in \mathbb{N}, \ (n \text{ est pair ou } n \text{ est impair }).$$

(b)

$$(\forall n \in \mathbb{N}, \ n \text{ est pair }) \text{ ou } (\forall n \in \mathbb{N}, \ n \text{ est impair }).$$

2. *(a)*

$$(\forall (x,y) \in \mathbb{R}^2, \ (x < y \Rightarrow f(x) < f(y))) \text{ ou } (\forall (x,y) \in \mathbb{R}^2, \ (x < y \Rightarrow f(x) > f(y)))$$

(b)

$$(\exists (x,y) \in \mathbb{R}^2, \ (x < y \text{ et } f(x) \geq f(y))) \text{ et } (\exists (x,y) \in \mathbb{R}^2, \ (x < y \text{ et } f(x) \leq f(y)))$$

Remarque 3.6.

1. *Le* 1) *doit de nouveau convaincre que l'on ne peut pas distribuer* $\forall$ *sur* « ***ou*** ».
   En a), chaque fois que l'on se donne un entier n, ou bien la phrase « n est pair » est vraie, ou bien la phrase « n est impair » est vraie. Par suite, la phrase « n est pair ou n est impair » est vraie.
   Par contre, en b), la phrase « $\forall n \in \mathbb{N}$ *, n est pair » est fausse et la phrase «* $\forall n \in \mathbb{N}$*, n est impair » est fausse. En conséquence, la phrase « (*$\forall n \in \mathbb{N}$*, n est pair) ou (*$\forall n \in \mathbb{N}$*, n est impair) » est fausse.*
   Les affirmations a) et b) ne sont pas les mêmes.
2. *Une fois que l'on est mis en garde sur l'utilisation de* $\forall$ *et « ou », la définition correcte d'une fonction monotone doit sortir naturellement. Cette définition n'est en aucun cas :*

$$\forall (x,y) \in \mathbb{R}^2, \ (x \leq y \Rightarrow (f(x) < f(y) \ \text{ ou } \ f(x) > f(y))).$$

   La négation de cette définition s'obtient alors mécaniquement. Il s'agit d'un calcul sur les symboles $\forall, \Rightarrow, \wedge, \ldots$ *et le chapitre en cours a pour but d'en exposer les règles. Une fois, ces règles et leurs significations acquises, il n'est plus besoin de réfléchir pour manipuler ces différents objets, de même que l'on ne réfléchit plus depuis longtemps (à tort) à la signification d'égalités du genre* $9 \times 8 = 72$ *ou* $2(x+y) = 2x + 2y$ *ou* $\frac{1}{2} + \frac{1}{3} = \frac{3+2}{6}$.

3.3 Propriétés des quantificateurs avec deux variables

Dans ce qui suit, $P(x,y)$ désigne une proposition dont les valeurs de vérité dépendent de deux variables x et y comme par exemple la proposition $2x + y > 0$ pour x et y réels donnés. Cette affirmation est vraie si le point de coordonnées (x,y) est strictement au-dessus de la droite d'équation $y = -2x$ et fausse sinon.

Théorème 3.3.

1. $((\forall x \in E), (\forall y \in E), P(x,y)) \Leftrightarrow ((\forall y \in E), (\forall x \in E), P(x,y))$
2. $((\exists x \in E), (\exists y \in E), P(x,y)) \Leftrightarrow ((\exists y \in E), (\exists x \in E), P(x,y))$

Remarque 3.7.

1. *On peut permuter des quantificateurs de même nature.*
   Si on note par E^2 *l'esemble des couples* (x, y) *tels que* $x \in E$ *et* $y \in E$*, la phrase*
$$\forall x \in E,\ \forall y \in E,\ \ P(x,y)$$
   peut alors s'écrire plus simplement
$$\forall (x,y) \in E^2,\ \ P(x,y).$$
   Et la phrase
$$\exists x \in E,\ \exists y \in E,\ \ P(x,y)$$
   peut alors s'écrire plus simplement
$$\exists (x,y) \in E^2,\ \ P(x,y).$$
2. *On ne peut pas permuter des quantificateurs de natures différentes.*

Théorème 3.4. *On a l'implication*

$$((\exists x \in E)/(\forall y \in E, P(x,y))) \Rightarrow: (\forall y \in E, \exists x \in E/P(x,y)).$$

mais l'implication inverse est fausse.

Remarque 3.8.

1. *Quand on écrit* $\exists x \,/\, \forall y$ *l'élément* x *est fourni une bonne fois pour toutes avant les* y *et est donc constant quand* y *varie.*
2. *Quand on écrit* $\forall y,\ \exists x$ *l'élément* x *est fourni après chaque* y*. Il dépend de* y *et peut donc varier quand* y *varie.*

Exemple 3.4.

En algèbre linéaire, pour résoudre l'exercice suivant

Soient E *un espace vectoriel et* f *une application linéaire de* E *dans lui-même vérifiant*

$$\forall \vec{u} \in E,\ \exists \lambda \in \mathbb{R} \,/\, f(\vec{u}) = \lambda \vec{u}. \tag{3.3.1}$$

Montrer que f *est une homothétie vectorielle (c'est-à-dire*

$$\exists \lambda \in \mathbb{R},\ \forall \vec{u} \in E,\ /\ f(\vec{u}) = \lambda \vec{u}.$$

Résoudre cet exercice consistera à montrer que le réel λ *fourni dans* (3.3.1) *est en fait indépendant du vecteur* $\vec{u}$ *ou encore que ce réel ne varie pas quand* $\vec{u}$ *varie.*

Exercice

Exercice 3.6. *Ecrire avec des quantificateurs les propositions suivantes :*

1. (a) *f est constante sur $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
   (b) *f n'est pas constante sur $\mathbb{R}$.*
2. (a) *f est une homothétie (où f est une transformation du plan $\mathcal{P}$).*
   (b) *f n'est pas une homothétie.*
3. (a) *Pour chaque entier, on peut trouver un entier strictement plus grand (cette affirmation est vraie).*
   (b) *Il y a un entier plus grand que tous les entiers (cette affirmation est fausse).*

Corrigé de l'exercice 3.6.

1. (a)
$$\exists \alpha \in \mathbb{R} \,/\, \forall x \in \mathbb{R},\ f(x) = \alpha$$
ou encore
$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R},\ f(x) = f(y)$$
ou encore plus simplement
$$\forall x \in \mathbb{R},\ f(x) = f(0)$$
   (b)
$$\forall \alpha \in \mathbb{R},\ \exists x \in \mathbb{R} \,/\ f(x) \neq \alpha$$
ou encore
$$\exists x \in \mathbb{R}, \exists y \in \mathbb{R} \,/\ f(x) \neq f(y)$$
ou encore plus simplement
$$\exists x \in \mathbb{R} - \{0\} \,/\ f(x) \neq f(0)$$
2. (a)
$$\exists \alpha \in \mathbb{R},\ \exists \Omega \in \mathcal{P} \,/\, \forall M \in \mathcal{P},\ \overrightarrow{\Omega f(M)} = \alpha \overrightarrow{\Omega M}$$
   (b)
$$\forall \alpha \in \mathbb{R},\ \forall \Omega \in \mathcal{P},\ \exists M \in \mathcal{P} \,/\ \overrightarrow{\Omega f(M)} \neq \alpha \overrightarrow{\Omega M}$$
3. (a)
$$\forall n \in \mathbb{N},\ \exists m \in \mathbb{N} \,/\, m > n$$
   (b)
$$\exists n \in \mathbb{N} \,/\ \forall m \in \mathbb{N} \,/\, m > n$$

Remarque 3.9.

1. *La définition correcte d'une fonction constante, donnée en (1.), est à mémoriser. Elle sera par exemple utile pour calculer des primitives ou plus généralement pour résoudre certaines équations différentielles. Cette définition n'est sûrement pas*
$$\forall x \in \mathbb{R},\ \exists \alpha \in \mathbb{R} \,/\, f(x) = \alpha. \tag{3.3.2}$$

Cette dernière affirmation est vérifiée par toute fonction de $\mathbb{R}$ *dans* $\mathbb{R}$*, car malheureusement, l'ordre* $\forall x$*,* $\exists \alpha$ *permet au nombre* α *de changer de valeur quand* x *change lui-même de valeur.*

Accessoirement, on doit noter que le phrase

$$\forall x \in \mathbb{R},\ f(x) = cte$$

est une version catastrophique de la phrase (3.3.2)*, phrase qui était déjà fausse.*

2. *Le problème est identique en* 2.*a*) *et en* 3..

   *En*2.*a*)*, le centre* Ω *et le rapport* α *doivent être indépendants du point variable* M*. Le bon ordre est donc* $\exists \alpha,\ \exists \Omega \ / \ \forall M\ \cdots$

   En 3.*, on sait bien que seul a*) *est vrai. Ainsi, pour chaque* n*, on peut fournir un* m *dépendant de* n *et strictement plus grand que* n*, et c'est ce que l'on a fait : l'entier* $m = n + 1$ *est effectivement variable quand* n *varie.*

Chapitre 3

Le langage propositionnel

On rappelle ici qu'une proposition est un assemblage de mots d'une langue naturelle vérifiant les trois propositions suivantes :

1. Il est reconnu syntaxiquement correct ;
2. Il est sémantiquement correct ;
3. Il est possible de lui assigner sans ambiguïté une valeur de vérité (vrai ou faux).

Exemple 0.1.

1. *Le roi du Maroc Mohamed* 6 *est une nombre pair !*
   Un littéraire attribuera à cette phrase la première propriété mais pas la deuxième ! Ce n'est donc pas une proposition.
2. *Dans, un triangle rectangle, le carré de l'hypoténuse est égale à la somme des carrés des deux cotés de l'angle droit.*
   Les trois propriétés sont vérifiées, c'est donc une proposition vraie.
3. *Il pleut à Setif.*
   Les deux premières propriétés sont vérifiées, mais pas la troisième ! ce n'est don pas une proposition.

Le langage propositionnel est composé de formules représentant des propositions. Comme les autres langages, le langage du calcul propositionnel est caractérisé par sa syntaxe et sa sémantique.

1 La syntaxe du langage propositionnel

La syntaxe d'un langage définit l'alphabet et les règles (Grammaire) des expressions du langage. Elle ne s'intéresse pas à leurs sens.

L'alphabet

L'alphabet est composé des symboles du langage, il comporte :

— Un ensemble dénombrable de variables propositionnelles. On convient d'utiliser les lettres de l'alphabet latin ($a, b, c, \ldots$) éventuellement indicées.

— Des connecteurs logiques ($\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$).
— Des symboles auxiliaires

Les règles d'écriture

Les règles d'écriture précisent la manière dont sont assemblés les symboles de l'alphabet pour former des expressions bien formées (ou formules) du langage propositionnel :

1. Toute variable propositionnelle est une formule ;
2. Si α est une formule, alors non $\neg\alpha$ est une formule ;
3. Si α et β sont deux formules alors $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \Rightarrow \beta)$ et $(\alpha \Leftrightarrow \beta)$ sont des formules.
4. Toute expression n'est pas une formule que si elle est écrite conformément aux trois règles précédentes.

Exemple 1.1.

1. *Si P et Q sont des variables propositionnelle, alors se sont des formules.*
2. *$P \vee Q$ est une formule.*
3. *$P\neg Q \vee P$ n'est pas une formule.*

1.1 Priorité des connecteurs

Les connecteurs sont appliqués dans l'ordre suivant :

$$\neg \;,\quad \wedge \;,\quad \vee \;,\quad \Rightarrow \;,\quad \Leftrightarrow .$$

Exemple 1.2.

1. *$\neg P \wedge Q$: Première priorité pour la négartion, ensuite la conjonction et on lit : non P et Q et on écrit $(\neg P) \wedge Q$.*
2. *$P \vee Q \wedge R$: On écrit $P \vee (Q \wedge R)$ et on lit : P ou (Q et R).*
3. *$P \vee Q \vee R$ ici c'est l'associativité et la commutativité du connecteur $\vee$ qui entre en jeu.*
4. *$P \wedge Q \Rightarrow R$ ici la conjonction passe avant l'implication.*

2 Satisfiabilité

Une formule α est dite satisfiable si et seulement si sa table de vérité contient au moins une ligne où la valeur de vérité de α est vraie (ou $\mathcal{V}(\alpha) = 1$).

α est dite insatisfiable si elle est fausse sur toutes les lignes de sa table de vérité.

Exemple 2.1.

1. *Soit*
$$\alpha : P \vee Q \Rightarrow R$$
α est satisfiable. En effet ;
$$\begin{aligned} \alpha : P \vee Q \Rightarrow R &\Leftrightarrow \neg(P \vee Q) \vee R \\ &\Leftrightarrow (\neg P \wedge \neg Q) \vee R \\ &\Leftrightarrow (\neg P \vee R) \wedge (\neg Q \vee R). \end{aligned}$$
On peut voir facilement que par exemple :
$$\mathcal{V}(\alpha) = \begin{cases} 1 & si \quad \mathcal{V}(R) = 1 \ \vee \ (\mathcal{V}(P) = 0 \ \wedge \ \mathcal{V}(Q) = 0) \\ 0 & si \quad (\mathcal{V}(R) = 0 \ \wedge \ \mathcal{V}(P) = 1) \vee (\mathcal{V}(R) = 0 \ \wedge \ \mathcal{V}(Q) = 1) \end{cases}$$

2. *Soit*
$$\beta : (P \wedge Q) \wedge \neg(P \Leftrightarrow Q)$$
On rappel ici que la négation d'une equivalence est le non exclusive ou le Xor q'on note :
$$\neg(P \Leftrightarrow Q) \equiv P \otimes Q$$
définit par
$$\mathcal{V}(P \otimes Q) = \begin{cases} 1 & si \quad \mathcal{V}(P) \neq \mathcal{V}(Q) \\ 0 & si \quad \mathcal{V}(P) = \mathcal{V}(Q) \end{cases}$$
et la conjonction de P et Q est donnée par
$$\mathcal{V}(P \wedge Q) = \begin{cases} 1 & si \quad \mathcal{V}(P) = \mathcal{V}(Q) = 1 \\ 0 & si \quad sinon \end{cases}$$
Ce qui montre que les valeur de vérité de la conjonction de $P \wedge Q$ et $P \otimes Q$ est toujours 0*. Donc β est insatisfiable.*

Remarque 2.1. *Une formule insatisfiable est dite antilogie ou contradiction.*

3 Satisfiabilité d'un ensemble de formules

On généralise la notion de *satisfiabilité* à un ensemble de formules :

Définition 3.1. *Soit $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ un ensemble de formules. Γ est dit satisfiable si et seulement si étant donné la table de vérité de toutes les formules $\alpha_1, \alpha_2, \cdots, \alpha_n$, il existe au moins une lignes où toutes ces formules sont vraies simultanément.*

La satisfiabilité d'un ensemble de formules est assimilée à la conjonction de toutes ses formules.

Exemple 3.1.

1. *L'ensemble*
$$\Gamma_1 = \{P \wedge Q,\ P \vee Q,\ P \Rightarrow Q\}$$
est satisfiable. En effet ;
La table de vérité de Γ_1 est

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$
1	1	1	1	1
1	0	0	1	0
0	1	0		1
0	0	0	0	1

Table 3.1 – Table de vérité de Γ_1 de l'exemple 3.1

On peut observer que les valeurs de vérité de la première ligne sont toutes 1*, ce qui montre que Γ_1 est satisfiable.*

2. *L'ensemble*
$$\Gamma_2 = \{P \wedge Q,\ P \vee Q,\ \neg P\}$$
est insatisfiable. En effet ;
La table de vérité de Γ_2 est

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$
1	1	1	1	0
1	0	0	1	0
0	1	0	1	1
0	0	0	0	1

Table 3.2 – Table de vérité de Γ_2 de l'exemple 3.1

On peut observer que les valeurs de vérité ne sont jamais identiques sur toutes les lignes, ce qui montre que Γ_2 est insatisfiable.

3.1 Tautologie

Définition 3.2. *Une formule α est une tautologie (on note $\models \alpha$), si et seulement si α est vraie sur toutes les lignes de sa table de vérité.*

On peut résumer
$$\models \alpha \Leftrightarrow \mathcal{V}(\alpha) \in \{1\}.$$

Exemple 3.2.
La formule
$$\alpha : P \wedge Q \Rightarrow Q$$
est une tautologie. En effet ;
La table de vérité de α est

P	Q	$P \wedge Q$	$P \Rightarrow Q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

Table 3.3 – Table de vérité de α de l'exemple 3.2

Les valeurs de vérité de la dernière colonne sont toutes identiques et leurs valeurs est 1*, donc* $\models \alpha$*.*

Remarque 3.1.

1. *Si* $\models \alpha \Rightarrow \beta$*, on dit que* α *implique logiquement* β*.*
2. *Si* $\models \alpha \Leftrightarrow \beta$*, on dit que* α *est logiquement équivalente à* β *et on note* $\alpha \equiv \beta$*.*

Lemme 3.1. *Une formule* α *est une tautologie si et seulement si* $\neg\alpha$ *est insatisfiable.*

Démonstration.

$\Rightarrow$ Par l'absurde, on suppose que $\models \alpha$ et $\neg\alpha$ est satisfiable. Donc, il existe au moins une ligne de la table de vérité où $\neg\alpha$ est vraie. Pour cette ligne, α est fausse mais $\models \alpha$, absurde. Alors $\neg\alpha$ est insatisfiable.

$\Leftarrow$ Toujours par l'absurde, supposons maintenant que $\neg\alpha$ est insatisfiable mais α n'est pas une tautologie.

Donc, il existe au moins une ligne de la table de vérité où α est fausse. Pour cetteligne, $\neg\alpha$ doit être vraie ce qui contredit le fait que $\neg\alpha$ est insatisfiable.

□

Théorème 3.1. *Soit* α *et* β *deux formules logique.*

$$\textit{Si} \quad \models \alpha \ \textit{ et } \ \models \alpha \Rightarrow \beta, \ \textit{ alors } \ \models \beta.$$

Autrement dit : Si α est une tautologie, et α implique logiquement β, alors β est une tautologie.

Démonstration. Par l'absurde.

Supposons que α est une tautologie, et α implique logiquement β, mais β est insatisfiable ($\not\models \beta$). Donc, il existe au moins une ligne où β est fausse. Pour cette ligne, $\alpha \Rightarrow \beta$ est fausse car $\models \alpha$. Contradiction avec le fait que $\models \alpha \Rightarrow \beta$. □

4 Conséquence logique

En langage propositionnel, une formule β est conséquence logique d'une formule β (et on note $\alpha \models \beta$), si et seulement si étant donné la table de vérité de α et β, la valeur de vérité de β est vraie sur toutes les lignes où la valeur de vérité de α est vraie.

De manière générale, une formule β est conséquence logique d'un ensemble de formules $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ (et on note $\Gamma \models \beta$ ou encore $\alpha_1, \alpha_2, \cdots, \alpha_n \models \beta$) si et seulement si étant donné la table de vérité des formules $\alpha_1, \alpha_2, \cdots, \alpha_n, \beta$, la valeur de vérité de β est vraie sur toutes les lignes où les formules $\alpha_1, \alpha_2, \cdots, \alpha_n$ sont vraie simultanément.

Remarque 4.1.

1. $$\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \models \alpha \textit{ si et seulement si } \models \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n \Rightarrow \alpha.$$

   Autrement dit, si $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ est un ensemble de formules, dire que α est une conséquence logique de Γ est équivalent à dire que la conjonction de toutes les $\{\alpha_i,\ 1 \leq i \leq n\}$ ($\bigwedge_{i=1}^{n} \alpha_i$) implique logiquement α.
2. *Soit E un ensemble de formules et $A \subseteq E$. Alors, si E est satisfiable, A est satisfiable.*
3. *L'ensemble vide est satisfiable.*
4. *L'ensemble de toutes les formules est insatisfiable.*
5. *Soit E un ensemble de formules et $A \subseteq E$. Alors, si A est insatisfiable alors E est insatisfiable.*
6. *Toute formule est conséquense logique d'un ensemble insatisfiable.*
7. *Toute tautologie est conséquense logique d'un ensemble quelconque de formules, en particulier de l'ensemble vide.*

5 Théorème de substitution

On note par T une tautologie, ou un théorème logique. Sa négation sera notée par $\neg T := \perp$.

On rappel les règles suivante pour toute proposition logique P :

1. $P \wedge \neg P \equiv \perp$.
2. $P \vee \neg P \equiv T$.
3. $T \wedge P \equiv P$.
4. $T \vee P \equiv T$.
5. $\perp \wedge P \equiv \perp$.
6. $\perp \vee P \equiv P$.
7. $\alpha \equiv T$ si et seulement si $\models \alpha$.
8. $\alpha \equiv \perp$ si et seulement si $\not\models \alpha$.

Soit β une formule où figure la variable propositionnelle x, et soit β' la formule obtenue à partir de β en substituant à x, en toutes ses occurrences, une formule α.

$$\textit{Si} \quad \models \beta, \ \textit{alors} \quad \models \beta'.$$

Exemple 5.1.

Soit

$$\beta \equiv x \Rightarrow ((y \Rightarrow z) \Rightarrow x).$$

β est une tautologie. En effet ;

$$\begin{aligned} x \Rightarrow ((y \Rightarrow z) \Rightarrow x) &\equiv \neg x \vee (\neg(\neg y \vee z) \vee x) \\ &\equiv \neg x \vee ((y \wedge \neg z) \vee x) \\ &\equiv (\neg x \vee (y \wedge \neg z)) \vee (\neg x \vee x) \\ &\equiv (\neg x \vee (y \wedge \neg z)) \vee T \\ &\equiv T \end{aligned}$$

Donc $\models \beta$.

Soit

$$\beta' \equiv (a \wedge b) \Rightarrow ((y \Rightarrow z) \Rightarrow (a \wedge b)).$$

obtenue en substituant dans β, $(a \wedge b)$ à x. Alors, $\models \beta'$.

6 Théorème de remplacement

Soit α une formule dans laquelle apparaît en une ou plusieurs occurrences la formule β, et soit α' la formule obtenue à partir de α en remplaçant β en une ou plusieurs de ses occurrences par la formule β'.

$$\textit{Si} \quad \beta \equiv \beta', \quad \textit{alors} \quad \alpha \equiv \alpha'.$$

Exemple 6.1.

Soit

$$\alpha : x \vee (x \Rightarrow y) \Leftrightarrow (z \vee (z \Rightarrow y)).$$

Si on note par

$$\beta : z \Rightarrow y \quad \textit{et} \quad \beta' : \neg z \vee y$$

Dans α, si on remplace β par β' on obtient

$$\alpha' : x \vee (x \Rightarrow y) \Leftrightarrow (z \vee (\neg z \vee y)).$$

Pour montrer que $\alpha \equiv \alpha'$, il suffit de montrer que $\beta \equiv \beta'$. En effet ;

Par application du théorème 2.5, on obtient

$$\beta : z \Rightarrow y \ \equiv \ \neg z \vee y : \beta'.$$

7 Système complet de connecteurs

Définition 7.1. *Un ensemble Γ de connecteurs est dit complet, si étant donné une formule quelconque α du calcul propositionnel, on peut trouver une formule α' dans laquelle n'interviennent que les éléments de Γ et telle que $\alpha \equiv \alpha'$.*

Théorème 7.1. *Les deux ensembles*

$$\Gamma_\wedge = \{\neg, \wedge\} \quad et \quad \Gamma_\vee = \{\neg, \vee\}$$

sont complets.

Démonstration.

1. Commençant par $\Gamma_\wedge = \{\neg, \wedge\}$
   Soit P et Q deux proposition logiques. L'espace des connecteurs est conçu de
   $$\neg,\ \wedge,\ \vee,\ \Rightarrow \quad et \quad \Leftrightarrow.$$
   — Pour les deux premiers connecteurs, pas de problème !
   — Si on pose $\alpha : P \vee Q$, par les lois de Morgan on peut écrire
   $$\alpha : P \vee Q \equiv \neg(\neg P \wedge \neg Q).$$
   — Si on pose $\beta : P \Rightarrow Q$, Par le théorème 2.5 et les lois de Morgan dans le théorème 2.3, on obtient
   $$\begin{aligned} \beta : P \Rightarrow Q &\equiv \neg P \vee Q \\ &\equiv \neg(P \wedge \neg Q). \end{aligned}$$
   — Si on pose $\gamma : P \Leftrightarrow Q$ Par les théorèmes 2.7 et 2.5 et les lois de Morgan dans le théorème 2.3, on obtient
   $$\begin{aligned} \gamma : P \Leftrightarrow Q &\equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\ &\equiv (\neg P \vee Q) \wedge (\neg Q \vee P) \\ &\equiv \neg(P \wedge \neg Q) \wedge \neg(Q \wedge \neg P). \end{aligned}$$
2. Pour $\Gamma_\vee = \{\neg, \vee\}$
   Soit P et Q deux proposition logiques. L'espace des connecteurs est conçu de
   $$\neg,\ \wedge,\ \vee,\ \Rightarrow \quad et \quad \Leftrightarrow.$$
   — Pour le premier et le troisième connecteurs, pas de problème !
   — Si on pose $\alpha : P \wedge Q$, par les lois de Morgan on peut écrire
   $$\alpha : P \wedge Q \equiv \neg(\neg P \vee \neg Q).$$
   — Si on pose $\beta : P \Rightarrow Q$, Par le théorème 2.5 et les lois de Morgan dans le théorème 2.3, on obtient
   $$\beta : P \Rightarrow Q \equiv \neg P \vee Q.$$
   — Si on pose $\gamma : P \Leftrightarrow Q$ Par les théorèmes 2.7 et 2.5 et les lois de Morgan dans le théorème 2.3, on obtient
   $$\begin{aligned} \gamma : P \Leftrightarrow Q &\equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\ &\equiv (\neg P \vee Q) \wedge (\neg Q \vee P) \\ &\equiv \neg(\neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)). \end{aligned}$$

□

8 Forme normale

Définition 8.1. *Un atome ou formule atomique est une formule ne comportant qu'une variable propositionnelle (pas de connecteurs).*

Définition 8.2. *Un littéral est une formule atomique ou la négation d'une formule atomique.*

Définition 8.3. *Un monôme conjonctif est une conjonction de littéraux.*

Définition 8.4. *Une clause est une disjonction de littéraux.*

Définition 8.5. *Une formule est en forme normale conjonctive si elle est une conjonction de clauses.*

Définition 8.6. *Une formule est en forme normale disjonctive si elle est une disjonction de monômes.*

Il est nécessaire d'avoir un moyen algorithmique pour obtenir la (FND) et la (FNC) à partir de la table de vérité.

8.1 Forme normale disjonctive (FND)

Soit α une formule du calcul propositionnel ayant n variables $x_1, x_2, \cdots, x_n$.

Supposons que A est la table de vérité de α. La FND de α est obtenue de la manière suivante :

1. Soit p le nombre de lignes de A telles que $\mathcal{V}(\alpha) = 1$.
2. Pour chaque ligne i, $1 \leq i \leq p$ où $\mathcal{V}(\alpha) = 1$, soit M_i le monôme conjonctif correspondant.

$$M_i = \bigwedge_{k=1}^{n} m_{ik}, \quad \textit{tels que} \quad m_{ik} = \begin{cases} x_k & si \quad \mathcal{V}(x_k) = 1 \\ \neg x_k & si \quad \mathcal{V}(x_k) = 0 \end{cases}.$$

3. La (FND) de α est alors

$$FND(\alpha) : \bigvee_{i=1}^{p} M_i.$$

8.2 Forme normale conjonctive (FNC)

D'une manière analogue, on obtient la FNC d'une formule α.

Soit α une formule du calcul propositionnel ayant n variables $x_1, x_2, \cdots, x_n$. Supposons que A est la table de vérité de α. La FNC de α est obtenue de la manière suivante :

1. Soit q le nombre de lignes de A telles que $\mathcal{V}(\alpha) = 0$.
2. Pour chaque ligne i, $1 \leq i \leq q$ où $\mathcal{V}(\alpha) = 0$, soit C_i le monôme conjonctif correspondant.

$$C_i = \bigvee_{k=1}^{n} c_{ik}, \quad \textit{tels que} \quad c_{ik} = \begin{cases} x_k & si \quad \mathcal{V}(x_k) = 0 \\ \neg x_k & si \quad \mathcal{V}(x_k) = 1 \end{cases}.$$

3. La (FNC) de α est alors

$$FNC(\alpha) : \bigwedge_{i=1}^{q} C_i.$$

Remarque 8.1.

1.

$$FND(\alpha) \ \equiv \ \alpha \ \equiv \ FNC(\alpha).$$

2. Par convention,

$$\textit{Si} \quad \models \alpha, \ \textit{alors} \quad FND(\alpha) \equiv 1.$$

3. Par convention,

$$\textit{Si} \quad \not\models \alpha, \ \textit{alors} \quad FNC(\alpha) \equiv 0.$$

9 Erreurs classiques à ne pas commettre

1. Croire que le contraire de $x \geq 0$ est $x \leq 0$.

   Le contraire de $x \geq 0$ est $x < 0$.

2. Confondre $\Rightarrow$ et $\Leftrightarrow$.

   Une équivalence est constituée de deux implications.

3. Refuser l'usage des quantificateurs $\forall$ et $\exists$.
   Par exemple, la phrase $\sin(x) \neq x$ n'a pas de sens.
   Signifie-t-elle $\forall x \in \mathbb{R},\ \sin(x) \neq x$, auquel cas elle est fausse car $\sin(0) = 0$, ou signifie-t-elle que la fonction *sinus* n'est pas la fonction $x \mapsto x$, auquel cas elle devrait être proprement écrite sous la forme $\exists x \in \mathbb{R} \ / \ \sin(x) \neq x$ ou aussi $\sin x \neq Id_{\mathbb{R}}$? De manière générale,

   Tout résultat contenant une variable doit être précédé du quantificateur adéquat.

4. Placer n'importe où des quantificateurs.

   Par exemple, la phrase $f(x) \neq 0,\ \forall x \in \mathbb{R}$ n'est pas vraiment correcte car dans cette phrase, la première fois que l'on parle de x ($f(x) \neq 0$), on ne sait pas ce que x représente et on doit attendre encore le $\forall x \in \mathbb{R}$ pour savoir qu'il s'agit d'un réel ou encore, la première fois que l'on parle de x, x n'est pas défini.

   La bonne phrase est $\forall x \in \mathbb{R},\ f(x) \neq 0$ et se lit de manière naturelle : pour tout réel x, $f(x)$ est différent de 0.

   Une phrase du genre « $\forall$ point $M \in$ au plan, ... » n'est pas correcte non plus, car elle mélange deux langages. On doit l'écrire ou bien « $\forall M \in \mathcal{P}$ », ou bien « pour tout point M du plan ».

5. Penser que les phrases

$$\forall n \in \mathbb{N},\ \exists m \in \mathbb{N}\ /\ m > n\ et\ \exists m\ /\ \forall n \in \mathbb{N} \in \mathbb{N},\ m > n$$

signifient la même chose et donc, ne prêter aucune attention à l'ordre des quantificateurs.

6. Penser que les phrases

$$\forall x \in \mathbb{R},\ (f(x) = 0\ ou\ g(x) = 0)$$

et

$$((\forall x \in \mathbb{R},\ f(x) = 0)\ ou\ (\forall x \in \mathbb{R},\ g(x) = 0))$$

signifient la même chose. Encore une fois, on ne peut pas distribuer $\forall$ sur **ou**.

Chapitre 4

La logique d'ordre 0

Enormément de problèmes peuvent être formulés en logique des propositions, mais quand le nombre de variables est important ou inconnu, l'utilisation des tables de vérité devient difficile et parfois impossible. Nous allons présenter une méthode formelle (qui ne fait pas appel aux tables de vérité) pour montrer que les formules sont des tautologies ou des conséquences logiques d'autres formules : *la théorie de la démonstration.*

Le calcul propositionnel a de bonnes propriétés (on peut décider si une formule est valide ou satisfiable), mais manque d'expressivité surtout quand il faut modéliser des espaces infinis comme les entiers. On pourrait utiliser une infinité de variables propositionnelles et une infinité d'hypothèses, mais ce n'est pas facile à manipuler pour des humains et encore moins pour des machines. Il peut être utile d'avoir des descriptions finies qui rendent compte de situations potentiellement infinies. Cette notion est le calcul des prédicats. Nous allons donner une présentation du calcul des prédicats du premier ordre.

1 Les grands types de raisonnement

1.1 Le raisonnement déductif

Le schéma du raisonnement déductif est le suivant :

Quand P est une proposition vraie, et $P \Rightarrow Q$ est une proposition vraie, on peut affirmer que Q est une proposition vraie.

Un résultat connu comme étant vrai (c'est à dire un théorème) ne peut entraîner qu'un autre résultat vrai. Cette règle est connue sous le nom de « modus ponens ».

C'est le raisonnement de base que nous reproduirons un grand nombre de fois. Et même, nous tiendrons ce raisonnement tellement de fois (ou encore, nous serons tellement souvent dans la situation où l'hypothèse P est vraie) que nous risquons à terme de commettre une confusion entre la phrase simple « $P \Rightarrow Q$ est vraie » et la phrase plus complète « P est vraie et $P \Rightarrow Q$ est vraie ».

Seule la deuxième permet d'affirmer que Q est vraie.

Sachant de plus que l'implication est transitive, une démonstration prend très souvent la forme suivante :

$$P \text{ est vraie et } P \Rightarrow Q \Rightarrow R \Rightarrow \cdots \Rightarrow S \Rightarrow T \text{ est vraie,}$$

et on a donc montré que T est vraie.

1.2 Le raisonnement par l'absurde

Le méchanisme du raisonnement par l'absurde se fait en trois étapes :

1. On veut montrer qu'une proposition P est vraie.
2. On suppose que c'est sa négation $\neg P$ qui est vraie et on montre que cela entraîne une proposition fausse.
3. On en conclut que P est vraie (puisque Q est fausse, l'implication $\neg P \Rightarrow Q$ ne peut être vraie que si $\neg P$ est fausse ou encore si P est vraie).

Le schéma du raisonnement par l'absurde est le suivant :

Quand $\neg P \Rightarrow Q$ est une proposition vraie, et Q est une proposition fausse, on peut affirmer que P est une proposition vraie.

Exemple 1.1. *Montrons que $\sqrt{2}$ est irrationnel.*

Supposons par l'absurde que $\sqrt{2} \in \mathbb{Q}$. Il existe alors deux entiers naturels non nuls a et b tels que $\sqrt{2} = \frac{a}{b}$, ce qui donne $a^2 = 2b^2$.

Maintenant, dans la décomposition en facteurs premiers de l'entier a^2 (qui est à l'évidence supérieur à 2), le nombre premier 2 apparaît à un exposant pair

$$\textit{si} \;\; a = 2^\alpha \times c \quad \textit{alors} \quad a^2 = 2^{2\alpha} \times c^2$$

alors qu'il apparaît à un exposant impair dans $2b^2$

$$\textit{si} \;\; b = 2^\beta \times d \quad \textit{alors} \quad 2b^2 = 2^{2\beta+1} \times d^2.$$

Si l'on admet l'unicité de la décomposition en facteurs premiers d'un entier naturel supérieur à 2 (unicité qui sera démontrée plus tard dans ce cours), l'égalité des nombres a^2 et $2b^2$ est donc impossible.

Par suite, l'hypothèse faite ($\sqrt{2} \in \mathbb{Q}$) est absurde et on a montré (par l'absurde) que $\sqrt{2} \notin \mathbb{Q}$.

1.3 Le raisonnement par contraposition

Le schéma est le suivant :

Pour montrer que $P \Rightarrow Q$ est une proposition vraie, il (faut et) il suffit de montrer que $\neg Q \Rightarrow \neg P$ est une proposition vraie.

Exemple 1.2. *Soient k et k' deux entiers naturels non nuls.*

Montons que

$$kk' = 1 \Rightarrow k = k' = 1.$$

Supposons que $k \neq 1$ ou $k' \neq 1$. Alors, on a

$$(k \geq 2 \;\; et \;\; k' \geq 1) \;\; ou \;\; (k \geq 1 \;\; et \;\; k' \geq 2).$$

Dans les deux cas, on a $kk' \geq 2$ et en particulier, $kk' \neq 1$. Donc,

$$(k \neq 1 \;\; ou \;\; k' \neq 1) \Rightarrow (kk' \neq 1).$$

Par contraposition, on a montré que

$$kk' = 1 \Rightarrow (k = 1 \;\; et \;\; k' = 1).$$

2 Théorie de la démonstration pour le calcul propositionnel

La théorie de la démonstration, aussi connue sous le nom de théorie de la preuve (de l'anglais *proof theory*), est une branche de la logique mathématique. Elle a été fondée par *David Hilbert* au début du $20^{ème}$ siècle. Hilbert a proposé cette nouvelle discipline mathématique lors de son célèbre exposé au $2^{ème}$ congrès international des mathématiciens en 1900 avec pour objectif de démontrer la cohérence des mathématiques.

Après une période de calme, qui a tout de même permis d'établir un certain nombre d'autres résultats de cohérence relative et d'esquisser une classification des théories axiomatiques, la théorie de la démonstration a connu une renaissance spectaculaire au cours des années 1960 avec la découverte de la correspondance de *Curry-Howard* qui a exhibé un lien structurel nouveau et profond entre logique et informatique.

En logique, les systèmes à la Hilbert servent à définir les déductions formelles en suivant un modèle proposé par David Hilbert au début du $20^{ème}$ siècle : un grand nombre d'axiomes logiques exprimant les principales propriétés de la logique que l'on combine au moyen de quelques règles, notamment *la règle de Modus Ponens*, pour dériver de nouveaux théorèmes. Les systèmes à la Hilbert héritent du système défini par *Gottlob Frege* et constituent les premiers systèmes déductifs, avant l'apparition de la déduction naturelle ou du calcul des séquents, appelés parfois par *opposition systèmes à la Gentzen.*

Définition 2.1. *Une théorie formelle T est définie par :*

1. *L'alphabet ;*
2. *Les formules de T ;*
3. *Un sous ensemble de formules formant les axiomes ;*
4. *Une ou plusieurs règles d'inférence.*

Définition 2.2. *Une preuve dans T est une séquence de formules $\alpha_1, \alpha_2, \cdots, \alpha_n$, telles que chaque α_i est soit un axiome, soit un théorème déjà démontré, soit obtenue à partir de l'application d'une des règles d'inférence.*

Définition 2.3. *Si une formule α admet une preuve, on dit que α est démontrable ou α est un théorème et on note $\vdash \alpha$.*

Définition 2.4. *Une déduction (ou démonstration) d'une formule α à partir d'un certain ensemble de formules Γ est une séquence de formules $\alpha_1, \alpha_2, \cdots, \alpha_n$ telles que $\alpha_n = \alpha$ et chaque α_i est soit un axiome, soit un théorème déjà démontré, soit une formule de Γ, soit obtenue à partir de l'application d'une des règles d'inférence. Et on note $\Gamma \vdash \alpha$.*

Dans le cadre de ce cours, on convient de considérer l'alphabet et les formules du calcul propositionnel.

2.1 Liste des axiomes

La liste des axiomes peut varier d'un auteur à un autre ou d'une institution à une autre. Les axiomes sont des formules dont on admet qu'elles sont des théorèmes sans pouvoir leur donner une démonstration formelle. Nous donnons ici la liste des axiomes de *Hilbert-Ackerman* $(H.A)$; et on considère le système complet de connecteurs $\{\neg, \vee\}$.

Définition 2.5. *On rappel ici que l'exprssion $x \Rightarrow y$ n'est qu'une abréviation de l'écriture $\neg x \vee y$. Les axiômes de Hilbert-Ackerman ou d'H.A sont :*

$(H.A)_1$. $(x \vee x) \Rightarrow x$;

$(H.A)_2$. $x \Rightarrow x \vee y$;

$(H.A)_3$. $x \vee y \Rightarrow y \vee x$;

$(H.A)_4$. $(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow x \vee y)$.

2.2 Les règles ou schémas de déduction

Les règles de déduction ont pour objet la déduction de nouveaux théorèmes à partir de théorèmes connus. Une règle de déduction n'est pas un axiome mais en quelque sorte un procédé permettant d'obtenir de nouveaux théorèmes.

Règle de détachement (ou Modus Ponens)

Contrairement à la liste des axiomes et les autres règles de déduction, la règle du Modus Ponens est commune à toutes les théorie. Le terme Modus Ponens (ou plus exactement Modus Ponendo Ponens) vient de ce que l'on pose α (Ponens est le participe présent de verbe latin Ponere, poser) afin d'en tirer la conclusion. Elle est donnée comme suit :

$$\textit{De} \quad \vdash \alpha, \ \vdash \alpha \Rightarrow \beta, \ \textit{on déduit} \quad \vdash \beta.$$

cette règle peut être formulée ainsi : soient deux formules α et β, telles que α et $\alpha \Rightarrow \beta$ sont des théorèmes, alors β est un théorème.

On peut utiliser un schéma pour illustrer cette règle : $\dfrac{\begin{array}{l}\vdash \alpha \\ \vdash \alpha \Rightarrow \beta\end{array}}{\vdash \beta}$.

Cette figure fait bien apparaître pourquoi la règle s'appelle *règle de détachement* : elle permet de détacher le conséquent β de l'antécédent α dans l'implication $\alpha \Rightarrow \beta$, pourvu que $\vdash \alpha$ et $\vdash \alpha \Rightarrow \beta$.

Règle de substitution

Cette règle est indispensable pour les théorie où les axiomes sont donnés avec des variables propositionnelles (comme le cas de la théorie d'$H.A.$).

Soit α un théorème dans lequel figure la variable propositionnelle x, alors pour toute formule β (où β n'est pas nécessairement un théorème), la substitution de β à x en chacune de ses occurrences engendre un théorème.

Autrement dit :

$$De \quad \vdash \alpha, \;\; on\ déduit \;\; \vdash \alpha(x := \beta).$$

Exemple 2.1. *Montrons le théorème :* $\vdash \neg x \vee x$.

Démonstration. On peut démontrer le théorème dans l'exemple on suivant les étapes suivantes :

Étape	Théorème	Règle suivie
(1)	$(x \vee x) \Rightarrow x$	$(H.A)_1$
(2)	$x \Rightarrow x \vee y$	$(H.A)_2$
(3)	$x \Rightarrow x \vee x$	Sub $y := x$ dans (2)
(4)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(5)	$(x \vee x \Rightarrow y) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee y)$	Sub $x := x \vee x$ dans (4)
(6)	$(x \vee x \Rightarrow x) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee x)$	Sub $y := x$ dans (5)
(7)	$(z \vee (x \vee x) \Rightarrow z \vee x)$	Modus Ponens $(1),(6) \to (7)$
(8)	$(\neg z \vee (x \vee x) \Rightarrow \neg z \vee x)$	Sub : $z := \neg z$ dans (7)
(9)	$(z \Rightarrow (x \vee x) \Rightarrow z \Rightarrow x)$	Abréviation de $\Rightarrow$
(10)	$(x \Rightarrow (x \vee x) \Rightarrow x \Rightarrow x)$	Sub $z := x$ dans (9)
(11)	$x \Rightarrow x$	Modus Ponens $(3),(10) \to (11)$
(12)	$\neg x \vee x$	Définition de $\Rightarrow$.

□

Les démonstrations donnent rapidement lieu à des textes de longueur démesurée. On peut arriver plus vite au but en prenant des raccourcis qui consistent à adopter des Règles dérivées.

Théorème 2.1 (Règle S)**.** *Soient α, β et γ trois formules. Alors*

$$De \quad \vdash \alpha \Rightarrow \beta \;\; et \;\; \vdash \beta \Rightarrow \gamma \;\; on\ déduit \;\; \vdash \alpha \Rightarrow \gamma.$$

Démonstration. Les étapes de la peuve sont :

Étape	Théorème	Règle suivie
(1)	$\alpha \Rightarrow \beta$	Hypothèse
(2)	$\beta \Rightarrow \gamma$	Hypothèse
(3)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(4)	$(\beta \Rightarrow \gamma) \Rightarrow (\neg\alpha \vee \beta \Rightarrow \neg\alpha \vee \gamma)$	Sub $(x := \beta,\ y := \gamma,\ z := \neg\alpha)$
(5)	$(\beta \Rightarrow \gamma) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$	Abréviation
(6)	$(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)$	Modus Ponens $(2),(5) \to (6)$
(7)	$\alpha \Rightarrow \gamma$	Modus Ponens $(1),(6) \to (7)$.

□

Théorème 2.2 (Règle I). *Soit α une formule. Alors*

$$\text{De} \quad \vdash \alpha \vee \alpha, \quad \text{on déduit} \quad \vdash \alpha.$$

Démonstration. Les étapes de la peuve sont :

Étape	Théorème	Règle suivie
(1)	$(x \vee x) \Rightarrow x$	$(H.A)_1$
(2)	$(\alpha \vee \alpha) \Rightarrow \alpha$	Sub $(x := \alpha)$
(3)	$\alpha \vee \alpha$	Hypothèse
(4)	α	Modus Ponens $(3),(2) \rightarrow (4)$.

□

Théorème 2.3 (Règle II). *Soient α et β deux formules. Alors*

$$\text{De} \quad \vdash \alpha, \quad \text{on déduit} \quad \vdash \alpha \vee \beta.$$

Démonstration. Les étapes de la peuve sont :

Étape	Théorème	Règle suivie
(1)	$x \Rightarrow x \vee y$	$(H.A)_2$
(2)	$\alpha \Rightarrow \alpha \vee \beta$	Sub $(x := \alpha,\ y := \beta)$
(3)	α	Hypothèse
(4)	$\alpha \vee \beta$	Modus Ponens $(3),(2) \rightarrow (4)$.

□

Théorème 2.4 (Règle III). *Soient α et β deux formules. Alors*

$$\text{De} \quad \vdash \alpha \vee \beta, \quad \text{on déduit} \quad \vdash \beta \vee \alpha.$$

Démonstration. Les étapes de la peuve sont :

Étape	Théorème	Règle suivie
(1)	$x \vee y \Rightarrow y \vee x$	$(H.A)_3$
(2)	$\alpha \vee \beta \Rightarrow \beta \vee \alpha$	Sub $(x := \alpha,\ y := \beta)$
(3)	$\alpha \vee \beta$	Hypothèse
(4)	$\beta \vee \alpha$	Modus Ponens $(3),(2) \rightarrow (4)$.

□

Théorème 2.5 (Règle IV). *Soient α, β et γ des formules. Alors*

$$\text{De} \quad \vdash \alpha \Rightarrow \beta, \quad \text{on déduit} \quad \vdash \gamma \vee \alpha \Rightarrow \gamma \vee \beta.$$

Démonstration. Les étapes de la peuve sont :

Étape	Théorème	Règle suivie
(1)	$(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(2)	$(\alpha \Rightarrow \beta) \Rightarrow (\gamma \vee \alpha \Rightarrow \gamma \vee \beta)$	Sub $(x := \alpha,\ y := \beta,\ z := \gamma)$
(3)	$\alpha \Rightarrow \beta$	Hypothèse
(4)	$\gamma \vee \alpha \Rightarrow \gamma \vee \beta$	Modus Ponens $(3),(2) \rightarrow (4)$.

□

Définition 2.6. *On rappel ici que l'expression $x \wedge y$ n'est qu'une abréviation de l'expression $\neg(\neg x \vee \neg y)$.*

Théorème 2.6 (Règle V). *Soient α et β deux formules. Alors*

$$(De \quad \vdash \alpha \;\; et \;\; \vdash \beta, \;\; on\ déduit \;\; \vdash \alpha \wedge \beta) \;\; et \;\; (de \quad \vdash \alpha \wedge \beta, \;\; on\ déduit \;\; \vdash \alpha \;\; et \;\; \vdash \beta).$$

Démonstration. La démonstration de cette règle se fait en trois partie.

►⇒► D'abord, on démontre que

$$De \quad \vdash \alpha \;\; et \;\; \vdash \beta, \;\; on\ déduit \;\; \vdash \alpha \wedge \beta.$$

Pour ce faire, on procède comme suit :

(a) On démontre le théorème $x \Rightarrow (y \Rightarrow (x \wedge y))$;

(b) Faire les substitutions adéquates ;

(c) Obtenir le résultat en utilisant le Modus Ponens.

◄⇐◄ Ensuite, on démontre la réciproque

$$de \quad \vdash \alpha \wedge \beta, \;\; on\ déduit \;\; \vdash \alpha \;\; et \;\; \vdash \beta$$

On procède de la manière suivante :

(a) On démontre le théorème $(x \Rightarrow y) \Rightarrow (y \Rightarrow x)$;

(b) On utilise $(H : A)_2$;

(c) Quelques substitutions et abréviations, on obtient le résultats.

◄⇔► De ⇒ et ⇐ on a la démostration.

□

Définition 2.7. *On rappel aussi que l'expression $\alpha : x \Leftrightarrow y$ est une abréviation permettant d'écrire la formule*

$$\beta : (x \Rightarrow y) \wedge (y \Rightarrow x).$$

Il est impossible de donner une liste complète des théorèmes du calculs des propositions car elle est infinie. Néanmoins, on peut donner les plus utilisés. Ces théorèmes, combinés avec les règles de déduction ainsi que les règles dérivées, permettent de démontrer les autres théorèmes du calcul des propositions.

2.3 Liste des théorèmes

Les théorèmes les plus connus sont :

	Abréviation du théorème	Nom du théorème
(1)	$x \wedge x \Leftrightarrow x$ et $x \vee x \Leftrightarrow x$	Lois de tautologie
(2)	$x \Leftrightarrow \neg(\neg x)$	Loi de la double négation
(3)	$\vdash (x \vee \neg x)$ ou $\vdash (\neg x \vee x)$	Loi du tiers exclu (commutative)
(4)	$\nvdash (x \wedge \neg x)$ ou $\nvdash (\neg x \wedge x)$	Négation du tiers exclu (commutative)
(5)	$(x \Rightarrow y) \Leftrightarrow (\neg y \Leftrightarrow \neg x)$	Loi de la contraposition
(6)	$x \wedge (y \wedge z) \Leftrightarrow (x \wedge y) \wedge z$	Associativité de $\wedge$
(7)	$x \vee (y \vee z) \Leftrightarrow (x \vee y) \vee z$	Associativité de $\vee$
(8)	$\neg(x \vee y) \Leftrightarrow (\neg x \wedge \neg y)$	Loi de Morgan 1
(9)	$\neg(x \wedge y) \Leftrightarrow (\neg x \vee \neg y)$	Loi de Morgan 2
(10)	$x \vee (y \wedge z) \Leftrightarrow (x \vee y) \wedge (x \vee z)$	Distribution de $\vee$ sur $\wedge$
(11)	$x \wedge (y \vee z) \Leftrightarrow (x \wedge y) \vee (x \wedge z)$	Distribution de $\wedge$ sur $\vee$
(12)	$x \wedge y \Leftrightarrow y \wedge x$	Commutativité de $\wedge$
(13)	$x \vee y \Leftrightarrow y \vee x$	Commutativité de $\vee$
(14)	$x \wedge y \Rightarrow x$	
(15)	$x \Rightarrow x \vee y$	
(16)	$x \Rightarrow (y \Rightarrow (x \wedge z))$	
(17)	$(x \Rightarrow y) \Rightarrow ((x \Rightarrow z) \Rightarrow (y \Rightarrow z))$	
(18)	$(x \Rightarrow y) \Rightarrow ((z \Rightarrow y) \Rightarrow (z \Rightarrow x))$	

Table 4.1 – Liste des théorèmes les plus connus

Dans ce qui suit, nous donnons quelques définitions nécessaires à la présentation et à la démonstration du plus important résultat du calcul des propositions qui est le théorème fondamental.

Définition 2.8. *Deux formules α et β sont dites équivalentes si* $\vdash \alpha \Leftrightarrow \beta$.

Exemple 2.2. *Les deux formules $x \Rightarrow y$ et $\neg y \Rightarrow \neg x$ sont équivalentes*

En effet ;

Étape	Théorème	Règle suivie
(1)	$x \Rightarrow y$	Hypothèse
(2)	$\neg x \vee y$	Définition
(3)	$\neg y \Rightarrow \neg x$	Hypothèse
(4)	$y \vee \neg x$	Définition
(5)	$\alpha \vee \beta \Leftrightarrow \beta \vee \alpha$	Commutativité
(6)	$y \vee \neg x \Leftrightarrow \neg x \vee y$	Sub ($\alpha := y,\ \beta := \neg x$)
(7)	$x \Rightarrow y \Leftrightarrow \neg y \Rightarrow \neg x$	Abréviation

□

Définition 2.9. *On appelle monôme disjonctif par rapport aux variables $x, y, z, \cdots$, une formule présentant les caractéristiques suivantes :*
— *Chaque variable présente exactement une occurrence. Cette variable peut être précidée d'une négation $\neg$.*
— *Outre les variables, le monôme disjonctif ne comporte que le connecteur $\vee$.*

Exemple 2.3.

$$x, \ \neg x, \ x \vee y, \ x \vee \neg y, \ \neg x \vee y \vee \neg z.$$

Définition 2.10. *Une formule α qui se présente sous la forme*

$$\alpha := \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n := \bigwedge_{i=1}^{n} \alpha_i$$

où $\alpha_1, \alpha_2, \cdots, \alpha_n$ sont des monômes disjonctifs, est dite formule sous forme normale conjonctive.

Chapitre 5

Le langage du calcul des prédicats d'ordre 1

1 Quelques définitions

Le calcul propositionnel reste très limité, et ne permet essentiellement que d'exprimer des opérations booléennes sur des propositions. Si l'on veut pouvoir raisonner sur des assertions mathématiques, il nous faut autoriser des constructions plus riches. Ainsi la formule

$$\forall x \in \mathbb{N},\ x \leq x^2$$

représente toutes les formules

$$0 \leq 0^2 = 0,\ 1 \leq 1^2 = 1,\ 2 \leq 2^2 = 4,\ 3 \leq 3^2 = 9,\ \cdots$$

Un tel énoncé n'est pas capturé par la logique propositionnelle. Tout d'abord par ce qu'il utilise des prédicats comme $x \in \mathbb{N}$ dont la valeur de vérité dépend d'une variable x, ce qui n'est pas possible en logique propositionnelle. Par ailleurs, on utilise ici des quantificateurs comme $\exists$ et $\forall$ qui ne sont pas présents en logique propositionnelle.

L'énoncé précédent est un exemple de formule du calcul des prédicats du premier ordre. Dans ce cours, on ne parlera que de logique du premier ordre. La terminologie premier ordre fait référence au fait que les quantifications existentielles et universelles ne sont autorisées que sur les variables.

Un énoncé du second ordre, on parle plus généralement d'ordre supérieur, serait un énoncé où l'on autoriserait les quantifications sur les fonctions ou des relations : par exemple, on peut écrire

$$\neg \forall f\ (\exists x\ (f(x) > f(x+1)))$$

pour signifier qu'il n'existe pas de suite infiniment décroissante. On ne cherchera pas à comprendre la théorie derrière ce type d'énoncé, car on le verra, les problèmes et les difficultés avec le premier ordre sont déjà suffisamment nombreux.

L'objectif de ce chapitre est alors de définir la logique du premier ordre. Comme pour la logique propositionnelle, on va le faire en parlant d'abord de la syntaxe, c'est-à-dire comment écrire les formules, puis de leur sémantique.

Le calcul des prédicats, reste le formalisme le plus courant pour exprimer des propriétés mathématiques. C'est aussi un formalisme très utilisé en informatique pour décrire les objets.

Définition 1.1. *En littérature, un prédicat est ce qui est affirmé d'un sujet ou est dit lui appartenir. (Sagesse/sage est prédicat dans La sagesse appartient à Socrate ou dans Socrate est sage.)*

Définition 1.2. *En logique mathématique, un prédicat est un moule à propositions. C'est un énoncé qui est syntaxiquement correct, il est sémantiquement correct mais sa valeur de vérité dépend de l'objet. Ainsi, le prédicat "x est premier" dépend de la valeur de l'entier x.*

Définition 1.3. *On peut avoir un prédicat à une variable $P(x)$ (dans ce cas, on parle d'une propriété de l'objet x), un prédicat à deux variables (ex : $x > y$, dans ce cas, c'est une relation entre l'objet x et l'objet y) ou encore un prédicat à n variables (On dit alors un prédicat n-aire).*

2 Le langage des prédicats du premier ordre

2.1 L'alphabet

L'alphabet est formé :

1. Des connecteurs logiques :
$$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow;$$
2. Des quantificateurs : $\forall$ et $\exists$;
3. D'un ensemble dénombrable de symboles de variables :
$$x, y, z, t, \cdots;$$
4. D'un ensemble dénombrable éventuellement vide de symboles de constantes :
$$a, b, c, d, e, \cdots;$$
5. D'un ensemble dénombrable éventuellement vide de symboles de fonctions :
$$f_0, f_1, \cdots, g_0, g_1, \cdots, h_0, h_1, \cdots, \cdots;$$
6. D'un ensemble dénombrable de symboles de prédicats :
$$P_0, P_1, \cdots, Q_0, Q_1, \cdots, R_0, R_1, \cdots, \cdots;$$
7. Des symboles auxiliaires : $(,)\cdots$.

2.2 Les expressions du langage

Les termes

1. Toute constante est un terme ;
2. Toute variable est un terme ;
3. Si f est un symbole de fonction à n arguments et $t_1, t_2, \cdots, t_n$ sont des termes, alors $f(t_1, t_2, \cdots, t_n)$ est un terme ;
4. Rien d'autres n'est un terme, s'il n'est pas obtenu en vertus des règles 1, 2 et 3.

Les formules

1. Une variable propositionnelle est une formule ;
2. Si $t_1, t_2, \cdots, t_n$ sont des termes et P un prédicat à n variables, alors $P(t_1, t_2, \cdots, t_n)$ est une formule ;
3. Si α et β sont des formules, alors : $\neg\alpha$, $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \Rightarrow \beta$, $\alpha \Leftrightarrow \beta$ sont aussi des formules ;
4. Si α est une formule et x une variable, alors $\forall x\ \alpha$ et $\exists x\ \alpha$ sont des formules ;
5. Rien n'est une formule, s'il n'est pas obtenu en vertus des règles 1, 2, 3 et 4.

2.3 Priorité des connecteurs

Les connecteurs et les quantificateurs sont appliqués dans l'ordre suivant :

$$\neg,\ \wedge,\ \vee,\ \Rightarrow,\ \Leftrightarrow$$

Exemple 2.1. *La formule*

$$\forall x\ P(x) \vee \exists y\ Q(y) \wedge P(x)$$

se lit

$$\forall x\ (P(x) \vee \exists y\ (Q(y) \wedge P(x))).$$

2.4 Champ d'un quantificateur

Définition 2.1. *Le Champ d'un quantificateur est la partie de la formule couverte par un quantificateur.*

Exemple 2.2.

1.

$$\forall x\ \ \alpha \wedge \beta \quad \exists x\ \ \alpha \wedge \beta$$

2.

$$\forall x\ \ \alpha \vee \beta \quad \exists x\ \ \alpha \vee \beta$$

3.

$$\forall x\ \ \alpha \Rightarrow \beta \quad \exists x\ \ \alpha \Rightarrow \beta$$

4.

$$\forall x\ \ (\alpha \Rightarrow \beta) \quad \exists x\ \ (\alpha \Rightarrow \beta)$$

2.5 Variable libre et variable liée

Définition 2.2. *Dans une formule α, l'occurrence d'une variable x est liée si elle se trouve dans le champ d'un quantificateur $\forall x$ ou $\exists x$; sinon elle est libre.*

Définition 2.3. *Une variable x est libre dans une formule α s'il existe dans α une occurrence libre de x.*

Définition 2.4. *Une variable x est liée dans une formule α s'il existe dans α une occurrence liée de x.*

Exemple 2.3. *Soit α la formule suivante :*

$$\forall y\ P(x,y) \land Q(y) \ \Rightarrow\ \exists x\ Q(x) \Rightarrow R(z).$$

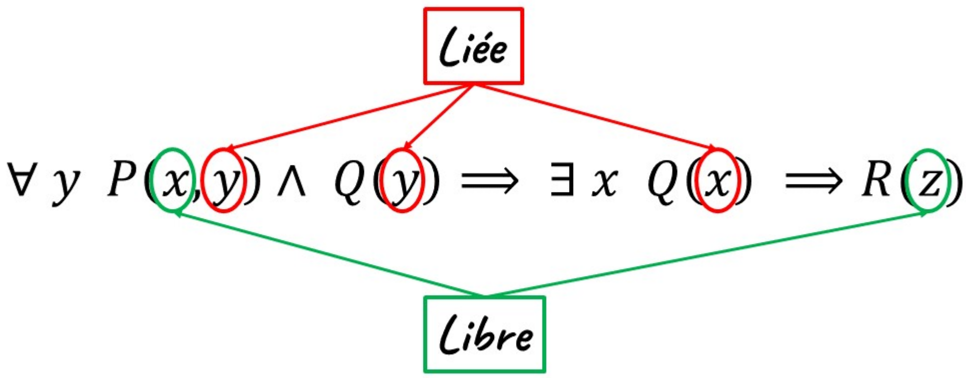


Figure 5.1 – Exemple des variables libres et variables liées

2.6 Formule close (fermée)

Définition 2.5. *Une formule α est dite close (ou fermée), si et seulement si, α ne possède que des variables liées.*

Autrement dit : α ne passède pas des variables libres.

3 Sémantique de la logique des prédicats du premier ordre

En calcul propositionnel, il existe des moyens algorithmiques relativement efficaces pour déterminer si une formule est satisfiable ou est une tautologie. En calcul des pré- dicats, nous ne pouvons pas dire d'une formule qu'elle est vraie ou fausse si nous ne connaissons pas la signification de chacun des symboles qui apparaissent dans la formule.

Définition 3.1 (Interprétation)**.** *Etant donné un langage $\mathcal{L}$ du premier ordre, une interprétation I sur ce langage, est une fonction de domaine D non vide qui assigne :*

1. *à chaque symbole de prédicat n-aire P, une relation n-aire*

$$I(P) : D^n \to \{0,1\};$$

2. *à chaque symbole de fonction f à n arguments ($n > 0$), une opération sur les éléments du domaine de l'interprétation*

$$I(f) : D^n \to D;$$

3. *à chaque symbole de constante a_i un élément*

$$I(a_i) = d_i, \quad d_i \in D.$$

Définition 3.2 (Valuation). *Etant donné un langage $\mathcal{L}$ du premier ordre et une interprétation I de domaine D sur ce langage, une valuation est une fonction qui associe à chaque variable un élément de D.*

Définition 3.3 (Interprétation d'un terme). *On désigne par $I(t)_v$ l'élément de D associé au terme t par l'interprétation I de domaine D et la valuation $\mathcal{V}$ sur ce domaine. Cet élément est défini comme suit :*

— *Si $t = c$, alors*

$$I(t)_v = I(c)_v = I(c) \quad \text{où} \quad c \quad \text{est une constante;}$$

— *Si $t = x_i$, alors*

$$I(t)_v = I(x_i)_v = \mathcal{V}(x_i) \quad \text{où} \quad x_i \ \text{ est une variable;}$$

— *Si $t = f(t_1, t_2, \cdots, t_n)$, alors*

$$I(t)_v = I(f)(I(t_1)_v, I(t_2)_v, \cdots I(t_n)_v)$$

où f est un symbole de fonction et $t_1, t_2, \cdots, t_n$ des termes.

Définition 3.4 (Interprétation d'une formule). *Etant donné un langage $\mathcal{L}$ du premier ordre et une interprétation I de domaine D et une valuation $\mathcal{V}$ sur ce domaine. $I(\alpha)_v$ d'une formule α du premier ordre est définie comme suit :*

1. *Si α est une formule atomique, alors :*

$$I(\alpha)_v = I(P(t_1, t_2, \cdots, t_n))_v = I(P)(I(t_1)_v, I(t_2)_v, \cdots I(t_n)_v);$$

2. *Si $\alpha = \neg\beta$, alors :*

$$I(\alpha)_v = I(\neg\beta)_v = \neg I(\beta)_v;$$

3. *Si $\alpha = \beta_1 \wr \beta_2$ avec $\wr \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, alors :*

$$I(\alpha)_v = I(\beta_1)_v \wr I(\beta_2)_v.$$

Définition 3.5 (Satisfiablité d'une formule). *Etant donnés un langage $\mathcal{L}$ et une interprétation I. Une valuation $\mathcal{V}$ satisfait une formule α, si et seulement si, après substitution de l'élément du domaine de I associé par $\mathcal{V}$ à chaque variable libre de α, on obtient une proposition vraie pour l'interprétation considérée. Et on note*

$$I \models \alpha_v.$$

Exemple 3.1.

Soit la formule

$$\beta \equiv P(f(x,y),y).$$

On se donne l'interprétation I de domaine $D = \mathbb{N}$, telle que $I(P) = " > "$, $I(f) = " - "$, et la valuation $\mathcal{V}$ telle que $\mathcal{V}(x) = 4$ et $\mathcal{V}(y) = 1$ qui satisfait β pour I. Donc :

$$I \models \beta_v.$$

Alors que la valuation $\mathcal{V}'$ telle que $\mathcal{V}'(x) = 4$ et $\mathcal{V}'(y) = 3$, ne satisfait pas la formule β pour I.

$$I \not\models \beta_v.$$

Définition 3.6. *Une formule α est satisfiable, si et seulement si, il existe une interprétation I pour laquelle il existe au moins une valuation qui satisfait α.*

On note que le formule β ci-dessus est satisfiable.

Définition 3.7 (Modèle d'une formule)**.** *Une formule α est vraie pour une interprétation I et on note $I \models \alpha$, si et seulement si, toute valuation satisfait α pour l'interprétation I. Dans ce cas, I est appelée modèle de α. Autrement dit :*

$$I \models \alpha \quad \Leftrightarrow \quad (\forall \mathcal{V},\ I \models \alpha_v).$$

Exemple 3.2.

Soit α la formule

$$\alpha \equiv P(f(x,y),x).$$

L'interprétation I de domaine $D = \mathbb{N}$, $I(P) = " > "$, $I(f) =$ "le est successeur de x" est un modèle de α. Donc $I \models \alpha$.

Définition 3.8. *Une formule α est fausse pour une interprétation I si et seulement si, aucune valuation de I ne satisfait α.*

Exemple 3.3.

Soit α la formule

$$\alpha \equiv P(f(x,y),x).$$

Et soit l'interprétation I de domaine $D = \mathbb{N}$, $I(P) = " < "$, $I(f) = " + "$. Aucune valuation de D ne satisfait α pour I. Donc α est fausse pour I.

Définition 3.9 (Formule valide)**.** *Une formule α est valide et on note $\models \alpha$, si et seulement si, α est vraie pour toutes les interprétations. Toute interprétation est modèle pour α. Autrement dit*

$$\models \alpha \quad \Leftrightarrow \quad (\forall I,\ \forall \mathcal{V},\ I \models \alpha_v).$$

Pour montrer qu'une formule α est valide, on procède généralement par l'absurde. On suppose l'existence d'une interprétation I et d'une valuation v, telles que $I \not\models \alpha_v$ et on arrive à une contradiction.

Exemple 3.4.

Soit $\alpha : \neg P(x) \vee P(x)$. Montrons que $\models \alpha$.

Supposons le contraire, i.e. qu'il existe une interprétation I et une valuation $\mathcal{V}$ telles que

$$\begin{array}{rcl} I \not\models (\neg P(x) \vee P(x))_v & \Leftrightarrow & \exists I,\ \exists \mathcal{V}\ /\ I \models \neg(\neg P(x) \vee P(x))_v \\ & \Leftrightarrow & \exists I,\ \exists \mathcal{V}\ /\ I \models (P(x) \wedge \neg P(x))_v \\ & \Leftrightarrow & \exists I,\ \exists \mathcal{V}\ /\ I \models (P(x))_v \ et\ I \models (\neg P(x))_v \\ & \Leftrightarrow & \exists I,\ \exists \mathcal{V}\ /\ I \models (P(x))_v \ et\ I \not\models (P(x))_v \\ & \Leftrightarrow & \perp \quad (\ Contradiction.) \end{array}$$

Donc on a $\models \alpha$.

□

On rappel que pour montrer qu'une formule n'est pas valide, il suffit de trouver un contre exemple.

Définition 3.10 (Satisfiabilité d'un ensemble de formules)**.** *Un ensemble de formules $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ est satisfiable, si et seulement si, il existe une interprétation I et une valuation $\mathcal{V}$, telles que*

$$I \models (\alpha_1)_v,\ I \models (\alpha_2)_v,\ \cdots, I \models (\alpha_n)_v.$$

Exemple 3.5.

Soient l'ensemble des formules $\Gamma = \{P(x,y),\ Q(x,y),\ R(x,y)\}$ et I l'interprétation de domaine $D = \{1,2,3\}$ telles que $I(P) =$ "$\cdots$ est diviseur de $\cdots$", $I(Q) =$ "$\cdots$ est multiple de $\cdots$" et $I(R) =$ "$\cdots$ est égal à $\cdots$". Pour la valuation $\mathcal{V}(x) = \mathcal{V}(y) = 1$ l'ensemble Γ est satisfiable.

Définition 3.11 (Modèle d'un ensemble de formules)**.** *Une interprétation I est un modèle d'un ensemble de formules Γ, si et seulement si, I est un modèle de chacune des formules de Γ.*

Définition 3.12 (Conséquence logique)**.** *Une formule β est une conséquence logique d'un ensemble de formules Γ (et on note $(\Gamma \models \beta)$, si et seulement si, pour toute interprétation, toute valuation qui satisfait chacune des formule de Γ, satisfait aussi β. Tout modèle de Γ est aussi un modèle de β.*

Définition 3.13 (Renommage)**.** *Soit α une formule du calcul des prédicats du premier ordre. Et soit y une variable n'apparaissant pas dans α. Soit x une variable liée de α. Le remplacement de x par y dans α est appelé renommage.*

L'opération est faite pour distinguer les variables libres des variables liées et faire en sorte qu'une variable ne soit concernée que par un seul cuantificateur.

Exemple 3.6.

Soit la formule

$$\alpha_1 \equiv (\forall x,\ \exists y\ /\ P(x,y)\ \Rightarrow\ P(x,z))\ \vee\ (\exists x\ /\ R(x)) \wedge (\forall y,\ P(x,y))).$$

Après renommage on aura la formule

$$\alpha_2 \equiv (\forall u,\ \exists y\ /\ P(u,y)\ \Rightarrow\ P(x,z))\ \vee\ (\exists v\ /\ R(v)) \wedge (\forall t,\ P(x,t))).$$

Alors

$$\alpha_1 \equiv \alpha_2.$$

Propriété 3.1.

1. $\forall x\ \alpha \equiv \alpha$ *si* x *n'apparaît pas libre dans* α.
2. $\exists x\ \alpha \equiv \alpha$ *si* x *n'apparaît pas libre dans* α.

4 Normalisation

Les formes normales (conjonctives et disjonctives) permettent de simplifier l'étude de la satisfiabilité et la validité en calcul propositionnel. En calcul des prédicats, cette mise en forme se fait en quatres étapes :

1. Mise sous forme prénexe (déplacement de tous les quantificateurs au début de la formule) ;
2. Skolemisation (suppression des $\exists$) ;
3. Mise en forme normale conjonctive ;
4. Mise en forme clausale (suppression des $\forall$) ;

Forme prénexe

Une formule est dite en forme prénexe si tous ses quantificateurs apparaissent au début. Ainsi, la formule est composée de deux parties, la partie quantificateur (au début) et la matrice. Il est toujours possible de transformer une formule en une formule équivalente sous forme prénexe. Pour cela, on applique autant de fois que nécessaire les équivalences suivantes :

Equivalence sous forme prénexe	Remarque
$\neg(\forall x\ \alpha) \equiv \exists x\ \neg\alpha$	
$\neg(\exists x\ \alpha) \equiv \forall x\ \neg\alpha$	
$(\forall x\ \alpha) \wedge \beta \equiv \forall x\ (\alpha \wedge \beta)$	x n'apparaît pas libre dans β ;
$(\forall x\ \alpha) \vee \beta \equiv \forall x\ (\alpha \vee \beta)$	x n'apparaît pas libre dans β ;
$(\exists x\ \alpha) \wedge \beta \equiv \exists x\ (\alpha \wedge \beta)$	x n'apparaît pas libre dans β ;
$(\exists x\ \alpha) \vee \beta \equiv \exists x\ (\alpha \vee \beta)$	x n'apparaît pas libre dans β ;
$\alpha \wedge (\forall x\ \beta) \equiv \forall x\ (\alpha \wedge \beta)$	x n'apparaît pas libre dans α ;
$\alpha \vee (\forall x\ \beta) \equiv \forall x\ (\alpha \vee \beta)$	x n'apparaît pas libre dans α ;
$\alpha \wedge (\exists x\ \beta) \equiv \exists x\ (\alpha \wedge \beta)$	x n'apparaît pas libre dans α ;
$\alpha \vee (\exists x\ \beta) \equiv \exists x\ (\alpha \vee \beta)$	x n'apparaît pas libre dans α ;
$\forall x\ \alpha \Rightarrow \beta \equiv \exists x\ (\alpha \Rightarrow \beta)$	x n'apparaît pas libre dans β ;
$\exists x\ \alpha \Rightarrow \beta \equiv \forall x\ (\alpha \Rightarrow \beta)$	x n'apparaît pas libre dans β ;
$\alpha \Rightarrow \forall x\ \beta \equiv \forall x\ (\alpha \Rightarrow \beta)$	x n'apparaît pas libre dans α ;
$\alpha \Rightarrow \exists x\ \beta \equiv \exists x\ (\alpha \Rightarrow \beta)$	x n'apparaît pas libre dans α ;

Table 5.1 – Liste des équivalences sous forme *Prénexe*

Exemple 4.1.

Soit la formule

$$\begin{aligned} \alpha &\equiv \forall x, \forall y, E(x,y) \Rightarrow \exists z, A(x,z) \\ &\equiv \forall t, \forall y, E(t,y) \Rightarrow \exists z, A(x,z) \\ &\equiv \exists t, \exists y, (E(t,y) \Rightarrow \exists z, A(x,z)) \\ &\equiv \exists t, \exists y, \exists z, (E(t,y) \Rightarrow A(x,z)). \end{aligned} \tag{4.0.1}$$

Forme de Skolem (Skolemisation)

Soit α une formule ayant la forme prénexe.

Transformons α ainsi :

— On remplace chaque variable, quantifiée par un existentiel, par une fonction des variables quantifiées universellement avant, et on supprime les quantificateurs existentiels.

— On convient de n'introduire que des fonctions nouvelles et différentes.

La formule obtenue est la skolémisée de α, elle notée α^{Sko}.

La skolémisée d'une formule ne lui est pas en général équivalente, néanmoins :

— Tout modèle de la formule skolémisée est modèle de la formule initiale.

— Tout modèle de la formule initiale peut être étendu en un modèle de la formule skolémisée, obtenu en conservant les interprétations des symboles de la formule initiale, et en interprétant correctement les nouveaux symboles de fonction introduits pas la skolemisation.

— Une formule close et sa forme de Skolem sont dites équisatisfaisables : si l'une possède un modèle, l'autre également et réciproquement.

Exemple 4.2.

1. *Reprenons la formule précédente (sous forme prénexe* (4.0.1)*)*
$$\alpha \equiv \exists t, \exists y, \exists z, (E(t,y) \Rightarrow A(x,z))$$
alors
$$\alpha^{Sko} \equiv E(a,b) \Rightarrow A(x,c) \quad \text{où } a, b \text{ et } c \text{ sont des constatntes.}$$
2. *Soit*
$$\beta \equiv \forall x, \exists u, \exists y, \exists z, (P(x,u) \Rightarrow (Q(u,y) \wedge R(y,z))).$$
Alors
$$\beta^{Sko} \equiv \forall x, \forall y, (P(x,f(x)) \Rightarrow (Q(f(x),y) \wedge R(y,g(x,y))).$$

Théorème 4.1. *Une formule α est satisfiable si et seulement si α^{Sko} est satisfiable.*

Forme clausale

Une fois que la formule a été skolémisée, il ne reste que des variables quantifiées universellement. On peut donc se passer de l'écriture explicite des quantificateurs. La formule restante est composée d'atomes et de connecteurs logiques. On peut alors appliquer la même technique qu'en logique propositionnelle pour la mettre en forme normale conjonctive, puis sous forme d'un ensemble de clauses.

Losqu'une formule est sous forme clausale, on peut ensuite la décomposer en appliquant la règle
$$\forall x,\ (\alpha \wedge \beta) \equiv (\forall x,\ \alpha) \wedge (\forall x,\ \beta).$$

Exemple 4.3. *Si on repart de la formule skolémisée*
$$\beta^{Sko} \equiv \forall x, \forall y, (P(x,f(x)) \Rightarrow (Q(f(x),y) \wedge R(y,g(x,y))).$$
l'élimination des quantificateurs universels donne
$$P(x,f(x)) \Rightarrow (Q(f(x),y) \wedge R(y,g(x,y)))$$
En appliquant la transformation de $\Rightarrow$ dans le système complet $\{\neg, \vee\}$, on obtient :
$$\neg P(x,f(x)) \vee (Q(f(x),y) \wedge R(y,g(x,y)))$$
Puis, par distributivité, on aura :
$$(\neg P(x,f(x)) \vee Q(f(x),y))) \wedge (\neg P(x,f(x)) \vee R(y,g(x,y)))$$
Et donc on a deux clauses :
$$C_1 : (\neg P(x,f(x)) \vee Q(f(x),y))) \quad \text{et} \quad C_2 : (\neg P(x,f(x)) \vee R(y,g(x,y)))$$

Définition 4.1 (Forme clausale)**.** *Une formule est sous forme clausale si elle est sous forme de Skolem et si sa matrice est sous forme normale conjonctive.*

Théorème 4.2. *Soit S un ensemble de clauses résultant de la mise sous forme clausale d'une formule α. Alors, α est insatisfiable si et seulement si S est insatisfiable.*

Ce théorème forme la base de nombreux démonstrateurs automatiques utilisant une représentation des formules sous forme de clauses. Il établit que la recherche de l'insatisfiabilité d'une formule α est équivalente à la recherche d'insatisfiabilité de sa représentation sous forme clausale S. Cependant, α et S ne sont pas logiquement équivalentes : *seule la satisfiabilité est préservée.*

5 Complétude et décidabilité

On admet sans démonstrations les deux théorèmes suivants :

Théorème 5.1 (Théorème de complétude de Gödel)**.** *Le calcul des prédicats est complet.*

Autrement dit : On peut donner un nombre fini de principes (axiomes logiques, schémas d'axiomes logiques et règles de déduction) qui suffisent pour déduire de façon mécanique toutes les formules universellement valide de la logique du premier ordre.

Théorème 5.2. *La logique du premier ordre n'est pas décidable, mais elle est semi-décidable.*

Bien qu'il existe un système de preuve correct et complet, le calcul des prédicats n'est pas décidable. Si par exemple on considère le calcul des séquents, on ne va pas pouvoir déterminer qu'une formule n'est pas universellement valide car il y a un nombre non borné d'explorations possibles.

Toutefois, puisqu'une preuve est un objets finis et que tous les objets considérés sont dénombrables, et donc énumérables, il est possible d'énumérer toutes les preuves, et donc tous les théorèmes.

Le calcul des prédicats est donc semi-décidable :

Si on veut déterminer si une formule α est universellement valide, il suffit de la comparer avec chacun des théorèmes : le calcul se terminera si α est effectivement un théorème (mais dans un temps non borné), le calcul peut ne pas se terminer mais dans ce cas, on n'a pas la certitude que α n'est pas un théorème.

En effet, on ne sait pas si le calcul des théorèmes n'a pas été mené assez loin pour identifier α comme théorème ou si ce calcul ne se terminera pas parce que α n'est pas un théorème.

Bibliographie

[1] R. Cori and D. Lascar. *Logique mathématique : cours et exercices. Calcul propositionnel, algèbres de Boole, calcul des prédicats*. Number vol. 1 in Axiomes (Paris). Masson, 1993.

[2] A. Delessert. *Introduction à la logique*. Mathématiques (Lausanne, Switzerland). Presses polytechniques romandes, 1988.

[3] David Hilbert. Sur les problèmes futurs des mathématiques. In *Les 23 problèmes - Conférence de David Hilbert, au 2e Congrès international des mathématiques, tenu à Paris en 1900*.

[4] E.P. Northrop and D.S. Silver. *Riddles in Mathematics : A Book of Paradoxes*. Dover Recreational Math. Dover Publications, 2014.

[5] P.S. Novikov. *Introduction à la logique mathématique*. Collection universitaire de mathématiques. Dunod, 1964.

[6] Christophe Raffalli, René David, and Karim Nour. *Introduction à la Logique, Théorie de la démonstration (2nd édition)*. Sciences Sup. Dunod, 2004.

[7] J. Sebestik. *Logique et mathématique chez Bernard Bolzano*. Histoire des sciences : Textes et études. J. Vrin, 1992.

Annexe A

Séries d'exercices

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Série de TD N^o 1 "

Logique Mathématiques - L2 Mathématiques

Exercice 1 *Soient P et Q deux propostions logiques :*

1. *Faire les tableaux de vérité pour*
$$\neg P,\ \ P \vee Q,\ \ P \wedge Q,\ \ P \rightarrow Q \ \text{ et } \ P \leftrightarrow Q$$
2. *Lequel parmis les connecteurs* $\vee, \wedge, \rightarrow, \leftrightarrow$ *est commutatif ?*
3. *Démontrer les deux lois de Morgan par les tableaux de vérité.*
$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q \quad \text{et} \quad \neg(P \wedge Q) \equiv \neg P \vee \neg Q$$
4. *Démontrer que*
$$(P \longrightarrow Q) \longleftrightarrow (\neg P \vee Q) \longleftrightarrow \neg(P \wedge \neg Q)$$

Exercice 2 *Soient P et Q les affirmations suivantes :*

- *P : Haroune est fort en algèbre.*
- *Q : Haroune est fort en analyse.*

Représentez sous formes symboliques les affirmations suivantes :

1. *Haroune est fort en algèbre mais faible en analyse ;*
2. *Haroune n'est ni fort en algèbre, ni fort en analyse ;*
3. *Haroune est fort en algèbre s'il est fort en analyse.*

Exercice 3 *construire les tables de vérité des formules suivantes :*

1. $\neg P \rightarrow P \vee Q$;
2. $(\neg P \vee \neg Q)$

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Série de TD N^o 2 "

Logique Mathématiques - L2 Mathématiques

Exercice 1 *Ecrire la négation des propositions suivantes :*

1. *Tout les étudiants du département de mathématiques sont intélligent ;*
2. *Il existe au moins un étudiant étranger à l'université Batna2 ;*
3. *Pour tout* $\varepsilon > 0$, *il existe* $\eta \in \mathbb{Q}$ *tel que* $0 < \eta < \varepsilon$;
4. *Pour tout* $x \in \mathbb{R}$, *on a* $x^2 > 0$.

Exercice 2 *Enoncer la négation des assertions suivantes :*

1. *Tout triangle isocèle possède deux angles de même mesure ;*
2. *Dans tout les lycées, tout les élèves détestent les mathématiques ;*
3. *Pour tout* $x \in \mathbb{Z}$ *il existe* $y \in \mathbb{Q}$ *tel que pour tout* $z \in \mathbb{Q}$, *si* $z < y$ *alors* $z - 1 < x$.

Exercice 3 *Soient* x, y *et* z *des réels. Ecrire la négation de chacune des propositions suivantes :*

$$1.\ x < y \ \vee\ z \geq x\ ; \quad 2.\ x = y \ \wedge\ z \neq x\ ; \quad 3.\ x > y \ \vee\ z \neq x\ ; \quad 4.\ x = y \ \wedge\ z \leq x\ .$$

Exercice 4 *Supposons qu'on a le proverbe : les chiens aboient et que la caravane passe. Si on note par :*

"P : Les chiens aboient" et "Q : La caravane passe"

Traduiser les propositions suivantes en langage propositionnel :

1. *Si la caravane passe, alors les chiens aboient.*
2. *Les chiens n'aboient pas.*
3. *La caravane ne passe pas ou les chiens n'aboient pas.*
4. *Les chiens n'aboient pas et la caravane ne passe pas.*

Exercice 5 *Dans chaque exemple, y a-t-il équivalence entre la proposition A et la proposition B ? Donner l'implication vraie, s'il y en a une.*

Exemple 1 :

Proposition A : Pour toute porte, il existe une seule clé qui ouvre la porte.
Proposition B : Il existe une clé, pour toute porte, la clé ouvre la porte.

Exemple 2 :

Proposition A : $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R} \mid y < x$.
Proposition B : $\exists y,\ \forall x \in \mathbb{R} \in \mathbb{R} \mid y < x$.

Exercice 6 *Evaluer les formules suivantes en considérant uniquement les valeurs des variables données :*

1. $Q \to (P \to R)$ (*avec* $Q \equiv 0$), 2. $P \wedge (P \vee Q)$ (*avec* $Q \equiv 0$), 3. $P \wedge (Q \to R)$ (*avec* $Q \equiv 0$),
4. $Q \to (P \to R)$ (*avec* $Q \equiv 1$), 5. $P \wedge (P \vee Q)$ (*avec* $Q \equiv 1$), 6. $P \wedge (Q \to R)$ (*avec* $Q \equiv 1$) .

Exercice 7 *Evaluer les formules suivantes :*

1. $(P \to Q \wedge Q \to R) \to (P \to R)$, 2. $(P \to Q) \vee (Q \to P)$, 3. $(P \leftrightarrow Q) \wedge (P \leftrightarrow \neg Q)$.

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Série de TD N^o 3 "

Logique Mathématiques - L2 Mathématiques

Exercice 1 *Ecrire avec des quantificateurs les propositions suivantes :*

1. *f est la fonction nulle (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
2. *Le dénominateur D de f s'annule au moins une fois sur $\mathbb{R}$.*
3. *f est l'identité de $\mathbb{R}$ (c'est-à-dire la fonction qui, à chaque réel, associe lui-même.*
4. *Le graphe de f coupe la droite d'équation $y = x$.*
5. *f est croissante sur $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$.*
6. *L'équation $\sin x = x$ a une et une seule solution dans $\mathbb{R}$.*
7. *Pour tout point M du plan P, M est sur le cercle C de centre Ω et de rayon R si et seulement si la distance de M à Ω vaut R.*

Exercice 2 *Ecrire avec des quantificateurs les propositions suivantes :*

1. *f n'est pas nulle (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
2. *Le dénominateur D de la fraction ne s'annule pas sur $\mathbb{R}$.*
3. *f n'est pas l'identité de $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
4. *f n'est pas croissante sur $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*

Exercice 3 *Ecrire avec des quantificateurs les propositions suivantes :*

1. (a) *Tout entier naturel est pair ou impair.*
   (b) *Tout entier naturel est pair ou tout entier naturel est impair.*
2. (a) *f est strictement monotone sur $\mathbb{R}$ (où f désigne une foncftion de $\mathbb{R}$ dans $\mathbb{R}$).*
   (b) *f n'est pas strictement monotone sur $\mathbb{R}$.*

Exercice 4 *Ecrire avec des quantificateurs les propositions suivantes :*

1. (a) *f est constante sur $\mathbb{R}$ (où f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$).*
   (b) *f n'est pas constante sur $\mathbb{R}$.*
2. (a) *f est une homothétie (où f est une transformation du plan P).*
   (b) *f n'est pas une homothétie.*
3. (a) *Pour chaque entier, on peut trouver un entier strictement plus grand (cette affirmation est vraie).*
   (b) *Il y a un entier plus grand que tous les entiers (cette affirmation est fausse).*

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Série de TD N^o " 4 "

Logique Mathématiques - L2 Mathématiques

Exercice 1 *Soient α une antilogie*[1] *et β une formule quelconque. Montrer que $\alpha \Rightarrow \beta$ est une tautologie*[2].

Exercice 2 *On considère la proposition*

H : " Si les hirondelles se rassemblent, elle commencent leur migration. "

Parmi les propositions suivantes, dites lesquelles sont logiquement équivalentes à H, lesquelles sont en contradiction avec H et lesquelles sont sa réciproque.

1. *Si les hirondelles ne commencent pas leur migration, alors elles ne se rassemblent pas.*
2. *Il suffit que les hirondelles se rassemblent pour qu'elle commencent leurs migration.*
3. *Les hirondelles se rassemeblent si elle elles commencent leur migration.*
4. *Les hirondelles commencent leur migraration.*
5. *Les hirondelles se rassemblent et elles ne commencent pas leur migration.*
6. *Il suffit que les hirondelles commencent leur migration pour qu'elles se rassemblent.*
7. *Il est nécessaire que les hirondelles se rassemblent pour qu'elles commencent leur migration.*
8. *Si les hirondelles ne se rassemblent pas, alors elle ne commencent pas leur migration.*
9. *Les hirondelles ne se rassemblent pas ou elles commencent leurs migrartion.*
10. *Il faut que les hirondelles se rassemblent pour qu'elles commencent leur migration.*
11. *Après le rassemblement des hirondelles, c'est l'hiver.*
12. *Les hirondelles se rassemblent.*

Exercice 3 *Que peut-on dire des formules suivantes ? Satisfiables ? Tautologie ? Insatisfiable ? (Utiliser les tables de vérité).*

1. $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$
2. $((p \Rightarrow q) \wedge (s \Rightarrow m)) \Rightarrow ((p \vee s) \Rightarrow q)$
3. $p \Rightarrow q \wedge p \wedge \neg p$
4. $(p \wedge \neg p) \Rightarrow q$

Exercice 4 *Montrer que :*

1. *P implique logiquement p*
2. *p implique logiquement $(p \Rightarrow p)$*
3. $\models (q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
4. $\neg(p \vee \neg q) \Rightarrow (q \Rightarrow r) \equiv q \Rightarrow (p \vee r)$

Exercice 5 *Soient p et q deux propositions logiques, on définit la proposition*

$$(p \Delta q) :\equiv (\neg p \wedge \neg q)$$

Exprimer, à l'aide du seul symbole Δ les proposition :

$$\neg p, \quad p, \quad p \wedge q, \quad p \vee q, \quad p \Rightarrow q$$

1. P est une antilogie si elle est toujour fausse
2. P est une tautologie si elle est toujour vraie

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Série de TD N^o " 5 "

Logique Mathématiques - L2 Mathématiques

Exercice 1 1. *Mettre sous forme normale conjonctive ensuite sous forme disjonctive les formules suivantes :*

(a) $\neg(\neg\beta) \Rightarrow \beta$

(b) $\beta \Rightarrow \neg(\neg\beta)$

(c) $\neg\alpha \Rightarrow (\alpha \Rightarrow \beta)$

(d) $(\neg\beta \Rightarrow \neg\alpha) \Rightarrow ((\neg\beta \Rightarrow \alpha) \Rightarrow \beta)$

(e) $(\alpha \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$

(f) $\alpha \Rightarrow (\neg\beta \Rightarrow \neg(\alpha \Rightarrow \beta))$

(g) $(\alpha \Rightarrow \beta) \Rightarrow ((\neg\alpha \Rightarrow \beta) \Rightarrow \beta)$

2. *Montrer que les formules précidentes sont des théorèmes.*

Exercice 2 *Démonter les deux théorème suivant :*

1. $\models \alpha \Leftrightarrow \not\models \neg\alpha$
2. $(\models \alpha \wedge (\models \alpha \Rightarrow \beta)) \Rightarrow \models \beta$

Exercice 3 *Soient les formules suivantes :*

$$\alpha_1 : (x \vee y) \Rightarrow (x \wedge y) \quad , \quad \alpha_2 : (x \wedge z) \Rightarrow (x \Rightarrow y) \quad , \quad \alpha : (x \vee z) \Rightarrow (x \Rightarrow y)$$

Montrer que

$$\alpha_1, \alpha_2 \models \alpha$$

Exercice 4 *Mettre sous forme normale disjonctive :*

1. $P \Rightarrow ((Q \wedge R) \Rightarrow S)$
2. $(\neg P \wedge Q) \Rightarrow S$

Exercice 5 *Mettre sous forme normale conjonctive :*

1. $P \wedge \neg Q \vee (\neg P \vee Q)$
2. $\neg(P \Rightarrow Q) \vee (P \wedge Q)$

Annexe B

Examens corrigés

Université BATNA 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

جامعة باتنة 2
كلية الرياضيات و الإعلام الآلي
قسم الرياضيات

Corrigé Type de l'Examen Final de "Logique Mathématiques"

Janvier 2022

Question de cours :

1. Donner la définition d'une proposition logique.
   Une proposition est un assemblage de mots d'une langue naturelle vérifiant les trois propriétés : (1)- Syntaxiquement correct, (2)- Sémantiquement correct, (3)- admet une et une seule valeur de vérité (vrai ou faux).
2. Donner la définition d'une formule satisfiable.
   Une formule est satisfiable si sa table de vérité contient au moins une ligne vraie.
3. Donner la définition d'un théorème logique (Tautologie).
   Une tautologie est une formule qui est toujours vraie.

Exercice 1 *Soient A, B et C trois propositions logiques données par :*

$$A : (\neg P \wedge Q) \Rightarrow R \;,\quad B : \neg(P \vee \neg Q) \wedge (S \Rightarrow T) \;,\quad C : \neg(P \wedge Q) \wedge (P \vee Q)$$

telles que P, Q, S et T sont des propositions logiques élémentaires.

1. *Ecrire A, B et C uniquement avec les deux connecteurs logiques $\wedge$ et $\neg$.*

$$\begin{array}{ll} A: & (\neg P \wedge Q) \Rightarrow R \\ A: & \neg(\neg P \wedge Q) \vee R \\ A: & \neg\big((\neg P \wedge Q) \wedge \neg R\big) \end{array} \qquad \begin{array}{ll} B: & \neg(P \vee \neg Q) \wedge (S \Rightarrow T) \\ B: & (\neg P \wedge Q) \wedge (\neg S \vee T) \\ B: & (\neg P \wedge Q) \wedge \neg(S \wedge \neg T) \end{array} \qquad \begin{array}{ll} C: & \neg(P \wedge Q) \wedge (P \vee Q) \\ C: & \neg(P \wedge Q) \wedge \neg(\neg P \wedge \neg Q) \end{array}$$

2. *Ecrire A, B et C uniquement avec les deux connecteurs logiques $\vee$ et $\neg$.*

$$\begin{array}{ll} A: & (\neg P \wedge Q) \Rightarrow R \\ A: & \neg(\neg P \wedge Q) \vee R \\ A: & (P \vee \neg Q) \vee R \end{array} \qquad \begin{array}{ll} B: & \neg(P \vee \neg Q) \wedge (S \Rightarrow T) \\ B: & \neg(P \vee \neg Q) \wedge (\neg S \vee T) \\ B: & \neg\big((P \vee \neg Q) \vee \neg(\neg S \vee T)\big) \end{array} \qquad \begin{array}{ll} C: & \neg(P \wedge Q) \wedge (P \vee Q) \\ C: & (\neg P \vee \neg Q) \wedge (P \vee Q) \\ C: & \neg\big(\neg(\neg P \vee \neg Q) \vee \neg(P \vee Q)\big) \end{array}$$

3. *Pour chacune des propositions A, B et C, dire si elle est satisfaisable ? tautologie ? ou insatisfaisable ?*

P	Q	R	$\neg P$	$\neg P \wedge Q$	$(\neg P \wedge Q) \Rightarrow R$
1	1	1	0	0	1
1	1	0	0	0	1
1	0	1	0	0	1
1	0	0	0	0	1
0	1	1	1	1	1
0	1	0	1	1	0
0	0	1	1	0	1
0	0	0	1	0	1

TABLE 1 – Table de vérité de A

Donc A est satisfaisable.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$P \vee Q$	$\neg(P \wedge Q) \wedge (P \vee Q)$
1	1	1	0	1	0
1	0	0	1	1	1
0	1	0	1	1	1
0	0	0	1	0	0

TABLE 2 – Table de vérité de C

Donc C est satisfaisable.

P	Q	$\neg Q$	S	T	$P \vee \neg Q$	$\neg(P \vee \neg Q)$	$S \Rightarrow T$	$\neg(P \vee \neg Q) \wedge (S \Rightarrow T)$
1	1	0	1	1	1	0	1	0
1	1	0	1	0	1	0	0	0
1	1	0	0	1	1	0	1	0
1	1	0	0	0	1	0	1	0
1	0	1	1	1	1	0	1	0
1	0	1	1	0	1	0	0	0
1	0	1	0	1	1	0	1	0
1	0	1	0	0	1	0	1	0
0	1	0	1	1	0	1	1	1
0	1	0	1	0	0	1	0	0
0	1	0	0	1	0	1	1	1
0	1	0	0	0	0	1	1	1
0	0	1	1	1	1	0	1	0
0	0	1	1	0	1	0	0	0
0	0	1	0	1	1	0	1	0
0	0	1	0	0	1	0	1	0

TABLE 3 – Table de vérité de B

Donc B est satisfaisable.

Exercice 2 *Le connecteur logique "ou exclusif" noté par $\otimes$ est défini par :*

"Pour toutes propositions P et Q : $P \otimes Q$ est vrai uniquement lorsque P est vrai ou Q est vrai, mais pas les deux simultanément."

1. *Donner la table de vérité du connecteur logique $\otimes$.*

P	Q	$P \otimes Q$
1	1	0
1	0	1
0	1	1
0	0	0

2. *Vérifier que :*

(a) $\forall P, Q : P \otimes Q \equiv Q \otimes P$.

On a

P	Q	$P \otimes Q$	$Q \otimes P$
1	1	0	0
1	0	1	1
0	1	1	1
0	0	0	0

Donc $P \otimes Q \equiv Q \otimes P$

(b) $\forall P, Q, S : (P \otimes Q) \otimes S \equiv P \otimes (Q \otimes S)$.

On a

P	Q	S	$P \otimes Q$	$(P \otimes Q) \otimes S$	$Q \otimes S$	$P \otimes (Q \otimes S)$
1	1	1	0	1	0	1
1	1	0	0	0	1	0
1	0	1	1	0	1	0
1	0	0	1	1	0	1
0	1	1	1	0	0	0
0	1	0	1	1	1	1
0	0	1	0	1	1	1
0	0	0	0	0	0	0

Donc $(P \otimes Q) \otimes S \equiv P \otimes (Q \otimes S)$

3. *Trouver $\neg(P \otimes Q)$ et on déduire une écriture pour $P \otimes Q$ uniquement avec les deux connecteurs logiques $\wedge$ et $\neg$.*
On a

P	Q	$P \otimes Q$	$\neg(P \otimes Q)$	$P \Leftrightarrow Q$
1	1	0	1	1
1	0	1	0	0
0	1	1	0	0
0	0	0	1	1

ce qui montre que $\neg(P \otimes Q) \equiv P \Leftrightarrow Q$*, et on*

$$\begin{aligned}
\neg(P \otimes Q) &\equiv P \Leftrightarrow Q \\
&\equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\
&\equiv (\neg P \vee Q) \wedge (\neg Q \vee P) \\
&\equiv \neg(P \wedge \neg Q) \wedge \neg(Q \wedge \neg P)
\end{aligned}$$

Université Mustapha Ben Boulaid - Batna 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

17 Janvier 2023
Durée: 90 Minutes

Examen Final : $^\heartsuit$ *Logique Mathématiques* $^\heartsuit$

Question de Cours (5 **points):**

1. Donner la défintion d'une forme normale conjonctive et une forme normele disjonctive.
2. Donner la définition d'un atôme et d'un litéral.
3. quand est ce que on dit qu'une formule est insatisfiable?

Exercice n°1 (5 points)

Quatre internautes A, B, C et D sont sortis de cybercafés, et ont fait chacun une déclaration :

- **A** : ≪ J'ai chaté avec B et C et D ≫ ;
- **B** : ≪ J'ai chaté avec A et C mais pas avec D ≫ ;
- **C** : ≪ J'ai chaté avec A et B mais pas avec D ≫ ;
- **D** : ≪ J'ai chaté avec B mais pas avec A ni avec C ≫.

Sachant que chaque internaute n'a pas dit la vérité une et une seule fois dans sa déclaration, et que B a chaté avec D et que C n'a pas chaté avec D, qui a réellement chaté avec qui ?
Indication: Si X chate avec au moins deux persons Y et Z, on ecrit: $X \wedge (Y \vee Z)$.

Exercice n°2 (5 points)

1. Donner les formes normales **conjonctive** et **disjonctive** des formules α , β et γ suivantes :

$$\begin{array}{lcl} \alpha & \equiv & \neg(\neg Q \vee \neg R) \rightarrow (P \leftrightarrow (R \vee \neg Q)) \\ \beta & \equiv & (P \wedge R) \rightarrow (P \rightarrow (R \vee Q)) \\ \gamma & \equiv & P \wedge R \vee Q \end{array}$$

2. Montrer que β est un théorème et on déduire que $\alpha, \gamma \models \beta$.

Exercice n°3 (5 points)

Soient les énoncés élémentaires suivantes:

$P \equiv$ **"Ali est étudiant"**, $Q \equiv$ **"Bilal est étudiant" et** $R \equiv$ **"Chiheb est étudiant"**.
Associer à chacun des énoncés suivants la formule propositionnelle qui semble lui correspondre sémantiquement:

❶ Ali et Bilal sont étudiants.

❷ Ali ou Bilal est étudiant.

❸ Exactement un seul parmi Ali et Bilal est étudiant.

❹ Ni Ali ni Chiheb ne sont étudiants.

❺ Au moins l'un des trois n'est pas étudiant.

❻ Un seul parmi les trois n'est pas étudiant.

❼ Seulement deux, parmi les trois, sont étudiants.

❽ Si Ali est étudiant, Bilal l'est aussi.

❽ Si Ali est étudiant, Bilal l'est aussi ; sinon Bilal ne l'est pas.

❾ Ali est étudiant à condition que Chiheb le soit.

❿ Que Chiheb soit étudiant est une condition nécessaire pour que Ali le soit aussi.

BON COURAGE.

Université Mustapha Ben Boulaid - Batna 2
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

17 Janvier 2023
Durée: 90 Minutes

Correction Examen Final : $^{\heartsuit}$ Logique Mathématiques $^{\heartsuit}$

Question de Cours (5 points):

1. Voir le cours........................ 2 points
2. Voir le cours........................ 2 points
3. Voir le cours........................ 1 points

Exercice n°1 (5 points)

$P = [A \wedge (B \vee C \vee D)] \wedge [B \wedge (A \vee C \vee \neg D)] \wedge [C \wedge (A \vee B \vee \neg D)] \wedge [D \wedge (B \vee \neg A \vee \neg C)]$

$= [(A \wedge B) \vee (A \wedge C) \vee (A \wedge D)] \wedge [(B \wedge A) \vee (B \wedge C) \vee (B \wedge \neg D)] \wedge [(C \wedge A) \vee (C \wedge B) \vee (C \wedge \neg D)]$

$\wedge [(D \wedge B) \vee (D \wedge \neg A) \vee (D \wedge \neg C)]$ .... 2 points

On a : $(B \wedge D)$ est vraie , $(C \wedge \neg D)$ est vraie et chaque internaute a menti une seul fois donc : $(D \wedge \neg A), (B \wedge \neg D)$ et $(A \wedge C)$ sont Fausses.

$P = [(A \wedge B)) \vee (A \wedge C) \vee (A \wedge D)] \wedge [(B \wedge A) \vee (B \wedge C) \vee (B \wedge \neg D)] \wedge$

$[(C \wedge A) \vee (C \wedge B) \vee (C \wedge \neg D)] \wedge [(D \wedge B) \vee (D \wedge \neg A) \vee (D \wedge \neg C)]$. ....1 points

⊚ Formules en bleue (Vraies), Formules en rouge (Fausses).

Donc :

- A a réellement chaté avec B et D. ....0.5 points
- B a réellement chaté avec A,C et D. ....0.5 points
- C a réellement chaté avec B. ....0.5 points
- D a réellement chaté avec A et B. ....0.5 points

Exercice n°2 (5 points)

1. Donner les formes **FNC** et **FND** des formules α , β et γ :

$$\alpha \equiv \neg(\neg Q \vee \neg R) \to (P \leftrightarrow (R \vee \neg Q)) \equiv (\neg Q \vee \neg R) \vee [(P \to ((R \vee \neg Q) \wedge ((R \vee \neg Q) \to P)]$$
$$\equiv (\neg Q \vee \neg R) \vee [(\neg P \vee ((R \vee \neg Q) \wedge ((\neg R \wedge Q) \vee P)]$$
$$\equiv (\neg Q \vee \neg R) \vee [(\neg P \vee R \vee \neg Q) \wedge (P \vee (\neg R \wedge Q))]$$
$$\equiv (\neg Q \vee \neg R) \vee [(\neg P \vee R \vee \neg Q) \wedge (P \vee \neg R) \wedge (P \vee Q)]$$
$$\equiv (\neg Q \vee \neg R \vee \neg P \vee R \vee \neg Q) \wedge (\neg Q \vee \neg R \vee P \vee \neg R) \wedge (\neg Q \vee \neg R \vee P \vee Q)$$
$$\equiv (\neg Q \vee \neg R \vee \neg P \vee R) \wedge (\neg Q \vee \neg R \vee P) \wedge (\neg Q \vee \neg R \vee P \vee Q) \equiv \textbf{FNC......}0.5 \textbf{ points}$$
$$\alpha \equiv \neg(\neg Q \vee \neg R) \to (P \leftrightarrow (R \vee \neg Q)) \equiv (\neg Q \vee \neg R) \vee [(P \wedge (R \vee \neg Q)) \vee (\neg P \wedge \neg(R \vee \neg Q))]$$
$$\equiv (\neg Q \vee \neg R) \vee [(P \wedge R) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg R \wedge Q)]$$
$$\equiv \neg Q \vee \neg R \vee (P \wedge R) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg R \wedge Q) \equiv \textbf{FND.....................}0.5 \textbf{ points}$$

$$\beta \equiv (P \wedge R) \to (P \to (R \vee Q)) \equiv (P \wedge R) \to (\neg P \vee (R \vee Q)) \equiv (\neg P \vee \neg R) \vee (\neg P \vee R \vee Q)$$
$$\equiv (\neg P \vee \neg R \vee \neg P \vee R \vee Q) \equiv (\neg P \vee \neg R \vee R \vee Q) \equiv \textbf{FND} \equiv H \equiv H \wedge H \equiv \textbf{FNC......}1 \textbf{ point}$$

$$\gamma \equiv P \wedge R \vee Q \equiv (P \wedge R) \vee (Q) \equiv \textbf{FND...}0.5 \textbf{ points}$$
$$\gamma \equiv P \wedge R \vee Q \equiv (P \wedge R) \vee Q \equiv (P \vee Q) \wedge (R \vee Q) \equiv \textbf{FNC...............}0.5 \textbf{ points}$$

2. Montron que β est un théorème et que $\alpha, \gamma \vDash \beta$:

P	Q	R	¬P	¬Q	¬R	P ∧R	P ∧¬Q	¬P ∧¬R ∧Q	β	γ	α
1	1	1	1	1	1	1	1	1	1	1	1
1	1	0	0	0	0	0	0	0	1	1	0
1	0	1	0	1	0	1	1	0	1	1	1
1	0	0	0	1	1	0	1	0	1	1	1
0	1	1	1	0	0	0	0	1	1	1	1
0	1	0	1	0	1	1	1	1	1	1	1
0	0	1	1	1	0	0	0	0	1	1	1
0	0	0	1	1	1	0	0	0	1	0	1

D'aprés la table de vérité (1 point) on remarque que:

- Toutes les lignes de β sont vraies; donc β est une tautologie.......................0.5 points
- Dans toutes les lignes ou α et γ sont vraies; β est aussi vraie. Alors $\alpha, \gamma \vDash \beta$. ....0.5 points

Exercice n°3 (5 points)

Soient les énoncés élémentaires suivantes:

P $\equiv$ **Ali est étudiant**, **Q** $\equiv$ **Bilal est étudiant et R** $\equiv$ **Chiheb est étudiant**.
Associer à chacun des énoncés suivants la formule propositionnelle qui semble lui correspondre sémantiquement:

$\twoheadrightarrow$ **(0.5 points).........pour chaque réponse:**

❶ Ali et Bilal sont étudiants $\equiv P \wedge Q$.

❷ Ali ou Bilal est étudiant $\equiv P \vee Q$.

❸ Exactement un seul parmi Ali et Bilal est étudiant $\equiv (P \wedge \neg Q) \vee (\neg P \wedge Q)$.

❹ Ni Ali ni Chiheb ne sont étudiants $\equiv \neg P \wedge \neg Q$.

❺ Au moins l'un des trois n'est pas étudiant $\equiv \neg P \vee \neg Q \vee \neg R$.

❻ Un seul parmi les trois n'est pas étudiant $\equiv (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R)$.

❼ Seulement deux, parmi les trois, sont étudiants $\equiv (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \equiv 6$.

❽ Si Ali est étudiant, Bilal l'est $\equiv P \rightarrow Q$.

❽ Si Ali est étudiant, Bilal l'est ; sinon Bilal ne l'est pas $\equiv (P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q)$.

❾ Ali est étudiant à condition que Chiheb le soit $\equiv P \rightarrow R$.

❿ Que Chiheb soit étudiant est une condition nécessaire pour que Ali le soit $\equiv P \rightarrow R$.