Ce qu'il en coûte de construire $\R$, Expédition mûrement planifiée en terrain constructi

Auteur : Schwickerath, Marc
Promoteur(s) : Zenaïdi, Naïm; Mathonet, Pierre
Faculté : Faculté des Sciences
Diplôme : Master en sciences mathématiques, à finalité didactique
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/13862

Faculté des Sciences
Département de Mathématique

Ce qu'il en coûte de construire $\mathbb{R}$

Expédition mûrement planifiée en terrain constructiviste

Mémoire de fin d'études présenté en vue de l'obtention du titre de
Master en Sciences Mathématiques, à finalité didactique

Année académique 2021-2022

Auteur :
Marc Schwickerath

Promoteur :
Naïm Zenaïdi

Co-Promoteur :
Pierre Mathonet

Introduction

L'idée conductrice de ce mémoire est de s'intéresser à une alternative aux mathématiques classiques. Il est ici question de proposer une présentation des réels dans le paradigme constructiviste. Cependant, il fallait avant cela se familiariser avec les enjeux du mouvement constructiviste. Cela passait aussi par une connaissance plus consciente des fondements des mathématiques classiques. C'est pourquoi, ce mémoire se découpe en quatre parties. D'abord, je présente dans la première partie la logique des propositions et la logique des prédicats classiques pour poser un cadre capable d'accueillir la théorie des ensembles de Zermelo-Fraenkel. Dans la deuxième partie, et en continuité avec la première, je présente la construction classique des nombres $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$. La construction classique des réels correspond à la troisième partie. Enfin, la quatrième partie est dédiée à la logique constructiviste et à la présentation des réels constructivistes.

Pour présenter la logique classique, une première approche a été celle du cours de *Théorie des ensembles et logique mathématique* ([18]) de Georges Hansoul. Cependant, il apparaît vite nécessaire de se détacher de notre chère Alma mater pour se figurer la portée d'un tel sujet d'étude. Aussi, ce cours a été un tremplin vers l'étude de la logique comme l'enseignent Hilbert et Ackermann ([21]), Łukasiewicz ([23]) ou encore Russell et Whitehead([32]) dans leurs différents ouvrages.

Le premier chapitre, "Logique Propositionnelle Classique", est dédié à la logique des propositions. D'abord, on y établit la définition de système formel ; définition qui structure chacun des chapitres de la première partie de ce mémoire. On présente alors la logique des propositions comme un système formel et l'on s'interdit, comme le veut le formalisme, toute interprétation, tout recours à l'arithmétique ou à une théorie (naïve) des ensembles. On expérimente ainsi le formalisme dans son expression la plus pure.

Dans la continuité du premier chapitre, on étudie dans le deuxième chapitre, "Théorie du premier ordre", la logique des prédicats. On y fait les mêmes considérations sur ce système formel que dans le premier chapitre. C'est cette logique qui fournit un cadre naturel pour formuler, dans le chapitre 3, la théorie des ensembles, selon Zermelo et Fraenkel, comme un système formel qui prolonge la logique du premier ordre.

Une fois la théorie des ensembles présentée, on entame la deuxième partie du mémoire. Dans le chapitre 4 "Construction de $\mathbb{N}$", on définit les naturels. On ne se contente pas ici d'une description axiomatique à la Peano ; on érige explicitement un modèle. On y définit les propriétés fondamentales de récurrence, d'ordre et d'opérations.

Dans les chapitres 5 et 6, on construit les entiers et les rationnels. Ceux-ci sont présentés

respectivement comme extension des naturels et des entiers. Bien que ces deux constructions sont très classiques et abordées rapidement dans le cursus, j'ai tenu à les présenter en détail, par souci de complétude d'une part et dans l'espoir de pouvoir comparer les paradigmes classique et constructiviste avec plus de pertinence d'autre part.

La construction des réels se fait avec plus d'attention. On présente ici deux constructions dont l'Histoire a voulu qu'elles passent à la postérité : la construction à la Dedekind, fondée sur la notion de coupure et la construction à la Cantor basée sur les suites de Cauchy. Pour chacune des constructions, on définit un ordre et les opérations attendues de sorte que ces structures deviennent des corps commutatifs totalement ordonnés prolongeant l'ensemble des rationnels.

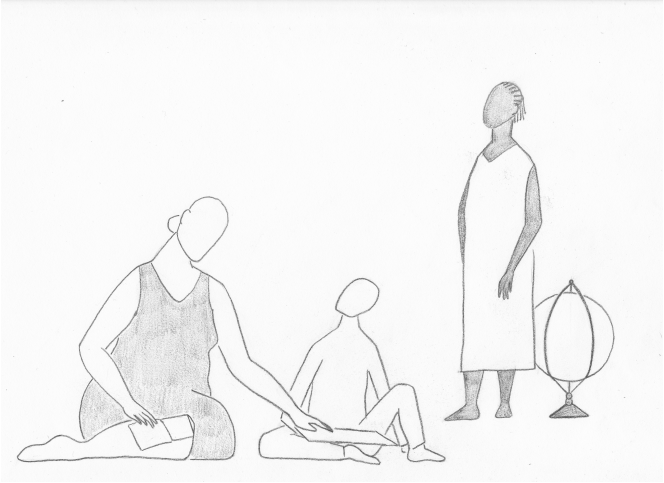
Dans le chapitre 9, on montre que ces deux constructions sont équivalentes. En fait, on établit un résultat plus général ; on montre que toute structure $\mathbb{K}$ ayant les qualités attendues de $\mathbb{R}$, à savoir être un corps archimédien complet, est isomorphe à $\mathbb{R}_C$. En particulier les réels à la Dedekind et les réels à la Cantor sont équivalents. Ce résultat conclut la partie dédiée aux mathématiques classiques.

Bien conscient à présent des enjeux mathématiques sous-tendant la construction des réels dans le paradigme classique, l'on s'engage, téméraire, dans les contrées inconnues du constructivisme (aussi appelé intuitionnisme).

Avec le chapitre 10 "Logique constructive", cette partie s'ouvre sur une présentation sommaire de la logique constructiviste. Nous la présentons pour appuyer les différences d'interprétations qu'il peut y avoir entre les deux paradigmes. Cependant, pour rester fidèle à l'intention initiale du constructivisme, nous ne nous embourberons pas dans un formalisme trop éloigné, selon Brouwer et Bishop, de l'activité et l'intuition mathématique.

Suit alors directement le chapitre 11 "Théorie des ensembles" dans lequel on présente les naturels, les entiers et les rationnels. À nouveau, le formalisme y est réduit à sa plus simple expression : les naturels sont considérés comme donnés, et les constructions de $\mathbb{Z}$ et $\mathbb{Q}$ sont semblables à celles des Classiques.

Le dernier chapitre du mémoire est alors consacré à la définition et à l'étude des réels constructivistes (définition, structure de corps, ordre). En fait, la définition n'est pas très éloignée de celle proposée par Cantor, la différence fondamentale résidant en la nécessité de pouvoir construire tous les objets qui apparaissent dans les développements.



"Clio et Uranie enseignant à un.e jeune élève"
Giorgia Calamia, 2022

Remerciements

Je me place dans le paradigme classique pour pouvoir adresser à mon promoteur Monsieur Zenaïdi et mon co-promoteur Monsieur Mathonet une infinité actuelle de remerciements. Merci pour votre soutien, merci pour cette liberté accordée, merci d'avoir fait de ce travail une expérience riche et exaltante. Merci pour cet enthousiasme partagé.

Merci aussi à "Google" et à mon petit monus sauvage pour avoir rendu chaque moment au B37 lumineux.

Merci à mon gang "Les Joyeux Lurons de L'étude" pour le soutien moral indéfectible et pour cette bulle de bienveillance (#girlpower).

Merci à mes parents, grâce à qui je n'ai jamais manqué de rien.

Merci à tous mes proches de m'avoir patiemment écouté parler de mon mémoire pendant deux ans (et demi). De m'avoir vu m'extasier pour un théorème puis m'énerver parce que dans l'autre bouquin ce n'est pas comme ça qu'il fait...

Merci à moi, de l'avoir fait.

Table des matières

Première partie

Logique classique et théorie des ensembles

Chapitre 1

Logique Propositionnelle Classique

De même qu'aujourd'hui, les féministes s'appliquent à concevoir un langage au moins épicène, au mieux inclusif, pour lutter contre les paradoxes, antinomies et absurdités d'une société viriarcale, de même les mathématicien.ne.s et philosophes du XX^{e} siècle ont travaillé à l'élaboration d'un langage et de fondements des mathématiques pour une théorie sans paradoxes, antinomies ni absurdités.

Dans cette première partie du travail, on présente d'abord les fondements de la logique dite classique. On propose ensuite une théorie des ensembles ; théorie qui sera suffisante pour définir successivement les nombres naturels, entiers, rationnels et enfin réels.

Le terme "logique" est directement issu du grec ancien "logikos" ($\lambda o \gamma \iota \kappa o \varsigma$) qui signifie " raisonnement". Le but premier de la logique est d'étudier les méthodes de raisonnement sans tenir compte du contenu sémantique des propositions. De plus, la logique est prescriptive : une fois sélectionnés les bons raisonnements et partant de prémisses supposées vraies, on se doit d'accepter les conséquences logiques qui en découlent.

Il est d'usage de faire remonter le début de la logique à Aristote (384-322 ACN). Par exemple, son ouvrage "Les analytiques" traite des syllogismes. Cependant, des tentatives de ce type sont perceptibles déjà chez des penseurs antérieurs, notamment chez Parménide d'Élée ($VI^{\text{ème}} - V^{\text{ème}}$ S ACN) qui s'interroge sur les conditions de validité du raisonnement. C'est à ce dernier que l'on doit trois principes fondamentaux de la logique que nous rencontrons dans le cours de ce travail sous une formulation plus moderne :

1. le principe d'identité : "ce qui est est, identique à soi, sans altérité à lui-même" [1] ;
2. le principe du tiers-exclu : il n'y a pas d'alternative entre ce qui est et ce qui n'est pas ;
3. le principe de non-contradiction : "ce qui est ne peut pas être ce qui n'est pas" [2].

À la fin du 19^{e} siècle, l'apparition de paradoxes a démontré la nécessité d'asseoir ces théories sur des bases plus solides [3]. À titre d'exemple, mentionnons le paradoxe du men-

1. Formulation empruntée à Marc-Antoine Gavray dans *Histoire de la philosophie de l'Antiquité.*
2. idem
3. On peut lire dans [1] : "Cependant comme le devoir d'établir la non-contradiction est inéluctable il est nécessaire, semble-t-il, d'axiomatiser la logique elle-même et de prouver que la théorie des nombres,

teur : "un menteur s'exclame qu'il ment" [4]. Ce paradoxe s'évanouit si l'on considère différents degrés de lecture, c'est-à-dire si on fait la distinction entre langage et métalangage (voir [10]). Par exemple, considérons les deux énoncés suivants :

1. Hypatie est née à Alexandrie ;
2. Hypatie comporte 7 lettres ;

L'intérêt porté à Hypatie n'est pas le même dans les deux cas. Dans le premier cas, Hypatie désigne bien une personne, une femme polymathe née à Alexandrie. Alors que dans le second, Hypatie est un mot dont on compte les lettres. Pour éviter ce genre d'ambiguïté, on peut adopter la convention de ceindre le mot, la lettre ou la phrase de guillemets lorsqu'on étudie celleux-ci en tant que tel.le.s. Dès lors, on écrira désormais :

1. Hypatie est née à Alexandrie ;
2. "Hypatie" comporte 7 lettres ;

Cette distinction permet de lever le paradoxe du menteur. En effet, la phrase "un menteur s'exclame qu'il ment" est alors remplacée par

un menteur dit : "je mens"

où "un menteur dit "x" " se situe à un niveau, et où "je mens" se situe à un autre niveau.

Dans la première section de ce chapitre, nous exposons une approche générale fondée sur la notion de système formel déductif en suivant la référence [1]. La seconde section est consacrée à l'étude d'un système formel déductif particulier, à savoir la Logique Propositionnelle Classique (LPC) alors que la section suivante traite de l'équivalence de deux système d'axiomes pour LPC, celui de Frege d'une part et celui de Łukasiewicz d'autre part. Les deux dernières sections sont consacrées à l'étude de deux méta-théorèmes importants : le méta-théorème de la déduction et celui de la complétude.

1.1 Systèmes Formels Déductifs

L'idée qui guide la conception de la définition de système formel est la création d'un langage qui se distingue de notre langage courant (métalangage) pour éviter toute ambiguïté. Il faut donc d'abord s'accorder sur l'alphabet : les signes primitifs qui représenteront les objets étudiés et les relations possibles entre eux. Ensuite, il faut établir une syntaxe, c'est à dire expliciter les règles permettant de différencier les énoncés bien formés des autres. Puis, viennent les axiomes : énoncés bien formulés (cf. infra) considérés comme base de notre connaissance du système. Enfin, les règles d'inférence, qui permettent, comme le nom l'indique, d'inférer de nouveaux énoncés bien formulés à partir des précédents. La définition suivante est capitale pour la suite.

Définition 1.1.1. *Un système formel déductif S est la donnée :*

comme celle des ensembles ne sont que des parties de la logique."

4. Si en effet il ment, alors il dit la vérité et si il ne ment pas, alors il dit ne dit pas la vérité.

1. *d'une liste de symboles (ou signes primitifs) ;*
2. *de règles formatives ;*
3. *d'axiomes ;*
4. *de règles d'inférence.*

Étant donné un système formel, on dira qu'un énoncé est bien formé ou bien formulé s'il est obtenu à partir des symboles conformément aux règles formatives.

Définition 1.1.2. *Étant donné un système formel S, une démonstration (ou preuve) dans S est une suite effectivement écrite d'énoncés bien formulés qui sont soit un axiome, soit une conséquence directe (inférence) d'énoncés bien formulés précédents.*

Au concept de démonstration suit le concept de théorème.

Définition 1.1.3. *Un théorème de S est un énoncé bien formulé $\mathfrak{A}$ qui fait partie d'une preuve. On note alors $S \vdash \mathfrak{A}$ ou simplement $\vdash \mathfrak{A}$ si le contexte est assez clair.*

Du concept de théorème, il résulte la notion de cohérence d'un système formel. En effet, l'idée est de distinguer, parmi les énoncés bien formulés, au moins un qui ne soit pas un théorème. Cela vient du souhait de pouvoir, a posteriori, attribuer une valeur significative aux énoncés du système. On pourrait prendre comme exemple imagé un jeu de société, où

1. La liste des symboles est fournie par les pions du jeu (plateau, pièces,...) ;
2. Les règles formatives sont les coups licites, opérés par les joueurs ;
3. Les axiomes sont l'état initial du jeu.

Une démonstration serait une partie (éventuellement en cours) et un théorème serait alors une position que l'on peut atteindre à partir de la position initiale, en se conformant aux règles du jeu. Si le système n'est pas cohérent, cela signifie que tous les coups sont permis et donc le premier à jouer peut annoncer sa victoire. Si le système formel dans lequel les mathématiques sont formulées n'est pas cohérent, cela signifie que tout énoncé, comme "$0 = 1$", est un théorème.

On peut aussi introduire la notion de complétude. On dira qu'un système est complet si, pour tout énoncé, l'on peut montrer qu'il s'agit d'un théorème ou non.

Enfin, la notion de système formel déductif permet de décrire un cadre général dans lequel on peut, si nécessaire, affiner le raisonnement, en ajoutant des axiomes.

Définition 1.1.4. *Une extension S' d'un système formel déductif S est un système formel déductif qui possède les symboles, les règles formatives, les axiomes et les règles d'inférences de S. Lorsqu'à un système S on ne fait qu'ajouter une liste Γ d'axiomes, on notera alors S' par $S + \Gamma$ et même Γ si le contexte est assez clair.*

1.2 Logique Propositionnelle Classique

La logique propositionnelle classique est un système formel. On la décrit ici en suivant la structure de la définition 1.1.1 comme proposé par [28].

Définition 1.2.1. *L'alphabet de la logique propositionnelle classique (LPC) est composé de 3 types de symboles :*

- *les propositions atomiques notées par des minuscules grecques : φ, ψ, χ,... ;*
- *les connecteurs logiques $\neg$ et $\rightarrow$;*
- *les symboles structurants :), (,], [, ...*

Par souci d'économie, on fera aussi usage de symboles métamathématiques. Ainsi, les lettres majuscules gothiques $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... représenteront des énoncés bien formulés. On notera $\mathfrak{A} \equiv \mathfrak{B}$ pour signifier, selon le contexte, que l'énoncé bien formulé $\mathfrak{B}$ est désigné par $\mathfrak{A}$ ou que l'énoncé bien formulé $\mathfrak{A}$ est désigné par $\mathfrak{B}$. Par exemple on pourra écrire $\mathfrak{A} \equiv \varphi \rightarrow \psi$.

Comme annoncé, des règles de syntaxe sont nécessaires pour distinguer, parmi tous les assemblages finis possibles de symboles, ceux qui appartiennent à LPC :

Définition 1.2.2. *Les énoncés bien formulés, aussi appelés propositions ou encore formules, de LPC sont les assemblages finis de symboles vérifiant une des règles de formation suivantes :*

RF 1. *Toute proposition atomique φ est un énoncé bien formulé.*

RF 2. *Si $\mathfrak{A}$ et $\mathfrak{B}$ sont des énoncés bien formulés alors*

$$(\neg\mathfrak{A}) \text{ et } (\mathfrak{A} \rightarrow \mathfrak{B})$$

sont des énoncés bien formulés. Dans une formule de la forme $\mathfrak{A} \rightarrow \mathfrak{B}$, $\mathfrak{A}$ est la prémisse. On appelle $\mathfrak{B} \rightarrow \mathfrak{A}$ la réciproque de $\mathfrak{A} \rightarrow \mathfrak{B}$.

Les parenthèses permettent de structurer l'ordre d'apparition des connecteurs. Par exemple dans "$\neg(\mathfrak{A} \rightarrow \mathfrak{B})$" le connecteur "$\neg$" porte sur la proposition "$\mathfrak{A} \rightarrow \mathfrak{B}$" et "$\rightarrow$" sur "$\mathfrak{A}$" et "$\mathfrak{B}$". Par contre, dans "$(\neg\mathfrak{A}) \rightarrow \mathfrak{B}$", "$\neg$" porte sur la proposition "$\mathfrak{A}$" et "$\rightarrow$" sur "$\neg\mathfrak{A}$" et "$\mathfrak{B}$". Aussi, en adoptant une autre convention d'écriture, on pourrait se passer de ces symboles : $\rightarrow \mathfrak{A}\mathfrak{B}$. Ainsi une proposition comme "$\mathfrak{A} \rightarrow \neg(\mathfrak{B} \rightarrow \neg\mathfrak{C})$" s'écrirait "$\rightarrow \mathfrak{A}\neg \rightarrow \mathfrak{B}\neg\mathfrak{C}$". Enfin, on prendra l'habitude d'oublier la paire de parenthèses extrémale ; on écrira alors $\neg\mathfrak{A}$ et $\mathfrak{A} \rightarrow \mathfrak{B}$. De manière générale, on écrira $\neg\mathfrak{A}$ à la place de $(\neg\mathfrak{A})$.

Exemple 1.2.1.

- *Si $\mathfrak{A}$ et $\mathfrak{B}$ sont des énoncés bien formulés alors*

$$\neg\mathfrak{A} \rightarrow \mathfrak{B}$$

est un énoncé bien formulé. En effet, vu la règle de formation **RF** *2, $\neg\mathfrak{A}$ est une proposition et donc $\neg\mathfrak{A} \rightarrow \mathfrak{B}$ est aussi bien formulé.*

- *Si* $\mathfrak{A}$ *et* $\mathfrak{B}$ *sont des énoncés bien formulés alors*

$$\neg(\mathfrak{A} \to \neg\mathfrak{B})$$

est un énoncé bien formulé. En effet, vu la règle **RF**2*,* $\neg\mathfrak{B}$ *est une proposition et donc* $\mathfrak{A} \to \neg\mathfrak{B}$ *aussi. Ainsi* $\neg(\mathfrak{A} \to \neg\mathfrak{B})$ *est une proposition.*

Il est d'usage, quand on présente les connecteurs logiques, de mentionner aussi les symboles $\vee$ et $\wedge$. En fait, ceux-ci sont des raccourcis d'écriture. En effet, si $\mathfrak{A}$ et $\mathfrak{B}$ sont des énoncés bien formulés, alors on écrira $\mathfrak{A} \vee \mathfrak{B}$ en lieu et place de $\neg\mathfrak{A} \to \mathfrak{B}$ et on écrira $\mathfrak{A} \wedge \mathfrak{B}$ en lieu et place de $\neg(\mathfrak{A} \to \neg\mathfrak{B})$. On a donc la définition suivante.

Définition 1.2.3. *Les symboles* $\wedge$ *et* $\vee$ *sont définis comme suit :*

- $\varphi \wedge \psi \equiv \neg(\varphi \to \neg\psi)$;
- $\varphi \vee \psi \equiv \neg\varphi \to \psi$.

On reviendra sur le choix de ces notations plus loin.

Viennent ensuite les axiomes. Il y a eu de nombreuses propositions d'axiomes pour la logique classique. Voici un premier exemple. Il s'agit du système proposé par Łukasiewicz (voir par exemple [21, chap.1 §10] ou [23]).

Définition 1.2.4. *Les axiomes de LPC selon Łukasiewicz sont les suivants :*

AŁ 1. $(\varphi \to \chi) \to \Big((\chi \to \psi) \to (\varphi \to \psi)\Big)$;

AŁ 2. $\varphi \to (\neg\varphi \to \chi)$;

AŁ 3. $(\neg\varphi \to \varphi) \to \varphi$;

Mais ce système est loin d'être le seul. Présentons le système proposé par un des pionniers de la logique formelle, G. Frege. Il propose un système d'axiomes composé de 6 propositions.

Définition 1.2.5. *Les axiomes de LPC selon Frege sont les suivants :*

AF 1. $\varphi \to (\psi \to \varphi)$;

AF 2. $\Big(\varphi \to (\psi \to \chi)\Big) \to \Big((\varphi \to \psi) \to (\varphi \to \chi)\Big)$;

AF 3. $\Big(\varphi \to (\psi \to \chi)\Big) \to \Big(\psi \to (\varphi \to \chi)\Big)$;

AF 4. $\Big(\varphi \to \psi\Big) \to \Big(\neg\psi \to \neg\varphi\Big)$;

AF 5. $\neg\neg\varphi \to \varphi$;

AF 6. $\varphi \to \neg\neg\varphi$;

Frege lui-même a proposé plusieurs systèmes, et Łukasiewicz également. Mentionnons également le fait que D. Hilbert proposa aussi des axiomes pour la logique propositionnelle classique.

On pourrait penser qu'il y a alors ici plusieurs logiques, chacune étant associée à son système d'axiomes. Mais nous allons montrer, à titre d'exemple, que ces systèmes sont équivalents, au sens que chaque axiome de l'un est un théorème dans la logique définie par l'autre système. Pour obtenir ces théorèmes, nous avons besoin de règles d'inférence. Mais avant de pouvoir les énoncer, il faut introduire la notion de substitution.

Définition 1.2.6. *Soit $\mathfrak{A}$ un énoncé bien formulé contenant la proposition atomique φ, et soit $\mathfrak{B}$ une proposition. On dit qu'on substitue φ par $\mathfrak{B}$ dans $\mathfrak{A}$ quand on remplace dans $\mathfrak{A}$ toute les occurrences de φ par $\mathfrak{B}$. On notera cette opération $(\mathfrak{B}|\varphi)\mathfrak{A}$. En d'autres termes, on note*

1. $(\mathfrak{B}|\varphi)\varphi \equiv \mathfrak{B}$;
2. $(\mathfrak{B}|\varphi)\neg\mathfrak{A} \equiv \neg\Big((\mathfrak{B}|\varphi)\mathfrak{A}\Big)$;
3. $(\mathfrak{B}|\varphi)\Big(\mathfrak{A}_1 \to \mathfrak{A}_2\Big) \equiv (\mathfrak{B}|\varphi)\mathfrak{A}_1 \to (\mathfrak{B}|\varphi)\mathfrak{A}_2$.

On dit que deux formules $\mathfrak{A}$ et $\mathfrak{B}$ ont la même forme si l'une peut être obtenue en effectuant une substitution dans l'autre.

Il faut cependant s'assurer que l'opération de substitution préserve le caractère ortho-syntaxique d'une proposition. C'est-à-dire qu'un énoncé obtenu après une substitution dans une proposition est un énoncé bien formulé.

Proposition 1.2.7. *Si $\mathfrak{A}$ est un énoncé bien formulé, alors l'énoncé $\mathfrak{A}'$ obtenu après substitution dans $\mathfrak{A}$ d'une proposition atomique est encore un énoncé bien formulé.*

Démonstration. On procède par étapes. D'abord on montre que la propriété est vérifiée pour les propositions atomiques. Ensuite, on montre que si la propriété est vérifiée pour les propositions $\mathfrak{A}_1$ et $\mathfrak{A}_2$ alors elle est encore vérifiée pour $\neg\mathfrak{A}_1$ et $\mathfrak{A}_1 \to \mathfrak{A}_2$. Ainsi on peut conclure que la propriété est vérifiée pour n'importe quelle proposition car alors il suffit d'appliquer les résultats de proche en proche.

- La propriété est trivialement vérifiée pour les propositions atomiques :

$$(\mathfrak{B}|\varphi)\varphi \equiv \mathfrak{B} \ ;$$

- On suppose que la propriété est vérifiée pour les propositions $\mathfrak{A}_1$ et $\mathfrak{A}_2$. Vu les points 2. et 3. de la définition 1.2.6 sur la substitution de propositions de la forme $\neg\mathfrak{A}$ et $\mathfrak{A}_1 \to \mathfrak{A}_2$, on a

$$(\mathfrak{B}|\varphi)\neg\mathfrak{A}_1 \equiv \neg\Big((\mathfrak{B}|\varphi)\mathfrak{A}_1\Big) \quad \text{et} \quad (\mathfrak{B}|\varphi)\Big(\mathfrak{A}_1 \to \mathfrak{A}_2\Big) \equiv (\mathfrak{B}|\varphi)\mathfrak{A}_1 \to (\mathfrak{B}|\varphi)\mathfrak{A}_2.$$

  Comme par hypothèse $(\mathfrak{B}|\varphi)\mathfrak{A}_1$ et $(\mathfrak{B}|\varphi)\mathfrak{A}_2$ sont bien formulés, on conclut que $(\mathfrak{B}|\varphi)\neg\mathfrak{A}_1$ et $(\mathfrak{B}|\varphi)\Big(\mathfrak{A}_1 \to \mathfrak{A}_2\Big)$ sont bien formulés. □

Exemple 1.2.2.

1. *Dans l'axiome* **AŁ**2*, on peut substituer* χ *par* $\psi \to \xi$*, on a alors :*
$$\big((\psi \to \xi)|\chi\big)\mathbf{A\L\,2} \equiv \varphi \to (\neg\varphi \to (\psi \to \xi)).$$
2. *Les formules* **AŁ**2$\equiv \varphi \to (\neg\,\varphi \to \chi)$*,* $\chi \to (\neg\,\chi \to \psi)$ *et* $\neg\,\varphi \to (\neg\neg\,\varphi \to \neg\,\varphi)$ *sont de la même forme.*

Il est à présent possible d'énoncer les règles d'inférence de la logique des propositions.

Définition 1.2.8. *Les règles d'inférences de la logique LPC sont les suivantes.*

RI 1. *La règle du détachement ou modus ponens (noté MP) : si les propositions* $\mathfrak{A}$ *et* $\mathfrak{A} \to \mathfrak{B}$ *sont des théorèmes, alors la proposition* $\mathfrak{B}$ *est un théorème.*

RI 2. *La règle de substitution : si* $\mathfrak{A}$ *est un théorème dans lequel apparaît la proposition atomique* φ*, et si* $\mathfrak{B}$ *est un énoncé bien formulé, alors* $(\mathfrak{B}|\varphi)\mathfrak{A}$ *est un théorème.*

Dans la suite, pour éviter toute confusion, nous noterons $LPC_{\text{Ł}}$ la logique propositionnelle classique où les axiomes sont ceux de Łukasiewicz et LPC_F la logique propositionnelle classique où les axiomes sont ceux de Frege. Le langage, les règles de formation et d'inférence sont identiques dans les deux systèmes. Ces notations seront abandonnées au profit de LPC dès que nous aurons démontré l'équivalence entre les deux systèmes, comme annoncé ci-dessus.

Nous allons illustrer comment toutes ces notions s'articulent dans la section suivante. Voici un premier exemple.

Proposition 1.2.9. *On a* $LPC_{\text{Ł}} \vdash \varphi \to \varphi$*.*

Démonstration. En effet, d'abord, on substitue dans l'axiome **AŁ**2 χ par φ. Ensuite, dans l'axiome **AŁ**1 on effectue les substitutions suivantes : $(\neg\varphi \to \varphi)|\chi$ et $\varphi|\psi$. Ainsi, les deux prémisses du théorème obtenu sont des théorèmes de sorte qu'il reste à effectuer le modus ponens. Formellement, on rédige les démonstrations comme suit (en omettant $LPC_{\text{Ł}}$ en début de ligne) :

$1. \vdash \varphi \to (\neg\varphi \to \varphi)$	$(\varphi\|\chi)\mathbf{A\L}2$
$2. \vdash \big[\varphi \to (\neg\varphi \to \varphi)\big] \to \big[\big((\neg\varphi \to \varphi) \to \varphi\big) \to \big(\varphi \to \varphi\big)\big]$	$\mathbf{A\L}1$
$3. \vdash \big((\neg\varphi \to \varphi) \to \varphi\big) \to \big(\varphi \to \varphi\big)$	$MP\,1, 2$
$4. \vdash \varphi \to \varphi$	$MP\,3, \mathbf{A\L}3$

On a donc bien le résultat annoncé. □

Remarquons que nous avons utilisé la formulation devenue classique en mathématiques d'insérer le résultat dans une "proposition". Ce n'est pas de cette façon que les développements logiques sont présentés usuellement, comme nous le verrons dans la section suivante.

1.3 Les axiomes de Frege sont des théorèmes de $LPC_{\mathbf{Ł}}$

On prouve ici que les axiomes de Frege sont logiquement déductibles des axiomes de Łukasiewicz, à l'aide uniquement des règles d'inférence que sont la substitution et le modus ponens, comme nous l'avons fait dans l'exemple ci-dessus.

Pour ce faire, on suit la résolution proposée par Łukasiewicz dans [23]. Notons que pour inférer chacune des propositions que constitue le systèmes de Frege, il faut établir toute une série de théorèmes intermédiaires. On utilisera alors deux types de labels : les théorèmes obtenus par modus ponens ont une numérotation précédée d'un "T" contrairement aux formules obtenues après substitution.

Afin de toujours assurer une bonne lisibilité des démonstrations, on convient du raccourci d'écriture suivant : on s'accorde le droit d'omettre le connecteur $\to$. Cette élision n'est pas systématique ; de plus celle-ci a lieu localement et ponctuellement, quand la nécessité s'en fait ressentir (pour une question de mise en page). Cette prise de liberté est aussi légitimée par l'usage des parenthèses qui permettent d'éviter tout risque d'ambiguïté. Par exemple les propositions $(\varphi \to (\chi \to \psi))$ et $((\varphi \to \chi) \to \psi)$ peuvent être notées $(\varphi(\chi\,\psi))$ et $((\varphi\,\chi)\,\psi)$ respectivement.

Théorème 1.3.1. *Les axiomes de Frege sont des théorèmes dans le système axiomatique de Łukasiewicz.*

On fait dans l'axiome **AŁ**1 les substitutions qui font de **AŁ**1 la prémisse : $(\varphi\to\chi)|\,\varphi$, $\big((\chi\to\psi)\to(\varphi\to\psi)\big)|\,\chi$ et $\sigma|\,\psi$. On a alors

$$\Big[\ \big\{\underbrace{\varphi\to\chi}_{\varphi'}\big\}\to\big\{\underbrace{(\chi\to\psi)\to(\varphi\to\psi)}_{\chi'}\big\}\ \Big]\to\Big[\Big(\ \big\{\underbrace{(\chi\to\psi)\to(\varphi\to\psi)}_{\chi'}\ \big\}\to\underbrace{\sigma}_{\psi'}\Big)\to(\ \{\underbrace{\varphi\to\chi}_{\varphi'}\}\to\underbrace{\sigma}_{\psi'})\Big]$$

Après modus ponens on a donc un nouveau théorème.

T 1. $\Big(\ \big\{(\chi\to\psi)\to(\varphi\to\psi)\ \big\}\to\sigma\Big)\to(\ \{\varphi\to\chi\}\to\sigma)$

Ensuite, on effectue dans **T**1 les substitutions $\sigma|\,\varphi$ et $\big(\varphi\to(\sigma\to\psi)\big)|\sigma$:

(1) $\Big[\ \big\{(\chi\,\psi)\to(\sigma\,\psi)\ \big\}\to\{\varphi\to(\sigma\,\psi)\}\Big]\to\Big[\ \{\sigma\,\chi\}\to\{\varphi\to(\sigma\,\psi)\}\Big]$.

On effectue alors les substitutions $(\chi\to\psi)|\,\chi$, $(\sigma\to\psi)|\,\psi$ et $((\sigma\to\chi)\to(\varphi\to(\sigma\to\psi)))|\sigma$, toujours dans le théorème **T**1 :

(2) $\underbrace{\Big(\ \big\{(\chi\,\psi\to\sigma\,\psi)\to(\varphi\to\sigma\,\psi)\ \big\}\to\big\{\sigma\,\chi\to(\varphi\to\sigma\,\psi)\big\}\Big)}_{(1)}\to(\ \{\varphi\to\chi\,\psi\}\to\big\{\sigma\,\chi\to(\varphi\to\sigma\,\psi)\big\})$

On a donc le théorème suivant, par modus ponens (MP) entre (1) et (2).

T 2. $\{\varphi\to(\chi\to\psi)\}\to\big\{(\sigma\to\chi)\to(\varphi\to(\sigma\to\psi))\big\}$

Dans **AŁ**1 on effectue la substitution $(\chi\,\psi)|\,\varphi$, $(\varphi\,\psi)|\,\chi$ et $\sigma|\,\psi$:

(3) $\quad((\chi\,\psi)\to(\varphi\,\psi))\to\Big(((\varphi\,\psi)\to\sigma)\to((\chi\,\psi)\to\sigma)\Big)$

On effectue dans **T**1 la substitution $((\varphi\,\psi)\to\sigma)\to((\chi\,\psi)\to\sigma)|\sigma$:

(4) $\quad\Big[\ \underbrace{\Big\{(\chi\,\psi)\to(\varphi\,\psi)\ \Big\}\to\Big(((\varphi\,\psi)\to\sigma)\to((\chi\,\psi)\to\sigma)\Big)}_{(3)}\Big]\to\Big[\{\varphi\,\chi\}\to\{((\varphi\,\psi)\to\sigma)\to((\chi\,\psi)\to\sigma)\}\ \Big]$

On a donc le théorème suivant, par modus ponens entre (3) et (4).

T 3. $(\varphi\to\chi)\to\Big[((\varphi\to\psi)\to\sigma)\to((\chi\to\psi)\to\sigma)\Big]$

Dans le théorème **T**2, on effectue la substitution suivante : $(\varphi\to\chi)|\,\varphi$, $((\varphi\to\psi)\to\sigma)|\,\chi$, $((\chi\to\psi)\to\sigma)|\,\psi$ et $(\tau)|\sigma$.

(5) $\quad\{\underbrace{\varphi\,\chi\to[(\varphi\,\psi\to\sigma)\to(\chi\,\psi\to\sigma)]}_{T3}\}\to\Big\{[\tau\to(\varphi\,\psi\to\sigma)]\to[\varphi\,\chi\to(\tau\to(\chi\,\psi\to\sigma))]\Big\}$

T 4. $[\tau\to((\varphi\to\psi)\to\sigma)]\to[(\varphi\to\chi)\to(\tau\to((\chi\to\psi)\to\sigma))]$

Dans l'axiome **AŁ**1, on substitue σ à ψ.

(6) $\quad(\varphi\to\chi)\to\Big((\chi\to\sigma)\to(\varphi\to\sigma)\Big)$

Cette formule devient la prémisse du théorème **T**4. En d'autres termes, on fait dans **T**4 les substitutions suivantes : $(\varphi\,\chi)|\tau$, $(\chi)|\,\varphi$, $(\sigma)|\,\psi$ $(\varphi\,\sigma)|\sigma$ et $(\psi)|\,\chi$.

(7) $\quad[\underbrace{\varphi\,\chi\to\{\chi\,\sigma\to\varphi\,\sigma\}}_{(6)}]\to[\chi\,\psi\to\{\varphi\,\chi\to(\psi\,\sigma\to\varphi\,\sigma)\}]$

Par modus ponens, on obtient le théorème suivant.

T 5. $(\chi\to\psi)\to\{(\varphi\to\chi)\to((\psi\to\sigma)\to(\varphi\to\sigma))\}$

Le théorème suivant est obtenu en substituant dans l'axiome **AŁ**1 χ par $\neg\,\varphi\to\chi$. Le modus ponens peut alors être effectué avec l'axiome **AŁ**2.

(8) $\quad(\varphi\to(\neg\,\varphi\to\chi))\to\Big(((\neg\,\varphi\to\chi)\to\psi)\to(\varphi\to\psi)\Big)$

T 6. $\Big((\neg\,\varphi\to\chi)\to\psi\Big)\to(\varphi\to\psi)$

Le théorème **T**6 peut être réexprimé à l'aide du raccourci dédié à $\neg\,\varphi\to\chi$:

$$(\varphi\vee\chi\to\psi)\to(\varphi\to\psi)$$

Dans **T**3, on effectue les substitutions suivantes : $(\neg\varphi)|\,\varphi$, $\varphi\,|\,\psi$ et $\varphi\,|\sigma$.

(9) $\Big[\neg\varphi\to\chi\Big]\to\Big[((\neg\varphi\to\varphi)\to\varphi)\to((\chi\to\varphi)\to\varphi)\Big]$

Ensuite, on effectue le substitution $\Big(((\neg\varphi\to\varphi)\to\varphi)\to((\chi\to\varphi)\to\varphi)\Big)|\,\psi$ dans **T**6.

(10) $\Big(\underbrace{(\neg\varphi\to\chi)\to[((\neg\varphi\to\varphi)\to\varphi)\to((\chi\to\varphi)\to\varphi)]}_{(9)}\Big)\to\Big(\varphi\to[((\neg\varphi\to\varphi)\to\varphi)\to((\chi\to\varphi)\to\varphi)]\Big)$

Par modus ponens entre (9) et (10), on obtient :

T 7. $\varphi\to[((\neg\varphi\to\varphi)\to\varphi)\to((\chi\to\varphi)\to\varphi)]$

On reconnaît dans **T**7 l'axiome **AŁ**3 :

$$\varphi\to[\,\underbrace{((\neg\varphi\to\varphi)\to\varphi)}_{\mathbf{A\text{Ł}3}}\to((\chi\to\varphi)\to\varphi)].$$

Dès lors, si l'on substitue φ par un théorème $\mathfrak{A}$, on peut appliquer le modus ponens. Le théorème $\mathfrak{B}$ obtenue aura à son tours une prémisse qui est un théorème, à savoir $(\mathfrak{A}|\,\varphi)\mathbf{A\text{Ł}3}$. On applique ainsi une fois encore le modus ponens. Aussi, pour $\mathfrak{A}\equiv(\neg\varphi\to\varphi)\to\varphi$, on établi le théorème suivant.

T 8. $(\chi\to((\neg\varphi\to\varphi)\to\varphi))\to((\neg\varphi\to\varphi)\to\varphi)$

Soit à présent le théorème $(\neg\tau|\,\chi)\mathbf{A\text{Ł}1}$:

(11) $[\neg\tau\to((\neg\varphi\to\varphi)\to\varphi)]\to[(\neg\varphi\to\varphi)\to\varphi]$

On substitue dans le théorème **T**6 de telle sorte que (11) apparaisse comme prémisse : $\tau|\,\varphi$, $((\neg\varphi\to\varphi)\to\varphi)|\,\chi$ et $(\neg\varphi\to\varphi)\to\varphi\,|\,\psi$

(12) $\Big[\underbrace{\Big(\neg\tau\to((\neg\varphi\,\varphi)\,\varphi)\Big)\to\Big((\neg\varphi\,\varphi)\,\varphi\Big)}_{(11)}\Big]\to\Big[\tau\to((\neg\varphi\,\varphi)\,\varphi)\Big]$

et cela fournit par MP entre (11) et (12)

T 9. $\tau\to((\neg\varphi\to\varphi)\to\varphi)$

En substituant dans **T**4 $\neg\varphi$ à φ et φ à ψ et σ, on fait apparaître **T**9 en prémisse :

(13) $\underbrace{[\tau\to((\neg\varphi\to\varphi)\to\varphi)]}_{T9}\to[(\neg\varphi\to\chi)\to(\tau\to((\chi\to\varphi)\to\varphi))]$

T 10. $(\neg\varphi\to\chi)\to(\tau\to((\chi\to\varphi)\to\varphi))$

À nouveau, on substitue dans **AŁ**1 pour faire apparaître le théorème **T**10 en prémisse. On a donc :

$$(14)\quad \Big[\underbrace{(\neg\varphi\,\chi)}_{\varphi'}\to\underbrace{(\tau((\chi\,\varphi)\,\varphi))}_{\chi'}\Big]\to\Big[\Big(\{\underbrace{\tau((\chi\,\varphi)\,\varphi)}_{\chi'}\}\to\{\psi\}\Big)\to\Big(\{\underbrace{\neg\varphi\,\chi}_{\varphi'})\to\{\psi\}\Big)\Big]$$

Après modus ponens, on a un nouveau théorème.

T 11. $\Big[\Big(\tau\to((\chi\to\varphi)\to\varphi)\Big)\to\psi\,\Big]\to\Big[(\neg\varphi\to\chi)\to\psi\,\Big]$

On constate que la prémisse du théorème **T**11 est de la forme $(\mathfrak{A}\to\mathfrak{B})\to\mathfrak{C}$. Dès lors, en substituant la formule $\mathfrak{A}$ par $\neg\mathfrak{B}$ et $\mathfrak{C}$ par $\mathfrak{B}$ on reconnaît l'axiome **AŁ**3 dans lequel on a substitué φ par $\mathfrak{B}$: $(\neg\mathfrak{B}\to\mathfrak{B})\to\mathfrak{B}$. On est alors en mesure d'effectuer le modus ponens. Explicitement, on fait dans **T**11 les substitutions $\neg((\chi\to\varphi)\to\varphi)|\tau$ et $(\chi\to\varphi)\to\varphi\,|\,\psi$. On obtient donc le théorème suivant.

T 12. $(\neg\varphi\to\chi)\to((\chi\to\varphi)\to\varphi)$

Ce théorème **T**12 peut être réexprimé avec le connecteur "$\vee$" :

$$\mathbf{T\,12}\equiv(\neg\varphi\vee\chi)\to((\chi\to\varphi)\to\varphi).$$

On effectue les substitutions dans **T**6 pour que **T**12 soit en prémisse :

$$(15)\quad [(\neg\varphi\to\chi)\to((\chi\to\varphi)\to\varphi)]\to[\varphi\to((\chi\to\varphi)\to\varphi)]$$

On a grâce au modus ponens le théorème suivant.

T 13. $\varphi\to((\chi\to\varphi)\to\varphi)$

On substitue dans **T**13 :

$$(16)\quad \chi\to((\neg\varphi\to\chi)\to\chi)$$

On substitue dans le théorème **T**2 pour faire apparaître (16) comme prémisse : $\chi\,|\,\varphi$, $\neg\varphi\to\chi\,|\,\chi$, $\chi\,|\,\psi$ et $\varphi\,|\sigma$:

$$(17)\quad [\underbrace{\chi\to((\neg\varphi\to\chi)\to\chi)}_{(16)}]\to[\underbrace{(\varphi\to(\neg\varphi\to\chi)}_{\mathbf{AŁ}2})\to(\chi\to(\varphi\to\chi))]$$

On voit ainsi apparaître l'axiome **AŁ**2 dans la seconde prémisse. En effectuant successivement le modus ponens, on a alors le théorème suivant.

T 14. $\chi\to(\varphi\to\chi)$

Nous avons ainsi démontré que dans le système de Łukasiewicz l'axiome 1. de Frege est un théorème.

Fait 1. *L'axiome* **AF**1 $\equiv \varphi \to (\chi \to \varphi)$ *théorème de* $LPC_Ł$.

On continue à démontrer que tous les axiomes de Frege sont des théorèmes dans le système Łukasiewicz. Cependant, afin d'optimiser le raisonnement, nous n'explicitons plus les substitutions entre les théorèmes. Elles sont indiquées à droite dans chaque ligne ci-dessous.

$(18) \vdash (\chi \to \varphi\, \chi) \to \Big((\varphi\, \chi \to \psi) \to (\chi \to \psi)\Big)$	**AŁ**1
$(19) \vdash \chi \to (\varphi \to \chi)$	**T**14
$\mathbf{T15} \vdash \Big((\varphi\, \chi \to \psi) \to (\chi \to \psi)\Big)$	$MP(18)(19)$
$(20) \vdash (\neg\, \chi\, \varphi \to (\varphi\, \chi \to \chi)) \to (\varphi \to (\varphi\, \chi \to \chi))$	(18)
$(21) \vdash (\neg\, \chi \to \varphi) \to ((\varphi \to \chi) \to \chi)$	**T**12
$\mathbf{T16} \vdash \varphi \to (\varphi\, \chi \to \chi)$	$MP(20)(21)$
$(22) \vdash \chi \to (\chi\, \psi \to \psi)$	**T16**
$(23) \vdash \{\chi \to (\chi\, \psi \to \psi)\} \to \Big\{(\varphi \to \chi\, \psi) \to (\chi \to (\varphi \to \psi))\Big\}$	**T**2
$(\mathbf{T17}) \vdash (\varphi \to (\chi \to \psi)) \to (\chi \to (\varphi \to \psi))$	$MP(22)(23)$

Nous avons ainsi obtenu un deuxième axiome de Frege.

Fait 2. *L'axiome* **AF**3 $\equiv (\varphi \to (\chi \to \psi)) \to (\chi \to (\varphi \to \psi))$ *est un théorème de* $LPC_Ł$.

(24) $\vdash [(\varphi(\chi\,\psi))\to(\chi(\varphi\,\psi))]\to[((\chi(\varphi\,\psi))\to\sigma)\to((\varphi(\chi\,\psi))\to\sigma)]$ **AŁ**1

(25) $\vdash (\varphi\to(\chi\to\psi))\to(\chi\to(\varphi\to\psi))$ **T17**

T18 $\vdash ((\chi\to(\varphi\to\psi))\to\sigma)\to((\varphi\to(\chi\to\psi))\to\sigma)$ $MP(24)(25)$

(26) $\vdash [(\neg\,\varphi\to(\varphi\,\chi))\to((\varphi\,\chi\to\varphi)\to\varphi)]\to[(\varphi\to(\neg\,\varphi\,\chi))\to((\varphi\,\chi\to\varphi)\,\varphi)]$ **T18**

(27) $\vdash (\neg\,\varphi\to\varphi\,\chi)\to((\varphi\,\chi\to\varphi)\to\varphi)$ **T12**

(28) $\vdash (\varphi\to(\neg\,\varphi\to\chi))\to((\varphi\,\chi\to\varphi)\,\varphi)$ $MP(26)(27)$

(29) $\vdash \varphi\to(\neg\,\varphi\to\chi)$ **AŁ**2

T19 $\vdash ((\varphi\to\chi)\to\varphi)\to\varphi$ $MP(28)(29)$

(30) $\vdash (\varphi\to\chi)\to[((\varphi\to\psi)\to\sigma)\to((\chi\to\psi)\to\sigma)]$ **T**3

(31) $\vdash ((\varphi\,\chi)\to(((\varphi\,\psi)\sigma)\to((\chi\,\psi)\sigma)))\to(((\varphi\,\psi)\sigma)\to((\varphi\,\chi)\to((\chi\,\psi)\sigma)))$ **T17**

T20 $\vdash ((\varphi\to\psi)\to\sigma)\to[(\varphi\to\chi)\to((\chi\to\psi)\to\sigma)]$ $MP(30)(31)$

(32) $\vdash ((\varphi\,\chi\to\varphi)\to\varphi)\to[((\varphi\,\chi)\to\psi)\to((\psi\to\varphi)\to\varphi)]$ **T20**

(33) $\vdash ((\varphi\to\chi)\to\varphi)\to\varphi$ **T19**

T21 $\vdash ((\varphi\to\chi)\to\psi)\to((\psi\to\varphi)\to\varphi)$ $MP(32)(33)$

T22 $\vdash ((\varphi\to\chi)\to\chi)\to((\chi\to\varphi)\to\varphi)$ **T21**

(34) $\vdash (((\varphi\,\chi)\,\psi)\to((\psi\,\varphi)\,\varphi))\to((((\psi\,\varphi)\,\varphi)\to\sigma)\to(((\varphi\,\chi)\,\psi)\to\sigma))$ **AŁ**1

T23 $\vdash [((\psi\to\varphi)\to\varphi)\to\sigma]\to[((\varphi\to\chi)\to\psi)\to\sigma]$ $MP(34)$**T21**

(35) $\vdash [((\psi\to\varphi)\to\varphi)\to((\varphi\to\psi)\to\psi)]\to[((\varphi\to\chi)\to\psi)\to((\varphi\to\psi)\to\psi)]$ **T23**

(36) $\vdash ((\psi\to\varphi)\to\varphi)\to((\varphi\to\psi)\to\psi)$ **T22**

T24 $\vdash ((\varphi\to\chi)\to\psi)\to((\varphi\to\psi)\to\psi)$ $MP(35)(36)$

(37) $\vdash ((\varphi\,\chi)\to(\varphi\,\chi))\to((\varphi\to(\varphi\,\chi))\to(\varphi\,\chi))$ **T24**

(38) $\vdash ((\varphi\,\chi)\to(\varphi\,\chi))$ *Prop.*1.2.9

T25 $\vdash (\varphi\to(\varphi\to\chi))\to(\varphi\to\chi)$ $MP(37)(38)$

(39)$[((\varphi\,\chi)\,\psi)\to((\varphi\to\psi)\to\psi)]\to[(\varphi\to\sigma)\to(((\varphi\,\chi)\,\psi)\to((\sigma\to\psi)\to\psi))]$ **T**4

(40) $\vdash ((\varphi\to\chi)\to\psi)\to((\varphi\to\psi)\to\psi)$ **T24**

T26 $\vdash (\varphi\to\sigma)\to[((\varphi\to\chi)\to\psi)\to((\sigma\to\psi)\to\psi)]$ $MP(39)(40)$

(41) $\vdash ((\varphi\,\sigma)\to(((\varphi\,\chi)\,\psi)\to((\sigma\,\psi)\,\psi)))\to(((\varphi\,\chi)\,\psi)\to((\varphi\,\sigma)\to((\sigma\,\psi)\,\psi)))$ **T17**

T27 $\vdash ((\varphi\to\chi)\to\psi)\to((\varphi\to\sigma)\to((\sigma\to\psi)\to\psi))$ $MP(41)$**T26**

(42) $\vdash ((\varphi\to\psi)\to(\chi(\varphi\,\psi)))\to((\varphi\to\sigma)\to((\sigma\to(\chi(\varphi\,\psi)))\to(\chi(\varphi\,\psi))))$ **T27**

(43) $\vdash (\varphi\,\psi)\to(\chi\to(\varphi\,\psi))$ **T**14

T28 $\vdash (\varphi\to\sigma)\to[(\sigma\to(\chi\to(\varphi\to\psi)))\to(\chi\to(\varphi\to\psi))]$ $MP(42)(43)$

(44) $\vdash ((\varphi\,\sigma)\to((\sigma(\chi(\varphi\,\psi)))\to(\chi(\varphi\,\psi))))\to((\sigma(\chi(\varphi\,\psi)))\to((\varphi\,\sigma)\to(\chi(\varphi\,\psi))))$ **T17**

T29 $\vdash [\sigma\to(\chi\to(\varphi\to\psi))]\to[(\varphi\to\sigma)\to(\chi\to(\varphi\to\psi))]$ MP**T28**(44)

(45) $\vdash ((\varphi\,\chi)\to((\chi\,\psi)\to(\varphi\,\psi)))\to((\chi\,\psi)\to((\varphi\,\chi)\to(\varphi\,\psi)))$ **T17**

(46) $\vdash (\varphi\to\chi)\to((\chi\to\psi)\to(\varphi\to\psi))$ **AŁ**1

T30 $\vdash (\chi\to\psi)\to((\varphi\to\chi)\to(\varphi\to\psi))$ $MP(45)(46)$

(47) $\vdash [(\chi\,\psi)\to((\varphi\,\chi)\to(\varphi\to\psi))]\to[(\varphi\to(\chi\,\psi))\to((\varphi\,\chi)\to(\varphi\to\psi))]$ **T29**

T31 $\vdash [\varphi\to(\chi\to\psi)]\to[(\varphi\to\chi)\to(\varphi\to\psi)]$ $MP(47)$**T30**

On a donc obtenu le résultat suivant.

Fait 3. *L'axiome* **AF**2 $\equiv (\varphi \to (\chi \to \psi)) \to ((\varphi \to \chi) \to (\varphi \to \psi))$ *est un théorème dans* $LPC_Ł$.

(48) $\vdash (\varphi \to (\neg\varphi \to \chi)) \to (\neg\varphi \to (\varphi \to \chi))$	**T17**
T32 $\vdash \neg\varphi \to (\varphi \to \chi)$	MP(**AŁ**2)(48)
(49)$(\neg\varphi \to (\varphi\,\chi)) \to [(\varphi\,\chi \to \psi) \to (\neg\varphi\,\psi)]$	(**AŁ**1)
T33 $\vdash ((\varphi \to \chi) \to \psi) \to (\neg\varphi \to \psi)$	MP(49)**T32**
(50) $\vdash ((\neg\varphi \to \varphi) \to \varphi) \to ((\varphi \to \neg\varphi) \to \neg\varphi)$	**T22**
T34 $\vdash (\varphi \to \neg\varphi) \to \neg\varphi$	MP(50)**AŁ**3
(51) $\vdash ((\neg\varphi \to \varphi) \to \varphi) \to (\neg\neg\varphi \to \varphi)$	**T33**
T35 $\vdash \neg\neg\varphi \to \varphi$	MP(51)**AŁ**3
(52) $\vdash \Big((\neg\varphi \to \neg\neg\varphi) \to \neg\neg\varphi\Big) \to (\varphi \to \neg\neg\varphi)$	(**T**6)
(53) $\vdash (\neg\varphi \to \neg\neg\varphi) \to \neg\neg\varphi$	**T34**
T36 $\vdash \varphi \to \neg\neg\varphi$	MP(52)(53)

Les théorèmes **T35** et **T36** ont une importance particulière pour notre propos.

Fait 4. *L'axiome* **AF**5 $\equiv \neg\neg\varphi \to \varphi$ *est un théorème de* $LPC_Ł$.

Fait 5. *L'axiome* **AF**6 $\equiv \varphi \to \neg\neg\varphi$ *est un théorème de* $LPC_Ł$.

(54) $\vdash (\neg\neg\varphi \to \varphi) \to [(\varphi \to \chi) \to (\neg\neg\varphi \to \chi)]$	**AŁ**1
T37 $\vdash (\varphi \to \chi) \to (\neg\neg\varphi \to \chi)$	MP(54)**T35**
(55) $\vdash (\varphi\,\chi \to (\neg\neg\varphi \to \chi)) \to [((\neg\neg\varphi \to \chi) \to \psi) \to (\varphi\,\chi \to \psi)]$	**AŁ**1
T38 $\vdash ((\neg\neg\varphi \to \chi) \to \psi) \to ((\varphi \to \chi) \to \psi)$	MP**T37**(55)
(56) $\vdash ((\neg\neg\varphi \to \chi) \to ((\chi\,\neg\varphi)\neg\varphi)) \to ((\varphi \to \chi) \to ((\chi\,\neg\varphi)\neg\varphi))$	**T38**
(57) $\vdash (\neg\neg\varphi \to \chi) \to ((\chi \to \neg\varphi) \to \neg\varphi)$	(**T**12
T39 $\vdash (\varphi \to \chi) \to ((\chi \to \neg\varphi) \to \neg\varphi)$	MP(56)(57)
(58) $\vdash \{(\varphi\,\chi) \to ((\chi \to \neg\varphi) \to \neg\varphi)\} \to \Big\{(\sigma \to (\chi\,\neg\varphi)) \to ((\varphi\,\chi) \to (\sigma \to \neg\varphi))\Big\}$	**T**2
T40 $\vdash (\sigma \to (\chi \to \neg\varphi)) \to ((\varphi \to \chi) \to (\sigma \to \neg\varphi))$	MP**T39**(58)
(59) $\vdash (\neg\chi \to (\chi \to \neg\varphi)) \to ((\varphi \to \chi) \to (\neg\chi \to \neg\varphi))$	**T40**
(60) $\vdash \neg\chi \to (\chi \to \neg\varphi)$	**T32**
T41 $\vdash (\varphi \to \chi) \to (\neg\chi \to \neg\varphi)$	MP(59)(60)

Nous avons ainsi obtenu le dernier axiome de Frege.

Fait 6. *L'axiome* **AF**4 $\equiv (\varphi \to \chi) \to (\neg\, \chi \to \neg\, \varphi)$ *est un théorème de* $LPC_Ł$.

Notons que la réciproque du théorème **T41** est aussi un théorème.

$(61) \vdash \{(\neg\, \varphi\, \chi) \to ((\chi \to \varphi) \to \varphi)\} \to \Big\{(\sigma \to (\chi\, \varphi)) \to ((\neg\, \varphi\, \chi) \to (\sigma \to \varphi))\Big\}$	**T**2
T42 $\vdash (\sigma \to (\chi \to \varphi)) \to ((\neg\, \varphi \to \chi) \to (\sigma \to \varphi))$	$MP(61)$**T12**
$(62) \vdash (\chi \to (\neg\, \chi \to \varphi)) \to ((\neg\, \varphi \to \neg\, \chi) \to (\chi \to \varphi))$	**T42**
T43 $\vdash (\neg\, \varphi \to \neg\, \chi) \to (\chi \to \varphi)$	$MP(62)$**AŁ**2

Fait 7. *La formule* $(\neg\, \varphi \to \neg\, \chi) \to (\chi \to \varphi)$ *est un théorème de* $LPC_Ł$.

On a donc réussi à inférer chaque axiome de Frege dans le système proposé par Łukasiewicz. Pour montrer que les deux systèmes sont équivalents, il reste à établir que les axiomes de Łukasiewicz peuvent être déduits de ceux de Frege. Cela peut très certainement se faire en utilisant les mêmes développements que ci-dessus. On reviendra sur ce fait plus loin pour profiter d'une technique de démonstration particulièrement efficace mais non encore établie à ce stade, à savoir le méta-théorème de la déduction.

1.4 Le méta-théorème de la déduction (dans LPC_F)

Un résultat incontournable sur la logique des propositions est le (méta-)théorème de la déduction. Ce résultat propose une technique pour établir des théorèmes. Nous allons le démontrer dans LPC_F et nous l'utiliserons pour obtenir, entre autres, les axiomes de Łukasiewicz comme théorèmes de LPC_F. Remarquons que nous avons démontré à la section précédente que les axiomes de Frege sont de théorèmes dans $LPC_Ł$. On pourra donc également utiliser le méta-théorème de la déduction dans $LPC_Ł$. Dans la suite, nous l'utiliserons donc dans LPC (sans indice).

L'idée est que si en adjoignant aux axiomes de LPC une proposition $\mathfrak{A}$, ce que l'on note par $LPC + \mathfrak{A}$, et que l'on est alors en mesure de montrer que $\mathfrak{B}$ est un théorème :

$$LPC + \mathfrak{A} \vdash \mathfrak{B},$$

alors, on voudrait [5] établir que $\mathfrak{A} \to \mathfrak{B}$ est un théorème de LPC_F. On note cependant que certaines précautions doivent être prises sur les règles d'inférence autorisées dans $LPC_F + \mathfrak{A}$. En effet, si l'on se place dans le cas le plus simple où l'on ajoute aux axiomes de LPC_F la proposition φ, cette proposition ayant à présent le statut d'axiome, elle possède dès lors le statut de théorème : $LPC + \varphi \vdash \varphi$. Si l'on substitue φ par ψ on a alors $LPC + \varphi \vdash \psi$. Or $\varphi \to \psi$ n'est pas a priori un théorème [6] de LPC_F. Aussi, on introduit la notion de formule déduite (dans LPC_F).

5. Cela tient de l'interprétation classique que l'on a du connecteur $\to$.
6. On reviendra plus tard sur ce fait.

Définition 1.4.1. *Une formule $\mathfrak{B}$ est déduite des formules $\mathfrak{A}_a$, $\mathfrak{A}_b, ...\mathfrak{A}_m$ si elle est un théorème de LPC_F, si elle est une des formule $\mathfrak{A}_i$ ou si elle inférée par modus ponens de formules déduites de $\mathfrak{A}_a$, $\mathfrak{A}_b, ...\mathfrak{A}_m$. On note alors*

$$LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_m \vdash \mathfrak{B}$$

Avant de passer au théorème, nous avons besoin d'un résultat préliminaire.

Proposition 1.4.2. *La formule $\varphi \to \varphi$ est un théorème de LPC_F.*

Démonstration. Écrivons la preuve formelle :

1. $LPC_F \vdash (\varphi \to (\psi \to \varphi)) \to ((\varphi \to \psi) \to (\varphi \to \varphi))$ **AF**2
2. $LPC_F \vdash \varphi \to (\psi \to \varphi)$ $(\varphi|\chi)$**AF**1
3. $LPC_F \vdash (\varphi \to \psi) \to (\varphi \to \varphi)$ $MP\,1.\,2.$
4. $LPC_F \vdash (\varphi \to (\psi \to \varphi)) \to (\varphi \to \varphi)$ $(\varphi \to \psi|\psi)3.$
5. $LPC_F \vdash \varphi \to \varphi$ $MP\,2.\,4.$

On a donc bien établi $\varphi \to \varphi$ dans LPC_F. □

On est maintenant en mesure d'énoncer et établir le théorème souhaité.

Théorème 1.4.3 (Méta-théorème de la déduction (Herbrand-Tarski, 1930))**.** *Si, ayant ajouté aux axiomes de LPC_F les formules $\mathfrak{A}_a$, $\mathfrak{A}_b, \ldots, \mathfrak{A}_m$, on établit, avec uniquement la règle du modus ponens, que $\mathfrak{B}$ est un théorème, alors $LPC \vdash \mathfrak{A}_a \to (\mathfrak{A}_b \to (...(\mathfrak{A}_m \to \mathfrak{B})...))$.*

Démonstration. On montre d'abord que si on a

$$LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l + \mathfrak{A}_m \vdash \mathfrak{B}$$

alors on a aussi

$$LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l \vdash \mathfrak{A}_m \to \mathfrak{B}\ .$$

Le résultat général s'obtient alors sans difficulté en procédant de proche en proche.

D'abord, on montre que la propriété est vérifiée si $\mathfrak{B}$ est un théorème de LPC_F ou une des formules parmi $\mathfrak{A}_a, ...\mathfrak{A}_m$. Ensuite, on montre que si la propriété est vérifiée pour les formules $\mathfrak{B}$ et $\mathfrak{B} \to \mathfrak{C}$ alors elle est vérifiée pour $\mathfrak{C}$.

1. D'abord, si $\mathfrak{B}$ est un théorème de LPC_F alors, par la définition 1.4.1, $\mathfrak{B}$ est déduit de $\mathfrak{A}_a$, $\mathfrak{A}_b$, ..., $\mathfrak{A}_l$. La formule $\mathfrak{B} \to (\mathfrak{A}_m \to \mathfrak{B})$ est un théorème de LPC_F (obtenu par substitution évidente dans l'axiome **AF**1). Donc par modus ponens, la formule $\mathfrak{A}_m \to \mathfrak{B}$ est également déduite de $\mathfrak{A}_a$, $\mathfrak{A}_b$, ..., $\mathfrak{A}_l$.
   Ensuite, si $\mathfrak{B}$ est une des formules parmi $\mathfrak{A}_a, ..., \mathfrak{A}_m$, alors deux cas sont possibles :
   (a) si $\mathfrak{B} \equiv \mathfrak{A}_m$: comme $\mathfrak{A}_m \to \mathfrak{A}_m$ est un théorème de LPC_F par la proposition 1.4.2, on a
   $$LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l \vdash \mathfrak{A}_m \to \mathfrak{B};$$

(b) si $\mathfrak{B}$ est une formule parmi $\mathfrak{A}_a, ..., \mathfrak{A}_l$: la formule $\mathfrak{A}_i \to (\mathfrak{A}_m \to \mathfrak{A}_i)$ est un théorème de LPC_F. On a donc, dans $LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l$, les théorèmes $\mathfrak{A}_i$ et $\mathfrak{A}_i \to (\mathfrak{A}_m \to \mathfrak{A}_i)$. En appliquant le modus ponens, on a donc bien $LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l \vdash \mathfrak{A}_m \to \mathfrak{B}$. Formellement, on écrit

$$\begin{aligned} LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l &\vdash \mathfrak{A}_i \\ &\vdash \mathfrak{A}_i \to (\mathfrak{A}_m \to \mathfrak{A}i) \\ &\vdash \mathfrak{A}_m \to \mathfrak{A}_i. \end{aligned}$$

2. On suppose à présent que la propriété est vérifiée pour les formules déduites $\mathfrak{B}$ et $\mathfrak{B} \to \mathfrak{C}$. Dès lors, $\mathfrak{A}_m \to \mathfrak{B}$ et $\mathfrak{A}_m \to (\mathfrak{B} \to \mathfrak{C})$ sont déduits de $LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l$. Comme la formule $\Big(\mathfrak{A}_m \to (\mathfrak{B} \to \mathfrak{C})\Big) \to \Big((\mathfrak{A}_m \to \mathfrak{B}) \to (\mathfrak{A}_m \to \mathfrak{C})\Big)$ (par substitution évidente dans l'axiome **AF**2), elle est déduite de $\mathfrak{A}_a, \mathfrak{A}_b, ..., \mathfrak{A}_l$. Il suffit alors d'appliquer le modus ponens :

$$\begin{aligned} LPC_F + \mathfrak{A}_a + \mathfrak{A}_b + ... + \mathfrak{A}_l &\vdash \mathfrak{A}_m \to \mathfrak{B} \\ &\vdash \mathfrak{A}_m \to (\mathfrak{B} \to \mathfrak{C}) \\ &\vdash \Big(\mathfrak{A}_m \to (\mathfrak{B} \to \mathfrak{C})\Big) \to \Big((\mathfrak{A}_m \to \mathfrak{B}) \to (\mathfrak{A}_m \to \mathfrak{C})\Big) \\ &\vdash (\mathfrak{A}_m \to \mathfrak{B}) \to (\mathfrak{A}_m \to \mathfrak{C}) \\ &\vdash \mathfrak{A}_m \to \mathfrak{C}. \end{aligned}$$

La preuve est alors complète. □

Passons maintenant en revue quelques applications du méta-théorème de la déduction.

Proposition 1.4.4. *La formule* $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$ *est un théorème de* LPC_F.

Démonstration. D'après le méta-théorème de la déduction il suffit de démontrer

$$LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \varphi.$$

Cela se fait simplement :

1. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \neg\varphi \to \neg\psi$
2. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash (\neg\varphi \to \neg\psi) \to (\neg\neg\psi \to \neg\neg\varphi)$ $(\neg\varphi|\varphi)(\neg\psi|\psi)$**AF**4
3. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \neg\neg\psi \to \neg\neg\varphi$ $MP\,1.\,2.$
4. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \psi$
5. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \neg\neg\psi$ $MP\,4.$ **AF**6.
6. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \neg\neg\varphi$ $MP\,3.\,6.$
7. $LPC_F + (\neg\varphi \to \neg\psi) + (\psi) \vdash \varphi$ $MP\,6.$ **AF**5.

On a donc bien déduit φ des théorèmes de LPC_F et des propositions $\neg\varphi \to \neg\psi$ et ψ. □

Remarquons que la déduction ci-dessus contient des substitutions. Cependant, ces substitutions ne sont faites que dans les axiomes et théorèmes de LPC_F, et fournissent donc des théorèmes de LPC_F.

De la même façon, on peut obtenir, à titre d'exercice, de nouveaux théorèmes impliquant le connecteur $\neg$.

Proposition 1.4.5. *Les formules*
1) $(\varphi \to \psi) \to (\varphi \to \neg\neg\psi)$,
2) $(\varphi \to \neg\neg\psi) \to (\varphi \to \psi)$,
3) $(\neg\neg\varphi \to \psi) \to (\varphi \to \psi)$,
4) $(\varphi \to \psi) \to (\neg\neg\varphi \to \psi)$
sont des théorèmes de LPC_F.

Démonstration. Démontrons que la première formule est un théorème. Par le méta-théorème de la déduction, il suffit de démontrer

$$LPC_F + (\varphi \to \psi) + (\varphi) \vdash \neg\neg\psi.$$

Mais on a directement

1. $LPC_F + (\varphi \to \psi) + (\varphi) \vdash (\varphi \to \psi)$
2. $LPC_F + (\varphi \to \psi) + (\varphi) \vdash \varphi$
3. $LPC_F + (\varphi \to \psi) + (\varphi) \vdash \psi$ $MP\,1.\,2.$
4. $LPC_F + (\varphi \to \psi) + (\varphi) \vdash \psi \to \neg\neg\psi$ $(\varphi|\psi)\mathbf{AF}6$
5. $LPC_F + (\varphi \to \psi) + (\varphi) \vdash \neg\neg\psi$ $MP\,3.\,4.$

Les autres théorèmes sont obtenus de la même façon. □

Passons maintenant aux axiomes de Łukasiewicz.

Proposition 1.4.6. *L'axiome* $\mathbf{AŁ}1 \equiv (\varphi \to \chi) \to \Big((\chi \to \psi) \to (\varphi \to \psi)\Big)$ *est un théorème de* LPC_F.

Démonstration. Il suffit ici encore d'appliquer le méta-théorème de la déduction et de démontrer

$$LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \psi.$$

Il suffit d'appliquer deux fois le modus ponens. Écrivons la preuve formelle :

1. $LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \varphi$
2. $LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \varphi \to \chi$
3. $LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \chi$ $MP\,1.\,2.$
4. $LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \chi \to \psi$
5. $LPC_F + (\varphi \to \chi) + (\chi \to \psi) + (\varphi) \vdash \psi$ $MP\,3.\,4.$

On a donc fait la déduction attendue. □

Passons maintenant au deuxième axiome de Łukasiewicz.

Proposition 1.4.7. *L'axiome* **AŁ2** $\equiv \varphi \to (\neg\varphi \to \chi)$ *est un théorème de* LPC_F.

Démonstration. On procède encore de la même manière en obtenant

$$LPC_F + (\varphi) + (\neg\varphi) \vdash \chi.$$

On peut le prouver simplement. Voici les détails :

1. $LPC_F + (\varphi) + (\neg\varphi) \vdash \neg\varphi \to (\neg\chi \to \neg\varphi)$ $(\neg\varphi|\varphi)(\neg\chi|\psi)$**AF**1
2. $LPC_F + (\varphi) + (\neg\varphi) \vdash \neg\varphi$
3. $LPC_F + (\varphi) + (\neg\varphi) \vdash (\neg\chi \to \neg\varphi)$ $MP\,1.\,2.$
4. $LPC_F + (\varphi) + (\neg\varphi) \vdash (\neg\chi \to \neg\varphi) \to (\varphi \to \chi)$ *Prop.*1.4.4
5. $LPC_F + (\varphi) + (\neg\varphi) \vdash \varphi \to \chi$ $MP.\,3.\,4.$
6. $LPC_F + (\varphi) + (\neg\varphi) \vdash \varphi$
7. $LPC_F + (\varphi) + (\neg\varphi) \vdash \chi$ $MP\,5.\,6.$

On a donc bien la déduction nécessaire. □

Afin de prouver que le troisième axiome de Łukasiewicz est un théorème de LPC_F, il est nécessaire d'établir encore quelques théorèmes.

Proposition 1.4.8. *Les formules*
1) $(\neg\varphi \to \psi) \to (\neg\psi \to \varphi)$ *;*
2) $\neg\psi \to \Big((\neg\psi \to \neg\varphi) \to \neg\varphi\Big)$ *;*
3) $\neg\psi \to \Big(\varphi \to \neg(\neg\psi \to \neg\varphi)\Big)$ *;*
4) $(\neg\psi \to \varphi) \to \big(\neg\psi \to \neg(\neg\psi \to \neg\varphi)\big)$
sont des théorèmes de LPC_F.

Démonstration. Pour 1), on prouve

$$LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \varphi.$$

On a

1. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \neg\varphi \to \psi$
2. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash (\neg\varphi \to \psi) \to (\neg\psi \to \neg\neg\varphi)$ **AF**4
3. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \neg\psi \to \neg\neg\varphi$ $MP\,1.\,2.$
4. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \neg\psi$
5. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \neg\neg\varphi$ $MP\,3.\,4.$
6. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \neg\neg\varphi \to \varphi$ **AF**5
7. $LPC_F + (\neg\varphi \to \psi) + (\neg\psi) \vdash \varphi$ $MP\,5.\,6.$

Pour 2), on peut démontrer

$$LPC_F + (\neg\psi) + (\neg\psi \to \neg\varphi) \vdash \neg\varphi.$$

C'est une application directe du modus ponens.

Pour 3), on démontre

$$LPC_F + (\neg\psi) \vdash \Big(\varphi \to \neg(\neg\psi \to \neg\varphi)\Big).$$

On a (sans mentionner les substitutions évidentes dans les axiomes de LPC_F) :

1. $LPC_F + (\neg\psi) \vdash (\neg\psi)$
2. $LPC_F + (\neg\psi) \vdash \neg\psi \to \Big((\neg\psi \to \neg\varphi) \to \neg\varphi\Big)$ 2)
3. $LPC_F + (\neg\psi) \vdash (\neg\psi \to \neg\varphi) \to \neg\varphi$ MP 1. 2.
4. $LPC_F + (\neg\psi) \vdash \Big((\neg\psi \to \neg\varphi) \to \neg\varphi\Big) \to \Big(\neg\neg\varphi \to \neg(\neg\psi \to \neg\varphi)\Big)$ **AF**4
5. $LPC_F + (\neg\psi) \vdash \neg\neg\varphi \to \neg(\neg\psi \to \neg\varphi)$ MP 3. 4.
6. $LPC_F + (\neg\psi) \vdash \Big(\neg\neg\varphi \to \neg(\neg\psi \to \neg\varphi)\Big) \to \Big(\varphi \to \neg(\neg\psi \to \neg\varphi)\Big)$ *Prop* 1.4.5
7. $LPC_F + (\neg\psi) \vdash \varphi \to \neg(\neg\psi \to \neg\varphi)$ MP 5. 6.

Pour 4), on utilise un modus ponens direct entre 3) et l'axiome **AF**2. □

On arrive au résultat souhaité.

Proposition 1.4.9. *La formule*

$$(\varphi \to \psi) \to \Big((\neg\varphi \to \psi) \to \psi\Big).$$

est un théorème de LPC_F. En particulier, l'axiome **AŁ**3 $\equiv (\neg\varphi \to \varphi) \to \varphi$ *est un théorème de LPC_F.*

Démonstration. Encore une fois, par le théorème de la déduction, il suffit de prouver

$$LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \psi.$$

On a alors la preuve formelle suivante, où on n'écrit pas les substitutions évidentes faites

dans les théorèmes de LPC_F :

1. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \neg\varphi \to \psi$
2. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash (\neg\varphi \to \psi) \to (\neg\psi \to \varphi)$ *Prop.*1.4.8
3. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \neg\psi \to \varphi$ MP 1. 2.
4. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash (\neg\psi \to \varphi) \to \big(\neg\psi \to \neg(\neg\psi \to \neg\varphi)\big)$ *Prop.*1.4.8
5. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \neg\psi \to \neg(\neg\psi \to \neg\varphi)$ MP 3. 4.
6. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \big(\neg\psi \to \neg(\neg\psi \to \neg\varphi)\big) \to \big((\neg\psi \to \neg\varphi) \to \psi\big)$ *Prop*1.4.4
7. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash (\neg\psi \to \neg\varphi) \to \psi$ MP 5. 6.
8. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \varphi \to \psi$
9. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$ **AF**4
10. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \neg\psi \to \neg\varphi$ MP 8. 9.
11. $LPC_F + (\varphi \to \psi) + (\neg\varphi \to \psi) \vdash \psi$ MP 7. 10.

La première partie de la preuve ainsi complète, vu le (méta-)théorème de la déduction. Pour la deuxième partie, on note qu'en substituant ψ par φ dans le premier théorème, on obtient la prémisse $\varphi \to \varphi$ qui est un théorème de LPC_F. On obtient alors le résultat annoncé par modus ponens. □

À partir de maintenant, on ne fera plus la distinction entre $LPC_Ł$ et LPC_F, puisque les axiomes d'un système étant des théorèmes de l'autre, tous les théorèmes de l'un sont des théorèmes de l'autre. On notera donc simplement LPC, comme il est d'usage.

1.5 Le méta-théorème de la complétude.

Pour pouvoir établir que LPC est cohérent, on présente la notion de table de vérité. Cet outil a aussi la qualité d'être une aide efficace pour déterminer si une proposition est un théorème ou non. On note que le problème est équivalent à montrer qu'il n'existe pas de théorème $\mathfrak{A}$ qui soit tel que la proposition $\neg\mathfrak{A}$ soit aussi un théorème. On parle alors de non-contradiction.

Proposition 1.5.1. *Si il existe un théorème $\mathfrak{A}$ de LPC_F qui soit tel que la proposition $\neg\mathfrak{A}$ soit aussi un théorème, alors toute proposition $\mathfrak{B}$ est un théorème.*

Démonstration. La proposition $\varphi \to (\neg\varphi \to \chi)$ est l'axiome **AŁ**2, et c'est un théorème de LPC_F par la proposition 1.4.7. Si on y substitue φ par $\mathfrak{A}$ et ψ par $\mathfrak{B}$, comme $\mathfrak{A}$ et $\neg\mathfrak{A}$

sont des théorèmes, il suffit d'appliquer le modus ponens :

$$\begin{aligned} LPC &\vdash \mathfrak{A} \\ &\vdash \neg\mathfrak{A} \\ &\vdash \mathfrak{A} \to (\neg\mathfrak{A} \to \mathfrak{B}) \\ &\vdash \neg\mathfrak{A} \to \mathfrak{B} \\ &\vdash \mathfrak{B}. \end{aligned}$$

□

La réciproque de cette proposition est immédiate. Si LPC est inconsistant, cela signifie que tout énoncé bien formulé est un théorème, en particulier on a bien, pour toute proposition $\mathfrak{A}$, que $\mathfrak{A}$ et $\neg\mathfrak{A}$ sont des théorèmes.

Soit une formule $\mathfrak{A}$; pour chaque proposition atomique de $\mathfrak{A}$ on va substituer chacune de ses occurrences par les symboles "1" ou "0". On dit qu'on alloue une valeur de vérité aux propositions atomiques de $\mathfrak{A}$.

Définition 1.5.2. *Une valuation d'une formule $\mathfrak{A}$ est un énoncé obtenu après substitution de toute les variables atomiques par les caractères "0" ou "1". Pour signifier qu'on a substitué "φ" par "0" (resp "1") on notera "$\varphi = 0$" (resp. "$\varphi = 1$").*

Remarque 1.5.3. *Plusieurs valuations d'une formule sont possibles, mais quand le choix d'une valuation est faite, il faut s'y tenir pendant le processus de simplification qui va suivre. Autrement dit, dans une valuation on ne peut avoir simultanément $\varphi = 0$ et $\varphi = 1$.*

On va simplifier l'expression obtenue (la valuation donc) en substituant successivement, et en procédant de proche en proche, chaque occurrence du type "$\neg X$" et "$X \to Y$" par "1" ou "0". Ces substitutions se font en suivant les règles résumées dans les deux tableaux suivants :

X	$\neg X$
0	1
1	0

X	Y	$(X \to Y)$
0	0	1
0	1	1
1	0	0
1	1	1

C'est à dire : si par exemple "X" a la valeur de "0" alors "$\neg X$" sera remplacé par le caractère "1". Si "X" a la valeur de "1" et "Y" la valeur de "0", alors "$(X \to Y)$", c'est-à-dire l'occurrence "$(1 \to 0)$", sera remplacée par "0". Pour une proposition plus complexe comme $(\varphi \to \neg\chi) \to \Big((\neg\chi \to \psi) \to (\varphi \to \psi)\Big)$, si l'on décide d'abord, et de façon tout à fait arbitraire, de substituer respectivement les propositions atomiques φ, χ et ψ par "0", "0", et "1", on obtient alors l'expression

$$(0 \to \neg 0) \to \Big((\neg 0 \to 1) \to (0 \to 1)\Big)$$

La simplification se fait alors comme suit :

- $(0 \to \neg 0) \to \Big((\neg 0 \to 1) \to (0 \to 1)\Big)$

- $(0 \to 1) \to \Big((1 \to 1) \to (0 \to 1)\Big)$
- $1 \to (1 \to 1)$
- $1 \to 1$
- 1

On pourrait se demander quel résultat on aurait obtenu si l'on avait choisi d'autres substitutions. En fait, étant donnée une formule $\mathfrak{A}$ on va déterminer le résultat pour toutes les valuations possibles, ceux-ci sont repris dans un tableau : une *table de vérité*.

Définition 1.5.4. *Une table de vérité associée à une formule $\mathfrak{A}$ est un tableau représentant tous les valuations possibles de $\mathfrak{A}$ et leurs simplifications respectives.*

Exemple 1.5.1. *Pour rappel, après avoir introduit les symboles de LPC et les règles de formation, nous avions convenu de raccourcis d'écriture : $\varphi \wedge \psi$, $\varphi \vee \psi$ et $\varphi \leftrightarrow \psi$. Établissons les tables de vérité de ces formules.*

(i) $\varphi \vee \psi \equiv \neg\varphi \to \psi$ *:*

φ	ψ	$\neg\varphi \to \psi$
0	*0*	*0*
0	*1*	*1*
1	*0*	*1*
1	*1*	*1*

(ii) $\varphi \wedge \psi \equiv \neg(\varphi \to \neg\psi)$ *:*

φ	ψ	$\varphi \to \neg\psi$	$\neg(\varphi \to \neg\psi)$
0	*0*	*1*	*0*
0	*1*	*1*	*0*
1	*0*	*1*	*0*
1	*1*	*0*	*1*

(iii) $\varphi \leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$ *:*

φ	ψ	$\varphi \to \psi$	$\psi \to \varphi$	$(\varphi \to \psi) \wedge (\psi \to \varphi)$
0	*0*	*1*	*1*	*1*
0	*1*	*1*	*0*	*0*
1	*0*	*0*	*1*	*0*
1	*1*	*1*	*1*	*1*

Exemple 1.5.2. *On détermine maintenant les tables de vérité des axiomes de Łukasiewicz.*

(i) **AŁ***1*

φ	χ	ψ	$\varphi \to \chi$	$\chi \to \psi$	$\varphi \to \psi$	$(\varphi \to \chi) \to [(\chi \to \psi) \to (\varphi \to \psi)]$
0	*0*	*0*	*1*	*1*	*1*	*1*
0	*0*	*1*	*1*	*1*	*1*	*1*
0	*1*	*0*	*1*	*0*	*1*	*1*
0	*1*	*1*	*1*	*1*	*1*	*1*
1	*0*	*0*	*0*	*1*	*0*	*1*
1	*0*	*1*	*0*	*1*	*1*	*1*
1	*1*	*0*	*1*	*0*	*0*	*1*
1	*1*	*1*	*1*	*1*	*1*	*1*

(ii) **AŁ***2*

φ	χ	$\neg\varphi \to \chi$	$\varphi \to (\neg\varphi \to \chi)$
0	*0*	*0*	*1*
0	*1*	*1*	*1*
1	*0*	*1*	*1*
1	*1*	*1*	*1*

(iii) **AŁ***3*

φ	$\neg\varphi \to \varphi$	$(\neg\varphi \to \varphi) \to \varphi$
0	*0*	*1*
1	*1*	*1*

On s'aperçoit que dans ce dernier exemple, après simplification, chaque valuation vaut 1. Dans ce cas, les formules correspondantes sont appelées tautologies.

Définition 1.5.5. *Une tautologie est une formule dont toutes les valuations se simplifient en "1".*

À l'inverse, si toute valuation d'une formule admet comme simplification 0, alors on dit que cette formule est une absurdité.

Définition 1.5.6. *Une absurdité est une formule dont tous les valuations se simplifient en "0".*

Comme annoncé, l'utilité des tables de vérité est multiple. Pour commencer, il s'avère qu'elles fournissent une technique de (méta-)démonstration particulièrement efficace car systématique et à l'errabilité[7] plus faible. En effet, nous allons démontrer maintenant qu'une formule est un théorème si et seulement si elle est une tautologie. Ce résultat porte le nom de (méta-)théorème de complétude. En corollaire de ce résultat, on montre que la logique des propositions est cohérente. Avant d'établir le (méta-)théorème de complétude, on convient de quelques notations qui sont présentées dans le lemme qui suit.

7. Terme emprunté à Étienne Souriau dans son ouvrage "Les différents modes d'existence". L'errabilité ou du de la mathématicien.ne désigne la possibilité qu'iel a de commettre une erreur.

Lemme 1.5.7. *Soit une formule $\mathfrak{A}$ dont les propositions atomiques sont exactement φ_a, φ_b, ...φ_n. Ayant choisi une valuation de $\mathfrak{A}$, on convient des notations suivantes :*

$\xi_i \equiv \varphi_i$ *si, pour la valuation, on a substitué "φ_i" par "1" ;*

$\xi_i \equiv \neg\varphi_i$ *si, pour la valuation, on a substitué "φ_i" par "0" ;*

$\mathfrak{B}_{\mathfrak{A}} \equiv \mathfrak{A}$ [8] *si la simplification de la valuation de $\mathfrak{A}$ est "1" ;*

$\mathfrak{B}_{\mathfrak{A}} \equiv \neg\mathfrak{A}$ *si la simplification de la valuation de $\mathfrak{A}$ est "0".*

On a alors

$$LPC + \xi_a + ... + \xi_n \vdash \mathfrak{B}_{\mathfrak{A}}.$$

Avant de prouver le résultat, on illustre le lemme par un exemple.

Exemple 1.5.3. *Soit la formule $\mathfrak{A} \equiv \varphi \to \psi$, quatre valuations sont possibles. En suivant la table de vérité de "$\to$", on a*

(i) $LPC + \neg\varphi + \neg\psi \vdash \varphi \to \psi$;
(ii) $LPC + \neg\varphi + \psi \vdash \varphi \to \psi$;
(iii) $LPC + \varphi + \neg\psi \vdash \neg(\varphi \to \psi)$;
(iv) $LPC + \varphi + \psi \vdash \varphi \to \psi$.

Démonstration. D'abord, on montre que le résultat est vrai pour les propositions atomiques. On montre ensuite que si le résultat est vérifié pour les formules $\mathfrak{A}_a$ et $\mathfrak{A}_b$, alors il est également vérifié pour les propositions $\neg\mathfrak{A}_a$, $\mathfrak{A}_a \to \mathfrak{A}_b$ et également pour toute formule $\mathfrak{A}'$ obtenue après substitution dans $\mathfrak{A}_a$. Pour conclure, il suffit alors de procéder de proche en proche.

Les propositions atomiques ne contiennent pas de connecteur logique. La propriété se réduit donc à montrer que $\xi \vdash \xi$. Ce qui est évident.

On suppose que la propriété est vérifiée pour les formules $\mathfrak{A}_a$ et $\mathfrak{A}_b$.

- *Montrons que la propriété est vraie pour* $\neg\mathfrak{A}_a$. On note que toutes les propositions atomiques de la formule $\neg\mathfrak{A}_a$ sont exactement celles de la formule $\mathfrak{A}_a$. Aussi, toute valuation de l'une induit une valuation pour l'autre ; et celles-ci partagent les mêmes notations introduites dans l'énoncé. Soit donc une valuation de $\neg\mathfrak{A}_a$. Elle induit une définition de $\xi_1, \ldots, \xi_n$, et de $\mathfrak{B}_{\neg\mathfrak{A}_a}$. On souhaite démontrer

$$LPC + \xi_a + ... + \xi_n \vdash \mathfrak{B}_{\neg\mathfrak{A}_a},$$

et on a par hypothèse

$$LPC + \xi_a + ... + \xi_n \vdash \mathfrak{B}_{\mathfrak{A}_a}.$$

Deux cas peuvent se produire.

(*i*) Si la simplification de $\neg\mathfrak{A}_a$ mène à 1, alors on a par définition $\mathfrak{B}_{\neg\mathfrak{A}_a} \equiv \neg\mathfrak{A}_a$. Mais, vu la table de vérité de $\neg$ on a que cette valuation pour $\mathfrak{A}_a$ se simplifie en 0. Donc, par définition, $\mathfrak{B}_{\mathfrak{A}_a} \equiv \neg\mathfrak{A}_a$, et la propriété demandée est directement satisfaite.

8. On notera aussi simplement $\mathfrak{B}$ si aucune confusion n'est possible.

(*ii*) Si la valuation de $\neg\mathfrak{A}_a$ se simplifie en 0, alors cette valuation se simplifie en 1 pour $\mathfrak{A}_a$ et donc, par hypothèse, $\mathfrak{B}_{\mathfrak{A}_a} \equiv \mathfrak{A}_a$ est déduit de $\xi_a, \ldots, \xi_n$. On souhaite montrer qu'il en est de même pour $\mathfrak{B}_{\neg\mathfrak{A}_a} \equiv \neg\neg\mathfrak{A}_a$. Or, comme $\varphi \to \neg\neg\,\varphi$ est un théorème de *LPC* (axiome **AF**6), on a

$$\begin{aligned} LPC + \xi_a + ... + \xi_n &\vdash \mathfrak{A}_a \\ &\vdash \mathfrak{A}_a \to \neg\neg\mathfrak{A}_a \\ &\vdash \neg\neg\mathfrak{A}_a \\ &\vdash \mathfrak{B}_{\neg\mathfrak{A}_a}\,. \end{aligned}$$

La propriété est donc bien satisfaite pour $\neg\,\mathfrak{A}_a$ dans les deux cas possibles.

- Montrons que la propriété est vraie pour $\mathfrak{A}_a \to \mathfrak{A}_b$.
  Comme toute valuation de $\mathfrak{A}_a \to \mathfrak{A}_b$ induit une valuation pour $\mathfrak{A}_a$ et $\mathfrak{A}_b$ respectivement, on a, par hypothèse, avec des notations naturelles

$$\begin{aligned} LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} &\vdash \mathfrak{B}_{\mathfrak{A}_a} \\ &\vdash \mathfrak{B}_{\mathfrak{A}_b}. \end{aligned}$$

  Deux cas sont alors possibles, selon la simplification de la valuation de $\mathfrak{A}_a \to \mathfrak{A}_b$.

  (*i*) La valuation de $\mathfrak{A}_a \to \mathfrak{A}_b$ se simplifie en 1. Dans ce cas, on a pose $\mathfrak{B}_{\mathfrak{A}_a \to \mathfrak{A}_b} \equiv \mathfrak{A}_a \to \mathfrak{A}_b$, et on souhaite donc démontrer

$$LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} \vdash \mathfrak{A}_a \to \mathfrak{A}_b.$$

  En se référant à la table de vérité de $\to$ on constate qu'à nouveau on peut distinguer deux cas : soit la valuation induite sur $\mathfrak{A}_b$ se simplifie par 1, soit que les valuations induites sur $\mathfrak{A}_a$ et $\mathfrak{A}_b$ se simplifient par 0.

  (a) La valuation induite sur $\mathfrak{A}_b$ se simplifie par 1. Par hypothèse, on a que $\mathfrak{B}_{\mathfrak{A}_b} \equiv \mathfrak{A}_b$ est déduit de $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$. Mais alors, comme $\mathfrak{A}_b \to (\mathfrak{A}_a \to \mathfrak{A}_b)$ est un théorème de LPC (par substitution dans l'axiome **AF**1 ou le Fait1), on infère que $\mathfrak{A}_a \to \mathfrak{A}_b$ est aussi un théorème déduit $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$:

$$\begin{aligned} LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} &\vdash \mathfrak{A}_b \\ &\vdash \mathfrak{A}_b \to (\mathfrak{A}_a \to \mathfrak{A}_b) \\ &\vdash \mathfrak{A}_a \to \mathfrak{A}_b \end{aligned}$$

  (b) Les valuations induites sur $\mathfrak{A}_a$ et $\mathfrak{A}_b$ se simplifient par 0. On a donc par définition $\mathfrak{B}_{\mathfrak{A}_a} \equiv \neg\mathfrak{A}_a$ et $\mathfrak{B}_{\mathfrak{A}_b} \equiv \neg\mathfrak{A}_b$. D'abord, avec les mêmes arguments qu'au point précédent on a que la formule $\neg\mathfrak{A}_b \to \neg\mathfrak{A}_a$ est déduite de $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$. Ensuite, comme la formule $(\neg\mathfrak{A}_b \to \neg\mathfrak{A}_a) \to (\mathfrak{A}_a \to \mathfrak{A}_b)$ est un théorème de

LPC (voir le **Fait**7 ou la proposition 1.4.4), on a alors bien que $\mathfrak{B} \equiv \mathfrak{A}_a \to \mathfrak{A}_b$ est déduit de $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$. Formellement on écrit

$$\begin{aligned} LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} &\vdash \neg\mathfrak{A}_a \\ &\vdash \neg\mathfrak{A}_a \to (\neg\mathfrak{A}_b \to \neg\mathfrak{A}_a) \\ &\vdash \neg\mathfrak{A}_b \to \neg\mathfrak{A}_a \\ &\vdash (\neg\mathfrak{A}_b \to \neg\mathfrak{A}_a) \to (\mathfrak{A}_a \to \mathfrak{A}_b) \\ &\vdash \mathfrak{A}_a \to \mathfrak{A}_b \end{aligned}$$

On a donc bien la propriété demandée dans ce premier cas.

(*ii*) La valuation de $\mathfrak{A}_a \to \mathfrak{A}_b$ se simplifie en 0. Dans cette situation, on a par définition $\mathfrak{B}_{\mathfrak{A}_a \to \mathfrak{A}_b} \equiv \neg(\mathfrak{A}_a \to \mathfrak{A}_b)$, et on souhaite donc démonter

$$LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} \vdash \neg(\mathfrak{A}_a \to \mathfrak{A}_b).$$

Vu la définition des tables de vérité, la valuation induite pour $\mathfrak{A}_a$ se simplifie par 1 et celle de $\mathfrak{A}_b$ par 0 de sorte que $\mathfrak{B}_{\mathfrak{A}_a} \equiv \mathfrak{A}_a$ et $\mathfrak{B}_{\mathfrak{A}_a} \equiv \neg\,\mathfrak{A}_b$. Par hypothèse, on a donc que $\mathfrak{A}_a$ et $\neg\mathfrak{A}_b$ sont déduits de $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$. Il en est de même pour la formule $\neg\mathfrak{A}_b \to \mathfrak{A}_a$, puisque $\mathfrak{A}_a \to (\neg\mathfrak{A}_b \to \mathfrak{A}_a)$ est un théorème de LPC (voir encore **AF**1). Soit alors le théorème obtenu à partir de l'axiome **AŁ**1 après la substitution qui fait apparaître $\neg\mathfrak{A}_b \to \mathfrak{A}_a$ en prémisse :

$$LPC \vdash [\neg\mathfrak{A}_b \to \mathfrak{A}_a] \to [(\mathfrak{A}_a \to \mathfrak{A}_b) \to (\neg\mathfrak{A}_b \to \mathfrak{A}_b)].$$

Dès lors par modus ponens, on obtient que $(\mathfrak{A}_a \to \mathfrak{A}_b) \to (\neg\mathfrak{A}_b \to \mathfrak{A}_b)$ est déduit de $\xi_a^{(a)}, \ldots, \xi_m^{(a)}, \xi_a^{(b)}, \ldots, \xi_n^{(b)}$. On considère l'axiome **AF**4 ou le **Fait**7 et le modus ponens et on obtient que la contraposée de cette formule est déduite également :

$$LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} \vdash \neg(\neg\mathfrak{A}_b \to \mathfrak{A}_b) \to \neg(\mathfrak{A}_a \to \mathfrak{A}_b).$$

On montre enfin que la formule $\neg(\neg\mathfrak{A}_b \to \mathfrak{A}_b)$ est déduite de $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$ et la conclusion suit, évidemment par modus ponens. Pour ce faire, on établit d'abord que la proposition $\neg\,\varphi \to (\neg(\neg\,\varphi \to \varphi))$ est un théorème. C'est en effet la contraposée de l'axiome **AŁ**3 :

1. $LPC \vdash [(\neg\,\varphi \to \varphi) \to \varphi] \to [\neg\,\varphi \to \neg(\neg\,\varphi \to \varphi)]$ **AF**4
2. $LPC \vdash (\neg\,\varphi \to \varphi) \to \varphi$ **AŁ**3
3. $LPC \vdash \neg\,\varphi \to \neg(\neg\,\varphi \to \varphi)$ MP 1. 2.

Et comme, rappelons le, $\neg\mathfrak{A}_b$ est déduit dans $\xi_a^{(a)}, ..., \xi_m^{(a)}, \xi_a^{(b)}, ..., \xi_n^{(b)}$, on a alors

$$\begin{aligned} LPC + \xi_a^{(a)} + ... + \xi_m^{(a)} + \xi_a^{(b)} + ... + \xi_n^{(b)} &\vdash \neg\mathfrak{A}_b \\ &\vdash \neg\mathfrak{A}_b \to (\neg(\neg\mathfrak{A}_b \to \mathfrak{A}_b)) \\ &\vdash \neg(\neg\mathfrak{A}_b \to \mathfrak{A}_b) \end{aligned}$$

- Soit $\mathfrak{A}'$ une formule obtenue après substitution d'une proposition atomique de $\mathfrak{A}$ par une formule $\mathfrak{C}$. Toute valuation de $\mathfrak{A}'$ induit une valuation de $\mathfrak{C}$ qui, après simplification, aura soit la valeur de 0 soit la valeur de 1 (qu'on va représenter ici par la lettre a). Cela revient donc à procéder à une succession de substitutions à savoir $(a|\mathfrak{C})\Big((\mathfrak{C}|\varphi)\mathfrak{A}\Big)$. Autrement dit, on substitue dans $\mathfrak{A}$ la proposition atomique φ par a. Cela signifie que l'on se place dans une valuation où φ est substitué par a et, dans ce cas, on a $\mathfrak{B}_{\mathfrak{A}'} \equiv \mathfrak{B}_{\mathfrak{A}}$. □

Proposition 1.5.8 ((méta-)théorème de la complétude)**.** *Une formule est un théorème si et seulement si elle est une tautologie.*

Démonstration.

- Tout théorème est une tautologie : D'abord on vérifie que chaque axiome de LPC est une tautologie. Ensuite on montre que les règles d'inférence dans LPC, appliquées à des tautologies, fournissent des tautologies.
  - les axiomes sont des tautologies ;
  - Soit $\mathfrak{A}$ et $\mathfrak{A} \to \mathfrak{B}$ deux tautologies. Lors de la simplification d'une valuation de $\mathfrak{A} \to \mathfrak{B}$ on arrivera à la configuration $1 \to 0$ ou $1 \to 1$, en effet, $\mathfrak{A}$ est une tautologie et donc mènera toujours à la simplification 1 quelle que soit la valuation. Or, vu la table de vérité de $\to$, pour que $\mathfrak{A} \to \mathfrak{B}$ puisse être simplifié par 1, ce qui est le cas car il s'agit d'une tautologie, il faut que $\mathfrak{B}$ vaille 1 après simplification ; et ce quel que soit la valuation. Ainsi, $\mathfrak{B}$ est une tautologie.
  - Soit $\mathfrak{A}$ une tautologie et soit $\mathfrak{A}'$ une formule obtenue après substitution dans $\mathfrak{A}$ d'une proposition atomique φ par une formule $\mathfrak{B}$. On simplifie la valuation de $\mathfrak{A}'$ en commençant par toutes les occurrences de $\mathfrak{B}$; celles-ci sont alors remplacées soit par 0 soit par 1. Mais alors, on a dans $\mathfrak{A}$ effectué deux substitutions consécutives : $(1|\mathfrak{B})\Big((\mathfrak{B}|\varphi)\mathfrak{A}\Big)$ ou $(0|\mathfrak{B})\Big((\mathfrak{B}|\varphi)\mathfrak{A}\Big)$. La suite de la simplification se fait donc comme pour $\mathfrak{A}$. Comme $\mathfrak{A}$ est une tautologie, on en déduit donc que le résultat de la simplification est 1, et ce quelle que soit la valuation de $\mathfrak{A}'$.
- Toute tautologie est un théorème : Soit donc une tautologie $\mathfrak{A}$ dont les propositions atomiques sont $\varphi_a, ..., \varphi_n$. Par définition, quelle que soit la valuation considérée, $\mathfrak{A}$ sera toujours réduit à 1. Dès lors, par le lemme 1.5.7 on a

$$LPC + \varphi_a + ... + \varphi_{n-1} + \varphi_n \vdash \mathfrak{A}$$

et

$$LPC + \varphi_a + ... + \varphi_{n-1} + \neg\varphi_n \vdash \mathfrak{A}.$$

C'est à dire, vu le théorème de la déduction,

$$\begin{aligned} LPC + \varphi_a + ... + \varphi_{n-1} &\vdash \varphi_n \to \mathfrak{A} \\ &\vdash \neg\varphi_n \to \mathfrak{A} \end{aligned}$$

Et donc, comme on a établi à la proposition 1.4.9 que $(\varphi \to \psi) \to \Big((\neg\varphi \to \psi) \to \psi\Big)$ est un théorème de LPC, il s'ensuit que

$$LPC + \varphi_a + ... + \varphi_{n-1} \vdash \mathfrak{A}.$$

En procédant successivement pour chacune des propositions atomiques de $\mathfrak{A}$, on en conclut qu'il s'agit bien d'un théorème :

$$LPC \vdash \mathfrak{A}. \qquad \square$$

Proposition 1.5.9. *Si la formule $\mathfrak{A}$ est un théorème, alors $\neg\mathfrak{A}$ est une absurdité. En particulier LPC est non-contradictoire.*

Démonstration. Cela découle directement de la table de vérité de "$\neg$". En effet, soit $\mathfrak{A}$ un théorème, on vient de voir qu'alors $\mathfrak{A}$ est une tautologie. Aussi, toute valuation de $\mathfrak{A}$ se simplifie en 1 de sorte que, dans toute valuation de $\neg\mathfrak{A}$, l'occurrence de $\mathfrak{A}$ est simplifiée par 1. Dès lors, quelle que soit la valuation de $\neg\mathfrak{A}$, on obtient la simplification $\neg 1$, c'est à dire 0. De ce résultat, on conclut qu'il n'existe pas de théorème $\mathfrak{A}$ tel que $\neg\mathfrak{A}$ soit aussi un théorème. $\square$

Voici quelques exemples de théorèmes établis grâce aux tables de vérité, et qui nous seront utiles dans les chapitres suivants.

Proposition 1.5.10. *La proposition $(\varphi \wedge \psi) \to \varphi$ est un théorème.*

Démonstration. Vu la proposition 1.5.8, il suffit d'établir que la formule en question est une tautologie. On calcule donc la table :

φ	ψ	$\varphi \wedge \psi$	$(\varphi \wedge \psi) \to \varphi$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

La formule de l'énoncé est donc bien un théorème. $\square$

Proposition 1.5.11. *La proposition $\varphi \to (\psi \to (\varphi \wedge \psi))$ est un théorème.*

Démonstration. On procède comme plus haut en calculant la table de vérité :

φ	ψ	$\varphi \wedge \psi$	$\psi \to (\varphi \wedge \psi)$	$\varphi \to (\psi \to (\varphi \wedge \psi))$
0	0	0	1	1
0	1	0	0	1
1	0	0	1	1
1	1	1	1	1

On constate que la proposition de l'énoncé est bien une tautologie. $\square$

Proposition 1.5.12. *La formule $(\varphi \wedge \psi) \to (\varphi \leftrightarrow \psi)$ est un théorème.*

Démonstration. On calcule la table de vérité :

φ	ψ	$\varphi \wedge \psi$	$\varphi \leftrightarrow \psi$	$(\varphi \wedge \psi) \rightarrow (\varphi \leftrightarrow \psi)$
0	0	0	1	1
0	1	0	0	1
1	0	0	0	1
1	1	1	1	1

et on conclut encore par le théorème de complétude. □

Proposition 1.5.13. *La formule qui suit est un théorème*

$$\Big((\varphi \rightarrow \psi) \wedge (\varphi \rightarrow \chi)\Big) \rightarrow \Big(\varphi \rightarrow (\psi \wedge \chi)\Big)$$

Démonstration. La preuve se réduit à écrire la table de vérité correspondante. □

Proposition 1.5.14. *La proposition*

$$\mathfrak{A} \equiv \Big[(\varphi \rightarrow \psi) \ \wedge (\rho \rightarrow \chi)\Big] \rightarrow \Big[(\varphi \vee \rho) \ \rightarrow \ (\psi \vee \chi)\Big].$$

est un théorème.

Démonstration. On pourrait encore calculer la table de vérité de $\mathfrak{A}$. Mais pour donner une autre démonstration, on montre qu'il est impossible que la proposition $\mathfrak{A}$ soit fausse (i.e. se simplifie en 0 pour une certaine valuation) en jouant sur les valeurs de vérité possibles des propositions atomiques qui la composent. Pour cela, on va réexprimer $\mathfrak{A}$ en une *forme normale disjonctive*, c'est-à-dire une proposition exprimée adéquatement à l'aide du connecteur $\vee$. On a successivement

$$\begin{aligned}
\mathfrak{A} &\leftrightarrow \neg\Big[(\varphi \rightarrow \psi) \ \wedge (\rho \rightarrow \chi)\Big] \vee \Big[(\varphi \vee \rho) \ \rightarrow \ (\psi \vee \chi)\Big] \\
&\leftrightarrow \neg\Big[(\neg\varphi \vee \psi) \ \wedge (\neg\rho \vee \chi)\Big] \vee \Big[\neg(\varphi \vee \rho) \ \vee \ (\psi \vee \chi)\Big] \\
&\leftrightarrow \Big[(\varphi \wedge \neg\psi) \ \vee (\rho \wedge \neg\chi)\Big] \vee \Big[(\neg\varphi \wedge \neg\rho) \ \vee \ (\psi \vee \chi)\Big] \\
&\leftrightarrow (\varphi \wedge \neg\psi) \ \vee \ (\rho \wedge \neg\chi) \ \vee \ (\neg\varphi \wedge \neg\rho) \ \vee \ \psi \ \vee \ \chi.
\end{aligned}$$

Pour qu'une valuation de $\mathfrak{A}$ se simplifie en 0, il faut que chaque conjonction vaille 0. Dès lors on a comme première contrainte que $\psi = 0$ et $\chi = 0$. De plus, $\neg\varphi \wedge \neg\rho$ est faux si $\varphi = 1$ ou $\rho = 1$. Si l'on suppose que $\varphi = 1$ alors $(\varphi \wedge \neg\psi) = 1$ ce qui n'est pas souhaité. Donc $\varphi = 0$ et $\rho = 1$. Mais alors $(\rho \wedge \neg\chi) = 1$ ce qui est contraire à ce qui est demandé. On en conclut qu'il n'existe pas de valuation pour laquelle $\mathfrak{A}$ n'est pas vérifié. Autrement dit, $\mathfrak{A}$ est une tautologie. □

Enfin, pour simplifier le discours, on peut aussi définir comme règles d'inférence des schémas de démonstration qui sont régulièrement utilisés.

Par exemple, si dans une démonstration on a un théorème de la forme $\mathfrak{A} \wedge \mathfrak{B}$ on peut en déduire que les formules $\mathfrak{A}$ et $\mathfrak{B}$ sont des théorèmes. En effet, on a établi à la proposition 1.5.10 que la proposition $(\varphi \wedge \psi) \rightarrow \varphi$ est un théorème. Dès lors il suffit d'appliquer le modus ponens après avoir fait les substitutions ad hoc. On convient alors des notations suivantes.

RI 3. *Si* $\mathfrak{A} \wedge \mathfrak{B}$ *est un théorème, alors on a* $\vdash \mathfrak{A}$ *et* $\vdash \mathfrak{B}$ *:*

$$\frac{\mathfrak{A} \wedge \mathfrak{B}}{\mathfrak{A}} \text{ et } \frac{\mathfrak{A} \wedge \mathfrak{B}}{\mathfrak{B}}$$

Réciproquement, si dans une démonstration on obtient le théorème $\mathfrak{A}$ et le théorème $\mathfrak{B}$, alors on peut démontrer qu'on a $\mathfrak{A} \wedge \mathfrak{B}$. Il suffit d'appliquer le modus ponens au théorème obtenu après substitution dans la formule $\varphi \to (\psi \to (\varphi \wedge \psi))$ qui a été établie à la proposition 1.5.11. À nouveau, on s'accorde sur les notations.

RI 4. *Si on a* $\vdash \mathfrak{A}$ *et* $\vdash \mathfrak{B}$ *alors on a* $\vdash \mathfrak{A} \wedge \mathfrak{B}$*. On résume ce résultat par la notation suivante :*

$$\frac{\mathfrak{A}, \mathfrak{B}}{\mathfrak{A} \wedge \mathfrak{B}}$$

Semblablement, comme la proposition $\varphi \to (\varphi \vee \psi)$ est une tautologie, donc un théorème, on a la règle d'introduction de $\vee$.

RI 5. *Si* $\vdash \mathfrak{A}$ *alors,* $\vdash \mathfrak{A} \vee \mathfrak{B}$*. On résume ce résultat par la notation suivante :*

$$\frac{\mathfrak{A}}{\mathfrak{A} \vee \mathfrak{B}}$$

Enfin, vu l'axiome **AŁ**1, on définit la règle du syllogisme.

RI 6. *Si les formules* $\mathfrak{A} \to \mathfrak{B}$ *et* $\mathfrak{B} \to \mathfrak{C}$ *sont des théorèmes alors* $\mathfrak{A} \to \mathfrak{C}$ *est un théorème.*

Pour terminer ce chapitre, nous mentionnons qu'il est possible de formaliser la logique propositionnelle classique à l'aide d'un seul connecteur, le symbole de Sheffer "|" (voir [32, Introduction to the second édition, §1]). Les connecteurs usuels sont définis comme étant des abréviations :

1. $\neg\mathfrak{A} \equiv \mathfrak{A}|\mathfrak{A}$;
2. $\mathfrak{A} \to \mathfrak{B} \equiv \mathfrak{A}|(\mathfrak{B}|\mathfrak{B})$.

Avec le symbole de Sheffer, le modus ponens prend alors la forme suivante :

$$\frac{\mathfrak{A}, \mathfrak{A}|(\mathfrak{B}|\mathfrak{C})}{\mathfrak{C}}$$

Le connecteur $\vee$ étant lui-même une abréviation, on a successivement

$$\begin{aligned} \mathfrak{A} \vee \mathfrak{B} &\equiv \neg\mathfrak{A} \to \mathfrak{B} \\ &\equiv (\neg\mathfrak{A})|(\mathfrak{B}|\mathfrak{B}) \\ &\equiv (\mathfrak{A}|\mathfrak{A})|(\mathfrak{B}|\mathfrak{B}) \end{aligned}$$

J. Nicod montre que l'on peut décrire LPC avec un unique axiome[9] :

$$\Big[\varphi\,|(\chi\,|\,\psi)\Big]\;\Big|\;\Big[\{\sigma|(\sigma|\sigma)\}\;|\;\{(\tau|\,\chi)|((\varphi\,|\tau)|(\varphi\,|\tau))\}\Big].$$

D'autre part, tout en maintenant le même langage, les mêmes règles de formation et d'inférence que pour $LPC_Ł$ ou LPC_F, Łukasiewicz montre dans l'article [24] qu'il est possible de déduire $LPC_Ł$ et donc aussi LPC_F du seul axiome

$$((\varphi \to \chi) \to \psi) \to ((\psi \to \varphi) \to (o \to \varphi)).$$

Dans la présentation de ce chapitre, nous avons choisi deux systèmes d'axiomes pour présenter LPC (sans indice, puisque les deux formulations sont équivalentes). Nous aurions pu nous limiter à un seul système, mais le travail consistant à montrer qu'ils sont équivalents nous a permis de mettre en œuvre les substitutions et le modus ponens d'une part, et le méta-théorème de la déduction d'autre part.

9. [32]

Chapitre 2

Théorie du premier ordre

En logique propositionnelle classique, on établit quel schéma de raisonnement est valide et quel schéma ne l'est pas et on se borne à discourir sur des propositions logiques sans jamais s'intéresser à leur structure interne. Cependant, on se rend rapidement compte des limites de cette théorie. En effet, le raisonnement très connu suivant

1. Tous les être humains sont mortels ;
2. Sappho est un être humain ;
3. Donc Sappho est mortelle ;

n'est pas formulable dans le contexte de la logique propositionnelle. En effet, dans LPC, on doit considérer les trois propositions distinctes

$$\varphi = \text{"Tous les être humains sont mortels"},$$

$$\chi = \text{"Sappho est un être humain"},$$

et

$$\psi = \text{"Sappho est mortelle"}$$

sans pouvoir formuler explicitement les liens entre ces trois propositions comme le fait que Sappho est à la fois un être humain et mortelle. Pour y parvenir, on sera amené d'une part à introduire des **individus** ou **objets individuels** [1], comme Sappho, et plus généralement des **variables**, et d'autre part, à considérer les symboles $\forall$ et $\exists$ permettant de construire un discours sur les individus et les variables. Évidemment, le sens et l'usage des symboles $\forall$ et $\exists$ doivent être régis par des axiomes et de nouvelles règles d'inférence.

L'ambition de ce chapitre est de proposer un cadre étendant celui de LPC dans lequel on pourra formuler une partie substantielle des mathématiques. Plusieurs propositions pour étendre la logique des prédicats ont été faites au cours de l'histoire, depuis l'Antiquité grecque avec Aristote, bien après avec Venn et ses diagrammes, ou encore Boole et son algèbre... Mais c'est finalement le formalisme de G. Frege qui l'emporte. On parle aujourd'hui de logique des prédicats ou logique du premier ordre.

1. Termes consacrés par [30] et [28].

2.1 Alphabet, Règles de formation et Axiomes

La logique du premier ordre peut donc être présentée comme un système formel. L'alphabet est composé de cinq types de signes différents :

1. les lettres minuscules latines pour les variables : $x, y, z, a, b, c \ldots$;
2. les lettres minuscules grecques pour les propositions : φ, χ, ψ,... ;
3. les connecteurs logiques : $\rightarrow$ et $\neg$, $\wedge$, $\vee$, $\leftrightarrow$,... ;
4. les symboles relationnels ou prédicats, aussi notés par des majuscules latines F, G, H... ;
5. les quantificateurs : $\forall$, $\exists$, ...

Comme pour LPC, les règles syntaxiques sont définies par induction. La présentation des règles de formation nécessite de distinguer variable libre et variable liée.

RF 3. *Toute proposition est une formule. Ces formules sont dites élémentaires ou atomiques.*

RF 4. *Si F est un prédicat d'arité n et si a, b, ..., n sont des variables alors*

$$F(a, b, ..., n)$$

est une formule (dites élémentaires ou atomiques).

Définition 2.1.1. *Comme dans les formules atomiques il n'est pas fait usage de quantificateur, on dit que les variables a, b, ..., n qui la composent sont libres.*

RF 5. *Si dans l'énoncé bien formulé $\mathfrak{A}$, la variable x est libre, alors $\forall x[\mathfrak{A}]$ est une proposition bien formulée.*

Définition 2.1.2. *Lorsque dans une formule, on trouve une occurrence de $\forall x$, on dit que la variable x est liée et que $\mathfrak{A}$ est le domaine d'action du quantificateur.*

Exemple 2.1.1. *Dans la formule $\forall y[x \in y]$, la variable désignée par y est liée et la variable désignée par x est libre alors que dans la formule $\forall x[\forall y[x \in y]]$ les deux variables sont liées. En effet, comme $x \in y$ est un énoncé bien formulé où y est libre, l'énoncé $\forall y[x \in y]$ est aussi bien formulé. Ainsi, comme $\forall y[x \in y]$ est bien formulé et comme x est libre dans cet énoncé, $\forall x[\forall y[x \in y]]$ est un énoncé bien formulé où toutes les variables sont liées. De plus, le champ d'action de $\exists x$ est $[\forall y[x \in y]]$ et le champ d'action de $\forall y$ est $[x \in y]$.*

RF 6. *Si $\mathfrak{A}$ et $\mathfrak{B}$ sont deux formules telles que toute variable liée (resp. libre) dans l'une ne soit pas libre (resp. liée) dans l'autre, alors*

$$\neg\mathfrak{A} \text{ et } \mathfrak{A} \rightarrow \mathfrak{B},$$

sont des propositions bien formulées.

Comme toute proposition est une formule, on retrouve en particulier la règle de formation **RF**2 de LPC :

$$\neg\varphi \text{ et } \varphi \rightarrow \psi.$$

Remarque 2.1.3. *Comme dans LPC, les connecteurs $\vee$ et $\wedge$ sont exprimés avec $\neg$ et $\rightarrow$. On notera aussi que $\exists x[F(x)]$ est une abréviation de $\neg(\forall x[\neg F(x)])$.*

Définition 2.1.4. *Une partie d'une formule est une partie de la formule qui est elle-même un énoncé bien formulé.*

Exemple 2.1.2. *Dans la formule* $\forall x \forall y \Big[\exists z[z \in x \leftrightarrow z \in y] \rightarrow (x = y)\Big]$ *les différentes parties sont*

1. $z \in x$;
2. $z \in y$;
3. $x = y$;
4. $z \in x \leftrightarrow z \in y$;
5. $\exists z[z \in x \leftrightarrow z \in y]$;
6. $\exists z[z \in x \leftrightarrow z \in y] \rightarrow (x = y)$;
7. $\forall y \Big[\exists z[z \in x \leftrightarrow z \in y] \rightarrow (x = y)\Big]$;
8. $\forall x \forall y \Big[\exists z[z \in x \leftrightarrow z \in y] \rightarrow (x = y)\Big]$.

Viennent ensuite les axiomes. Comme expliqué au début du chapitre, le souhait est de prolonger la logique propositionnelle classique. Aussi, comme on a à disposition les propositions, on peut reformuler pour la logique du premier ordre les axiomes de LPC (selon Łukasiewicz) qui sont rappelés ci-dessous [2]. Si φ, χ et ψ sont des propositions, alors

A 1. $(\varphi \rightarrow \chi) \rightarrow [(\chi \rightarrow \psi) \rightarrow (\varphi \rightarrow \psi)]$

A 2. $\varphi \rightarrow (\neg\varphi \rightarrow \chi)$

A 3. $(\neg\varphi \rightarrow \varphi) \rightarrow \varphi$

À ces axiomes s'ajoute un nouveau, relatif à l'emploi du quantificateur $\forall$:

A 4. $\forall x[F(x)] \rightarrow F(y)$

2.2 Règles de Substitution

Avant de donner les règles permettant de déduire de nouveaux théorèmes à partir de théorèmes déjà établis, il faut présenter comment effectuer des substitutions dans les formules. Trois opérations de substitution sont possibles. On peut substituer des variables, des propositions ou des prédicats. La présence de variables et leur caractère libre ou lié

2. On note que ceux-ci et ceux-là ont exactement la même forme. Cependant, on pendra garde de ne pas confondre les signifiés à cause de la similarité des signifiants.

rendent l'opération de substitution plus subtile que dans LPC. Par exemple si l'on considère l'axiome **A**4 :

$$\forall x[F(x)] \to F(y).$$

En substituant y par x, l'énoncé obtenu n'est pas bien formulé car alors x est lié d'un coté mais pas de l'autre. On commence donc par établir les règles de substitution pour les variables. Pour ce faire, on procède en trois temps. D'abord on établit, grâce aux règles syntaxiques, deux conditions nécessaires pour qu'une proposition soit bien formulée. Ensuite, en se basant sur ces règles, on définit l'opération de substitution. On montre alors que l'opération de substitution définie préserve le caractère orthosyntaxique de la formule. Enfin, on peut définir la règle d'inférence liée à la substitution d'une variable.

Proposition 2.2.1. *Dans une formule, une même lettre ne peut représenter une variable libre et une variable liée.*

Démonstration. Comme pour la définition de formule, on établira la propriété pour les cas fondamentaux puis on établira que, vu les règles de syntaxe, la propriété est conservée de proche en proche.

Vu la définition d'une formule élémentaire, on est assuré que toutes les variables y figurant sont libres et donc que la propriété est vérifiée.

Soit $\mathfrak{A}(x)$ une proposition bien formulée vérifiant la propriété, où x est une variable libre. En particulier, la variable x est distincte de toutes les autres variables libres de $\mathfrak{A}$. Ainsi, en passant à la formule $\forall x\mathfrak{A}$, la variable x reste bien distincte des autres variables libres et, par hypothèse, les lettres représentant les autres variables liées sont bien distinctes des lettres représentant les variables libres.

Soit $\mathfrak{A}$ et $\mathfrak{B}$ des formules vérifiant la propriété. Par définition, pour que $\mathfrak{A} \to \mathfrak{B}$ soit une formule, il faut qu'aucune variable liée dans une des parties de $\mathfrak{A} \to \mathfrak{B}$ ne soit liée dans l'autre partie (et réciproquement). Dès lors, toute lettre représentant une variable libre (resp. liée) dans $\mathfrak{A}$ ne peut représenter une variable liée (resp. libre) dans $\mathfrak{B}$ et, par hypothèse, ne peut représenter une variable liée (resp libre) dans $\mathfrak{A}$. Il en est de même avec toute lettre représentant une variable libre (resp. liée) dans $\mathfrak{B}$.

Enfin, si $\mathfrak{A}$ vérifie la propriété alors $\neg\mathfrak{A}$ la vérifie aussi. En effet, il n'y a aucun changement sur le caractère libre ou lié des variables lors du passage de $\mathfrak{A}$ à $\neg\mathfrak{A}$. □

Proposition 2.2.2. *Dans une formule, une variable ne peut être liée que par un quantificateur à la fois.*

Démonstration. À nouveau, on procède de proche en proche. D'abord, on note que la propriété est vraie pour les formules fondamentales car celles-ci ne possèdent pas de quantificateurs.

Soit $\mathfrak{A}$ une formule vérifiant la propriété. Par définition, la proposition $\forall x\mathfrak{A}$ n'est une formule que si x n'est pas lié dans $\mathfrak{A}$. Dès lors, la variable x n'est pas liée par plus d'un quantificateur et, par hypothèse, toute autre variable liée de $\mathfrak{A}(x)$ non plus.

Enfin, si les formules $\mathfrak{A}$ et $\mathfrak{B}$ vérifient la propriété, alors les nouvelles formules $\mathfrak{A} \to \mathfrak{B}$ et $\neg\mathfrak{A}$ aussi car il n'y a pas de nouvelles quantifications. □

Exemple 2.2.1. *Par exemple*

$$\forall x[\varphi(x)] \to \exists x[\psi(x)]$$

est une formule alors que

$$\forall x[\varphi(x)] \to \psi(x)$$

ne l'est pas car la propriété 2.2.1 n'est pas respectée, et la proposition

$$\forall x \exists x[\varphi(x) \to \psi(x)]$$

ne l'est pas car la propriété 2.2.2 n'est pas respectée.

Ces deux propriétés conditionneront aussi la substitution de propositions et de prédicats. On définit maintenant l'opération de substitution de variable.

Définition 2.2.3.

(i) *Substitution d'une variable libre :*
Soit $\mathfrak{A}$ une formule, on dit qu'on substitue une variable libre x en y si, dans $\mathfrak{A}$ on remplace toutes les occurrences de x par y de sorte que la nouvelle expression ainsi obtenue vérifie les propriétés 2.2.1 et 2.2.2.

(ii) *Substitution d'une variable liée :*
Soit $\mathfrak{A}$ une formule, on dit qu'on substitue une variable liée x en y si, dans $\mathfrak{A}$ on remplace toutes les occurrences de x appartenant au domaine d'application du quantificateur par y de sorte que la nouvelle expression ainsi obtenue vérifie les propriétés 2.2.1 et 2.2.2.

Proposition 2.2.4. *Si dans une formule $\mathfrak{A}$ on procède à une substitution d'une variable, alors l'énoncé $\mathfrak{A}'$ obtenu est encore une formule.*

Démonstration. D'abord, on montre que la propriété est vérifiée pour les formules fondamentales. On montre ensuite que la propriété est préservée par les autres règles syntaxiques. Ainsi, en procédant de proche en proche, on en déduit que la propriété est vérifiée pour une formule quelconque.

Comme dans les formules fondamentales toutes les variables sont libres, il n'y a que la règle 2.2.1 à observer. Or, par définition, quel que soit le choix d'identification des variables, ces propositions sont des formules.

On suppose que la propriété est vérifiée pour la formule $\mathfrak{A}$ et que x n'est pas lié dans $\mathfrak{A}$ de sorte que $\forall x\mathfrak{A}$ est une formule. On procède alors à une substitution conformément aux règles établies en 2.2.3. Si x est substitué, mettons par y, alors y ne peut être utilisé pour substituer les variables restantes dans $\mathfrak{B} \equiv (y|x)\forall x[\mathfrak{A}]$. En effet, y étant une variable liée dans $\mathfrak{B}$, toute variable distincte de y dans $\mathfrak{B}$ est soit libre, soit liée et donc distincte de y, conformément aux règles de substitution d'une variable. Toute substitution de variable dans $\forall x[\mathfrak{A}]$ distincte de x est donc une substitution dans $\mathfrak{A}$. Or, par hypothèse, toute

proposition $\mathfrak{A}'$ obtenue après substitution dans $\mathfrak{A}$ est une formule. Dès lors, toute variable liée dans $\mathfrak{A}'$ est désignée par une lettre distincte de x de sorte que $\forall x[\mathfrak{A}']$ est bien une formule.

On suppose maintenant que la propriété est vérifiée pour les formules $\mathfrak{A}$ et $\mathfrak{B}$ et on vérifie que toute substitution dans $(\neg\mathfrak{A})$ et dans $(\mathfrak{A} \to \mathfrak{B})$ produit des formules. Pour $\neg\mathfrak{A}$, tout changement de variable se résume à un changement de variable dans $\mathfrak{A}$; la propriété est donc vérifiée. Pour $\mathfrak{A} \to \mathfrak{B}$, le changement de désinence d'une variable liée, mettons x, se fait dans le domaine d'action du quantificateur et, conformément à la définition 2.2.3 d'une substitution, de telle sorte que la nouvelle désignation, disons y n'apparaisse pas libre dans une autre partie de la formule ni ne désigne déjà une variable liée. Dès lors, la condition 6 est respectée. Si maintenant, on procède à une substitution d'une variable libre, disons z, alors toute les occurrences de z doivent être remplacées par des occurrences d'une nouvelle désignation, t, qui ne désigne pas une variable liée. À nouveau, cela assure le caractère orthosyntaxique de $(t|z)\mathfrak{A} \to \mathfrak{B}$.

□

On notera que les restrictions sur l'opération de substitution sont suffisantes pour déterminer si une proposition obtenue après de telles substitutions est une formule, mais elles ne sont pas nécessaires. Par exemple, de la formule

$$\forall x[F(x) \to G(y)],$$

la substitution de y par la lettre x ne vérifie pas la condition 2.2.1 mais l'énoncé obtenu est bien une formule :

$$\forall x[F(x) \to G(x)].$$

2.3 Règles d'inférence

On peut à présent formuler les règles d'inférence. La première concerne la substitution d'une variable.

RI 7. *Si $\mathfrak{A}$ est un théorème, alors toute formule $\mathfrak{A}'$ obtenue par substitution d'une variable par une autre est un théorème.*

Exemple 2.3.1. *Soit l'axiome A4 $\forall x[F(x)] \to F(y)$, on peut effectuer les substitutions suivantes afin d'obtenir de nouveaux théorèmes :*

1. $\forall z[F(z)] \to F(y)$;
2. $\forall x[F(x)] \to F(t)$.

Par contre, la proposition suivante n'est pas un théorème car la condition 2.2.1 n'est pas respectée :

1. $\forall x[F(x)] \to F(x)$

En fait, il ne s'agit même pas d'une proposition bien formulée.

On peut à présent formuler les règles de substitution de proposition et de prédicat.

RI 8. *Soit $\mathfrak{A}$ un théorème. Si φ est une proposition contenue dans $\mathfrak{A}$, alors la substitution de toutes les occurrences de φ par une formule $\mathfrak{B}$ conduit à un nouveau théorème pour autant que les conditions suivantes soient respectées :*

RI8(i) les variables libres (resp. liées) de $\mathfrak{B}$ et les variables liées (resp. libre) de $\mathfrak{A}$ ont des désinences distinctes ;

RI8(ii) si dans $\mathfrak{A}$ la proposition φ entre dans le domaine d'action d'un quantificateur désignant une lettre, alors celle-ci ne rentre pas dans $\mathfrak{B}$.

RI 9. *Soit $\mathfrak{A}$ un théorème. Toutes les occurrences d'un prédicat $F(x_a, x_b, ...x_n)$ peuvent être substituées par une formule $\mathfrak{B}$ contenant les variables libres $y_a, x_b, ..., y_n$ désignées par des lettres distinctes de toute désignation de variables dans $\mathfrak{A}$ si la règle (RI8(i)) est respectée et si*

RI9(i) le prédicat que l'on substitue rentre dans le domaine d'action d'un quantificateur liant une lettre, alors cette lettre ne désigne aucune variable de $\mathfrak{B}$.

De plus, la substitution du prédicat $F(x_a, x_b, ..., x_n)$ par la formule $\mathfrak{B}$ induit la substitution des désinences des variables libres $y_a, y_b, ...y_n$ de $\mathfrak{B}$ par $x_a,\ x_b, ...,\ x_n$

Remarque 2.3.1. *Si l'on note par $\mathscr{S}$ l'opération substitution d'une proposition ou d'un prédicat, alors il apparaît que $\mathscr{S}(\mathfrak{A} \to \mathfrak{B}) \equiv \mathscr{S}\mathfrak{A} \to \mathscr{S}\mathfrak{B}$, et $\mathscr{S}(\neg\mathfrak{A}) \equiv \neg\mathscr{S}\mathfrak{A}$.*

Exemple 2.3.2. *Si l'on considère la formule suivante comme étant un théorème*

$$\exists x \forall y[F(x, y)],$$

on peut alors inférer un nouveau théorème comme suit. Comme il s'agit d'une formule contenant le prédicat $F(x, y)$, on peut substituer celui-ci par la formule $\mathfrak{B} \equiv G(a, b)$. En effet $\mathfrak{B}$ vérifie les conditions (RI8(i)) et (RI9(i)) :

- *$\mathfrak{A}$ ne contient que des variables liées, à savoir x et y, et celles-ci sont désignées par des lettres différentes des lettres désignant les variables libres a et b de $\mathfrak{B}$;*
- *les variables x et y de F sont liées mais n'apparaissent pas dans $\mathfrak{B}$.*

On a alors le théorème suivant :

$$\exists x \forall y[(x|a)(y|b)G(a, b)].$$

C'est à dire

$$\exists x \forall y[G(x, y)].$$

Enfin, on notera encore les deux règles d'inférence suivantes : le modus ponens, comme dans LPC, et la règle de généralisation.

RI 10. *Si $\mathfrak{A}$ est un théorème dans lequel la variable x n'est pas liée, alors $\forall x\mathfrak{A}$ est aussi un théorème. On notera*

$$\frac{\mathfrak{A}}{\forall x[\mathfrak{A}]}$$

Comme la logique des prédicats possède les axiomes et les règles d'inférence de LPC, il apparaît alors que tous les théorèmes de LPC sont des théorèmes de la logique des prédicats. Pour se familiariser avec les notions qui viennent d'être présentées, voici un exemple de démonstration. On notera que ce théorème est souvent présenté comme un axiome [3].

Théorème 2.3.2. *La formule* $F(y) \to \exists x[F(x)]$ *est un théorème.*

Démonstration. On procède, dans l'axiome 4, à la substitution du prédicat F par la formule $\neg F(y)$:

$$\vdash \forall x[F(x)] \to F(y)$$
$$\vdash \forall x[\neg F(x)] \to \neg F(y)$$

Ensuite, on substitue dans l'axiome **AF**4 la formule $\forall x[\neg F(x)]$ à la proposition φ et la formule $\neg F(y)$ à la proposition ψ on obtient

$$\vdash \Big(\forall x[\neg F(x)] \to \neg F(y)\Big) \to \Big(\neg\neg F(y) \to \neg\forall x[\neg F(x)]\Big).$$

Puis, par modus ponens il vient

$$\vdash \neg\neg F(y) \to \neg\forall x[\neg F(x)].$$

Avec les définitions consacrées, et en tenant compte de la proposition 1.4.5, on a donc

$$\vdash F(y) \to \exists x[F(x)].$$ □

2.4 Cohérence du Calcul des Prédicats

Avant de poursuivre dans la présentation de la logique des prédicats on montre d'abord que celle-ci est cohérente. Pour ce faire, on prouve que si Γ était incohérente, alors la logique des propositions serait elle aussi incohérente. On suit ici l'argument proposé dans [28] (§5 ch.4). On procède par étapes : d'abord on définit comment faire correspondre une formule $\mathfrak{A}$ de la logique des prédicats à une proposition de LPC. Ensuite, on montre qu'à tout théorème de la logique des prédicats correspond un théorème de la logique des propositions. Il faudra là encore discuter des cas de bases pour pouvoir conclure en procédant de proche en proche. Ainsi, on sera en mesure de affirmer que si la logique des prédicats n'était pas cohérentes il en serait de même pour LPC. La conclusion découle alors du fait que l'on sait que la logique propositionnelle est non-contradictoire. On note au passage, avec les mêmes arguments qu'en 1.5.1, que la question de cohérence et celle de non-contradiction sont équivalentes.

Définition 2.4.1. *On définit la correspondance suivante :*

1. *toute proposition* $\mathfrak{A} \equiv \varphi$ *est mise en correspondance avec elle même :* $\mathfrak{A}^* \equiv \varphi$ *;*

3. Voir [28, p.155] , [30, p.33] ou encore [29, p.87].

2. *tout prédicat* $\mathfrak{A} \equiv F(a, b, ..., n)$ *est mis en correspondance avec le caractère qui le représente, en omettant toutes les variables :* $\mathfrak{A}* \equiv F$*, où* F *prend le statut de proposition ;*
3. *si la formule* $\mathfrak{A}$ *est mise en correspondance avec* $\mathfrak{A}^*$ *alors la formule* $\forall x\mathfrak{A}$ *est mise en correspondance avec* $\mathfrak{A}^*$ *;*
4. *si les formules* $\mathfrak{A}_1$ *et* $\mathfrak{A}_2$ *sont mises en correspondance avec* $\mathfrak{A}_1^*$ *et* $\mathfrak{A}_2^*$ *alors les formules* $\mathfrak{A}_1 \to \mathfrak{A}_2$ *sont mises en correspondance avec* $\mathfrak{A}_1^* \to \mathfrak{A}_2^*$ *et* $\neg\mathfrak{A}_1$ *avec* $\neg\mathfrak{A}_1^*$*.*

Exemple 2.4.1. *Comme "*$\wedge$*", "*$\vee$*" et "*$\exists$*" sont exprimables à l'aide de "*$\neg$*", "*$\to$*" et "*$\forall$*", on montre que* $(\mathfrak{A}_1 \vee \mathfrak{A}_2)^*$ *correspond à* $\mathfrak{A}_1^* \vee \mathfrak{A}_2^*$*, que* $(\mathfrak{A}_1 \wedge \mathfrak{A}_2)^*$ *correspond à* $\mathfrak{A}_1^* \wedge \mathfrak{A}_2^*$ *et que* $(\exists x[\mathfrak{A}])^*$ *correspond à* $\mathfrak{A}^*$*.*

1. *Comme* $\mathfrak{A}_1 \vee \mathfrak{A}_2 \equiv \neg\mathfrak{A}_1 \to \mathfrak{A}_2$*, on a successivement*

$$\begin{aligned}&(\neg\mathfrak{A}_1 \to \mathfrak{A}_2)^*\\ &(\neg\mathfrak{A}_1)^* \to (\mathfrak{A}_2)^*\\ &\neg(\mathfrak{A}_1)^* \to \mathfrak{A}_2^* \equiv \mathfrak{A}_1^* \vee \mathfrak{A}_2^*.\end{aligned}$$

2. *Comme* $\mathfrak{A}_1 \wedge \mathfrak{A}_2 \equiv \neg(\mathfrak{A}_1 \to \neg\mathfrak{A}_2)$*, on a successivement*

$$\begin{aligned}&\Big(\neg(\mathfrak{A}_1 \to \neg\mathfrak{A}_2)\Big)^*\\ &\neg(\mathfrak{A}_1 \to \neg\mathfrak{A}_2)^*\\ &\neg\Big(\mathfrak{A}_1^* \to (\neg\mathfrak{A}_2)^*\Big)\\ &\neg\Big(\mathfrak{A}_1^* \to \neg\mathfrak{A}_2^*\Big) \equiv \mathfrak{A}_1^* \wedge \mathfrak{A}_2^*.\end{aligned}$$

3. *Comme* $\exists x[\mathfrak{A}] \equiv \neg(\forall x[\neg\mathfrak{A}])$*, on a successivement*

$$\begin{aligned}&\Big(\neg(\forall x[\neg\mathfrak{A}])\Big)^*\\ &\neg(\forall x[\neg\mathfrak{A}])^*\\ &\neg(\neg\mathfrak{A})^*\\ &\neg\neg(\mathfrak{A})^* \equiv (\mathfrak{A})^*.\end{aligned}$$

Exemple 2.4.2. *À la formule*

$$\forall x[F(x, y)] \to \exists x[F(x, y)],$$

on associe la proposition

$$F \to F.$$

Remarque 2.4.2. *À partir de l'exemple 2.4.1 et de la remarque 2.3.1, on montre que si* $\mathfrak{A}'$ *est obtenu après substitution, dans une formule* $\mathfrak{A}$*, d'un prédicat* $F(a, b, ..., n)$ *ou d'une proposition* φ *par une formule* $\mathfrak{B}$*, alors* $(\mathfrak{A}')^*$ *est obtenu après substitution dans* $\mathfrak{A}^*$ *du caractère* F *ou* φ *par* $\mathfrak{B}^*$*. D'abord, si* $\mathfrak{A}$ *est une formule élémentaire, c'est immédiat. Pour une formule quelconque de* Γ*, il suffit de procéder de proche en proche.*

Nous sommes prêts à formuler et prouver la cohérence de la logique du premier ordre (voir [28], p.163).

Théorème 2.4.3. *La logique du premier ordre est cohérente.*

Démonstration. Vu ce qui précède, il reste à montrer qu'à chaque théorème de la logique des prédicats correspond un théorème de LPC. Comme les axiomes **A**1 , **A**2 et **A**3 de la logique des prédicats portent sur les propositions, ceux-ci sont en correspondance avec les axiomes de LPC. Quant à l'axiome **A**4, il est mis en correspondance avec la proposition $F \to F$ qui est une tautologie dans LPC.

On montre que les théorèmes de la logique des prédicats, obtenus par les règles d'inférence depuis des théorèmes vérifiant la propriété, sont en correspondance avec des théorèmes de LPC.

(i) Modus ponens : si $\mathfrak{A} \to \mathfrak{B}$ et $\mathfrak{A}$ sont des théorèmes de Γ tels que $\mathfrak{A}^* \to \mathfrak{B}^*$ et $\mathfrak{A}^*$ sont des théorèmes de LPC, alors d'une part $\mathfrak{B}$ est un théorème de Γ et d'autre part $\mathfrak{B}^*$ est un théorème de LPC.

(ii) Substitution de variable : si $\mathfrak{A}$ vérifie la propriété, et comme dans $\mathfrak{A}^*$ toute occurrence de toute variable est supprimée, tout théorème $\mathfrak{A}'$ de Γ obtenu après substitution de variables dans $\mathfrak{A}$ sera en correspondance avec $\mathfrak{A}^*$.

(iii) Substitution de proposition ou de prédicat : si $\mathfrak{A}'$ est obtenu après substitution, dans un théorème $\mathfrak{A}$ de Γ, d'un prédicat $F(a, b, ..., n)$ ou d'une proposition φ par une formule $\mathfrak{B}$, alors, vu la remarque 2.4.2 $(\mathfrak{A}')^*$ est obtenu en substituant dans $\mathfrak{A}^*$, qui est donc un théorème de LPC, les occurrences de F ou de φ par une formule $\mathfrak{B}^*$. Dès lors $(\mathfrak{A}')^*$ est bien un théorème de LPC vu la règle d'inférence correspondant à la substitution dans LPC.

(iv) Introduction du quantificateur $\forall$: c'est évident vu les points 3. et 4. de la définition 2.4.1.

On est maintenant en mesure de conclure à la non-contradiction du système formel Γ. En effet, si Γ était contradictoire, on pourrait trouver un théorème $\mathfrak{A}$ dont la négation est aussi un théorème. En particulier on aurait le théorème suivant

$$\mathfrak{A} \wedge \neg\mathfrak{A}.$$

Mais à ce théorème correspond, dans LPC, le théorème $\mathfrak{A}^* \wedge \neg\mathfrak{A}^*$. On aurait alors que LPC est contradictoire.

□

2.5 Théorème de la déduction

Comme pour la logique des propositions, on peut établir un résultat qui fournira une technique de démonstration particulièrement efficace : le (méta)théorème de la déduction. Ce (méta)théorème ne peut être une transposition directe du théorème de la déduction de

LPC. En effet, il est possible de trouver des formules $\mathfrak{A}$ et $\mathfrak{B}$ telles que $\Gamma + \mathfrak{A} \vdash \mathfrak{B}$ mais $\Gamma \nvdash \mathfrak{A} \to \mathfrak{B}$.

Exemple 2.5.1. *On considère les deux formules* $\mathfrak{A} \equiv \forall x[F(x)]$ *et* $\mathfrak{B} \equiv F(x)$. *Si l'on rajoute aux axiomes de la logique des prédicats la formule* $\mathfrak{A}$ *alors, vu l'axiome* **A**4 *on en déduit, par modus ponens, que* $F(y)$ *est un théorème. En substituant* x *à* y *on a* $\Gamma + \mathfrak{A} \vdash \mathfrak{B}$ *:*

$$\begin{aligned} \mathfrak{A} &\vdash \forall x[F(x)] \\ &\vdash \forall x[F(x)] \to F(y) \\ &\vdash F(y) \\ &\vdash F(x) \end{aligned}$$

Cependant, l'énoncé $\mathfrak{A} \to \mathfrak{B}$ *n'est pas une formule car la règle de formation* **RF**6 *n'est pas respectée. En particulier,* $\Gamma \nvdash \mathfrak{A} \to \mathfrak{B}$.

On se rend compte par cet exemple que pour pouvoir appliquer le théorème de la déduction, il faut, a minima, que la formule obtenue soit telle que $\mathfrak{A} \to \mathfrak{B}$ est bien formulé. On introduit alors la notion de formule déduite.

Définition 2.5.1. *Une formule* $\mathfrak{B}$ *est déduite de* $\mathfrak{A}$*, et on note* $\mathfrak{A} \Rightarrow \mathfrak{B}$*, si une des conditions suivantes est vérifiée :*

1. $\mathfrak{B}$ *est un théorème de la logique des prédicats et* $\mathfrak{A} \to \mathfrak{B}$ *est une formule ;*
2. $\mathfrak{B}$ *est la formule* $\mathfrak{A}$ *elle-même :*
$$\mathfrak{A} \Rightarrow \mathfrak{A} \ ;$$
3. *si les formules* $\mathfrak{C}$ *et* $\mathfrak{C} \to \mathfrak{B}$ *sont déduites de* $\mathfrak{A}$*, alors* $\mathfrak{A} \Rightarrow \mathfrak{B}$ *;*
4. *si* $\mathfrak{A} \Rightarrow \mathfrak{B}_1 \to \mathfrak{B}_2$ *et si* x *n'est pas lié dans* $\mathfrak{B}_2$ *et n'a pas d'occurrence dans* $\mathfrak{A}$ *et* $\mathfrak{B}_1$ *alors*
$$\mathfrak{A} \Rightarrow \mathfrak{B}_1 \to \forall x[\mathfrak{B}_2] \ ;$$
5. *si* $\mathfrak{A} \Rightarrow \mathfrak{B}_1 \to \mathfrak{B}_2$ *et si* x *n'est pas lié dans* $\mathfrak{B}_1$ *et n'a pas d'occurrence dans* $\mathfrak{A}$ *et* $\mathfrak{B}_2$ *alors*
$$\mathfrak{A} \Rightarrow \exists x[\mathfrak{B}_1] \to \mathfrak{B}_2 \ ;$$
6. $\mathfrak{B}$ *est obtenue en substituant une variable liée dans une formule déduite de* $\mathfrak{A}$ *de telle sorte que* $\mathfrak{A} \to \mathfrak{B}$ *est bien formulé ;*
7. $\mathfrak{B}$ *est obtenue en substituant dans une formule déduite de* $\mathfrak{A}$ *une variable libre n'ayant pas d'occurrence dans* $\mathfrak{A}$ *et de telle sorte que* $\mathfrak{A} \to \mathfrak{B}$ *est bien formulé ;*
8. $\mathfrak{B}$ *est obtenue par substitution dans une formule déduite de* $\mathfrak{A}$ *d'un prédicat ou d'une proposition n'ayant pas d'occurrence dans* $\mathfrak{A}$ *et de telle sorte que* $\mathfrak{A} \to \mathfrak{B}$ *est bien formulé.*

De la définition, on peut déjà établir quelques propriétés utiles.

Exemple 2.5.2. *Si on a* $\mathfrak{A} \Rightarrow \mathfrak{B}_1 \wedge \mathfrak{B}_2$*, alors* $\mathfrak{A} \Rightarrow \mathfrak{B}_1$ *et* $\mathfrak{A} \Rightarrow \mathfrak{B}_2$.

Démonstration. Comme on sait que $(\mathfrak{B}_1 \wedge \mathfrak{B}_2) \to \mathfrak{B}_1$ est un théorème (voir la proposition 1.5.10), en appliquant successivement le point 1. et le point 3. de la définition, on a :

$$\begin{aligned} \mathfrak{A} &\Rightarrow \mathfrak{B}_1 \wedge \mathfrak{B}_2 \\ &\Rightarrow (\mathfrak{B}_1 \wedge \mathfrak{B}_2) \to \mathfrak{B}_1 \\ &\Rightarrow \mathfrak{B}_1. \end{aligned}$$

On procède semblablement pour montrer que $\mathfrak{A} \Rightarrow \mathfrak{B}_2$. □

Réciproquement, si on a $\mathfrak{A} \Rightarrow \mathfrak{B}_1$ et $\mathfrak{A} \Rightarrow \mathfrak{B}_2$, alors on a $\mathfrak{A} \Rightarrow \mathfrak{B}_1 \wedge \mathfrak{B}_2$.

Exemple 2.5.3. *Si $\mathfrak{B}_1$ et $\mathfrak{B}_2$ sont des formules déduites de la formule $\mathfrak{A}$, alors la formule $\mathfrak{B}_1 \wedge \mathfrak{B}_2$ est déduite de $\mathfrak{A}$.*

Démonstration. Comme la formule $\varphi \to (\chi \to (\varphi \wedge \chi))$ est un théorème (c.f. 1.5.11) il suffit d'appliquer le modus ponens :

$$\begin{aligned} \mathfrak{A} &\Rightarrow \mathfrak{B}_1 \\ &\Rightarrow \mathfrak{B}_2 \\ &\Rightarrow \mathfrak{B}_1 \to (\mathfrak{B}_2 \to (\mathfrak{B}_1 \wedge \mathfrak{B}_2)) \\ &\Rightarrow \mathfrak{B}_1 \wedge \mathfrak{B}_2 \end{aligned}$$

□

Théorème 2.5.2 ((méta)théorème de la déduction)**.** *Si la formule $\mathfrak{B}$ est déduite de la formule $\mathfrak{A}$, alors la formule $\mathfrak{A} \to \mathfrak{B}$ est un théorème de la logique des prédicats.*

Démonstration. Il suffit de démontrer que la propriété est vérifiée pour chacun des cas de la définition 2.5.1. Nous les énumérons ci-dessous et exposons les justifications dans la foulée.

1. si $\mathfrak{B}$ est un théorème et $\mathfrak{A} \to \mathfrak{B}$ est une formule alors $\mathfrak{A} \to \mathfrak{B}$ est un théorème ;
2. $\mathfrak{A} \to \mathfrak{A}$;
3. si la propriété est vraie pour les formules $\mathfrak{C}$ et $\mathfrak{C} \to \mathfrak{B}$ alors elle est vraie pour $\mathfrak{B}$;
4. si la propriété est vraie pour $\mathfrak{B}_1 \to \mathfrak{B}_2$ alors elle est vraie aussi pour $\mathfrak{B}_1 \to \forall x[\mathfrak{B}_2]$;
5. si la propriété est vraie pour $\mathfrak{B}_1 \to \mathfrak{B}_2$ alors elle est vraie aussi pour $\exists x[\mathfrak{B}_1] \to \mathfrak{B}_2$;
6. si la propriété est vraie pour $\mathfrak{B}$ et si $\mathfrak{B}'$ est obtenue suite à une substitution d'une variable liée dans $\mathfrak{B}$ de telle sorte que $\mathfrak{A} \to \mathfrak{B}'$ est bien formulé, alors $\mathfrak{A} \to \mathfrak{B}'$ est un théorème ;
7. si la propriété est vraie pour $\mathfrak{B}$ et si $\mathfrak{B}'$ est obtenue en substituant dans $\mathfrak{B}$ une variable libre de telle sorte que $\mathfrak{A} \to \mathfrak{B}'$ est bien formulé, alors $\mathfrak{A} \to \mathfrak{B}'$ est un théorème ;

8. si la propriété est vraie pour $\mathfrak{B}$ et si $\mathfrak{B}'$ est obtenue par substitution dans $\mathfrak{B}$ d'un prédicat ou d'une proposition n'ayant pas d'occurrence dans $\mathfrak{A}$ et de telle sorte que $\mathfrak{A} \to \mathfrak{B}'$ est bien formulé, alors $\mathfrak{A} \to \mathfrak{B}'$ est un théorème.

Voici à présent les justifications annoncées.

1. Dans LPC, on sait que si φ est un théorème, alors $\psi \to \varphi$ est un théorème (par l'axiome **AF**1 et le modus ponens). Dès lors, en substituant $\mathfrak{A}$ à ψ et $\mathfrak{B}$ à φ on a
$$\begin{aligned} &\vdash \mathfrak{B} \\ &\vdash \mathfrak{A} \to \mathfrak{B} \end{aligned}$$
2. La justification est directe car, dans LPC, $\varphi \to \varphi$ est un théorème (voir par exemple la proposition 1.4.2).
3. Dans ce cas, on suppose que la propriété est vérifiée pour $\mathfrak{A} \Rightarrow \mathfrak{C}$ et $\mathfrak{A} \Rightarrow \mathfrak{C} \to \mathfrak{B}$. Ainsi, en appliquant la distributivité de "$\to$" (voir l'axiome **AF**2), on a
$$\begin{aligned} &\vdash \mathfrak{A} \to \mathfrak{C} \\ &\vdash \mathfrak{A} \to (\mathfrak{C} \to \mathfrak{B}) \\ &\vdash \mathfrak{A} \to \mathfrak{B} \end{aligned}$$
4. Comme on suppose que la propriété est vérifiée pour $\mathfrak{A} \Rightarrow \mathfrak{B}_1 \to \mathfrak{B}_2$, on a
$$\vdash \mathfrak{A} \to (\mathfrak{B}_1 \to \mathfrak{B}_2),$$
avec $\mathfrak{A}$, $\mathfrak{B}_1$ et $\mathfrak{B}_2$ vérifiant les conditions du point 4. de la définition. Or, dans LPC, la formule $\mathfrak{F} \equiv \big(\varphi \to (\chi \to \psi)\big) \leftrightarrow \big((\varphi \wedge \chi) \to \psi\big)$ est un théorème ; de sorte que l'on a, dans la logique des prédicats
$$\vdash (\mathfrak{A} \wedge \mathfrak{B}_1) \to \mathfrak{B}_2.$$
Or, vu la règle d'introduction de $\forall$ (**RI**10), on a
$$\vdash (\mathfrak{A} \wedge \mathfrak{B}_1) \to \forall x[\mathfrak{B}_2].$$
Ainsi, vu $\mathfrak{F}$, on a
$$\vdash \mathfrak{A} \to (\mathfrak{B}_1 \to \forall x[\mathfrak{B}_2]).$$
5. Dans ce cas-ci, on procède comme au point précédent mais en considérant la formule $\mathfrak{F} \equiv \big(\varphi \to (\chi \to \psi)\big) \leftrightarrow \big(\chi \to (\varphi \to \psi)\big)$, qui n'est autre que l'axiome **AF**3.

Les points 6, 7 et 8 sont directs vu qu'aucune des substitutions ne porte sur des objets ayant une occurrence dans $\mathfrak{A}$ de sorte que, par exemple
$$(x|t)(\mathfrak{A} \to \mathfrak{B}) \equiv \mathfrak{A} \to (x|t)\mathfrak{B}.$$
De plus, ces substitutions respectent les conditions d'application des règles d'inférence qui y sont relatives. □

Théorème 2.5.3. *:* $\forall x[F(x) \wedge G(x)] \ \leftrightarrow \ \forall x[F(x)] \wedge \forall x[G(x)]$

Démonstration. On montre respectivement que

$$\forall x[F(x) \wedge G(x)] \ \rightarrow \ \forall x[F(x)] \wedge \forall x[G(x)]$$

et

$$\forall x[F(x)] \wedge \forall x[G(x)] \rightarrow \forall x[F(x) \wedge G(x)]$$

sont des théorèmes.

1. $\forall x[F(x) \wedge G(x)] \ \rightarrow \ \forall x[F(x)] \wedge \forall x[G(x)]$
   On substitue dans l'axiome **A**4 le prédicat F par la formule $F(a) \wedge G(a)$. La formule $\forall x[F(x) \wedge G(x)] \ \rightarrow \ F(y) \wedge G(y)$ est donc un théorème de Γ ; elle est ainsi déduite de $\forall x[F(x) \wedge G(x)]$, qui est elle même une formule déduite. En appliquant le modus ponens on a dès lors que $F(y) \wedge G(y)$ est une formule déduite.

   $$\begin{aligned} \forall x[F(x) \wedge G(x)] &\Rightarrow \forall x[F(x) \wedge G(x)] \\ &\Rightarrow \forall x[F(x) \wedge G(x)] \ \rightarrow \ F(y) \wedge G(y) \\ &\Rightarrow F(y) \wedge G(y). \end{aligned}$$

   Vu l'exemple 2.5.2, on sait qu'alors $F(y)$ et $G(y)$, et donc $\forall z[F(z)]$ et $\forall z[G(z)]$, sont des formules déduites de $\forall x[F(x) \wedge G(x)]$.

   $$\begin{aligned} \forall x[F(x) \wedge G(x)] &\Rightarrow F(y) \wedge G(y) \\ &\Rightarrow F(y) \\ &\Rightarrow G(y) \\ &\Rightarrow \forall z[F(z)] \\ &\Rightarrow \forall z[G(z)]. \end{aligned}$$

   Dès lors, par l'application du (méta-)théorème de la déduction, les formules $\forall x[F(x) \wedge G(x)] \ \rightarrow \ \forall z[F(z)]$ et $\forall x[F(x) \wedge G(x)] \ \rightarrow \ \forall z[G(z)]$ sont des théorèmes dans Γ. Enfin, vu la proposition 1.5.13, le théorème annoncé s'obtient par application successive du modus ponens et de la substitution $(x|z)$:

   $$\begin{aligned} \Gamma \vdash \forall x[F(x) \wedge G(x)] \ &\rightarrow \ \forall z[F(z)] \\ \vdash \forall x[F(x) \wedge G(x)] \ &\rightarrow \ \forall z[G(z)] \\ \vdash \forall x[F(x) \wedge G(x)] \ &\rightarrow \ \big(\ \forall z[F(z)] \wedge \forall z[G(z)] \ \big) \\ \vdash \forall x[F(x) \wedge G(x)] \ &\rightarrow \ \big(\ \forall x[F(x)] \wedge \forall x[G(x)] \ \big). \end{aligned}$$

2. $\big(\forall x[F(x)] \wedge \forall x[G(x)]\big) \rightarrow \forall x[F(x) \wedge G(x)]$
   Il a été établi dans **RI** 3 que $(\varphi \wedge \psi) \rightarrow \varphi$ (resp. $(\varphi \wedge \psi) \rightarrow \psi$) est un théorème. Dès lors, celui-ci est déduit de $\forall x[F(x)] \wedge \forall x[G(x)]$, et il en est de même pour $\forall x[F(x)]$

(resp. $\forall x[G(x)]$) obtenu après modus ponens. Ainsi, par le (méta-)théorème de la déduction, on a dans Γ les deux théorèmes suivants :

$$\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow \forall x[F(x)]$$

et

$$\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow \forall x[G(x)].$$

En appliquant la règle du syllogisme **RI** 6 avec l'axiome **A**4 et les deux précédents théorèmes, on infère $\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow F(y)$ et $\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow G(y)$. Or on a montré au point 1. qu'on a alors

$$\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow (F(y) \wedge G(y)).$$

En appliquant enfin la règle d'introduction du $\forall$ on a

$$\Big(\forall x[F(x)] \wedge \forall x[G(x)]\Big) \rightarrow \forall x[F(x) \wedge G(x)].$$ □

Chapitre 3

Théorie des ensembles

3.1 Introduction

En théorie naïve des ensembles, on se permet de définir des ensembles comme :

$$E = \{x \mid x \text{ est un entier défini en un nombre fini de caractères}\}.$$

Un tel ensemble fait alors apparaître une antinomie. En effet, soit le plus petit naturel qui n'est pas dans E. Celui-ci est défini en un nombre fini de caractères, donc il appartient a l'ensemble E [1].

Plusieurs axiomatisations ont été proposées pour la théorie des ensembles. Elles avaient pour but de formaliser, tout en l'améliorant, la théorie naïve des ensembles et d'ainsi dissiper les paradoxes qui y apparaissaient (comme le célèbre paradoxe de Russell, cf. infra). Cette théorie solidement axiomatisée s'est révélée utile pour la fondation des mathématiques classiques. On peut lire dans [7, Introduction p. E.I.9] :

"En effet, alors qu'autrefois on a pu croire que chaque branche des mathématiques dépendait d'intuitions particulières qui lui fournissaient notions et vérités premières, ce qui eût entraîné pour chacune la nécessité d'un langage formalisé qui lui appartint en propre, on sait aujourd'hui qu'il est possible, logiquement parlant, de faire dériver toute la mathématique actuelle d'une source unique, la Théorie des Ensembles."

Une première tentative est proposée par Zermelo (1871-1953). Celle-ci est ensuite affinée par Fraenkel. Enderton [14] que nous prenons comme référence pour la partie de ce travail sur les nombres, mentionne deux alternatives à la théorie naïve des ensembles. Celle de Zermelo-Fraenkel (Z-F) et celle de von Neumann-Bernays. Il explique alors que dans la théorie Z-F, pour ne pas avoir d'ensembles paradoxaux tels que l'ensemble qui contient tous les ensembles, on n'en parle pas [2]. Enderton suit donc la théorie Z-F mais s'autorise à parler de la classe de tous les ensembles si nécessaire.

1. Cet exemple peut avoir l'air artificiel, mais Dedekind propose une démonstration dans laquelle il considère "l'ensemble des objets de sa pensée" (cf. [11, p.176, 66]).

2. "The collection of all sets needs have no ontological status at all, and we need never speak of it. When tempted to speak ok it, we can seek a rephrasing that avoids it"([14, p.10]).

On note également qu'un glissement s'opère dans la forme. Du formalisme exsangue cher à Hilbert, on se met à parler d'ensemble, d'inclusion, on montre que "il en existe au moins un" ou "un unique ayant une certaine propriété". On constate cependant que ce changement n'est jamais explicité ni expliqué ou légitimé. Cela est particulièrement flagrant dans [14], où Enderton présente (de façon rudimentaire) le formalisme classique ; il énonce alors les axiomes de Z-F mais ceux-ci sont toujours traduits, et les démonstrations qui suivent sont dans un formalisme plus conventionnel.

La nécessité de reformuler une théorie des ensembles est apparue quand, dans les années 1900, Russell formule son célèbre paradoxe. Jusqu'alors, un ensemble était simplement défini comme une collection d'objets et l'on pouvait alors raisonner sur des ensembles définis par une propriété quelconque[3]. Le paradoxe de Russell est le suivant : on considère l'ensemble E des ensembles qui ne s'appartiennent pas à eux mêmes :

$$E = \{x \mid x \notin x\}$$

Rien n'interdit cette définition dans la théorie naïve des ensembles. Le paradoxe apparaît quand on se demande si E est un élément de E. Si $E \in E$, alors, par définition $E \notin E$. Réciproquement, si $E \notin E$ alors par définition $E \in E$. On a donc un paradoxe. Une première solution serait d'interdire d'avoir un ensemble x qui puisse être un élément de lui-même (on se place alors dans le prédicativisme [22]), mais l'on va procéder autrement.

Il y a deux problèmes à régler. D'abord, il faut s'assurer qu'on ne puisse pas définir des ensembles à l'aide de formules ambiguës. Pour y remédier, on se place dans une théorie du premier ordre qui ne permettra pas de telles choses. Ensuite, l'on doit s'assurer qu'on ne puisse définir des ensembles "trop grands" comme "l'ensemble" de tous les ensembles. Pour ce faire un nouvel ensemble dans Z-F ne peut être construit qu'en considérant une partie d'un ensemble déjà existant. On montrera alors qu'il n'est pas possible de définir un ensemble qui contient tous les ensembles.

La théorie de Zermelo-Fraenkel est une axiomatisation dans la logique du premier ordre avec égalité. C'est à dire que dans le système formel que constitue Z-F, on retrouve les symboles logiques $\neg$ et $\rightarrow$, le quantificateur $\forall$ et le symbole binaire $=$ ainsi que les règles de formation et les axiomes de la logique du premier ordre avec égalité. On ajoute un symbole binaire, $\in$, de nouveaux axiomes et une règle de formation. On appellera aussi "ensemble" les variables de la théorie Z-F.

Évidement, cette théorie ne fait pas table rase de tous les savoirs mathématiques accumulés jusqu'alors, bien au contraire. Par exemple Hilbert lui même exprime le souhait de construire un édifice mathématique dans lequel on conserverait le principe du transfini, "paradis créé par Cantor" ([3]). Dès lors, on établit une théorie des ensembles avec toutes les qualités que l'on convoite (rigueur, non-contradiction, ...) de manière à conserver la plupart des propriétés attendues de la théorie naïve des ensembles.

3. Notons par exemple que Dedekind, dans son ouvrage "Que sont les nombres et à quoi servent-ils", commence sa démonstration de la proposition 66 sur l'existence d'un ensemble infini par la phrase suivante : "Le monde de mes pensées, i.e. la totalité S de toutes les choses qui peuvent être objet de ma pensée, est infini".

3.2 La théorie de Zermelo-Fraenkel

La logique des prédicats a été présentée de la manière la plus générale. On y a donc défini des prédicats hypothétiques, d'arités arbitraires. Dans la théorie de Zermelo-Fraenkel, on a à disposition exactement deux prédicats binaires. Par commodité, on les notera $\in$ et $=$ et non par des majuscules latines. De plus, on écrira respectivement $x \in y$ et $x = y$ en lieu et place de $\in (x, y)$ et $= (x, y)$ pour les mêmes raisons de commodité. On a donc les règles formatives suivantes :

RF 7. *Si x et y sont des variables, alors $x = y$ est une proposition atomique et se lit "x est égal à y".*

RF 8. *Si x et y sont des variables, alors $x \in y$ est une proposition atomique et se lit "x appartient à y" ou encore "x est un élément de y".*

Il en résulte qu'un énoncé comme

$$\forall x \forall y (x \in y)$$

est bien formulé.

On introduit déjà ici quelques abréviations.

Définition 3.2.1. *On notera $x \subseteq y$ pour signifier $\forall z \Big(z \in x \to z \in y \Big)$. Dans ce cas, on dit que x est un sous-ensemble de y.*

Définition 3.2.2. *On notera $x \notin y$ pour signifier $\neg (x \in y)$.*

Définition 3.2.3. *On notera $x \neq y$ pour signifier $\neg (x = y)$.*

L'introduction des prédicats $\in$ et $=$ amène aussi l'introduction d'axiomes permettant de régler leurs usages. D'abord, on présente les axiomes liés à $=$. On notera que les trois premiers seront constitutifs de la notion de relation d'équivalence, que nous reverrons plus tard.

A 5. $\forall x (x = x)$

A 6. $\forall x \forall y (x = y \to y = x)$

A 7. $\forall x \forall y \forall z \Big(\ (x = y \wedge y = z) \to (x = z) \ \Big)$

A 8. $\forall x \forall y \Big[\ (x = y) \to \Big[F(x) \leftrightarrow F(y) \Big] \ \Big]$

Viennent ensuite les axiomes de la théorie des ensembles. Le premier est l'axiome d'extensionnalité.

A 9 (Axiome d'extensionnalité)**.** $\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \to x = y]$.

Autrement dit, si $x \subseteq y$ et $y \subseteq x$, alors $x = y$. C'est ce qu'on appelle l'argument par double inclusion. L'axiome d'extensionnalité permet donc de prouver l'égalité entre deux ensembles. Réciproquement , si $x = y$, vu l'axiome **A**8 de l'égalité, on a la double inclusion :

$$x = y \to \Big(x \subseteq y \wedge y \subseteq x\Big),$$

où l'axiome a été reformulé avec l'abréviation "$\subseteq$".

On l'a vu, dans la théorie naïve des ensembles, un ensemble est défini comme une collection d'objets ; on dit que x est l'ensemble des objets vérifiant la propriété φ, et on écrit $x = \{z \mid \varphi\}$. Ainsi, l'existence d'ensembles comme l'ensemble vide découle directement de la définition naïve d'ensembles :

$$\emptyset = \{z \mid z \neq z\}.$$

Il en est de même avec l'union, l'intersection, le pairage et les parties. Dès lors, comme l'on a rejeté la définition naïve des ensembles, les notions qui en découlaient doivent être repensées. Dans la théorie Z-F, l'existence de tels ensembles est en fait assurée par des axiomes. L'axiome qui suit postule l'existence d'un ensemble qui ne contient aucun élément.

A 10 (Axiome de l'existence de l'ensemble vide)**.** $\exists x \forall y\ (y \notin x)$

Théorème 3.2.4 (Unicité de l'ensemble vide)**.** *L'ensemble vide est unique.*

Démonstration. On montre que si deux ensembles x_1 et x_2 satisfont l'axiome 10, alors ils sont égaux :

$$\forall x_1 \forall x_2 \Big[\ \forall y [y \notin x_1 \wedge y \notin x_2] \to x_1 = x_2\ \Big]$$

D'abord on a

$$\begin{aligned} a \notin b_1 \wedge a \notin b_2 &\Rightarrow a \notin b_1 \\ &\Rightarrow a \notin b_2 \\ &\Rightarrow a \notin b_2 \to a \notin b_1 \\ &\Rightarrow a \notin b_1 \to a \notin b_2 \\ &\Rightarrow a \in b_2 \to a \in b_1 \\ &\Rightarrow a \in b_1 \to a \in b_2 \\ &\Rightarrow b_1 = b_2. \end{aligned}$$

Donc, par le (méta)théorème de la déduction dans Γ on a le théorème suivant :

$$a \notin b_1 \wedge a \notin b_2 \to b_1 = b_2.$$

Avec la règle d'introduction du quantificateur $\forall$ on a donc

$$\forall x_1 \forall x_2 \Big[\ \forall y [y \notin x_1 \wedge y \notin x_2] \to x_1 = x_2\ \Big].$$

□

Comme un tel ensemble est unique, on peut lui attribuer un nom et lui assigner une notation spécifique.

Définition 3.2.5. *L'ensemble vide, donné par l'axiome* **A***10 est noté* $\emptyset$*. Dès lors,* $\emptyset$ *devient un symbole constant de notre langage.*

Remarque 3.2.6. *L'exemple qui suit permet d'appuyer un peu plus la fracture qu'il y a entre le sens commun que l'on peut donner aux différents symboles et les possibilités factuelles dictées par le formalisme. Ainsi, lorsque les quantificateur* $\forall$ *et* $\exists$ *sont présentés, on les traduit habituellement par "pour tout" et "il existe"*[4] *respectivement. Avec l'interprétation de* $\forall$ *et* $\exists$ *susmentionnées, on a donc qu'il existe un* x *tel que pour tout* y*,* x *est différent de* y*. En particulier, on aurait que* x *est différent de* x *:*

$$\exists x[\neg(x = x)].$$

Ce résultat est contraire à un autre axiome **(A)***5 de la transitivité de l'égalité :*

$$\forall x[x = x].$$

A 11 (Axiome du pairage)**.**

$$\forall x \forall y \exists t \forall z \Big[z \in t \leftrightarrow (z = x \vee z = y) \Big]$$

On note alors $t = \{x, y\}$*.*

On peut montrer que, conformément à la notation introduite, on a $\{x, y\} = \{y, x\}$. Cela se devine dans l'énoncé de l'axiome car les formules $\forall x \forall y[F(x, y)]$ et $\forall y \forall x[F(x, y)]$ sont équivalentes.

A 12 (Axiome de la puissance)**.** *Pour tout ensemble* x*, il existe un ensemble* y *qui contient exactement tous les sous-ensembles de* x *:*

$$\forall x \ \exists y \ \forall z (z \in y \leftrightarrow z \subseteq x).$$

L'ensemble ainsi défini sera noté $\mathscr{P}(x)$.

A 13 (Axiome de la compréhension)**.**

$$\forall x \exists y \forall z [z \in y \ \leftrightarrow (z \in x \wedge F(z))]$$

On notera alors $y = \{z \in x \mid F(z)\}$. Il arrivera régulièrement que l'on omette de préciser que $z \in x$ dans l'expression si cela ne cause aucune ambiguïté. On parle alors du sous-ensemble de x défini par F.

4. Voir [28, p. 102], [21, p. 58-59] [6, p.80-81] pour plus d'informations.

Exemple 3.2.1. *Grâce à l'axiome du sous-ensemble, on peut définir l'intersection de deux ensembles. En effet, dans la formule* $\mathfrak{A} \equiv \varphi = z \in y$*, il n'y a pas d'occurrence de* x *on peut alors substituer* F *par* $\mathfrak{A}$ *dans l'axiome* **A**13 *:*

$$\forall x \forall y \exists t \forall z \Big[\ (z \in t) \ \leftrightarrow \ (z \in x \wedge z \in y) \ \Big].$$

On vérifie alors que les éléments appartiennent à l'ensemble t *si et seulement si ils appartiennent à l'ensemble* x *et à l'ensemble* y

$$t = \{z \mid z \in x \wedge z \in y\}$$

On note alors $t = x \cap y$*.*

Définition 3.2.7. *Soient deux ensembles* x *et* y*, l'intersection de* x *avec* y*, notée* $x \cap y$ *est l'ensemble*

$$\{z \mid z \in x \wedge z \in y\}.$$

Théorème 3.2.8. *Si* x *et* y *sont des ensembles, alors les ensembles* $x \cap y$ *et* $y \cap x$ *sont égaux.*

Démonstration. D'après l'axiome **A**13 du sous-ensemble, on sait qu'il existe deux ensembles t et t' tels que

$$\forall z \Big[\ (z \in t) \ \leftrightarrow \ (z \in x \wedge z \in y) \ \Big]$$

et

$$\forall z \Big[\ (z \in t') \ \leftrightarrow \ (z \in y \wedge z \in x) \ \Big].$$

Comme on sait que "$\wedge$" est symétrique, on a les équivalences suivantes

$$\begin{aligned} z \in t &\leftrightarrow z \in x \wedge z \in y \\ &\leftrightarrow z \in y \wedge z \in x \\ &\leftrightarrow z \in t'. \end{aligned}$$

Ainsi, vu l'axiome **A**9 d'extensionnalité, on a bien $t = t'$. □

Une autre façon d'obtenir un nouvel ensemble à partir d'un ensemble x à l'aide de l'axiome de la puissance et de l'axiome du sous-ensemble est de considérer l'ensemble $\{x\}$ qui contient exactement comme élément l'ensemble x.

Définition 3.2.9. *Pour tout ensemble* x *on appelle singleton, et on note* $\{x\}$*, l'ensemble qui vérifie*

$$\{x\} = \Big\{ z \in \mathscr{P}(x) \ \Big| \ z = x \Big\}.$$

Comme par hypothèse x est un ensemble, $\mathscr{P}(x)$ est un ensemble vu **A**12. De plus, $x \in \mathscr{P}(x)$. Ainsi, la définition est bien licite vu l'axiome **A**13 du sous-ensemble. Enfin, par construction, on a bien

$$z \in \{x\} \leftrightarrow z = x.$$

Pour définir l'union d'ensembles, on pourrait être tenté de transposer la définition d'union d'ensembles de la théorie naïve en un axiome.

Exemple 3.2.2 (Axiome de l'union ; première tentative)**.** *Quels que soient les ensembles x et y considérés, il existe un ensemble t dont les éléments sont exactement les éléments des éléments de x et de y*

$$\forall x \forall y\ \exists t\ \forall z (z \in t \leftrightarrow (z \in x\ \vee z \in y)).$$

Cependant, si l'on considère avoir à disposition un ensemble x et que l'on souhaite faire l'union des éléments de cet ensemble, l'axiome n'est pas suffisant car on souhaite exprimer l'ensemble suivant

$$\bigcup x = \{z \mid \exists y (y \in x \wedge z \in y)\ \}$$

L'axiome de l'union est alors le suivant.

A 14 (Axiome de l'union)**.** *Quel que soit l'ensemble x considéré, il existe un ensemble t tel que ses éléments sont les éléments des éléments de x :*

$$\forall x \exists t \forall z \Big[z \in t \leftrightarrow \exists y (z \in y \wedge y \in x)\Big]$$

Définition 3.2.10. *On notera $\bigcup x$ l'ensemble t apparaissant dans l'axiome 14 de l'union.*

Évidement, il faut s'assurer maintenant que l'union de deux ensembles telle qu'énoncée à l'exemple 3.2.2 soit valide.

Proposition 3.2.11. *Soit x et y deux ensembles, alors pour tout z on a l'équivalence suivante*

$$z \in \bigcup\{x, y\}\ \leftrightarrow\ (z \in x \vee z \in y).$$

Démonstration. Soit x et y deux ensembles. Par définition, et vu l'axiome **A** 14 de l'union, être un élément z de $\bigcup\{x, y\}$ signifie qu'il existe un ensemble c tel que $z \in c$ et $c \in \{x, y\}$. Or vu l'axiome **A** 11 de la paire, on en déduit que $c = x$ ou $c = y$. En appliquant ensuite l'axiome **A** 8 de l'égalité, on a que $z \in x$ ou $z \in y$. Formellement, on écrit la preuve comme suit :

$$\begin{aligned} z \in \bigcup\{x, y\} &\leftrightarrow \exists t \Big[z \in t \wedge t \in \{x, y\}\Big] \\ &\leftrightarrow \exists t \Big[z \in t \wedge (t = x \vee t = y)\Big] \\ &\leftrightarrow \exists t \Big[(z \in t \wedge t = x)\ \vee\ (z \in t \wedge t = y)\Big] \\ &\leftrightarrow z \in x \vee z \in y. \end{aligned}$$

Il reste cependant à démontrer la dernière équivalence. Comme annoncé juste avant, le sens "$\rightarrow$" est assuré grâce à l'axiome **A** 8 de l'égalité. En effet, d'une part on a

$$(z \in t \wedge t = x)\ \rightarrow\ (z \in x)$$

vu qu'on a successivement

$$\begin{aligned} z \in t \wedge t = x &\vdash z \in t \\ &\vdash t = x \\ &\vdash (t = x) \to \forall z\Big[(z \in t \to z \in x) \wedge (t \in z \to x \in z)\Big] \\ &\vdash z \in t \to z \in x \\ &\vdash z \in x \end{aligned}$$

et d'autre part, comme on a montré à la proposition 1.5.14 que la proposition

$$\Big[(p \to q) \ \wedge (r \to s)\Big] \to \Big[(p \vee r) \ \to \ (q \vee s)\Big]$$

est une tautologie, on a

$$\Big[(z \in t \wedge t = x) \ \vee \ (z \in t \wedge t = y)\Big] \ \to \ (z \in x \vee z \in y).$$

En résumé, on a

$$\begin{aligned} &\vdash (z \in t \wedge t = x) \ \to \ (z \in x) \\ &\vdash (z \in t \wedge t = y) \ \to \ (z \in y) \\ &\vdash \Big[(z \in t \wedge t = x) \ \to \ (z \in x)\Big] \ \wedge \ \Big[(z \in t \wedge t = y) \ \to \ (z \in y)\Big] \\ &\vdash \Big[(p \to q) \ \wedge (r \to s)\Big] \to \Big[(p \vee r) \ \to \ (q \vee s)\Big] \\ &\vdash \Big[(z \in t \wedge t = x) \ \vee \ (z \in t \wedge t = y)\Big] \ \to \ (z \in x \vee z \in y). \end{aligned}$$

Pour montrer que $(z \in x \vee z \in y) \ \to \ \exists t\Big[(z \in t \wedge t = x) \ \vee \ (z \in t \wedge t = y)\Big]$, on considère d'abord la formule $\mathfrak{A} \equiv (z \in a \wedge a = x)$. Ainsi, comme pour tout x l'axiome **A** 5 assure que $x = x$ est vrai, on a

$$(z \in x) \ \to \ (z \in x \wedge x = x)$$

autrement dit, $(z \in x) \ \to \ \varphi(x)$. Or, vu le théorème 2.3.2, et par transitivité de "$\to$" on a

$$z \in x \to \exists t\Big[\varphi(t)\Big]$$

c'est à dire

$$z \in x \to \exists t\Big[z \in t \wedge t = x\Big]$$

Enfin, il reste à montrer que $\exists c\Big[\varphi(c) \vee \psi(c)\Big]$ est équivalent à $\exists c\Big[\varphi(c)\Big] \vee \exists c'\Big[\psi(c')\Big]$. Ce résultat est déjà établi en 2.5.3. □

Remarque 3.2.12 (Intersection et complémentaire)**.** *En procédant comme précédemment, on peut définir l'intersection d'ensembles et le complémentaire d'un ensemble dans un autre.*

1. *Soient s et t deux ensembles, l'intersection de s avec t, noté $s \cap t$ est une abréviation de $\{z \in s \mid z \in t\}$. La définition a bien un sens car, vu l'axiome du sous-ensemble, on a*

$$\forall s\ \forall t\ \exists y\ \forall z[(z \in y) \ \leftrightarrow\ (z \in s \wedge z \in t)].$$

2. *On peut évidement généraliser les arguments précédents. Étant donné un ensemble non vide x, alors $\bigcap x$ est l'ensemble des éléments qui appartiennent à tous les éléments de x.*
3. *Soient x et y deux ensembles, le complémentaire de x dans y, noté $\complement_y x$, est une abréviation de $\{z \in y \mid \neg(z \in x)\}$. La bonne définition de cet ensemble, c'est une conséquence directe de l'axiome du sous-ensemble.*

Nous voyons de la sorte que les opérations élémentaires usuelles sur les ensembles se trouvent être facilement à disposition dans le contexte de ZF. Il reste à établir que Z-F échappe au paradoxe de Russell.

Théorème 3.2.13. *Il n'existe pas d'ensemble qui contient tous les ensembles.*

Démonstration. Étant donné un ensemble x, on veut montrer qu'il existe un ensemble y qui n'appartient pas à x. Pour cela, on pose

$$y = \{z \in x \mid z \notin z\}.$$

Il s'ensuit qu'alors

$$(y \in y) \ \leftrightarrow\ (y \in x \wedge y \notin y).$$

Donc si $y \in x$, alors $(y \in x) \wedge (y \notin y)$ est équivalent à $y \notin y$ et donc

$$y \in y \ \leftrightarrow\ y \notin y,$$

ce qui est absurde. On en déduit donc que $y \notin x$. □

Une partie substantielle des mathématiques peut alors être définie naturellement dans le contexte de la théorie Z-F. On présente maintenant deux notions mathématiques qui seront utilisées ultérieurement dans ce travail. On a pu, grâce à l'axiome **A**11, définir à l'aide de deux ensembles x et y un nouvel ensemble que l'on peut noter indifféremment $\{x, y\}$ ou $\{y, x\}$. Pour enrichir notre vocabulaire, on voudrait pouvoir définir des ensembles distincts mais contenant les deux mêmes éléments.

Définition 3.2.14. *Pour tous ensembles x et y, on note*

$$(x, y) = \Big\{\{x\}, \{x, y\}\Big\}.$$

On dit de (x, y) que c'est une paire bien ordonnée.

Proposition 3.2.15. *Par la définition 3.2.14 on a*

$$\forall x \forall y \forall z \forall t\Big[\ (x, y) = (z, t) \ \leftrightarrow\ (x = z) \wedge (y = t)\ \Big]$$

Démonstration. Si $x = z$ et $y = t$, l'implication est directement vérifiée. On suppose donc que $(x, y) = (z, t)$, c'est à dire

$$\Big\{\{x\}, \{x, y\}\Big\} = \Big\{\{z\}, \{z, t\}\Big\}.$$

Cela signifie que l'on a d'une part

$$\Big\{\{x\}, \{x, y\}\Big\} \subseteq \Big\{\{z\}, \{z, t\}\Big\}$$

et d'autre part

$$\Big\{\{z\}, \{z, t\}\Big\} \subseteq \Big\{\{x\}, \{x, y\}\Big\}.$$

De la première inclusion, on déduit que

$$\{x\} = \{z\} \text{ ou } \{x\} = \{z, t\} \quad \text{et} \quad \{x, y\} = \{z\} \text{ ou } \{x, y\} = \{z, t\}.$$

Semblablement on déduit de la seconde inclusion que

$$\{z\} = \{x\} \text{ ou } \{z\} = \{x, y\} \quad \text{et} \quad \{z, t\} = \{x\} \text{ ou } \{z, t\} = \{x, y\}.$$

Au final, on obtient bien

$$x = z \ \text{ et } \ y = t$$

comme souhaité. □

Grâce à la notion de paire, on peut définir le produit cartésien de deux ensembles. Naïvement, pour deux ensembles x et y, on définit le produit cartésien $x \times y$ comme étant l'ensemble des paires bien ordonné des éléments de x et de y. Cependant, il faut s'assurer que "l'ensemble des paires" est bien défini.

Proposition 3.2.16. *Si $x, y \in b$ alors*

$$(x, y) \in \mathscr{P}(\mathscr{P}(b))$$

Démonstration. On a successivement

$$\begin{aligned}
&x \in b \ \text{ et } \ y \in b \\
&\{x\} \subseteq b \ \text{ et } \ \{x, y\} \subseteq b \\
&\{x\} \in \mathscr{P}(b) \ \text{ et } \ \{x, y\} \in \mathscr{P}(b) \\
&\Big\{\{x\}, \{x, y\}\Big\} \subseteq \mathscr{P}(b) \\
&\Big\{\{x\}, \{x, y\}\Big\} \in \mathscr{P}(\mathscr{P}(b))
\end{aligned}$$

□

On peut alors définir le produit cartésien.

Définition 3.2.17. *Soit deux ensembles x et y, le produit cartésien, qu'on note $x \times y$, est l'ensemble défini par*

$$x \times y \ = \ \Big\{ w \in \mathscr{P}(\mathscr{P}(x \cup y)) \mid \exists z \in x \exists t \in y [w = (z,t)] \Big\}$$

Définition 3.2.18. *(i) Une relation R est un sous-ensemble de paires ordonnées.*

(ii) Étant donné une relation R, on définit $dom(R)$ comme l'ensemble des éléments x tels que il existe un élément y tel que $(x,y) \in R$.

(iii) Étant donné une relation R, on définit $Im(R)$ comme l'ensemble des éléments y tels que il existe un élément x tel que $(x,y) \in R$.

Définition 3.2.19. *Une application, ou fonction, F est une relation telle que pour tout élément x du domaine, il existe au plus un élément de l'image tel que $(x,y) \in F$.*

Remarque 3.2.20. *La notion de fonction définie ici n'est pas celle primitive de la logique de premier ordre tel que ϵ où $=$. Aussi quand on quantifiera sur une fonction (cf bijection/isomorphisme) on quantifiera bien sur un ensemble.*

On note aussi le fait que les définitions proposées de relation (et d'ensemble domaine et d'ensemble image) et de fonction sont celles de Enderton (cf. [14, pp. 40-42]). Ce choix est légitimé par le fait que l'ouvrage sus-mentionné est la référence principale utilisée pour la construction des nombres naturels présentée dans la partie suivante.

Deuxième partie

Constructions classiques de $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$

Armé désormais d'une méthode, et à l'aide uniquement de ce que l'on sait des ensembles, on se propose de parcourir les constructions classiques des ensembles

(i) $\mathbb{N}$ des nombres naturels,
(ii) $\mathbb{Z}$ des nombres entiers,
(iii) $\mathbb{Q}$ des nombres rationnels,
(iv) $\mathbb{R}$ des nombres réels.

On ne présente pas ici les constructions chronologiquement, révolution après révolution, mais bien un produit fini ; une théorie aboutie, cohérente et satisfaisante. On y insère cependant quand c'est possible quelques considérations historiques et philosophiques. Il s'agit aussi pour nous de parcourir en détail des pans entiers de théorie exposés et parfois effleurées [5], de parachever effectivement l'entreprise de reconstruction de l'édifice mathématique initié lors du bachelier, et surtout de préparer le terrain en vue d'étudier et comparer dans la seconde partie de ce travail ces dernières constructions avec leurs analogues intuitionnistes/constructivistes.

Ce chapitre permet ainsi d'exhiber des mathématiques construites sous l'égide de la logique classique tout en espérant éveiller un intérêt didactique pour l'enseignement de cette matière. En effet, en plus de répondre d'une part au souhait de reprendre la formation des mathématicien.ne.s depuis le début et d'autre part à la volonté de tout reconstruire et démontrer, ce chapitre est prétexte à l'introduction de notions fondamentales. On peut citer par exemple les concepts de groupe, d'anneau, de suite (de Cauchy) ou encore de relation d'équivalence.

Dans ce qui suit, tout ce qui est énoncé est démontré. Les lecteurices qui découvrent cette matière pourraient être quelque peu rebuté.e.s par l'apparence que prennent les démonstrations, souvent longues ou austères. Cependant, elles consistent, dans la très large majorité des cas, en de simples vérifications où le seul travail à fournir est d'écrire les définitions et de se laisser porter par les évidences mathématiques. Attention toutefois à ne pas se méprendre ; il importe de se rendre compte que cette évidence n'est que relative.

Frege dans [15] explique que : "Le concept de nombre entier positif est, estime-t-on, à ce point dépourvu de difficultés qu'on peut en donner la science aux enfants, et que chacun sait exactement de quoi il s'agit sans réfléchir davantage, et sans s'aviser de ce qu'un autre en pense. Mais il manque ici la première condition pour qu'on veuille se mettre à l'étude : savoir qu'on ne sait pas."

D'ailleurs, dans [3] R. Apéry écrit : "un texte mathématique se lit la plume à la main", faisant écho à une opinion défendue par H. Poincaré : "Celui qui possède des textes mathématiques dont il ne comprend pas l'articulation ne possède rien".

5. Par exemple, la construction des réels n'apparaît pas au programme bien qu'elle soit mentionnée en passant dans le cadre des cours de Bloc 1.

Chapitre 4

Construction de $\mathbb{N}$

"Ce qui est démontrable ne doit pas être admis sans démonstration" Dedekind [11]

Pour rappel, le projet est de suivre le mouvement formaliste classique. Dès lors, n'ayant à disposition que la logique et la théorie des ensembles, la définition des nombres doit découler de celles-ci uniquement. Ce chapitre propose une construction de l'ensemble $\mathbb{N}$ des nombres naturels fondée sur la notion d'ensemble inductif. Cette construction mène à la définition de système de Peano. Une fois l'ensemble des naturels donné, on munit celui-ci d'opérations et d'un ordre. Nous suivons ici l'ouvrage [14] de H. B. Enderton.

4.1 Ensembles Inductifs

Comme annoncé, l'objectif est de parcourir une construction classique de l'ensemble des nombres naturels tout en évitant de recourir à la 'nature' de ces derniers, toujours élusive. On attribue souvent au mathématicien hongrois John von Neumann (voir [2] ou encore [14]) la définition inductive, astucieuse et complètement ensembliste suivante

$$\begin{cases} 0 = \emptyset; \\ 1 = \{0\} = \{\emptyset\}; \\ 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}; \\ 3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}; \\ 4 = \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}; \\ \dots \end{cases}$$

qui s'interprète de la manière suivante :

- on convient de définir l'entier 0 comme étant l'ensemble vide,
- l'entier 1 est l'ensemble $\{\emptyset\}$ dont l'unique élément est l'ensemble vide,
- l'entier 2 est l'ensemble dont les éléments sont $\emptyset$ et l'ensemble $\{\emptyset\}$
- ...

Bien que satisfaisante du point de vue ensembliste, cette définition perd en pertinence dès qu'il s'agit d'interpréter, comme souvent en mathématiques, la signification du symbole "...". Cette première tentative permet néanmoins de dégager deux définitions qui permettront par la suite, au prix d'un axiome, de définir les nombres naturels.

Définition 4.1.1. *Soit un ensemble A. Le successeur de A, noté A^+ est défini par*

$$A^+ = A \cup \{A\}.$$

Vu l'axiome **A**14 de l'union et la définition du singleton, comme A est un ensemble, A^+ est aussi un ensemble.

Définition 4.1.2. *Un ensemble A est dit inductif si*

1. $\emptyset \in A$;
2. $\forall a[a \in A \rightarrow a^+ \in A]$.

Il n'est pas possible de démontrer l'existence d'un ensemble inductif, on postule donc l'existence d'un tel ensemble par l'axiome suivant.

A 15 (Axiome de l'infini)**.** *Il existe un ensemble inductif.*

On peut à présent définir ce qu'est un nombre naturel.

Définition 4.1.3. *Un nombre naturel est un ensemble qui appartient à tous les ensembles inductifs.*

Cette situation n'est pas sans rappeler les propos de Dedekind. Selon lui, "même les entiers ne sont pas donnés par la nature", il s'agit en fait d'une "création libre de l'esprit humain" [1]. La notion de nombre naturel n'est pas purement dérivée de la logique, comme le souhaitait Frege, car il faut asserter l'existence d'un tel ensemble.

Remarque 4.1.4. *Avec cette définition, on retrouve les naturels définis par von Neumann :*

1. *$\emptyset$ est un nombre naturel : en effet, si A un ensemble inductif, par définition $\emptyset \in A$ et donc $\emptyset$ appartient à tous les ensembles inductifs ;*
2. *$\emptyset^+ = \{\emptyset\}$ est un nombre naturel : soit A un ensemble inductif, comme $\emptyset \in A$, on a, par définition $\emptyset^+ \in A$ et donc $\emptyset^+$ appartient à tous les ensembles inductifs ;*

   ...
3. *si n est un nombre naturel, alors n^+ est un nombre naturel. En effet, si A est un ensemble inductif, comme n est un nombre naturel, $n \in A$ et donc $n^+ \in A$. Ainsi, n^+ appartient à tous les ensembles inductifs. Ce point sera abordé plus en profondeur par la suite.*

Théorème 4.1.5 (Existence et Unicité)**.** *Il existe un unique ensemble N tel que ses éléments sont exactement les nombres naturels.*

1. Voir [13, p. 12].

Démonstration. Soit A_0 un ensemble inductif dont l'existence est garantie par l'axiome de l'infini. On pose alors

$$N = \cap\{A | A \text{ est inductif et } A \subseteq A_0\}.$$

D'abord, vu l'axiome A13 du sous-ensemble, on a que N est un ensemble. Ensuite, N contient exactement tous les nombres naturels. En effet, si $n \in N$ alors, par définition de N, n appartient à tous les ensembles inductifs. Donc n est un nombre naturel. Réciproquement, si n est un nombre naturel, alors n appartient à tous les ensembles inductifs et donc à N.

Enfin, si N' est un ensemble qui contient exactement tous les naturels, alors, vu l'axiome **A**9 d'extensionnalité, on a $N = N'$. □

L'ensemble N ainsi construit sera notre ensemble des naturels. On notera à présent cet ensemble $\mathbb{N}$.

Définition 4.1.6. *L'ensemble $\mathbb{N}$ des naturels est l'unique ensemble qui contient tous les naturels.*

Pour rappel, on a montré dans l'exemple 4.1.4 que $\emptyset$ est un naturel et que si n est un naturel, alors n^+ est un naturel. On peut en fait formuler le résultat suivant.

Proposition 4.1.7. *L'ensemble $\mathbb{N}$ est inductif et est inclus dans tout ensemble inductif.*

Démonstration. Comme susmentionné, on sait déjà que $\emptyset \in \mathbb{N}$ et que si $n \in \mathbb{N}$ alors $n^+ \in \mathbb{N}$. Dès lors, $\mathbb{N}$ est inductif. Le deuxième point découle directement de la construction de $\mathbb{N}$ donnée dans la preuve du théorème précédent. □

Le théorème qui suit permet de légitimer ce qui est habituellement présenté comme la démonstration par récurrence et sera dès lors très fréquemment invoqué dans la suite de ce travail.

Théorème 4.1.8 (Principe d'induction)**.** *Tout sous-ensemble inductif de $\mathbb{N}$ coïncide avec $\mathbb{N}$.*

Démonstration. Soit N un sous-ensemble inductif non vide de $\mathbb{N}$. On montre, par double induction, que $N = \mathbb{N}$. D'une part, on a, par définition de N, $N \subseteq \mathbb{N}$. D'autre part, comme N est inductif, on a $\mathbb{N} \subseteq N$ vu la proposition 4.1.7. □

Comme susmentionné, le principe d'induction permet de formaliser la méthode de démonstration par récurrence. En effet, on peut montrer qu'une proposition P est vraie pour tous les naturels : $\forall n \in \mathbb{N}[\mathfrak{A}]$, en procédant comme suit :
On définit l'ensemble T par

$$T = \{n \in \mathbb{N} \mid \mathfrak{A}\}.$$

Il s'agit bien d'un ensemble vu l'axiome **A**13 du sous-ensemble. Dès lors, si on arrive à prouver que T est inductif, alors on a $T = \mathbb{N}$ et donc $\forall n \in \mathbb{N}[\mathfrak{A}]$. Or, montrer que T est inductif revient à montrer que l'on a (i) $\emptyset \in T$, et (ii) que si $n \in T$ alors $n^+ \in T$. On retrouve alors le principe naïf de démonstration par récurrence. Le théorème suivant est un exemple du principe de démonstration par récurrence.

Théorème 4.1.9. *Tout nombre naturel qui n'est pas* 0 *est le successeur d'un nombre naturel.*

Démonstration. Soit l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid n = 0 \text{ ou } \exists p \in \mathbb{N}[n = p^+]\}.$$

On montre que l'ensemble T est inductif ; c'est à dire, conformément à la définition 4.1.2, que

- $0 \in T$ par définition de T ;
- induction : soit $n \in T$, alors il existe $p \in \mathbb{N}$ tel que $n = p^+$, et donc $n^+ = (p^+)^+$ où p^+ est un naturel. Donc $n^+ \in T$.

Donc, T est sous-ensemble inductif de $\mathbb{N}$. Par le théorème 4.1.8 on a $T = \mathbb{N}$. □

Il reste à présent à prouver un résultat essentiel concernant l'application successeur : son caractère injectif. En effet, lorsque Peano formule ses axiomes, il exige que l'application successeur soit injective : " deux nombres distincts a et b possèdent deux successeurs a^+ et b^+ distincts ; " (cf. [31]). Pour ce faire, et conformément à l'approche de [14], on introduit d'abord la notion d'ensemble transitif.

Définition 4.1.10. *Un ensemble A est dit transitif si*

$$x \in a \in A \to x \in A.$$

Exemple 4.1.1.

1. *L'ensemble $A = \{0, \{0\}, \{0, \{0\}\}\}$ est transitif : soit $a \in A$ et $x \in a$,*
   a) *si $a = \{0\}$, alors $x = 0$ et $x \in A$;*
   b) *si $a = \{0, \{0\}\}$, alors $x = 0$ ou $x = \{0\}$. Là encore $x \in A$;*
   c) *si $a = 0$ alors x n'est pas défini. Il n'y a donc rien à vérifier.*
2. *L'ensemble $B = \{0, \{\{0\}\}\}$ n'est pas transitif. En effet, $\{0\} \in \{\{0\}\} \in B$ et $\{0\} \notin B$.*

Voici quelques caractérisations des ensembles transitifs.

Proposition 4.1.11. *Les propositions suivantes sont équivalentes.*

(i) $x \in a \in A \to x \in A$;

(ii) $\bigcup A \subseteq A$;

(iii) $a \in A \to a \subseteq A$;

(iv) $A \subseteq \mathcal{P}(A)$.

Démonstration.

- $(i) \to (ii)$: soit $x \in \bigcup A$. Par définition de $\bigcup$, il existe $a \in A$ tel que $x \in a$. On a donc $x \in a \in A$. Dès lors, vu (i), $x \in A$. Donc $\bigcup A \subseteq A$.

- $(ii) \to (iii)$: soit $a \in A$, comme $\bigcup A \subseteq A$, on a donc que $x \in a \to x \in A$ et donc $a \subseteq A$.
- $(iii) \to (vi)$: soit $a \in A$, vu (iii) $a \subseteq A$ et donc $a \in \mathcal{P}(A)$.
- $(vi) \to (i)$: soit $A \subseteq \mathcal{P}(A)$; cela signifie que A est un ensemble de sous-ensembles de A. Dès lors, si x et a sont tels que $x \in a \in A$ alors comme x est un élément de a qui est un sous-ensemble de A, x est un élément de A : $x \in A$. □

Proposition 4.1.12. *Si A est un ensemble transitif, alors*

$$\bigcup(A^+) = A.$$

Démonstration. On a successivement

$$\begin{aligned}\bigcup(A^+) &= \bigcup(A \cup \{A\}) \\ &= (\bigcup A) \cup (\bigcup\{A\}) \\ &= (\bigcup A) \cup A = A.\end{aligned}$$

La dernière étape est justifiée par le point (ii) de la proposition précédente. □

Proposition 4.1.13. *Tout nombre naturel est un ensemble transitif.*

Démonstration. On montre que l'ensemble $T = \{n \in \mathbb{N} \mid n \text{ est transitif }\}$ est inductif.

- $0 \in T$: c'est immédiat vu que $\bigcup 0 = 0 \subseteq 0$. On applique alors le point (ii) de la proposition 4.1.11 ;
- induction : soit $n \in T$. Comme n est transitif, vu la proposition précédente on a

  $$\bigcup(n^+) = n \subseteq n^+,$$

  et donc, encore vu la proposition 4.1.11, n^+ est transitif.

On conclut par le principe d'induction (Théorème 4.1.8). □

On est maintenant en mesure de démontrer que l'application successeur est injective.

Théorème 4.1.14. *L'application successeur est injective.*

Démonstration. On considère deux naturels m et n pour lesquels $m^+ = n^+$. On en déduit immédiatement que $\bigcup(m^+) = \bigcup(n^+)$ par l'axiome **A**8 de l'égalité. Or m et n sont des naturels et sont donc transitifs par la proposition 4.1.13. Ainsi, on obtient

$$m = \bigcup m^+ = \bigcup n^+ = n$$

et finalement l'injectivité annoncée. □

Proposition 4.1.15. *Pour tout naturel n, on vérifie que $n \notin n$.*

Démonstration. On procède par récurrence. Soit donc l'ensemble T défini par

$$T = \{n \in \mathbb{N} \,|\, n \notin n\}$$

- $0 \in T$: c'est évident, vu la définition de 0 ;
- induction : on suppose que $n \notin n$. Alors par définition du successeur, on a $n^+ = n \cup \{n\}$ et par définition 3.2.11 de l'union, on a

$$n^+ \in n \cup \{n\} \leftrightarrow n^+ \in n \text{ ou } n^+ \in \{n\}.$$

Or, si $n^+ = n$, puisqu'on a $n \in n^+$, par définition du successeur, on a alors $n \in n$, ce qui est contraire à l'hypothèse sur n. Donc il n'est pas possible que $n^+ \in \{n\}$. D'autre part, si $n^+ \in n$, alors puisqu'on a toujours $n \in n^+$, on a $n \in n^+ \in n$, puis $n \in n$ par transitivité de n (voir la proposition 4.1.13), ce qui est contraire à l'hypothèse. On en déduit donc que $n^+ \notin n^+$. □

Présentons encore un petit lemme qui sera utilisé dans la suite.

Lemme 4.1.16. *Pour tout naturel n, on a $0 \in n^+$.*

Démonstration. On procède par récurrence sur n. Soit donc l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid 0 \in n^+\}.$$

- $0 \in T$: en appliquant la définition 4.1.1 du successeur à 0 on a

$$0^+ = 0 \cup \{0\}$$

Et comme $0 \in \{0\}$, par définition de $\cup$ on a bien $0 \in 0^+$;
- induction : soit $n \in T$, on montre qu'alors $n^+ \in T$. D'une part on a $n \in n^+$ et $0 \in n$ par hypothèse, et d'autre part on a établi en 4.1.13 que tout naturel est un ensemble transitif. Par conséquent $0 \in n^+$:

$$0 \in n \in n^+ \rightarrow 0 \in n^+.$$ □

4.2 Systèmes de Peano et Récursion sur $\mathbb{N}$

Définition 4.2.1. *Un système de Peano est la donnée d'un triplet $\langle N, F, e\rangle$ où N est un ensemble non vide, F une application de N dans N et e un élément de N tel.le que*

(i) $e \notin Im(F)$,

(ii) F *est injectif,*

(iii) si A est sous-ensemble de N contenant e et stable par F, alors $A = N$.

Dans cette section, on montre que tout système de Peano est isomorphe à la structure $\langle \mathbb{N}, \cdot^+, 0\rangle$ au sens naturel du terme (cf. infra).

La preuve de ce résultat repose sur le théorème de récursion formulé ci-dessous. Ce résultat permettra également, dans la section suivante, de définir les opérations sur $\mathbb{N}$.

Théorème 4.2.2 (Récursion)**.** *Soient un ensemble A non vide, un élément a de A et une fonction $F : A \to A$. Alors, il existe une unique fonction $h : \mathbb{N} \to A$ dont le domaine est $\mathbb{N}$ et telle que*

(i) $h(0) = a$;

(ii) $h(n^+) = F(h(n)), \forall n \in \mathbb{N}$.

Pour les besoins de la démonstration, définissons d'abord la notion de fonction acceptable et démontrons un résultat relatif à celle-ci.

Définition 4.2.3. *Avec les notations du théorème 4.2.2, on définit une fonction acceptable comme étant une fonction f vérifiant*

(0) $dom(f) \subset \mathbb{N}$ *et* $Im(f) \subseteq A$;

(i) $0 \in dom(f) \Rightarrow f(0) = a$;

(ii) $n^+ \in dom(f) \Rightarrow \Big(n \in dom(f)$ *et* $f(n^+) = F(f(n))\ \Big)$.

Comme exemples de fonctions acceptables, on peut citer $\{(0, a)\}$, $\{(0, a), (1, F(a))\}$, ...

Le lemme suivant montre que des fonctions acceptables coïncident nécessairement sur l'intersection de leurs domaines de définition. Il sera utile pour construire une fonction acceptable ayant un domaine égal à $\mathbb{N}$, ce qui est précisément le contenu de la partie existence du théorème 4.2.2.

Lemme 4.2.4. *Soient f et g deux fonctions acceptables. Pour tout naturel n, si $n \in dom(f) \cap dom(g)$, alors $f(n) = g(n)$.*

Démonstration. Soient donc f et g deux fonctions acceptables. L'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid (n \in dom(f) \cap dom(g)) \Rightarrow (f(n) = g(n))\}$$

est inductif :

- $0 \in T$: en effet, si $0 \in dom(f) \cap dom(g)$ alors, comme f et g sont acceptables on a aussi $f(0) = a = g(0)$;
- induction : supposons $n \in T$. Si $n^+ \in dom(f) \cap dom(g)$, alors $n \in dom(f) \cap dom(g)$ et $f(n^+) = F(f(n)) = F(g(n)) = g(n^+)$, par le point (ii) de la définition 4.2.3. Sinon, $n^+ \notin dom(f) \cap dom(g)$ mais l'implication reste vraie et donc $n^+ \in T$.

On conclut par le principe d'induction. □

On peut à présent passer à la démonstration du théorème proprement dite.

Preuve du théorème 4.2.2. On opère en cinq étapes. D'abord on définit un certain objet h, qui "prolonge" en quelque sorte toutes les fonctions acceptables. On montre ensuite que h est une fonction acceptable dont le domaine est $\mathbb{N}$ et que l'ensemble image de h est inclus dans A. On a alors bien l'existence souhaitée. Le dernier point consiste à montrer que h est l'unique fonction possible.

1) Définition de h. Soit $\mathscr{H}$ l'ensemble de toutes les fonctions acceptables ; on pose

$$h = \bigcup \mathscr{H}.$$

2) L'objet h est une fonction. En effet, h est une relation de $\mathbb{N}$ dans A. Explicitement, on peut l'écrire

$$h = \bigcup \mathscr{H} \subseteq \{(x, y) \mid x \in \mathbb{N} \text{ et } \exists g \text{ acceptable tel que } y = g(x)\},$$

De plus, soient (n, y_1) et (n, y_2) deux éléments de h. Alors, par définition, il existe deux fonctions acceptables f_1 et f_2 telles que $y_1 = f_1(n)$ et $y_2 = f_2(n)$. Vu le lemme 4.2.4, on a donc $y_1 = y_2$ et donc h est une fonction.

3) La fonction h est acceptable. Vu la définition de h, il est clair que $dom(h) \subseteq \mathbb{N}$ et $Im(h) \subseteq A$. Comme $g = \{(0, a)\}$ est acceptable, $g \subseteq h$ et donc $0 \in dom(h)$ et $h(0) = a$. Si $n^+ \in dom(h)$ cela signifie qu'il existe g acceptable tel que $n^+ \in dom(g)$. Par définition de h, on a alors $h(n^+) = g(n^+)$. Par définition des fonctions acceptables, on a aussi $n \in dom(g)$ et $g(n^+) = F(g(n))$. On en déduit que n appartient au domaine de h et que $h(n) = g(n)$. On a alors bien

$$h(n^+) = g(n^+) = F(g(n)) = F(h(n)).$$

4) On a $dom(h) = \mathbb{N}$ et $Im(h) \subseteq A$. On sait déjà que $Im(h) \subseteq A$ et que $0 \in dom(h)$. On montre que $dom(h) = \mathbb{N}$ en prouvant que $dom(h)$ est inductif. On suppose que $n \in dom(h)$. Si $n^+ \notin dom(h)$ on considère alors la fonction g définie par :

$$g = h \cup \{(n^+, F(h(n)))\}.$$

Puisque $n^+ \notin dom(h)$, g est une fonction. De plus, g est acceptable vu que

(i) $dom(g) \subseteq \mathbb{N}$ et $Im(g) \subseteq A$, par définition de g ;

(ii) $0 \in dom(g)$ et $g(0) = h(0) = a$;

(iii) si $k^+ \in dom(g)$, alors soit $k^+ = n^+$, soit $k^+ \neq n^+$. Dans le premier cas, on a $n = k$ et, par construction,

$$g(k^+) = g(n^+) = F(h(n)) = F(g(k)).$$

Dans le second cas, $k^+ \in dom(h)$ et donc

$$g(k^+) = h(k^+) = F(h(k)) = F(g(k)).$$

Donc, comme g est acceptable, $g \subseteq h$ et donc $n^+ \in dom(h)$, ce qui mène à une absurdité. Donc $n^+ \in dom(h)$ et $dom(h)$ est inductif. Il en résulte que $dom(h) = \mathbb{N}$.

5) La fonction h est unique. Soient h_1 et h_2 deux fonctions vérifiant le théorème. Ce sont alors deux fonctions acceptables dont le domaine est $\mathbb{N}$. Par le lemme 4.2.4, elles sont égales.

On a donc démontré l'existence d'une unique fonction ayant les propriétés demandées. □

Le théorème de récursion nous permettra de définir les opérations d'addition et de multiplication. Ici, il permet déjà de prouver qu'il n'existe, à isomorphisme près, qu'un seul système de Peano.

Théorème 4.2.5 (Equivalence des systèmes de Peano)**.** *Soit $\langle N, F, e\rangle$ un système de Peano. Alors il existe une bijection $h : \mathbb{N} \to N$ telle que*

(i) $h(0) = e$,

(ii) $h(n^+) = F(h(n))$.

En d'autres termes, la bijection h échange d'une part 0 et e, et d'autre part le "successeur" et la fonction F.

Démonstration. Par le théorème de la récursion, on sait déjà qu'il existe une unique fonction $h : \mathbb{N} \to N$ satisfaisant les conditions (i) et (ii) de l'énoncé. Il reste donc à montrer que h est une bijection.

- Pour montrer que $Im(h) = N$, il suffit de montrer que $Im(h)$ contient e et est stabilisé par F, vu la définition 4.2.1. On a d'une part $e \in Im(h)$ vu que $h(0) = e$. D'autre part, si $y \in Im(h)$, il existe un naturel n tel que $y = h(n)$. On sait alors que

$$h(n^+) = F(h(n)) = F(y).$$

  Donc $F(y) \in Im(h)$ et $Im(h)$ est bien stabilisé par F.

- Pour montrer que h est injectif, on considère le domaine d'injectivité de h défini par

$$T = \{n \in \mathbb{N} \mid \forall m \neq n, h(m) \neq h(n)\}.$$

  On cherche à établir que T est inductif. Vu le théorème 4.1.9, on sait que pour tout $n \neq 0$ il existe p tel que $n = p^+$ et donc, par définition d'un système de Peano, on a

$$h(n) = h(p^+) = F(h(p)) \neq e.$$

  On a donc bien $0 \in T$.
  Ensuite, soit $n \in T$ et montrons que n^+ appartient à T. Si $p \in \mathbb{N}$ est tel que $h(n^+) = h(p)$, on a $p \neq 0$ car $h(0) = e$ et comme on vient de le voir, $h(n^+) \neq e$. Donc il existe un naturel k tel que $p = k^+$. Par définition de h et de T et comme F est injectif (par définition des systèmes de Peano), on a les implications suivantes

$$\begin{aligned} h(n^+) = h(p) &\to F(h(n)) = F(h(k)) \\ &\to h(n) = h(k) \\ &\to n = k \\ &\to n^+ = k^+ = p \end{aligned}$$

  Ainsi, $n^+ \in T$ et on en conclut que T est inductif. Ce qui montre bien que h est injectif sur $\mathbb{N}$. □

4.3 Arithmétique de Peano

Cette section est dédiée à la définition et à l'étude des propriétés des opérations d'addition et de multiplication usuelles définies sur l'ensemble des naturels $\mathbb{N}$. Ces définitions reposent sur le théorème 4.2.2 de récursion.

Remarque 4.3.1. *Dans cette section, on considère l'opération successeur (4.1.1) restreint à* $\mathbb{N}$ *:*

$$\cdot^+ = \{(m,n) \mid m \in \mathbb{N} \ \wedge n \in \mathbb{N} \ \wedge n = m^+\}$$

Ainsi, $\cdot^+$ *est une fonction de* $\mathbb{N}$ *dans* $\mathbb{N}$*.*

Dès lors, en vertu du théorème 4.2.2 de récursion, appliqué à la fonction $\cdot^+$ de $\mathbb{N}$ dans $\mathbb{N}$, on peut alors poser la définition suivante.

Définition 4.3.2. *Pour tout naturel* n*, on note* h_n *l'unique fonction de* $\mathbb{N}$ *dans* $\mathbb{N}$ *telle que*

(i) $h_n(0) = n$ *;*

(ii) $h_n(m^+) = (h_n(m))^+$*.*

Pour des raisons de commodité, on notera souvent $h_n^+(m)$ *au lieu de* $(h_n(m))^+$*.*

On est maintenant en mesure de définir la somme de deux naturels.

Définition 4.3.3. *L'addition, ou somme,* $+$ *est la relation définie sur le produit cartésien* $\mathbb{N} \times \mathbb{N}$ *par*

$$+ = \left\{\Big((m,n),p\Big) \mid m \in \mathbb{N} \ \wedge n \in \mathbb{N} \ \wedge p = h_m(n)\right\}.$$

Pour tout $m, n \in \mathbb{N}$*, on notera* $m + n$ *au lieu de* $+(m,n)$*.*

Comme l'application $+$ est définie pour tout couple de naturels et comme elle est à image dans $\mathbb{N}$, on dit qu'elle est binaire, interne et partout définie. On note que, à l'instar de la somme, les opérations binaires qui sont usuellement étudiées ont une notation spécifique et semblable à celle de $+$[2]. Ainsi, on écrira plus volontiers $a \star b$ au lieu de $f(a,b)$.

Le travail consiste maintenant à montrer que l'opération $+$ ainsi définie a les propriétés attendues.

Lemme 4.3.4. *Pour tous naturels* m *et* n*, on a*

(i) $m + 0 = m = 0 + m$ *;*

(ii) $m + n^+ = (m+n)^+$ *:*

(iii) $m + n^+ = m^+ + n$*.*

Démonstration.

2. Comme on le verra pour le produit

(*i*) Par définition, on sait déjà que pour tout naturel m on a $m + 0 = h_m(0) = m$. On montre par induction qu'on a aussi $m = 0 + m$. Soit donc l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid 0 + n = n\}.$$

- $0 \in T$: c'est évident, vu la définition de $+$;
- induction : soit $p \in T$, il s'ensuit que $0 + p^+ = (0 + p)^+ = p^+$.

(*ii*) Il s'agit de la réécriture de la définition de $+$:

$$m + n^+ = h_m(n^+) = h_m^+(n) = (m + n)^+.$$

(*iii*) On procède par induction sur n. Soient $m \in \mathbb{N}$ et $T = \{n \in \mathbb{N} \mid m + n^+ = m^+ + n\}$.

- $0 \in T$: vu les deux points précédents, on a

$$\begin{aligned} m + 0^+ &= (m + 0)^+ \\ &= (0 + m)^+ \\ &= 0 + m^+ \\ &= m^+ + 0. \end{aligned}$$

- induction : si $k \in T$, on a successivement

$$\begin{aligned} m + k^{++} &= (m + k^+)^+ \\ &= (m^+ + k)^+ \\ &= m^+ + k^+. \end{aligned}$$

On conclut comme d'habitude par le principe d'induction. □

Notons que dans l'axiomatique de Peano, ce sont les points (*i*) et (*ii*) du lemme qui font office de définition pour l'opération $+$.

Proposition 4.3.5.

(i) Pour tout naturel m, n et p on a

$$(m + n) + p = m + (n + p).$$

(ii) Pour tou t naturel m et n on a

$$m + n = n + m.$$

Démonstration.

(*i*) On utilise le principe d'induction sur p. Soit T l'ensemble défini comme suit :

$$T = \{p \in \mathbb{N} \mid (m + n) + p = m + (n + p)\}.$$

- $0 \in T$: par définition on a successivement

$$\begin{aligned}(m+n)+0 &= h_{m+n}(0)\\ &= m+n\\ &= h_m(n)\\ &= h_m(n+0)\\ &= m+(n+0).\end{aligned}$$

- induction : On suppose maintenant que $k \in T$. Par définition, on a

$$(m+n)+k^+ = h_{m+n}(k^+).$$

de sorte que, vu le point (ii) du lemme 4.3.4 (ou la définition de h_{m+n}), on a

$$h_{m+n}(k^+) = h^+_{m+n}(k)$$

et, comme par hypothèse $(m+n)+k = m+(n+k)$, on a

$$((m+n)+k)^+ = (m+(n+k))^+$$

c'est à dire

$$h^+_{m+n}(k) = h^+_m((n+k)).$$

À nouveau, vu le point (ii) du lemme, on a

$$\begin{aligned}h^+_m((n+k)) &= h_m((n+k)^+)\\ &= h_m(n+k^+).\end{aligned}$$

Ainsi, vu la transitivité de "=", on a

$$h_{m+n}(k^+) = h_m(n+k^+),$$

c'est à dire

$$(m+n)+k^+ = m+(n+k^+).$$

Donc, $k^+ \in T$ et on conclut.

(ii) Soit $m \in \mathbb{N}$. L'ensemble $T = \{n \in \mathbb{N} \mid m+n = n+m\}$ est inductif.

- $0 \in T$: c'est évident vu le point (i) du lemme 4.3.4 ;
- induction : Soit $n \in T$. Vu les points (ii) et (iii) du lemme 4.3.4, on a successivement

$$\begin{aligned}m+n^+ &= (m+n)^+\\ &= (n+m)^+\\ &= n^+ + m.\end{aligned}$$

□

Les propriétés démontrées dans ce théorème sont d'une très grande utilité et se retrouvent dans de nombreuses structures. C'est pourquoi on introduit les définitions suivantes.

Définition 4.3.6. *Une opération $\star$ interne, binaire et partout définie sur un ensemble A est associative si pour tous éléments a, b et c de A on a*

$$(a \star b) \star c = a \star (b \star c).$$

On note au passage que dans le cas où l'opération est associative, l'usage des parenthèses n'est dès lors plus nécessaire. Les expressions "$(a \star b) \star c$" et "$a \star (b \star c)$" étant égales, on peut noter simplement "$a \star b \star c$".

Définition 4.3.7. *Une opération $\star$ interne binaire et partout définie sur une ensemble A est commutative si pour tous éléments a et b de A, on a*

$$a \star b = b \star a.$$

Après la présentation de l'opération d'addition vient ensuite la définition du produit. On applique à présent le théorème 4.2.2 de la récursion à la fonction h_n. Ainsi, on définit le "produit par tout naturel n".

Définition 4.3.8. *Pour tout naturel n, on note p_n l'unique fonction vérifiant*

$$p_n : \mathbb{N} \to \mathbb{N} : \begin{cases} p_n(0) = 0 \\ p_n(m^+) = h_n(p_n(m)) \end{cases}$$

La fonction décrite ci-dessus permet de définir l'opération binaire de multiplication et d'en déduire ses propriétés principales.

Définition 4.3.9. *Le produit, ou multiplication, sur $\mathbb{N}$ est l'opération binaire définie par*

$$\cdot = \left\{ \Big((n, m), p \Big) \;\middle|\; n \in \mathbb{N} \ \wedge\ m \in \mathbb{N} \ \wedge\ p = p_n(m) \right\}$$

On notera alors $n \cdot m = p$ au lieu de $\cdot(m, n) = p$.

À nouveau, on montre que la définition de l'opération de multiplication vérifie les axiomes de Peano.

Proposition 4.3.10. *Pour tout naturel $m, n \in \mathbb{N}$, on a :*

(i) $m \cdot 0 = 0 = 0 \cdot m$;

(ii) $m \cdot n^+ = m \cdot n + m$.

Démonstration.

(*i*) Par définition de p_m on a $m \cdot 0 = p_m(0) = 0$. Pour montrer que $0 = 0 \cdot m$, on procède par induction sur l'ensemble T défini par

$$T = \{m \in \mathbb{N} \mid 0 \cdot m = 0\}.$$

- $0 \in T$: cela est immédiat vu la définition du produit.
- induction : si m un élément de T, on a par définition du produit

$$\begin{aligned} 0 \cdot m^+ &= h_0(p_0(m)) \\ &= 0 + 0 \cdot m \end{aligned}$$

et comme par hypothèse $0 \cdot m = 0$ on a bien $0 \cdot m^+ = 0$.

(*ii*) Il s'agit d'une réécriture de la définition. En effet, on a $m \cdot n = p_m(n)$ quels que soient m et n et donc

$$m \cdot n^+ = p_m(n^+) = h_m(p_m(n)) = m + p_m(n) = m + m \cdot n.$$

On conclut vu la commutativité de $+$. □

En plus de propriétés propres au produit comme la commutativité et l'associativité, semblablement à la somme, que l'on démontre ci-après, on définit une autre propriété relative aux deux opérations simultanément : la distributivité du produit sur la somme.

Définition 4.3.11. *Soient deux opérations binaires $\star$ et $\bullet$, internes et partout définies sur un ensemble A. On dit que $\star$ est distributive par rapport à $\bullet$ si pour tous éléments a, b et c de A on a*

$$a \star (b \bullet c) = (a \star b) \bullet (a \star c).$$

Remarque 4.3.12. *Afin de ne pas alourdir l'écriture avec des parenthèses, on convient d'un ordre de priorité pour les opérations. Si $\star$ est distributive par rapport à $\bullet$ alors on dit qu'on effectue d'abord l'opération $\star$ puis l'opération $\bullet$:*

$$a \star b \bullet a \star c = (a \star b) \bullet (a \star c).$$

Théorème 4.3.13. *Le produit sur $\mathbb{N}$ est*

(i) commutatif ;

(ii) distributif par rapport à la somme ;

(iii) associatif.

Démonstration.

(*i*) On applique le principe d'induction sur l'ensemble

$$T = \{m \in \mathbb{N} \mid n \in \mathbb{N} \to m \cdot n = n \cdot m\}.$$

En effet, si T est inductif on a bien que pour tout m et pour tout n, $m \cdot n = n \cdot m$.

- $0 \in T$: Il s'agit de montrer que pour tout n on a $0 \cdot n = 0 = n \cdot 0$. Or ce fait est établi au point (i) de la proposition 4.3.10.
- induction : Soit $m \in T$. On montre que pour tout n on a $m^+ \cdot n = n \cdot m^+$. Là encore on procède par induction. Soit donc l'ensemble S défini par

$$S = \{n \in \mathbb{N} \,|m^+ \cdot n = n \cdot m^+\}.$$

  - $0 \in S$: à nouveau, ce fait est établi au point (i) de la proposition 4.3.10.
  - induction : soit $n \in S$. Par définition, on a

$$m^+ \cdot n^+ = m^+ \cdot n + m^+$$

    et, par hypothèse, $m^+ \cdot n = n \cdot m^+$. En développant à nouveau l' expression $n \cdot m^+$ et en utilisant l'associativité de $+$, on a

$$m^+ \cdot n^+ = n \cdot m + n + m^+.$$

    D'autre part, on a aussi par définition

$$n^+ \cdot m^+ = n^+ \cdot m + n^+.$$

    Puisque $m \in T$, on a finalement

$$n^+ \cdot m^+ = m \cdot n^+ + n^+ = m \cdot n + m + n^+.$$

    Puisque par hypothèse, $n \cdot m = m \cdot n$, vu la commutativité de l'addition et le point (iii) du lemme 4.3.4, on a finalement

$$m^+ \cdot n^+ = n^+ \cdot m^+.$$

  On a donc bien montré que pour tout n on a $m^+ \cdot n = n \cdot m^+$. On en conclut que l'ensemble S, puis l'ensemble T est inductif.

(ii) Soient $a, b \in \mathbb{N}$, pour tout $n \in \mathbb{N}$, on a

$$n \cdot (a + b) = n \cdot a + n \cdot b.$$

On procède par récurrence sur n. Soit alors l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid n \cdot (a + b) = n \cdot a + n \cdot b\}.$$

- $0 \in T$: cela découle directement de la définition du produit et de la somme.
- induction : soit $n \in T$, grâce à la commutativité du produit établie au point précédent, et vu la définition du produit on a

$$\begin{aligned} n^+ \cdot (a + b) &= (a + b) \cdot n^+ \\ &= (a + b) \cdot n + (a + b) \\ &= n \cdot (a + b) + (a + b). \end{aligned}$$

Mais alors, comme par hypothèse on a $n \cdot (a+b) = n \cdot a + n \cdot b$ on a successivement

$$\begin{aligned} n^+ \cdot (a+b) &= n \cdot (a+b) + (a+b) \\ &= n \cdot a + n \cdot b + a + b \\ &= (a \cdot n + a) + (b \cdot n + b) \\ &= a \cdot n^+ + b \cdot n^+. \end{aligned}$$

(iii) Soient $m, n \in \mathbb{N}$. On prouve que pour tout $p \in \mathbb{N}$, on a

$$(m \cdot n) \cdot p = m \cdot (n \cdot p).$$

On procède donc par récurrence sur p. Soit donc l'ensemble T défini par

$$T = \{p \in \mathbb{N} \mid m \cdot (n \cdot p) = (m \cdot n) \cdot p\}.$$

- $0 \in T$: ce cas est établi par le point (i) de la proposition 4.3.10.
- induction : soit $p \in T$. On a successivement

$$\begin{aligned} m \cdot (n \cdot p^+) &= m \cdot (n \cdot p + n) \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= (m \cdot n) \cdot p + m \cdot n \\ &= (m \cdot n) \cdot p^+. \end{aligned}$$

On conclut encore une fois par le principe d'induction. □

En algèbre, les propriétés d'associativité et de commutativité, ainsi que l'existence d'un neutre permettent de caractériser un type de structure : les monoïdes.

Définition 4.3.14. *Un monoïde est un ensemble muni d'une opération binaire, interne et partout définie qui est associative et pour laquelle il existe un élément neutre.*

Il reste encore un peu de travail concernant le produit.

Définition 4.3.15. *On note* 1 *le nombre naturel* 0^+.

Proposition 4.3.16. *L'élément* $1 \in \mathbb{N}$ *est neutre pour la multiplication : on a* $1 \cdot n = n = n \cdot 1$ *pour tout naturel* n.

Démonstration. On a directement par définition, et pour tout $n \in \mathbb{N}$,

$$n \cdot 1 = n \cdot 0^+ = n \cdot 0 + n.$$

On conclut que $n \cdot 1 = n$ par la proposition 4.3.10 et par le fait que 0 est neutre pour l'addition. On a aussi $1 \cdot n = n$ car la multiplication est commutative. □

Ainsi, on a prouvé que $\left(\mathbb{N}, +, 0\right)$ et $\left(\mathbb{N}, \cdot, 1\right)$ sont des monoïdes commutatifs.

4.4 Ordre sur $\mathbb{N}$

On présente dans cette section la notion de relation d'ordre. On propose deux définitions naturelle d'ordre sur l'ensemble $\mathbb{N}$ et on montre qu'elles sont équivalentes. Leurs propriétés vis à vis des opérations sont ensuite étudiées en détail. Cette notion sous-tend les définitions des ordres sur $\mathbb{Z}, \mathbb{Q}$ et finalement $\mathbb{R}$ qui, on le verra, sont fondamentales pour la suite. D'ailleurs, c'est la notion d'ordre qui sous-tend la définition des naturels chez Dedekind : "Si, en considérant un système[3] simplement infini N, ordonné par une représentation φ, on fait totalement abstraction de la nature particulière des éléments, que l'on ne retient simplement le fait qu'ils sont différents et ne considère que les relations établies entre eux par la représentation φ qui définit l'ordre, alors ces éléments s'appellent nombres naturels"(voir [11, p.178]).

Définition 4.4.1. *Une relation d'ordre sur un ensemble A est une relation binaire réflexive, transitive et antisymétrique. C'est à dire, si on note $\preceq$ la relation d'ordre, on a $\forall x, y, z \in A$*

(i) la réflexivité : $x \preceq x$;

(ii) la transitivité : si $x \preceq y$ et $y \preceq z$, alors $x \preceq z$;

(iii) l'antisymétrie : si $x \preceq y$ et $y \preceq x$ alors $x = x$.

Exemple 4.4.1. *Pour tout ensemble A, l'inclusion $\subseteq$ est une relation d'ordre définie sur $\mathscr{P}(A)$:*

(i) réflexivité : cela est immédiat vu la définition 3.2.1 de l'inclusion : $\forall a[a \in x \to a \in x]$;

(ii) transitivité : cela découle directement de la transitivité de "$\to$" (c.f. **RI***6) car on a $a \in x \to a \in y$ et $a \in y \to a \in z$*

(iii) antisymétrie : c'est une application directe de l'axiome **A***9 d'extensionnalité.*

Cependant, comme l'inclusion $\subseteq$ n'est pas une notion première, on privilégie une définition d'ordre sur $\mathbb{N}$ par l'intermédiaire de l'appartenance $\in$.

Définition 4.4.2. *La relation $\leq$ est la relation binaire sur $\mathbb{N}$ définie par*

$$\leq = \Big\{(m, n) \;\Big|\; m \in \mathbb{N} \wedge n \in \mathbb{N} \wedge \Big(m \in n \vee m = n\Big)\Big\}.$$

On note alors $m \leq n$ si $(m, n) \in \leq$.

On vérifie aisément que la relation $\leq$ est bien une relation d'ordre.

Lemme 4.4.3. *La relation $\leq$ définie en 4.4.2 est une relation d'ordre.*

Démonstration. D'abord, on note que comme $\mathbb{N}$ est un ensemble, $\leq$ est bien une relation, conformément à la définition 3.2.18. On montre ensuite que la relation ainsi définie est réflexive, transitive, et antisymétrique :

3. On dirait aujourd'hui ensemble.

(i) réflexivité : c'est une conséquence directe de l'axiome A5 de la réflexivité de l'égalité. Comme, pour tout naturel n on a $n = n$, on a bien $n \leq n$.

(ii) transitivité : soient $m, n, p \in N$ satisfaisant

$$m \leq n \quad \text{et} \quad n \leq p.$$

Si $m = n$ ou $n = p$, le résultat est direct par définition. Sinon, on a $m \in n \in p$. Or on a montré au théorème 4.1.13 que tout naturel est un ensemble transitif (cf. définition 4.1.10). Dès lors on a $m \in p$.

(iii) antisymétrie : soient $m, n \in \mathbb{N}$ satisfaisant $m \leq n$ et $n \leq m$. Si $m \neq n$, on obtient

$$m \in n \in m$$

et donc, comme pour le point précédent, on en déduit que $m \in m$ ce qui est absurde, vu la proposition 4.1.15. □

On note que le choix de préférer l'ordre défini par l'appartenance et non pas par l'inclusion est aussi motivé par le fait que dans $\mathbb{N}$ ces définitions sont équivalentes. On démontre ce résultat plus bas.

Comme déjà évoqué au début de cette section, c'est la notion d'ordre qui fonde, selon Dedekind, la notion de naturel, et plus spécifiquement celle d'ensemble "simplement infini". Aujourd'hui, on parle d'ensemble totalement ordonné infini dénombrable[4]. Un ensemble est totalement ordonné si n'importe quel élément de l'ensemble peut être comparé avec n'importe quel autre élément de l'ensemble. On dit aussi que l'ordre est total.

Définition 4.4.4. *Soit A un ensemble et $\preceq$ un ordre sur A. On dit que l'ordre est total, ou que A est totalement ordonné si, pour tous éléments x et y de A on a*

$$x \preceq y \quad ou \quad y \preceq x.$$

Aussi, ayant défini un ordre sur $\mathbb{N}$, on vérifie que celui-ci est total.

Théorème 4.4.5. *L'ordre $\leq$ sur $\mathbb{N}$ est total.*

Démonstration. Soient $m, n \in \mathbb{N}$. Si $m = n$ on sait déjà que $m \leq n$ (et $n \leq m$). On suppose alors que m et n sont distincts. Ainsi, on montre que dans ce cas, on a soit $m \in n$ soit $n \in m$; et donc que $m \leq n$ ou $n \leq m$. On procède par récurrence sur m : pour tout $m \in \mathbb{N}$ on montre que pour tout $n \in \mathbb{N}$ on a soit $m \in n$ soit $n \in m$. Soit donc T l'ensemble défini par

$$T = \{m \in \mathbb{N} \mid n \in \mathbb{N} \rightarrow \ m \in n \ \vee \ n \in m\},$$

- $0 \in T$: c'est à dire : $\forall n \in \mathbb{N}[0 \leq n \vee n \leq 0]$. On notera que comme on sait déjà que 0 n'est le successeur d'aucun naturel, il faut en fait montrer que $\forall n \in \mathbb{N}[0 \leq n]$. On procède alors par récurrence. Soit l'ensemble S défini par

$$S = \{n \in \mathbb{N} \mid n = 0 \ \vee \ 0 \in n\},$$

4. Un ensemble A est infini dénombrable s'il est en bijection avec $\mathbb{N}$.

- $\diamond$ $0 \in S$: c'est immédiat, vu la définition de S ;
- $\diamond$ induction : si $n \in S$, alors $0 \in n \in n^+$, donc $n^+ \in S$ par transitivité.

- induction : si $m \in T$, alors, pour tous $n \in \mathbb{N}$, $m \in n$ ou $n \in m$. Or
  - (i) si $m \in n$, alors $m^+ \in n^+$ et donc $m^+ \in n$ ou $m^+ = n$, i.e. $m^+ \leq n$;
  - (ii) si $n \in m$, alors $n \in m \in m^+$.

  Dans les deux cas on a bien que si $m \in T$, alors $m^+ \in T$. Ce qui termine la preuve. □

En corollaire de ce résultat, on peut maintenant établir que les relations d'ordre définies avec l'inclusion et avec l'appartenance sont équivalentes.

Proposition 4.4.6. *Pour tous naturels distincts m et n, on a*

$$m \subseteq n \leftrightarrow m \leq n.$$

Démonstration.

- (i) $m \leq n \rightarrow m \subseteq n$: si $m = n$ la propriété est trivialement vérifiée. On suppose alors que $m \in n$. Comme tout naturel est un ensemble transitif (voir la proposition 4.1.13) on en déduit, vu le point (iii) de la proposition 4.1.11 qu'alors $m \subseteq n$:

$$m \in n \rightarrow m \subseteq n.$$

- (ii) $m \subseteq n \rightarrow m \leq n$: soient donc deux naturels m et n tels que $m \subseteq n$; comme l'ordre $\leq$ défini sur $\mathbb{N}$ est total, on sait que l'on a une des propositions suivantes :

$$m = n \quad \text{ou} \quad m \in n \quad \text{ou} \quad n \in m.$$

  - $m = n$: si $m = n$ alors $m \leq n$, comme souhaité ;
  - $m \in n$: à nouveau, dans ce cas la propriété est immédiatement vérifiée ;
  - $n \in m$: on déduit avec les mêmes arguments qu'au point précédent que $n \subseteq m$. Or, vu l'axiome **A**9 d'extensionnalité, il s'ensuit que $m = n$, et donc $n \in n$, ce qui est impossible. Ce cas n'existe donc pas. □

On établit maintenant quelques résultats relatifs à $\leq$ qui seront utilisés dans la suite.Dans $\mathbb{N}$, on peut montrer que quelque soit le sous-ensemble A considéré, celui-ci possède toujours un élément qui est plus petit que tous les autres éléments de A. On dit alors qu'on a un bon ordre.

Définition 4.4.7. *Un ensemble A muni d'un ordre $\preceq$ est dit bien ordonné si pour tout sous-ensemble non-vide B de A, il existe un élément x de B tel que*

$$\forall y \in B[x \preceq y].$$

On dit alors que $\preceq$ est un bon ordre (sur A) et que x est un élément minimum de B.

Proposition 4.4.8. *L'ordre $\leq$ est un bon ordre sur $\mathbb{N}$.*

Démonstration. Soit A un sous-ensemble de $\mathbb{N}$ tel que A ne possède pas d'élément minimum. On montre par récurrence que A est vide. Cependant, on ne peut appliquer le principe d'induction sur l'ensemble T défini avec la formule $\forall n \in \mathbb{N}[n \notin A]$ comme on le ferait habituellement. En effet, lors de l'induction, le fait que n soit un élément de T tel que $n \notin A$ n'assure pas le fait qu'on ne puisse pas trouver d'élément m plus petit que n et tel que $m \in A$; de sorte que n^+ pourrait ou pourrait ne pas appartenir à A. En fait, on va appliquer ce qu'on appelle la récurrence forte : on montre d'abord que la propriété est vérifiée pour $n = 0$, ensuite on montre que si la propriété est vérifiée pour tous les naturels $k \leq n$, alors la propriété est vérifiée pour n^+ et on conclut. Que l'on ne se méprenne pas, cette nouveauté n'est que superficielle. L'argument moteur reste l'application de la proposition 4.1.8 du principe d'induction, comme on le voit en définissant l'ensemble T suivant, et en appliquant le principe d'induction classique.

Soit donc l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid k \leq n \ \rightarrow \ k \notin A\},$$

- $0 \in T$: pour rappel, on a démontré au lemme 4.1.16 que pour tout naturel n différent de 0, on a $0 \in n$. En particulier, on a que tout élément a de A vérifie $0 \leq a$. Dès lors, $0 \notin A$, sinon A aurait un élément minimum ;
- induction : soit $n \in T$. Comme $\mathbb{N}$ est totalement ordonné, pour tout $a \in A$ on a $a \in n^+$ ou $n^+ \in a$ ou $a = n^+$. Or, il n'est pas permis que $a \in n^+$ car si oui, vu la définition du successeur, on a $a \leq n$; ce qui mène à une contradiction. En effet, dans un tel cas, on a simultanément $a \notin A$, car $n \in T$, et $a \in A$. Dès lors, on a $n^+ = a$ ou $n^+ \in a$, en d'autres termes : $\forall a \in A[n^+ \leq a]$. Mais alors n^+ ne peut être un élément de A car sinon il serait le minimum. On en déduit que $n^+ \in T$. En effet, si $k \leq n^+$ alors $k \in n^+$ ou $k = n^+$. Dans le premier cas, on a $k \leq n$ par définition, et donc $k \notin A$ et dans le second cas, on vient de montrer que k n'appartient pas à A.

On a donc $T = \mathbb{N}$, et on en déduit que A est vide, comme attendu. □

On peut établir à présent qu'il n'existe jamais de naturel qui soit plus grand qu'un naturel n et plus petit que son successeur n^+.

Proposition 4.4.9. *Pour tout naturel n, il n'existe pas de naturel strictement compris*[5] *entre n et son successeur.*

Démonstration. Soit $k \in \mathbb{N}$ satisfaisant $k < n^+$. On montre alors que $k \leq n$. Par définition, on a

$$k \leq n^+ \leftrightarrow (k \in n^+ \vee k = n^+).$$

5. La relation stricte associée à l'ordre est définie de manière usuelle : n est strictement compris entre a et b si $a \in n \in b$.

On en déduit les équivalences suivantes :

$$\begin{aligned} k < n^+ &\leftrightarrow k \in n^+ \\ &\leftrightarrow (k \in n \vee k = n) \\ &\leftrightarrow k \leq n. \end{aligned}$$

□

Enfin, on montre quelques résultats relatifs au comportement de l'ordre par rapport à la somme et au produit. Ces résultats seront utilisés dans le chapitre suivant.

Lemme 4.4.10. *Pour tous naturels m et n, on a*

$$m \leq m + n.$$

Démonstration. On procède par récurrence sur n. Soit donc l'ensemble T défini par

$$T = \{n \in \mathbb{N} \mid m \leq m + n\}.$$

- $0 \in T$: c'est immédiat puisque $m + 0 = m$;
- induction : si $n \in T$, on a d'une part $m \leq m + n$ et d'autre part, vu le point (ii) du lemme 4.3.4, on a $m + n^+ = (m + n)^+$. On conclut grâce à la transitivité de $\leq$:

$$m \leq m + n \leq (m + n)^+ = m + n^+.$$

On conclut par le principe d'induction. □

On notera qu'en particulier, si $n \neq 0$ alors on a montré que $m \in m + n$.

Proposition 4.4.11. *Pour tous naturels m et n on a*

$$m \leq n \leftrightarrow m^+ \leq n^+.$$

Démonstration.

(i) $m \leq n \rightarrow m^+ \leq n^+$:

Soit $m, n \in \mathbb{N}$ tels que $m \leq n$. Si $m = n$ la propriété est vérifiée ; aussi on suppose dans la suite que $m \neq n$. Comme l'ordre sur $\mathbb{N}$ est total, on a soit $m^+ = n^+$ soit $m^+ \in n^+$ soit $n^+ \in m^+$. Or, le premier et le troisième cas ne sont pas permis. En effet,

- $m^+ = n^+$: alors, vu l'injectivité de $\cdot^+$ on a $m = n$, ce qui est absurde car on a supposé que $m \neq n$;
- $n^+ \in m^+$: ce cas mène aussi à une absurdité. En effet, par hypothèse, on a $m \in n$, puisque $n \in n^+$, on a par transitivité $m \in n^+ \in m^+$. C'est impossible par la proposition 4.4.9.

Dès lors, on a $m^+ \in n^+$.

(*ii*) $m^+ \leq n^+ \to m \leq n$:
À nouveau, si $m = n$ la propriété est vérifiée. Ainsi, on suppose dans la suite que $m \neq n$ et donc $m^+ \neq n^+$, en d'autres termes on a $m^+ \in n^+$. Comme l'ordre est total, on a soit $m \in n$ soit $n \in m$. Or, par transitivité, comme $m \in m^+ \in n^+$, on a $m \in n^+$ et donc $m \in n$. Dès lors, il n'est pas permis que $n \in m$ car on aurait $n \in n$ ce qui est absurde vu la proposition 4.1.15. □

On peut généraliser ce résultat.

Proposition 4.4.12. *Quels que soient les naturels m, n, et p, on a*

$$m \leq n \leftrightarrow m + p \leq n + p.$$

Démonstration. On procède par récurrence sur p. Soient donc a et b deux naturels et l'ensemble T défini par

$$T = \Big\{ p \in \mathbb{N} \;\Big|\; \forall m, n \in \mathbb{N}[m \leq n \leftrightarrow m + p \leq n + p] \Big\}.$$

- $0 \in T$: cela découle directement du point (*ii*) du lemme 4.3.4 : $m + 0 = m$ et $n + 0 = n$;
- induction : soit donc $p \in T$. En appliquant le théorème 4.4.11, on a successivement

$$\begin{aligned} m \leq n &\leftrightarrow m + p \leq n + p \\ &\leftrightarrow (m + p)^+ \leq (n + p)^+ \\ &\leftrightarrow m + p^+ \leq n + p^+. \end{aligned}$$

On conclut de la manière habituelle. □

On notera qu'en particulier, on a montré que si $m \neq n$ alors on a $m \in n \leftrightarrow m+p \in n+p$. Passons maintenant à la propriété correspondante pour la multiplication.

Proposition 4.4.13. *Quels que soient les naturels m, n, et p, si $p \neq 0$ alors*

$$m \leq n \leftrightarrow m \cdot p \leq n \cdot p.$$

Démonstration. On procède par récurrence sur p. Soit l'ensemble T défini par :

$$T = \Big\{ p \in \mathbb{N} \;\Big|\; \forall m, n \in \mathbb{N}[m \leq n \leftrightarrow m \cdot p^+ \leq n \cdot p^+] \Big\}$$

- $0 \in T$: par définition de T, et parce que $m \cdot 0^+ = m$ et $n \cdot 0^+ = n$;
- induction : soit $p \in T$. D'abord on montre que $m \leq n \to m \cdot p^+ \leq n \cdot p^+$. Si $m \leq n$, on note d'abord que comme $p \in T$, on a $m \cdot p \leq n \cdot p$. Dès lors, vu le résultat précédent on a d'une par $m + m \cdot p \leq n + m \cdot p$ et d'autre part $n + m \cdot p \leq n + n \cdot p$. Par transitivité de $\leq$, on a alors $m \cdot p^+ \leq n \cdot p^+$:

$$\begin{aligned} m \cdot p^+ &= m \cdot p + m \\ &\leq m \cdot p + n \\ &\leq n \cdot p + n \\ &= n \cdot p^+. \end{aligned}$$

Ensuite, on montre la réciproque : $m \cdot p^+ \leq n \cdot p^+ \to m \leq n$. Comme $\mathbb{N}$ est totalement ordonné, on sait qu'on a soit $m \in n$ soit $n \in m$ soit $m = n$. Or, si on a $n \in m$, avec les mêmes arguments qu'au point précédent on a $n + n \cdot p \in n + m \cdot p$ et $m \cdot p + n \in m \cdot p + m$ et donc $n \cdot p^+ \in m \cdot p^+$:

$$\begin{aligned} n \cdot p^+ &= n \cdot p + n \\ &\in m \cdot p + n \\ &\in m \cdot p + m = m \cdot p^+. \end{aligned}$$

On a alors $m \cdot p^+ \in n \cdot p^+ \in m \cdot p^+$ ce qui est absurde. Dès lors, on a $m = n$ ou $m \in n$, en d'autre termes $m \leq n$. □

Nous terminons ce chapitre en formulant un résultat concernant la solubilité dans $\mathbb{N}$ de certaines équations du premier degré :

Théorème 4.4.14. *Pour tous naturels $m, n \in \mathbb{N}$, satisfaisant $m \leq n$, il existe un (unique) naturel $l \in \mathbb{N}$ tel que $n = m + l$.*

Démonstration. L'unicité découle directement de la proposition 4.4.12 : si $n = m + l_1$ et $n = m + l_2$, alors $m + l_1 = m + l_2$, donc $l_1 = l_2$.

Passons à l'existence. Le cas $m = n$ est direct : $l = 0$ convient puisque $m + 0 = m$ (par la proposition 4.3.4 ou même la définition de la somme). Soient deux naturels distincts $m, n \in \mathbb{N}$ tels que $m < n$. On considère l'ensemble

$$A = \{a \in \mathbb{N} \,|\, m + a \geq n\}.$$

Comme $m + n \geq n$ par le lemme 4.4.10, on sait déjà que A est non vide. Il possède ainsi un (unique) minimum que l'on note a_0. Il s'avère que $m + a_0 = n$. En effet, on a $a_0 \neq 0$ parce que $m + 0 = m$ et $m \neq n$, si bien qu'il existe existe $p \in \mathbb{N}$ tel que $a_0 = p^+$. On a donc $m + p^+ \geq n$ par définition de A. Donc

$$(m + p)^+ = m + p^+ \geq n.$$

Comme p^+ est un minimum de A, et comme p est strictement inférieur à p^+, on a $p \notin A$, donc $m + p < n$. On a donc

$$m + p^+ \geq n > m + p.$$

Vu la proposition 4.4.9, on doit avoir $n = m + p^+ = m + a_0$. □

Chapitre 5

Construction de $\mathbb{Z}$

Comme nous venons de l'établir (théorème (4.4.14)), on peut toujours résoudre dans $\mathbb{N}$ une équation du type $a + x = b$, du moins sous la condition $a \leq b$. De plus, en utilisant le lemme (4.4.10), on observe qu'une équation du type $a + x = b$ (avec $a, b \in \mathbb{N}$) admet une solution dans $\mathbb{N}$ si et seulement si $a \leq b$. La construction de l'ensemble $\mathbb{Z}$ des entiers est motivée par la volonté d'étendre $\mathbb{N}$ afin de rendre soluble toute équation de ce type et sera présentée dans la première section de ce chapitre. On profitera ensuite de l'occasion pour étudier de près les propriétés de cette extension, d'une part du point de vue de la théorie des anneaux et d'autre part du point de vue de la théorie des ensembles ordonnés.

5.1 Définition de l'ensemble $\mathbb{Z}$

Le résultat précédent justifie la définition suivante.

Définition 5.1.1. *Soient $a,\ b \in \mathbb{N}$ tels que $a \leq b$ et soit $c \in \mathbb{N}$ tel que $a + c = b$ alors on notera $c = b - a$.*

Lemme 5.1.2. *Soient $a,\ b,\ c \in \mathbb{N}$, les conditions suivantes sont équivalentes :*

(i) $a + c = b$;

(ii) $c = b - a$;

(iii) $a = b - c$.

Démonstration. Vu la commutativité de l'addition, la première condition s'écrit de manière équivalente $c + a = b$. On en déduit que $a \leq b$ et $c \leq b$. Alors on applique la définition 5.1.1. □

Comme nous allons le voir, la construction usuelle de l'ensemble $\mathbb{Z}$ est fondée sur la considération d'une relation d'équivalence sur l'ensemble $\mathbb{N} \times \mathbb{N}$. Elle est basée sur des considérations empiriques des gains et des pertes. On se donne donc des couples (a, b) de nombres naturels, où on pense le nombre a comme un "gain de a" et b comme une "perte de b". On souhaite identifier les couples qui donnent le même "résultat comptable", quand

le gain est plus grand que la perte. Cela conduit à la définition d'une relation d'équivalence sur une partie de $\mathbb{N} \times \mathbb{N}$.

Lemme 5.1.3. *La relation binaire $\mathscr{R}$ définie sur $\{(a,b) \in \mathbb{N} \times \mathbb{N} \,|\, a \geq b\}$ par*

$$(a,b)\mathscr{R}(c,d) \;\leftrightarrow a - b = c - d.$$

est une relation d'équivalence.

Démonstration. On vérifie directement les trois propriétés adéquates en se ramenant aux propriétés de l'égalité : on a $(a,b)\mathscr{R}(a,b)$ car $a - b = a - b$ (l'égalité est réflexive). Si $(a,b)\mathscr{R}(c,d)$, alors on a $a - b = c - d$, donc $c - d = a - b$, puisque l'égalité est symétrique et finalement $(c,d)\mathscr{R}(a,b)$. Enfin, si $(a,b)\mathscr{R}(c,d)$ et $(c,d)\mathscr{R}(e,f)$, on a $a - b = c - d$ et $c - d = e - f$. On conclut que $(a,b)\mathscr{R}(e,f)$ vu la transitivité de l'égalité. □

On constate que la relation d'équivalence $\mathscr{R}$ considérée dans le lemme 5.1.3 garantit que les couples de naturels $(a,b), (c,d) \in \mathbb{N} \times \mathbb{N}$ appartiennent à $\mathscr{R}$ si et seulement s'ils définissent deux équations qui ont le même résultat, à savoir

$$b + x = a, \quad \text{et} \quad d + x = c.$$

S'il est facile de démontrer que c'est une relation d'équivalence, elle a l'inconvénient de n'être définie que sur une partie de $\mathbb{N} \times \mathbb{N}$. On voudrait l'étendre à $\mathbb{N} \times \mathbb{N}$ tout entier et généraliser l'opération $-$. Pour ce faire, on constate qu'on a

$$\begin{aligned}(a,b)\mathscr{R}(c,d) &\leftrightarrow a - b = c - d \\ &\leftrightarrow (a - b) + (b + d) = c - d + (b + d) \\ &\leftrightarrow a + d = c + b.\end{aligned}$$

On est alors amené à considérer la définition suivante.

Définition 5.1.4. *On définit la relation binaire $\sim$ sur $\mathbb{N} \times \mathbb{N}$ par*

$$(a,b) \sim (c,d) \text{ si et seulement si } \; a + d = b + c.$$

Mnémosyne nous offre de se souvenir de la définition sans difficulté grâce à la petite poésie suivante : deux couples sont équivalents si la "somme des extrêmes" est égale à la "somme des moyens". On établit le résultat élémentaire mais essentiel suivant.

Proposition 5.1.5. *La relation $\sim$ est une relation d'équivalence.*

Démonstration. Il s'agit de vérifier que la relation $\sim$ est réflexive, symétrique et transitive :

(*i*) Réflexivité : il suffit de vérifier que $(a,b) \sim (a,b)$, c'est-à-dire

$$a + b = b + a.$$

C'est le cas vu la commutativité de l'addition dans $\mathbb{N}$.

(*ii*) Symétrie : soient (a, b) et (a', b') deux éléments de $\mathbb{N} \times \mathbb{N}$ tels que $(a, b) \sim (a', b')$. Il s'ensuit par définition que

$$a + b' = b + a'.$$

On en déduit $a' + b = b' + a$ comme l'addition dans $\mathbb{N}$ est commutative.

(*iii*) Transitivité : soient (a, b), (a', b') et (a'', b'') trois éléments de $\mathbb{N} \times \mathbb{N}$ satisfaisant

$$(a, b) \sim (a', b') \quad \text{et} \quad (a', b') \sim (a'', b'').$$

On a donc par définition $a + b' = b + a'$ et $a' + b'' = b' + a''$, et on souhaite montrer $a + b'' = b + a''$. On obtient alors directement (puisque l'addition est bien définie) :

$$a + b' + (a' + b'') = b + a' + (b' + a'').$$

Puisque l'addition est associative et commutative, cette condition est équivalente à

$$a + b'' + (a' + b') = b + a'' + (a' + b').$$

On a donc $a + b'' = b + a''$, soit $(a, b) \sim (a'', b'')$, par la proposition 4.4.12. □

On est à présent en mesure de définir l'ensemble $\mathbb{Z}$ des entiers.

Définition 5.1.6. *L'ensemble quotient* $(\mathbb{N} \times \mathbb{N})/\sim$ *du produit* $\mathbb{N} \times \mathbb{N}$ *par la relation d'équivalence* $\sim$ *est appelé ensemble des entiers. On le note* $\mathbb{Z}$*. On notera* $[a, b]$ *la classe d'équivalence déterminée par* (a, b) *dans ce quotient.*

Comme le souhait est prolonger $\mathbb{N}$,on montre qu'a minima on a une injection de $\mathbb{N}$ dans $\mathbb{Z}$.

Proposition 5.1.7. *L'application* ϕ *définie par*

$$\phi \ : \ n \in \mathbb{N} \mapsto [n, 0] \in \mathbb{Z}$$

est une injection de $\mathbb{N}$ *dans* $\mathbb{Z}$*.*

Démonstration. Si $m, n \in \mathbb{N}$ satisfont $\phi(m) = \phi(n)$, on a alors par définition de ϕ

$$[m, 0] = [n = 0]$$

Or, par définition de $\sim$, on a alors successivement

$$\begin{aligned} [m, 0] = [n, 0] &\leftrightarrow m + 0 = 0 + n \\ &\leftrightarrow m = n, \end{aligned}$$

Dès lors, on a bien $\phi(m) = \phi(n) \to m = n$. □

5.2 Arithmétique sur $\mathbb{Z}$

L'objectif de cette section est de définir les opérations usuelles d'addition et de multiplication sur l'ensemble $\mathbb{Z}$, avec la contrainte de faire de $\mathbb{Z}$ un extension de $\mathbb{N}$. Ces opérations sur $\mathbb{Z}$ ont des propriétés "dont la spécificité est de ne pas être spécifique" ; nous les résumerons en les termes de "groupe", "anneau" ou "corps". Nous ne nous étalerons pas sur ce fait et nous nous contenterons d'en donner les définitions au travers des différentes démonstrations. Pour plus de détails, nous renvoyons au cours *Algèbre II* de Georges Hansoul [17].

5.2.1 L'addition dans $\mathbb{Z}$

Définition 5.2.1. *On définit l'opération d'addition $+_{\mathbb{Z}}$ sur $\mathbb{Z}$ par*

$$+_{\mathbb{Z}} : ([a,b],[c,d]) \in \mathbb{Z}\times\mathbb{Z} \mapsto [a+c, b+d] \in \mathbb{Z}\,.$$

Étant donné que la définition 5.2.1 semble dépendre de choix auxiliaires, à savoir le choix des représentants qui déterminent les classes d'équivalence, la proposition suivante est indispensable pour la légitimer.

Proposition 5.2.2. *La définition 5.2.1 est indépendante du choix des représentants en jeu.*

Démonstration. C'est une simple vérification. Soient $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$. On a alors

$$\begin{aligned}(a+c)+(b'+d') = (b+d)+(a'+c') &\leftrightarrow\ (a+b')+(c+d') = (a'+b)+(d+c')\\ &\leftrightarrow\ (a+b')+(c+d') = (a+b')+(c+d').\end{aligned}$$

Ainsi, on a bien $(a+c, b+d) \sim (a'+c', b'+d')$ comme attendu. □

De plus, on vérifie que l'application ϕ définie en 5.1.7 préserve la somme.

Proposition 5.2.3. *Pour tout naturel m et n l'application ϕ définie en 5.1.7 vérifie*

$$\phi(m+n) = \phi(m) +_{\mathbb{Z}} \phi(n).$$

Démonstration. Il suffit d'appliquer d'une part la définition 5.1.7 de l'application ϕ et d'autre part la définition 5.2.1 de la somme dans $\mathbb{Z}$:

$$\phi(m+n) = [m+n, 0] = [m,0] +_{\mathbb{Z}} [n,0].$$

□

Nous avons vu que $\mathbb{N}$ est un monoïde additif commutatif (c.f. 4.3.5), l'ensemble $\mathbb{Z}$ muni de l'opération $+_{\mathbb{Z}}$ possède aussi cette propriété. De plus, pour tout entier z il existe un entier k tel que $z +_{\mathbb{Z}} k = 0_Z$. On dit alors que tout élément possède un opposé. On résume en disant que $\mathbb{Z}$, muni de l'opération $+_{\mathbb{Z}}$ est un groupe (additif).

Théorème 5.2.4. *L'ensemble des entiers $\mathbb{Z}$ muni de l'opération $+_{\mathbb{Z}}$ est un groupe commutatif.*

Démonstration. On passe en revue les propriétés à démontrer. On se ramène, via la définition de l'addition dans $\mathbb{Z}$ et de la relation $\sim$ qui définit $\mathbb{Z}$, aux propriétés de l'addition dans $\mathbb{N}$.

(*i*) L'opération $+_{\mathbb{Z}}$ est associative : soient $[a,b]$, $[c,d]$ et $[e,f]$ des éléments de $\mathbb{Z}$. On a successivement

$$\begin{aligned}([a,b]+_{\mathbb{Z}}[c,d])+_{\mathbb{Z}}[e,f] &= [a+c,b+d]+_{\mathbb{Z}}[e,f]\\ &= [(a+c)+e,(b+d)+f]\\ &= [a+(c+e),b+(d+f)]\\ &= [a,b]+_{\mathbb{Z}}[c+e,d+f]\\ &= [a,b]+_{\mathbb{Z}}([c,d]+_{\mathbb{Z}}[e,f]).\end{aligned}$$

(*ii*) Il existe un neutre pour $+_{\mathbb{Z}}$:
Comme 0 est le neutre pour $+$ dans $\mathbb{N}$, et étant donné le lien fort entre $\mathbb{N}$ et $\mathbb{Z}$ entretenu par le truchement de ϕ, il semble opportun de vérifier si $\phi(0)$ convient ; cela se fait sans peine vu la définition de $+_{\mathbb{Z}}$:

$$[a,b]+_{\mathbb{Z}}[0,0]=[a,b].$$

(*iii*) Soient $[a,b]$ et $[c,d]$ deux éléments de $\mathbb{Z}$ on a alors

$$[a,b]+_{\mathbb{Z}}[c,d]=[0,0]\leftrightarrow a+c=b+d$$

Ainsi, $[b,a]$ est un opposé pour $[a,b]$.

(*iv*) L'opération $+_{\mathbb{Z}}$ est commutative :
Soient $[a,b]$ et $[c,d]$ deux entiers, on a d'une part

$$[a,b]+_{\mathbb{Z}}[c,d]=[a+c,b+d]$$

et d'autre part

$$[c,d]+_{\mathbb{Z}}[a,b]=[c+a,d+b].$$

La conclusion découle directement de la commutativité de la somme dans $\mathbb{N}$. □

Remarque 5.2.5. *On note $-z$ l'opposé de z, et, par souci d'économie, $z-k$ au lieu de $z+(-k)$. On a alors une partition de $\mathbb{Z}$ en deux ensembles définis à partir de $\mathbb{N}$:*

$$\mathbb{Z}=-\phi(\mathbb{N})\cup\phi(\mathbb{N})\quad et\quad -\phi(\mathbb{N})\cap\phi(\mathbb{N})=\{0\}.$$

En effet, soit l'élément $[a,b]$ de $\mathbb{Z}$.

- *Si $a\geq b$, alors on a $[a,b]=[a-b,0]=\phi(a-b)$, vu la définition de $\sim$;*
- *Si $a\leq b$, alors on a $[a,b]=[0,b-a]=-\phi(b-a)$, encore vu la définition de $\sim$;*

Enfin, si z appartient à $\phi(\mathbb{N})$ et à $-\phi(\mathbb{N})$, alors il existe m et n dans $\mathbb{N}$ tels que

$$z=[m,0]=[0,n].$$

On a alors $m+n=0$, et donc $m=n=0$, par exemple vu la proposition 4.4.10.

5.2.2 Le produit dans $\mathbb{Z}$

Toujours dans l'objectif de prolonger $\mathbb{N}$, définissons une seconde opération sur $\mathbb{Z}$.

Définition 5.2.6. *Le produit sur $\mathbb{Z}$ est l'opération*

$$.\mathbb{z} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : ([a,b],[c,d]) \mapsto [a,b] \,.\mathbb{z}[c,d] = [ac+bd, ad+bc].$$

Comme lors de la définition de l'addition sur l'ensemble $\mathbb{Z}$, on vérifie que la définition 5.2.6 est licite et que l'application ϕ préserve le produit.

Lemme 5.2.7. *La définition 5.2.6 du produit $.\mathbb{z}$ est indépendante du choix des représentants.*

Démonstration. Soit $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, on a successivement

$$\begin{aligned}
[a',b'] \,.\mathbb{z}[c',d'] &= [a'c'+b'd', a'd'+b'c'] \\
&= [a'c'+b'd', a'd'+b'c'] + [a'd+b'c, a'd+b'c] \\
&= [a'c'+a'd+b'd'+b'c, a'd'+b'c'+a'd+b'c] \\
&= [a'(c'+d)+b'(d'+c), a'd'+b'c'+a'd+b'c] \\
&= [a'(c+d')+b'(d+c'), a'd'+b'c'+a'd+b'c] \\
&= [a'c+a'd'+b'd+b'c', a'd'+b'c'+a'd+b'c] \\
&= [a'c+b'd, a'd+b'c] + [a'd'+b'c', a'd'+b'c'] \\
&= [a'c+b'd, a'd+b'c] + [bc+ad, bc+ad] \\
&= [a'c+b'd+bc+ad, a'd+b'c+bc+ad] \\
&= [c(a'+b)+d(b'+a), a'd+b'c+bc+ad] \\
&= [c(a+b')+d(b+a'), a'd+b'c+bc+ad] \\
&= [ca+cb'+db+da', a'd+b'c+bc+ad] \\
&= [ac+bd, ad+bc] + [cb'+a'd] \\
&= [ac+bd, ad+bc] \\
&= [a,b] \,.\mathbb{z}[c,d].
\end{aligned}$$

□

Soient deux naturels m et n, en appliquant la définition du produit à $\phi(m)$ et $\phi(n)$, il apparaît que la propriété est trivialement vérifiée :

$$\phi(m) \,.\mathbb{z}\, \phi(n) = [m,0] \,.\mathbb{z}[n,0] = [m.n, 0].$$

Tout est à présent en place pour prouver le résultat essentiel concernant l'ensemble $\mathbb{Z}$ muni des opérations d'addition et de multiplication données par les définitions 5.2.1 et 5.2.6.

Théorème 5.2.8. *Le quintuple $(\mathbb{Z}, +, 0, .\mathbb{z}, 1)$, où $1 = [1,0]$ est un anneau commutatif.*

Démonstration. On sait déjà que $(\mathbb{Z}, +, 0)$ est un groupe commutatif vu le théorème 5.2.4. Pour conclure, il suffit alors de procéder aux vérifications suivantes :

(i) le produit $.\mathbb{z}$ est associatif :

$$\begin{aligned}([a,b]\,._{\mathbb{Z}}[c,d])\,._{\mathbb{Z}}[e,f] &= [ac+bd, ad+bc]\,._{\mathbb{Z}}[e,f]\\ &= [ace+bde+adf+bcf, acf+bdf+ade+bce]\\ &= [a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)]\\ &= [a,b]\,._{\mathbb{Z}}[ce+df, cf+ed]\\ &= [a,b]\,._{\mathbb{Z}}([c,d]\,._{\mathbb{Z}}[e,f]).\end{aligned}$$

(ii) On vérifie sans peine que $1 = [1,0] \in \mathbb{Z}$ est un neutre multiplicatif. En effet, on a

$$[a,b]\,._{\mathbb{Z}}[1,0] = [a.1+b.0, a.0+b.1] = [a,b]$$

pour tous $a, b \in \mathbb{N}$, vu les propriétés de la multiplication dans $\mathbb{N}$. On montre de même que $[1,0]\,._{\mathbb{Z}}[a,b] = [a,b]$ pour tous $a, b \in \mathbb{N}$.

(iii) le produit $.\mathbb{z}$ est commutatif : on calcule, à partir de la définition du produit dans $\mathbb{Z}$, et pour tous $a, b, c, d \in \mathbb{N}$:

$$[a,b]\,._{\mathbb{Z}}[c,d] = [ac+bd, ad+bc] \quad \text{et} \quad [c,d]\,._{\mathbb{Z}}[a,b] = [ca+db, cb+da].$$

Ces deux expressions sont égales vu la commutativité de la somme et du produit dans $\mathbb{N}$.

(iv) Le produit distribue l'addition : comme plus haut, on exprime l'égalité à démontrer, on calcule et on applique les propriétés adéquates dans $\mathbb{N}$. On a donc, pour tous $a, b, c, d, e, f \in \mathbb{N}$, d'une part

$$[a,b]\,._{\mathbb{Z}}([c,d]+[e,f]) = [a,b]\,._{\mathbb{Z}}[c+e, d+f] = [a(c+e)+b(d+f), a(d+f)+b(c+e)],$$

et d'autre part

$$\begin{aligned}([a,b]\,._{\mathbb{Z}}[c,d]) + ([a,b]\,._{\mathbb{Z}}[e,f]) &= [ac+bd, ad+bc] + [ae+bf, af+be]\\ &= [ac+bd+ae+bf, ad+bc+af+be].\end{aligned}$$

Ces deux expressions sont égales vu la distributivité du produit sur la somme dans $\mathbb{N}$ (théorème 4.3.13) et la commutativité de la somme dans $\mathbb{N}$ (proposition 4.3.5). □

Nous comprenons ainsi que $\mathbb{Z}$ est muni d'une structure plus riche que celle de $\mathbb{N}$, puisque l'addition et la multiplication dans $\mathbb{Z}$ étendent celles de $\mathbb{N}$, en conservent les propriétés, et en acquièrent une nouvelle, à savoir l'existence d'un opposé pour chaque élément (vis-à-vis de la somme). Cependant, le résultat suivant exhibe une carence qui sera corrigée avec l'introduction des nombres rationnels dans le chapitre suivant.

Proposition 5.2.9. *Le triple $(\mathbb{Z}\setminus\{0\}, ._{\mathbb{Z}}, 1)$ n'est pas un groupe. Plus précisément, les seuls entiers inversibles pour l'opération $._{\mathbb{Z}}$ sont $1 = [1,0]$ et $-1 = [0,1]$.*

Démonstration. Par définition du produit, on obtient directement que $[1,0]._{\mathbb{Z}}[1,0] = [1,0]$ et $[0,1]._{\mathbb{Z}}[0,1] = [1,0]$. Montrons que ce sont les seuls éléments inversibles. Supposons que $[a,b]._{\mathbb{Z}}\mathbb{Z}$ soit inversible. Il existe alors $[c,d]._{\mathbb{Z}}\mathbb{Z}$ tel que $[a,b]._{\mathbb{Z}}[c,d] = [1,0]$. Par définition du produit dans $\mathbb{Z}$, on a alors

$$[ac+bd, ad+bc] = [1,0].$$

Par définition de $\mathbb{Z}$, cette condition est équivalente à l'égalité (entre nombres naturels)

$$ac+bd = ad+bc+1.$$

Traitons le cas $a \leq b$. Le cas $b \leq a$ se traite de façon similaire.

Si $a \leq b$, alors par le théorème 4.4.14, il existe $l \in \mathbb{N}$ tel que $b = a+l$. La condition ci-dessus s'écrit alors

$$ac+ad+ld = ad+ac+lc+1,$$

ou encore, vu la proposition 4.4.12, à

$$ld = lc+1.$$

On a donc $lc \leq ld$. Vu la proposition 4.4.13, on a $l = 0$, ou $c \leq d$. Le premier cas est impossible car $l = 0$ ne permet pas de satisfaire l'équation ci-dessus. On a donc $c \leq d$, et toujours par le théorème 4.4.14, il existe $e \in \mathbb{N}$ tel que $d = c+e$. L'équation ci-dessus devient alors

$$lc+le = lc+1,$$

ou encore $le = 1$. La proposition 4.4.13 montre alors que la solution unique de cette équation est donnée par $e = l = 1$. On a donc $[a,b] = [a,a+1] = [0,1]$ et $[c,d] = [c,c+1] = [0,1]$. □

Notons enfin que la structure d'anneau permet de dégager quelque propriétés générales dont on pourra faire usage.

Proposition 5.2.10. *Si $(A,+,0,.,1)$ est un anneau alors*

(i) l'opposé de tout élément est unique ;
(ii) si $a \in A$ alors $-(-a) = a$;
(iii) si $a \in A$ alors, $-a = (-1).a$;
(iv) $(-1).(-1) = 1$.

Démonstration.

(*i*) Soient e et f deux opposés de a, on a alors $e = e+f+a = f$;

(*ii*) $-(-a)$ est l'opposé de $-a$ don on a $-(-a)-a = 0$ et donc $-(-a)-a+a = a$ i.e., $-(-a) = a$;

(*iii*) comme . est distributif par rapport à $+$ on a $-1.a+a = (-1+1).a = 0$ donc $-1.a$ est un opposé de a et, vu (i) en conclut que $-1.a = -a$;

(*iv*) vu les points (ii) et (iii) on a $(-1).(-1) = -(-1) = 1$.

□

5.3 Ordre sur $\mathbb{Z}$

Maintenant que nous avons étendu raisonnablement les opérations + et . à l'ensemble $\mathbb{Z}$, nous pouvons envisager d'étendre la structure d'ordre. On voudrait définir sur $\mathbb{Z}$ une relation d'ordre qui soit cohérente avec la relation d'ordre définie sur $\mathbb{N}$. Plus précisément, on voudrait que l'extension en vue satisfasse

$$n \leq m \leftrightarrow \phi(n) \leq \phi(m)$$

pour tous $m, n \in \mathbb{N}$. Cette condition fixe naturellement l'ordre sur $\phi(\mathbb{N})$.

Lemme 5.3.1. *Soient $[a, b], [c, d] \in \mathbb{Z}$ satisfaisant $b \leq a$ et $d \leq c$. Alors, si l'extension de $\mathbb{N}$ à $\mathbb{Z}$ est croissante, on a*

$$[a, b] \leq [c, d] \leftrightarrow a + d \leq b + c.$$

Démonstration. C'est direct. En effet, soient $a, b, c, d \in \mathbb{N}$ satisfaisant $b \leq a$ et $d \leq c$. Alors, on obtient

$$\begin{aligned} [a, b] \leq [c, d] &\leftrightarrow [a - b, 0] \leq [c - d, 0] \\ &\leftrightarrow a - b \leq c - d \\ &\leftrightarrow a + d \leq b + c, \end{aligned}$$

en utilisant la proposition 4.4.12. □

La définition suivante est à présent tout à fait naturelle.

Définition 5.3.2. *La relation $\leq$ est définie sur $\mathbb{Z}$ par*

$$[a, b] \leq [c, d] \leftrightarrow a + d \leq b + c.$$

Ayant posé cette définition, faisons les vérifications habituelles des caractères correct et d'ordre de la relation ainsi définie. Nous nous intéresserons ensuite à ses propriétés.

Théorème 5.3.3.

(i) La relation $\leq$ est bien définie ;

(ii) La relation $\leq$ est une relation d'ordre ;

(iii) L'ordre $\leq$ ainsi défini est total ;

(iv) L'ensemble $\mathbb{Z}$ muni de l'ordre $\leq$ n'est pas bien ordonné.

Démonstration.

(i) D'abord, on montre que la définition a bien un sens en vérifiant qu'elle ne dépend pas du choix des représentants. Soient donc $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$ tels que $[a,b] \leq [c,d]$. On a donc $a+d \leq b+c$, $a+b' = b+a'$ et $c = d' = c'+d$. On établit alors l'inégalité $a'+d' \leq b'+c'$. On utilise la proposition 4.4.12 pour obtenir successivement

$$\begin{aligned} a'+d'+b+d &= a'+b+d+d' \\ &= a+b'+d+d' \\ &= a+d+b'+d' \\ &\leq b+c+b'+d' \\ &\leq c+d'+b+b' \\ &\leq c'+d+b+b' \\ &\leq b'+c'+b+d. \end{aligned}$$

Finalement, grâce au théorème 4.4.12 on a bien $a'+d' \leq b'+c'$.

(ii) On prouve que $\leq$ est une relation d'ordre sur $\mathbb{Z}$ en passant en revue les propriétés de la définition.

- La relation est réflexive : il s'agit de montrer que $[a,b] \leq [a,b]$ pour tous $a,b \in \mathbb{N}$. Vu la définition de $\leq$, c'est équivalent à $a+b \leq b+a$. Cette relation est vraie, puisque $\leq$ est un ordre dans $\mathbb{N}$ (et est donc réflexif) et puisque $a+b = b+a$, vu la commutativité de l'addition dans $\mathbb{N}$.
- La relation est transitive : soient $[a,b],[c,d],[e,f] \in \mathbb{Z}$ satisfaisant $[a,b] \leq [c,d]$ et $[c,d] \leq [e,f]$. On a alors $a+d \leq b+c$ et $c+f \leq d+e$ et donc, en appliquant la proposition 4.4.12 :

  $$\begin{aligned} a+d+c+f &\leq b+c+c+f \\ &\leq b+c+e+d. \end{aligned}$$

  On a donc bien

  $$a+f \leq b+e$$

  encore via la proposition 4.4.12.
- la relation est antisymétrique : en effet, soient $[a,b]$ et $[c,d]$ deux entiers tels que $[a,b] \leq [c,d]$ et $[c,d] \leq [a,b]$. On obtient alors

  $$a+d \leq b+c \leq a+d.$$

  Puisque $\leq$ est une relation d'ordre sur $\mathbb{N}$, elle est antisymétrique et donc on a

  $$a+d = b+c$$

  et finalement $[a,b] = [c,d]$ vu la définition de la relation $\sim$ qui définit $\mathbb{Z}$.

(*iii*) Soient $[a,b]$ et $[c,d]$ des éléments de $\mathbb{Z}$. On a évidement

$$a+d \leq b+c \quad \text{ou} \quad c+b \leq d+a$$

puisque l'ordre est total dans $\mathbb{N}$ et puisque l'addition dans $\mathbb{N}$ est commutative. On a donc bien $[a,b] \leq [c,d]$ ou $[c,d] \leq [a,b]$.

(*iv*) Il suffit d'exhiber un sous-ensemble A de $\mathbb{Z}$ qui ne possède pas d'élément minimal. Soit

$$A = \{z \in \mathbb{Z} \,|\, z < 0\}.$$

Par définition, $[a,b] \in A$ si et seulement si $a < b$. En effet $[a,b] \leq [0,0]$ est équivalent à $a \leq b$ par définition de $\leq$, et $[a,b] \neq [0,0]$ est équivalent à $a \neq b$ par définition de $\sim$. Alors A est non vide, puisqu'il contient $[0,1]$. Mais alors, si $[a,b]$ appartient à A, il en est de même pour $z = [a,b+1]$ (car $a < b$ implique $a < b+1$). Mais on a aussi en utilisant la définition de l'ordre

$$[a,b+1] \leq [a,b]$$

et également $[a,b+1] \neq [a,b]$ en vertu de la définition de $\sim$. Il s'ensuit que l'ensemble A ne possède pas d'élément minimal et finalement que l'ensemble $\mathbb{Z}$ n'est pas bien ordonné par $\leq$. □

Pour terminer, analysons rapidement les propriétés de l'ordre vis-à-vis de la somme et du produit. Sans surprise, la propriété vis-à-vis du produit dépend du fait que le nombre par lequel on multiplie est positif ou non.

Proposition 5.3.4. *Pour tous* $[a,b],[c,d],[e,f] \in \mathbb{Z}$, *on a*

(i) $[a,b] \leq [c,d] \leftrightarrow [a,b]+[e,f] \leq [c,d]+[e,f]$;

(ii) *si* $0 < [e,f]$, $[a,b] \leq [c,d] \leftrightarrow [a,b] \cdot_{\mathbb{Z}} [e,f] \leq [c,d] \cdot_{\mathbb{Z}} [e,f]$;

(iii) *si* $[e,f] < 0$, $[a,b] \leq [c,d] \leftrightarrow [a,b] \cdot_{\mathbb{Z}} [e,f] \geq [c,d] \cdot_{\mathbb{Z}} [e,f]$.

Démonstration. On applique évidemment la définition de l'ordre dans $\mathbb{Z}$ et les propriétés correspondantes dans $\mathbb{N}$.

(*i*) La première condition s'écrit alors

$$a+d \leq b+c \leftrightarrow (a+e)+(d+f) \leqslant (b+f)+(c+e).$$

Cette condition est satisfaite vu l'associativité et la commutativité de l'addition dans $\mathbb{N}$ et la proposition 4.4.12.

(*ii*) La condition s'écrit

$$a+d \leq b+c \leftrightarrow (ae+bf)+(cf+de) \leq (ce+df)+(af+be),$$

ou encore, par associativité, commutativité de $+$ et par distributivité :

$$a+d \leq b+c \leftrightarrow (a+d)e+(b+c)f \leq (a+d)f+(b+c)e.$$

On a $[e, f] > [0, 0]$ si et seulement si $e > f$. On peut alors écrire $e = f + l$ pour $l \neq 0$ (par le théorème 4.4.14). La condition s'écrit alors

$$a + d \leq b + c \leftrightarrow (a + d)(f + l) + (b + c)f \leq (a + d)f + (b + c)(f + l),$$

ou encore, via la distributivité et la proposition 4.4.12,

$$a + d \leq b + c \leftrightarrow (a + d)l \leq (b + c)l.$$

Cette condition est satisfaite vu la proposition 4.4.13.

(iii) On procède de la même manière qu'en (ii). La condition à démontrer est alors

$$a + d \leq b + c \leftrightarrow (a + d)e + (b + c)f \geq (a + d)f + (b + c)e.$$

Mais on écrit ici $f = e + l$, on simplifie, et on conclut encore par les propositions 4.4.12 et 4.4.13.

□

Chapitre 6

Construction de $\mathbb{Q}$

Comme pour les entiers, la construction moderne des nombres rationnels n'apparaît qu'au 19^e siècle. Avant cela, on se bornait à manipuler des proportions. Ainsi, au lieu d'écrire $\frac{3}{6} = \frac{2}{4}$, on exprimait "le fait que 3 est à 6 ce que 2 est à 4".

L'objet de ce chapitre est de construire en détail l'ensemble $\mathbb{Q}$ des nombres rationnels et de prouver qu'il s'agit d'un corps commutatif archimédien et totalement ordonné [1]. Notons que dans tout ce chapitre, nous désignerons la somme et le produit dans $\mathbb{N}$ et dans $\mathbb{Z}$ avec les mêmes symboles, à savoir . et +.

6.1 Définition de l'ensemble $\mathbb{Q}$

Comme indiqué ci-dessus, les mathématiciens ont longtemps travaillé avec des rapports de grandeurs. Ces rapports se sont traduits par des notations du type $\frac{a}{b}$ où b est non nul, celui-ci servant en quelque sorte d'étalon pour "mesurer a". Si on souhaite s'affranchir de ces considérations empiriques, on arrive assez naturellement à la construction actuelle de l'ensemble $\mathbb{Q}$ fondée sur une relation d'équivalence sur l'ensemble des couples d'entiers que nous venons de construire ; où le premier correspondant "au numérateur" et le second "au dénominateur".

On considère sur $\mathbb{Z} \times \mathbb{Z}_0$ (où $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$) la relation suivante :

Définition 6.1.1. *On définit sur $\mathbb{Z} \times \mathbb{Z}_0$ la relation*

$$(a, b) \sim (c, d) \ \leftrightarrow ad = bc.$$

Notons que la notation $\sim$ a déjà été utilisée pour la relation qui définit $\mathbb{Z}$ dans le chapitre précédent. On aurait pu utiliser les notations explicites $\sim_{\mathbb{Z}}$ et $\sim_{\mathbb{Q}}$, mais il y a peu de risque de confusion, donc nous conservons, sauf si la situation l'impose, la notation $\sim$.

1. Dans [13], on peut lire à propos de la définition de l'ensemble des rationnels : "En 1910, Steinitz donna une définition abstraite, mettant ainsi en évidence le fait que cette extension (de $\mathbb{Z}$ à $\mathbb{Q}$) est en fait un cas particulier d'un énoncé général, à savoir celui concernant le plongement d'un anneau intègre dans son corps des fractions."

Notons également que la relation se retient facilement avec la formule classique : "le produit des extrêmes est égal au produit des moyens".

Le résultat suivant garantit la légitimité de la définition 6.1.1.

Lemme 6.1.2. *La relation $\sim$ est une relation d'équivalence sur l'ensemble $\mathbb{Z} \times \mathbb{Z}_0$.*

Démonstration. Il suffit de vérifier et de se référer aux propriétés adéquates des opérations définies sur $\mathbb{Z}$:

- la relation $\sim$ est réflexive : en effet, pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z}_0$, on $(a, b) \sim (a, b)$ vu que $ab = ba$ par la commutativité de la multiplication dans $\mathbb{Z}$.
- la relation $\sim$ est symétrique : soient $a, c \in \mathbb{Z}$ et $b, d \in \mathbb{Z}_0$ et supposons $(a, b) \sim (c, d)$. On en déduit par définition que $ad = bc$. En utilisant la commutativité de la multiplication dans $\mathbb{Z}$ ainsi que la symétrie et la transitivité de la relation d'égalité, on obtient alors

  $$cb = bc = ad = da$$

  et enfin $(c, d) \sim (a, b)$.
- la relation $\sim$ est transitive : soient $a, c, e, \in \mathbb{Z}$ et $b, d, f \in \mathbb{Z}_0$ satisfaisant $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$. Ainsi $ad = bc$ et $cf = de$ par la définition 6.1.1. Puisque le produit dans $\mathbb{Z}$ est bien défini, on a

  $$adf = bcf \quad \text{et} \quad bcf = bde,$$

  qui donnent $adf = bde$ par transitivité de l'égalité. Vu la commutativité du produit dans $\mathbb{Z}$ et la proposition 4.4.13, cette dernière égalité implique $af = de$, soit $(a, b) \sim (e, f)$, par définition de $\sim$. □

On en vient à la définition de l'ensemble $\mathbb{Q}$.

Définition 6.1.3. *L'ensemble $\mathbb{Q}$ des nombres rationnels est l'ensemble quotient du produit $\mathbb{Z} \times \mathbb{Z}_0$. On note $[a, b]$ (ou encore $\frac{a}{b}$) la classe de l'élément $(a, b) \in \mathbb{Z} \times \mathbb{Z}_0$.*

On peut maintenant formaliser les opérations connues du point de vue empirique sur les éléments de $\mathbb{Q}$. On formalise simplement les opérations que l'on s'est appropriées sur les fractions dans l'enseignement primaire et secondaire.

Définition 6.1.4. *On définit sur $\mathbb{Q}$ l'opération d'addition*

$$+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} : ([a, b], [c, d]) \mapsto [ad + bc, bd]$$

et de multiplication

$$\cdot_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} : ([a, b], [c, d]) \mapsto [ac, bd].$$

Comme d'habitude, il est indispensable de vérifier que ces définitions formulées en termes de représentants sont bien posées.

Lemme 6.1.5. *Les définitions proposées sont indépendantes des choix des représentants.*

Démonstration.

- l'application $+_{\mathbb{Q}}$ est bien définie : si $(a,b) \sim (a',b')$ et si $(c,d) \sim (c',d')$ alors on a par définition
$$ab' = ba' \quad \text{et} \quad cd' = dc'.$$
Au vu de la définition de la somme, celle-ci est bien définie si on a
$$(a'd' + b'c', b'd') \sim (ad + bc, bd).$$
Vu la définition de $\sim$, c'est le cas si
$$(a'd' + b'c')bd = b'd'(ad + bc).$$
On obtient cette égalité par distributivité du produit sur la somme dans $\mathbb{Z}$ et commutativité du produit dans $\mathbb{Z}$, puisque
$$ab'dd' = ba'dd' \quad \text{et} \quad cd'bb' = dc'bb'.$$
- l'application $._{\mathbb{Q}}$ est bien définie : comme ci-dessus, si $(a,b) \sim (a',b')$ et si $(c,d) \sim (c',d')$ alors on a $ab' = ba'$ et $cd' = dc'$. L'application est bien définie si cela implique $(ac, bd) \sim (a'c', b'd')$, c'est-à-dire $acb'd' = bda'c'$. C'est visiblement le cas, vu la commutativité du produit dans $\mathbb{Z}$. □

Théorème 6.1.6. *La structure* $(\mathbb{Q}, +_{\mathbb{Q}}, 0, ._{\mathbb{Q}}, 1)$*, où* $0 = [0,1]$ *et* $1 = [1,1]$*, est un corps commutatif.*

Démonstration. On passe méthodiquement en revue chacun des axiomes déterminant cette structure algébrique. On utilise dans tous les cas la définition des opérations $+_{\mathbb{Q}}$ et $._{\mathbb{Q}}$ et de la relation d'équivalence $\sim$ (définitions 6.1.4 et 6.1.1). On se ramène ainsi à des propriétés connues dans $\mathbb{Z}$.

- L'opération $+_{\mathbb{Q}}$ est associative : soient $[a,b], [c,d], [e,f] \in \mathbb{Q}$. En utilisant la définition de $+_{\mathbb{Q}}$ et la distributivité de la multiplication sur l'addition dans $\mathbb{Z}$ (deux fois), on a successivement
$$\begin{aligned}([a,b] +_{\mathbb{Q}} [c,d]) +_{\mathbb{Q}} [e,f] &= [ad + bc, bd] +_{\mathbb{Q}} [e,f] \\ &= [(ad + bc)f + bde, bdf] \\ &= [adf + b(cf + de), bdf] \\ &= [a,b] +_{\mathbb{Q}} [cf + de, df] \\ &= [a,b] +_{\mathbb{Q}} ([c,d] +_{\mathbb{Q}} [e,f]),\end{aligned}$$
ce qu'il fallait démontrer.
- L'élément $[0,1]$ est neutre pour $+_{\mathbb{Q}}$: en effet, par définition de $+_{\mathbb{Q}}$ on a bien
$$[0,1] +_{\mathbb{Q}} [a,b] = [0.b + 1.a, 1.b] \quad \text{et} \quad [a,b] +_{\mathbb{Q}} [0,1] = [a.1 + b.0, b.1].$$
Ces deux expressions sont égales à $[a,b]$, vu les propriétés de 0 et 1 pour la multiplication dans $\mathbb{Z}$.

- Tout élément de $\mathbb{Q}$ admet un opposé additif : en effet, soit $[a,b] \in \mathbb{Q}$. Par définition de $+_{\mathbb{Q}}$, on a alors
$$[a,b] +_{\mathbb{Q}} [-a,b] = [ab + (-a)b, bb]$$
et de même
$$[-a,b] +_{\mathbb{Q}} [a,b] = [(-a)b + ab, bb].$$
Par la distributivité de la multiplication sur l'addition dans $\mathbb{Z}$, ces deux expressions sont égales à $[0,bb]$, qui est lui-même égal à $[0,1]$ par définition de $\sim$.
- La somme $+_{\mathbb{Q}}$ est commutative : soient $[a,b],[c,d] \in \mathbb{Q}$, on a alors par définition de $+_{\mathbb{Q}}$
$$[a,b] +_{\mathbb{Q}} [c,d] = [ad + bc, bq] \quad \text{et} \quad [c,d] +_{\mathbb{Q}} [a,b] = [cb + da, bq].$$
On constate que ces nombres sont égaux en utilisant la commutativité de la somme et du produit dans $\mathbb{Z}$.
- La multiplication $._{\mathbb{Q}}$ est associative : soient $[a,b],[c,d],[e,f] \in \mathbb{Q}$. On obtient, en utilisant la définition de $._{\mathbb{Q}}$ et l'associativité de la multiplication dans $\mathbb{Z}$:
$$\begin{aligned}([a,b] ._{\mathbb{Q}} [c,d]) ._{\mathbb{Q}} [ef] &= [ac, bd] ._{\mathbb{Q}} [e,f] \\ &= [ace, bdf] \\ &= [a,b] ._{\mathbb{Q}} [ce, df] \\ &= [a,b] ._{\mathbb{Q}} ([c,d] ._{\mathbb{Q}} [e,f]),\end{aligned}$$
comme attendu.
- L'élément $[1,1]$ est neutre pour $._{\mathbb{Q}}$: en effet, on a, par définition de $._{\mathbb{Q}}$
$$[a,b] ._{\mathbb{Q}} [1,1] = [a.1, b.1] \quad \text{et} \quad [1,1] ._{\mathbb{Q}} [a,b] = [1.a, 1.b]$$
Ces expressions sont égales à $[a,b]$ car 1 est neutre pour la multiplication dans $\mathbb{Z}$.
- Tout élément non nul de $\mathbb{Q}$ admet un inverse multiplicatif : soit $[a,b] \in \mathbb{Q} \setminus \{[0,0]\}$, c'est-à-dire $a \neq 0$. On constate que $[b,a] \in \mathbb{Q}$ est inverse de $[a,b]$. En effet, on a
$$[a,b] ._{\mathbb{Q}} [b,a] = [ab, ba] = [1,1]$$
et de même
$$[b,a] ._{\mathbb{Q}} [a,b] = [ba, ab] = [1,1],$$
par définition de $._{\mathbb{Q}}$ et de la relation $\sim$.
- La multiplication $._{\mathbb{Q}}$ est commutative : soient $[a,b],[c,d] \in \mathbb{Q}$. On a, par définition de $._{\mathbb{Q}}$,
$$[a,b] ._{\mathbb{Q}} [c,d] = [ac, bd] \quad \text{et} \quad [c,d] ._{\mathbb{Q}} [a,b] = [ca, db].$$
Ces expressions sont égales vu la commutativité du produit dans $\mathbb{Z}$.

- Le produit $._{\mathbb{Q}}$ distribue $+_{\mathbb{Q}}$: soient $[a,b],[c,d],[e,f] \in \mathbb{Q}$. D'une part, on vérifie que

$$\begin{aligned}([a,b] +_{\mathbb{Q}} [c,d]) \,._{\mathbb{Q}} [e,f] &= [ad+bc, bd] \,._{\mathbb{Q}} [e,f] \\ &= [ade+bce, bdf]\end{aligned}$$

en utilisant les définitions de $+_{\mathbb{Q}}$ et $._{\mathbb{Q}}$ et l'associativité de la multiplication dans $\mathbb{Z}$. D'autre part, toujours par définition et associativité de la multiplication dans $\mathbb{Z}$ on a

$$\begin{aligned}[a,b] \,._{\mathbb{Q}} [e,f] +_{\mathbb{Q}} [c,d] \,._{\mathbb{Q}} [e,f] &= [ae, bf] +_{\mathbb{Q}} [ce, df] \\ &= [aedf + bfce, bfdf].\end{aligned}$$

On constate que ces deux expressions sont égales en utilisant la commutativité du produit dans $\mathbb{Z}$ et la définition de $\sim$. □

Le résultat suivant est intéressant et nous apprend que l'ensemble $\mathbb{Q}$ est bien une extension de l'ensemble $\mathbb{Z}$ des entiers. On aurait d'ailleurs pu caractériser la structure de $\mathbb{Q}$ en utilisant cette propriété.

Théorème 6.1.7. *L'application*

$$\phi_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q} : a \mapsto [a,1]$$

est une injection préservant la structure d'anneau de $(\mathbb{Z}, +, 0, \cdot, 1)$.

Démonstration. Soient $a, b \in \mathbb{Z}$ satisfaisant $\phi_{\mathbb{Z}}(a) = \phi_{\mathbb{Z}}(b)$. Alors on a par définition

$$[a,1] = [b,1].$$

Par définition de $\sim$, c'est équivalent à $a.1 = 1.b$ ou encore à $a = b$ puisque 1 est neutre pour la multiplication dans $\mathbb{Z}$. De plus, pour tous $a, b \in \mathbb{Z}$, on obtient d'une part

$$\phi_{\mathbb{Z}}(a+b) = [a+b,1] = [a,1] +_{\mathbb{Q}} [b,1] = \phi_{\mathbb{Z}}(a) +_{\mathbb{Q}} \phi_{\mathbb{Z}}(b)$$

par définition de $\phi_{\mathbb{Z}}$ et $+_{\mathbb{Q}}$ et d'autre part

$$\phi_{\mathbb{Z}}(m.n) = [m.n,1] = [m,1] \,._{\mathbb{Q}} [n,1] = \phi_{\mathbb{Z}}(m) \,._{\mathbb{Q}} \phi_{\mathbb{Z}}(n).$$

par définition de $\phi_{\mathbb{Z}}$ et $._{\mathbb{Q}}$ Pour conclure, il reste à observer

$$\phi_{\mathbb{Z}}(0) = [0,1] = 0$$

et

$$\phi_{\mathbb{Z}}(1) = [1,1] = 1,$$

vu les définitions de $\phi_{\mathbb{Z}}$ et des neutres additif et multiplicatif de $\mathbb{Q}$. □

6.2 Ordre sur $\mathbb{Q}$

On souhaite à présent définir une relation d'ordre sur $\mathbb{Q}$ de manière à ce que le plongement

$$\phi_{\mathbb{Z}} : (\mathbb{Z}, \leq) \to (\mathbb{Q}, \leq)$$

soit un morphisme de structures ordonnées, i.e.

$$a \leq b \Rightarrow \phi(a) \leq \phi(b)$$

pour tous $a, b \in \mathbb{Z}$. La relation d'équivalence $\sim$ qui nous a permis de définir $\mathbb{Q}$ (voir la définition 6.1.1) et la définition de l'ordre sur $\mathbb{Z}$ semblent indiquer une manière de procéder. En effet, on pourrait alors vouloir définir l'ordre comme suit :

$$[a, b] \leq [c, d] \Leftrightarrow ad \leq bc$$

Cependant, cette définition n'est pas encore satisfaisante puisqu'elle dépend du représentant. En effet, soit par exemple $[-a, -b] \sim [a, b]$ [2], pour que la relation ci-dessus soit bien définie on devrait avoir

$$ad \leq bc \leftrightarrow (-a)d \leq (-b)c.$$

Il n'est pas difficile de voir que cette relation n'est pas valide, vu la proposition 5.3.4. Il faut donc prendre une précaution pour définir la relation d'ordre naturelle sur $\mathbb{Q}$.

Définition 6.2.1. *On considère la relation binaire $\leq$ définie sur $\mathbb{Q}$ par*

$$[a, b] \leq [c, d] \Leftrightarrow ad \leq bc$$

pour tous $[a, b], [c, d] \in \mathbb{Q}$, tels que $b > 0$ et $d > 0$.

On notera que la condition dans la définition n'est pas une restriction : tout élément $[a, b]$ de $\mathbb{Q}$ est égal à un élément $[a', b']$ tel que $b' > 0$, comme nous l'avons vu ci-dessus. Il reste alors à démontrer, comme d'habitude, que la définition est indépendante du choix des représentants et qu'il s'agit bien d'une relation d'ordre prolongeant celle définie sur l'ensemble $\mathbb{Z}$ des entiers (voir définition 5.3.2).

Lemme 6.2.2. *La relation $\leq$ est une relation d'ordre bien définie sur $\mathbb{Q}$. De plus cet ordre est total.*

Démonstration.

- La relation $\leq$ est bien définie :
  Soient $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ satisfaisant $(a, b) \sim (a', b')$ et $(c, d) \sim (c', d')$, tels que $[a, b] \leq [c, d]$, et $b, b', d, d' > 0$. On souhaite montrer qu'on a alors aussi $[a', b'] \leq [c', d']$. On a par définition
  $$ad \leq bc.$$

2. Un tel représentant existe toujours. En effet on peut montrer facilement que $a \cdot (-b) = b \cdot (-a)$ dans $\mathbb{Z}$, simplement après avoir constaté que $-a = (-1) \cdot a$ dans $\mathbb{Z}$.

En utilisant la proposition 5.3.4, on obtient, puisque $b' > 0$ et $d' > 0$,

$$adb'd' \leq bcb'd'.$$

En tenant compte de $ab' = a'b$ et $cd' = c'd$, cela donne

$$a'd'bd \leq c'b'bd,$$

et finalement $a'd' \leq c'b'$ vu que $b > 0$ et $d > 0$, comme souhaité.

- la relation $\leq$ est une relation d'ordre :

  (i) réflexivité : Il suffit d'utiliser la définition 6.2.1. En effet, si $[a, b] \in \mathbb{Q}, b > 0$, on obtient
  $$[a, b] \leq [a, b] \Leftrightarrow ab \leq ba.$$
  Cette condition est satisfaite vu que la relation $\leq$ dans le membre de droite est l'ordre sur $\mathbb{Z}$ et que la multiplication est commutative dans $\mathbb{Z}$.

  (ii) antisymétrie : Soient $[a, b], [c, d] \in \mathbb{Q}$ satisfaisant $b > 0$, $c > 0$ et $[a, b] \leq [c, d]$ et $[c, d] \leq [a, b]$. On a
  $$ad \leq bc \leq ad$$
  par définition et finalement $ad = bc$ (c'est-à-dire $[a, b] = [c, d]$, par définition de $\sim$) puisque dans cette relation $\leq$ est l'ordre sur $\mathbb{Z}$.

  (iii) transitivité :
  Soient $[a, b], [c, d], [e, f] \in \mathbb{Q}$ tels que $[a, b] \leq [c, d]$ et $[c, d] \leq [e, f]$, où b, d, f sont strictement positifs. La définition 6.2.1 garantit alors $ad \leq bc$ et $cf \leq de$. On souhaite prouver $[a, b] \leq [e, f]$, c'est à dire $af \leq be$. On utilise la proposition 5.3.4 pour obtenir
  $$adf \leq bcf \quad \text{et} \quad bcf \leq bde,$$
  qui par transitivité de l'ordre sur $\mathbb{Z}$ fournit $adf \leq bde$ et finalement $af \leq be$, toujours par la proposition 5.3.4. □

- La relation $\leq$ est un ordre total : soient $[a, b]$ et $[c, d]$ deux éléments de $\mathbb{Q}$ tels que $b > 0$ et $d > 0$. On a
  $$[a, b] \leq [c, d] \leftrightarrow ad \leq bc \quad \text{et} \quad [c, d] \leq [a, b] \leftrightarrow cb \leq ad.$$
  Puisque l'ordre sur $\mathbb{Z}$ est total vu le théorème 5.3.3, une de ces deux relations est satisfaite.

Nous aurons besoin dans la suite des propriétés suivantes :

Proposition 6.2.3. *Pour tous $[a, b], [c, d], [e, f] \in \mathbb{Q}$, on a*

(i) $[a, b] \leq [c, d] \leftrightarrow [a, b] + [e, f] \leq [c, d] + [e, f]$.

(ii) $[a, b] \leq [c, d] \leftrightarrow [a, b][e, f] \leq [c, d][e, f]$ *si* $0 < [e, f]$.

Démonstration. Comme d'habitude, on peut supposer $b, d, f > 0$. Pour prouver (i), on utilise la définition de l'ordre sur $\mathbb{Q}$, les propriétés des opérations dans $\mathbb{Z}$ et la proposition (5.3.4) et on obtient :

$$\begin{aligned}
[a,b]+[e,f] \leq [c,d]+[e,f] &\leftrightarrow [af+be, bf] \leq [cf+de, df] \\
&\leftrightarrow (af+be)df \leq (cf+de)bf \\
&\leftrightarrow adf^2 + bedf \leq bcf^2 + debf \\
&\leftrightarrow adf^2 \leq bcf^2 \\
&\leftrightarrow ad \leq bc \\
&\leftrightarrow [a,b] \leq [c,d].
\end{aligned}$$

Pour prouver le point (ii), on observe que l'hypothèse supplémentaire de l'énoncé (ii) garantit $e > 0$. En procédant comme précédemment, on obtient alors

$$\begin{aligned}
[a,b] \leq [c,d] &\leftrightarrow ad \leq bc \\
&\leftrightarrow aedf \leq cebf \\
&\leftrightarrow [ae, bf] \leq [ce, df] \\
&\leftrightarrow [a,b][e,f] \leq [c,d][e,f].
\end{aligned}$$

□

Nous prouvons à présent que le corps $(\mathbb{Q}, \leq)$ est archimédien [3] :

Proposition 6.2.4. *Soit $[a,b] \in \mathbb{Q}$. Alors il existe $n \in \mathbb{N}$ tel que $[a,b] \leq n$.*

Démonstration. Si $[a,b] \leq 0$, le résultat est direct. Sinon, on peut supposer $a, b > 0$ et on constate alors que l'entier a^+ répond à la question. En effet, on a

$$[a,b] \leq [a^+, 1] \leftrightarrow a \leq a^+ b = a + b.$$

La conclusion est alors une conséquence du lemme 4.4.10. □

On conclut cette section en vérifiant que le plongement $\phi_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$ a bien les propriétés voulues :

Théorème 6.2.5. *Le plongement $\phi_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$ est un morphisme de structures ordonnées.*

Démonstration. Soient $a, b \in \mathbb{Z}$ satisfaisant $a \leq b$. On a

$$[a,1] \leq [b,1]$$

vu que cette dernière relation est équivalente à $a.1 \leq 1.b$ en vertu de la définition 6.2.1. □

3. Pour rappel, cela signifie que tout rationnel est majoré par un entier. Cette notion sera approfondie dans le chapitre 9. Voir définition 9.2.1.

6.3 Une carence de $\mathbb{Q}$

Pour terminer ce chapitre, nous formulons un résultat négatif mettant en évidence une "carence" du corps $\mathbb{Q}$ que nous venons de construire :

Théorème 6.3.1. *Il n'existe pas de rationnel z tels que $z.z = 2$.*

Démonstration. On procède par l'absurde et l'on suppose qu'il existe $p \in \mathbb{Z}, q \in \mathbb{Z}_0$ tels que $pgcd(p, q) = 1$ et

$$[p, q].[p, q] = 2.$$

On en déduit $p^2 = 2q^2$ par définition du produit dans $\mathbb{Q}$. En particulier p^2 est pair et donc p est pair (le carré d'un nombre impair est impair). Comme $pgcd(p, q) = 1$, on obtient que q est impair. Or, soit $l \in \mathbb{Z}$ tel que $p = 2l$. On a alors, après simplification, $2l^2 = q^2$. Dès lors, q est pair, ce qui contredit notre hypothèse initiale. Ainsi, la racine carrée de 2 n'est pas un nombre rationnel. □

La découverte du résultat précédent remonte aux recherches des géomètres grecs et bouleversa les conceptions des mathématiciens de l'époque. D'un point de vue plus moderne, cette difficulté suggère que le processus d'extension menant de l'ensemble $\mathbb{N}$ à $\mathbb{Z}$ et ensuite de $\mathbb{Z}$ à $\mathbb{Q}$ devrait être poursuivi afin de définir des "nombres" qui ne sont pas rationnels et pourraient fournir une solution à ce genre d'équations.

La concrétisation de cette idée devra attendre la fin du 19^e siècle et sera proposée finalement par Dedekind et Cantor (Voir [9, 11]). Chemin faisant, notons que certaines idées de la construction de Cantor était déjà présentes dans les travaux des Anciens. Par exemple, la méthode de Héron permettant d'approximer la racine carrée d'un rationnel $a > 0$, fondée sur la considération de la suite $(x_n)_{n\in\mathbb{N}}$ définie par la récurrence suivante

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right),$$

fournit explicitement une suite de Cauchy [4] approximant $\sqrt{a}$ dont les termes sont tous rationnels dès que la condition initiale x_0 l'est aussi.

L'objectif de la partie suivante du travail est de détailler ces deux constructions classiques de l'ensemble des nombres réels, celle de Dedekind reposant sur la notion de coupure et celle de Cantor reposant sur la notion de suite de Cauchy et de prouver ensuite que ces deux constructions sont équivalentes dans le sens où il existe un isomorphisme (de corps commutatifs) entre les deux structures proposées.

4. Pour rappel, une suite $(x_n)_{n\in\mathbb{N}}$ de rationnels est de Cauchy si pour tout ϵ rationnel et strictement positif, il existe $N \in \mathbb{N}$ satisfaisant :

$$(r, s > N) \rightarrow |x_r - x_s| \leq \epsilon.$$

Voir [26] pour plus de détails.

Troisième partie

Constructions classiques de $\mathbb{R}$

Chapitre 7

La construction de Dedekind

Selon [4, p.65], le principe de départ, pour Dedekind, est de construire l'analyse sans le recours à la géométrie. Il s'inscrit alors dans le courant de l'arithmétisation de l'analyse (courant né au XIXe siècle). Dedekind écrit en effet que : "toute proposition - si peu évidente qu'elle soit - de l'algèbre et de l'analyse supérieure peut être exprimée sous forme d'une proposition sur les nombres naturels". En conséquence, Dedekind va définir les réels comme une extension du corps des fractions. Selon [4, p.67], Dedekind en déduit qu'il faut "raffiner de façon essentielle l'instrument $\mathbb{R}$ [...], en créant de nouveaux nombres tels que le domaine des nombres devienne aussi complet, ou nous dirons tout de suite aussi continu, que la droite".

La construction de Dedekind est fondée sur la notion de coupure. Nous commençons par la définition et l'étude des premières propriétés de ces dernières. Nous définissons sur l'ensemble formé par ces coupures des opérations algébriques (somme, produit) de façon à faire de cet ensemble un corps commutatif qui est une extension de $\mathbb{Q}$, satisfaisant la propriété de la borne supérieure.

7.1 Coupures de Dedekind

La construction proposée par Dedekind en 1872 dans son ouvrage intitulé "Stetigkeit und irrationale Zahlen" [1] repose sur la notion fondamentale de coupure.

Définition 7.1.1. *Une coupure de $\mathbb{Q}$ est la donnée d'un ensemble $A \subseteq \mathbb{Q}$ tel que*

C1 : A est un sous-ensemble non vide distinct de $\mathbb{Q}$;

C2 : tout élément de $A^c = \mathbb{Q} \setminus A$ est plus grand que tout élément de A ;

C3 : A est majoré mais ne possède pas de plus grand élément [2].

Remarque 7.1.2. *En pratique, pour établir C2 on utilisera l'équivalence suivante :*

$$[(a \in A) \wedge (b \in A^c)] \to [a < b] \quad \leftrightarrow \quad [(a \in A) \wedge (b \leq a)] \to (b \in A)$$

1. Continuité et nombres irrationnels.
2. C'est-à-dire un élément $x \in A$ tel que $y \in A \to y \leq x$.

Cette équivalence est obtenue en considérant la contraposée de C2 et en maintenant l'hypothèse $a \in A$.

Exemple 7.1.1. *Soit $q \in \mathbb{Q}$, alors l'ensemble A_q défini par*

$$A_q = \left\{ r \in \mathbb{Q} \;\middle|\; r < q \right\}$$

est une coupure. On vérifie en effet que les trois conditions de la définition sont satisfaites.

C1 : il est évident que A_q est non vide et distinct de $\mathbb{Q}$ car d'une part on a $q - 1 \in A_q$ et d'autre part $q \notin A_q$;

C2 : si $r \in A_q$ et $s \in A_q^c$, alors par définition on a $r < q \leq s$ et donc $r < s$;

C3 : par définition, pour tout élément r de A_q, on a $r < q$ donc A_q est majoré. De plus, on sait qu'alors il existe $r' \in \mathbb{Q}$ tel que $r < r' < q$ (par exemple $r' = \frac{1}{2}(r + q)$), ainsi $r' \in A_q$ et on en conclut que A_q ne possède pas de plus grand élément.

Définition 7.1.3. *L'ensemble des réels, noté $\mathbb{R}_{\mathrm{D}}$, est l'ensemble de toutes les coupures de $\mathbb{Q}$.*

On note que par définition, $\mathbb{R}_{\mathrm{D}}$ est une partie des parties de $\mathbb{Q}$, il s'agit donc bien d'un ensemble.

Comme on l'a déjà mentionné, le souhait de Dedekind était de pouvoir définir les réels comme une extension de $\mathbb{Q}$. On vérifie alors qu'il existe un plongement de $\mathbb{Q}$ vers $\mathbb{R}_{\mathrm{D}}$. D'abord, on montre qu'il existe une injection de $\mathbb{Q}$ dans $\mathbb{R}_{\mathrm{D}}$.

Proposition 7.1.4. *La fonction ϕ définie par*

$$\phi \;:\; \mathbb{Q} \to \mathbb{R}_{\mathrm{D}} \;:\; q \mapsto A_q = \{ r \in \mathbb{Q} \,|\, r < q \}.$$

est une injection.

Démonstration.

- L'application ainsi définie a bien un sens car, comme on l'a vu dans l'exemple 7.1.1, l'ensemble A_q obtenu est bien une coupure.
- On prouve à présent l'injectivité de la fonction ϕ. Soient $q, r \in \mathbb{Q}$ tels que $q \neq r$. Alors, comme l'ordre sur $\mathbb{Q}$ est total, on a soit $q < r$ soit $r < q$. Sans perte de généralité, on peut supposer $q < r$. Mais alors, il existe au moins un élément $t \in \mathbb{Q}$ tel que $q < t < r$ de sorte que $t \notin A_q$ et $t \in A_r$. Ainsi, on obtient

$$\phi(q) = A_q \neq A_r = \phi(r).$$

□

7.2 Ordre sur $\mathbb{R}_{\mathrm{D}}$

Les réels étant définis comme une partie des parties de $\mathbb{Q}$, l'inclusion semble tout à propos pour y définir un ordre.

Définition 7.2.1. *On définit la relation $\leq_{\mathbb{R}_{\mathrm{D}}}$ sur l'ensemble $\mathbb{R}_{\mathrm{D}}$ par*

$$x_1 \leq_{\mathbb{R}_{\mathrm{D}}} x_2 \leftrightarrow x_1 \subseteq x_2.$$

Il est évident que $\leq_{\mathbb{R}_{\mathrm{D}}}$ définit une relation d'ordre, puisqu'il s'agit de la relation d'inclusion entre des sous-ensembles de $\mathbb{Q}$. De plus, on vérifie que l'injection naturelle de $\mathbb{Q}$ dans $\mathbb{R}_{\mathrm{D}}$ définie ci-dessus préserve l'ordre.

Proposition 7.2.2. *Pour tous rationnels r et s, on a*

$$r \leq s \leftrightarrow \phi(r) \leq_{\mathbb{R}_{\mathrm{D}}} \phi(s).$$

Démonstration.

- On montre d'abord qu'on a $r \leq s \rightarrow \phi(r) \leq_{\mathbb{R}_{\mathrm{D}}} \phi(s)$. Si $r \leq s$ alors pour tout élément q de $\phi(r)$ on a $q < r \leq s$ et donc $q \in \phi(s)$. On a donc bien $\phi(r) \subseteq \phi(s)$, c'est-à-dire $\phi(r) \leq_{\mathbb{R}_{\mathrm{D}}} \phi(s)$;
- Réciproquement, si $\phi(r) \leq_{\mathbb{R}_{\mathrm{D}}} \phi(s)$, alors $q < r \rightarrow q < s$. Or, l'ordre sur $\mathbb{Q}$ est total (par le lemme 6.2.2). Dès lors, on a soit $r \leq s$ soit $s < r$. Si $s < r$, comme on sait qu'il existe $q \in \mathbb{Q}$ tel que $s < q < r$, on a d'une part $q \in \phi(r)$ et d'autre part $q \notin \phi(s)$ ce qui est contraire à notre hypothèse. Dès lors $r \leq s$. □

Proposition 7.2.3. *La relation $\leq_{\mathbb{R}_{\mathrm{D}}}$ est une relation d'ordre total sur $\mathbb{R}_{\mathrm{D}}$.*

Démonstration. On sait déjà que $\leq_{\mathbb{R}_{\mathrm{D}}}$ définit un ordre sur $\mathbb{R}_{\mathrm{D}}$. Montrons qu'il est total. Soient x et y deux réels, on montre que si ceux-ci ne vérifient pas $x \leq_{\mathbb{R}_{\mathrm{D}}} y$ alors on a $y \leq_{\mathbb{R}_{\mathrm{D}}} x$. Comme on suppose que $\neg(x \subseteq y)$, on peut alors exhiber un rationnel q tel que $q \in x$ et $q \notin y$. Soit alors $r \in y$, comme l'ordre sur $\mathbb{Q}$ est total, on a soit $q \leq r$ soit $r \leq q$. Or, vu la remarque 7.1.2 on a

$$q \leq r \rightarrow q \in y.$$

Donc, si $q \leq r$, alors on a $q \in y$ ce qui est contraire à nos hypothèses. Il en résulte que $r \leq q$. Avec les mêmes arguments, on déduit que $r \in x$. On a donc prouvé que $y \subseteq x$, ou encore que $y \leq_{\mathbb{R}_{\mathrm{D}}} x$, comme annoncé. □

Remarque 7.2.4. *Dans la suite, pour ne pas alourdir les notations, l'on se permettra de noter simplement $\leq$ l'ordre sur $\mathbb{R}_{\mathrm{D}}$ si aucune confusion n'est possible.*

Nous avons montré, dans la section sur les carences analytiques de $\mathbb{Q}$, qu'il existe dans $\mathbb{Q}$ des sous-ensembles qui ne possèdent pas de borne supérieure. Nous montrons ici que cette carence est dissipée dans $\mathbb{R}_{\mathrm{D}}$.

Théorème 7.2.5 (Borne Sup)**.** *Tout ensemble A majoré et non-vide de $\mathbb{R}_{\mathrm{D}}$ admet une borne supérieure*[3]*. Tout ensemble non-vide et minoré admet une borne inférieure.*

Démonstration. Étant donné $A \subset \mathbb{R}_{\mathrm{D}}$ majoré, on considère

$$\sup A = \bigcup A.$$

- On montre que $\sup A$ est une coupure au sens de Dedekind et que c'est la borne supérieure de A :

  C1 : D'une part, $\sup A$ est non-vide en tant qu'union d'ensembles non-vides et d'autre part, comme A est majoré, on sait qu'il existe $x \in \mathbb{R}_{\mathrm{D}}$ tel que $\forall y \in A,\ y \leq_{\mathbb{R}_{\mathrm{D}}} x$. Puisque x est une coupure, il existe $q \in \mathbb{Q}$ tel que $q \notin x$. Dès lors, on a $\forall y \in A[q \notin y]$, donc $q \notin \sup A$, si bien que $\sup A \neq \mathbb{Q}$.

  C2 : Soit un rationnel $q \in \sup A$, par définition on sait qu'il existe alors une coupure $x \in A$ tel que $q \in x$. Dès lors, pour tout rationnel $r \leq q$, on a $r \in x$ et donc $r \in \sup A$.

  C3 : Soit un rationnel $q \in \sup A$. À nouveau, on sait qu'il existe une coupure $x \in A$ telle que $q \in x$. Il s'ensuit qu'il existe un rationnel r appartenant à x, donc à $\sup A$, et tel que $q < r$. Donc $\sup A$ n'a pas de plus grand élément.

- Il reste à montrer que $\sup A$ est la borne supérieure de A. Cela est évident vu la définition de $\sup A$. En effet, si $x \in A$, alors $x \subseteq \sup A$ i.e. $x \leq_{\mathbb{R}_{\mathrm{D}}} \sup A$ et $\sup A$ est bien un majorant de A. Enfin, pour tout majorant $M \in \mathbb{R}_{\mathrm{D}}$ de A, on a par définition

  $$x \in A \to x \leq_{\mathbb{R}_{\mathrm{D}}} M.$$

  Ainsi pour tout $x \in A$, on a $x \subseteq M$ vu la définition d'un majorant et donc $\sup A = \bigcup_A x \subseteq M$.

Passons maintenant à la borne inférieure. Si A est un ensemble minoré, alors l'ensemble B des minorants de A est non vide (par hypothèse) et majoré par tout élément de A. On peut donc considérer $\sup B$. C'est une coupure vu la première partie de la proposition, parce que c'est une borne supérieure. Montrons que c'est une borne inférieure de A. Si $x \in A$, alors pour tout $y \in B$, $y \leq_{\mathbb{R}_{\mathrm{D}}} x$, donc x est un majorant de B, et donc $\sup B \leq_{\mathbb{R}_{\mathrm{D}}} x$, par définition. Donc $\sup B$ est un minorant de A. Enfin, par définition, $\sup B$ est supérieur à tous les minorants de A. □

Dans le même ordre d'idées, on peut établir le résultat technique suivant.

Proposition 7.2.6. *Pour tout $x \in \mathbb{R}_{\mathrm{D}}$ et tout rationnel $r > 0$, il existe $p \in x$ tel que $p + r \notin x$.*

3. La notion de borne supérieure d'un ensemble A est définie de manière usuelle : c'est un élément y de $\mathbb{R}_{\mathrm{D}}$ tel que $\forall x \in A[x \leq_{\mathbb{R}_{\mathrm{D}}} y]$, et si $\forall x \in A[x \leq_{\mathbb{R}_{\mathrm{D}}} M]$, alors $y \leq_{\mathbb{R}_{\mathrm{D}}} M$. La notion de borne inférieure est définie de manière analogue.

Démonstration. On considère $p_0 \in x$ et l'ensemble

$$A = \{n \in \mathbb{N} \,|p_0 + n.r \notin x\}.$$

Comme x est une coupure, il existe $q \in \mathbb{Q}$ tel que $q \notin x$. Puisque $\mathbb{Q}$ est archimédien, il existe $n \in \mathbb{N}$ tel que $p_0 + n.r > q$. On a alors $p_0 + n.r \notin x$. L'ensemble A n'est donc pas vide. Puisque $\mathbb{N}$ est bien ordonné, A admet un plus petit élément n_0, non nul puisque $p_0 \in x$. Alors pour $p = p_0 + (n_0 - 1).r$, on obtient $p \in x$ car n_0 est le plus petit élément de A et $p + r = p_0 + n_0.r \notin x$, comme souhaité. □

7.3 L'addition dans $\mathbb{R}_{\mathrm{D}}$

Comme pour le passage de $\mathbb{N}$ à $\mathbb{Z}$ et de $\mathbb{Z}$ à $\mathbb{Q}$, l'objectif est à présent de définir sur l'ensemble $\mathbb{R}_{\mathrm{D}}$ des coupures de Dedekind une opération d'addition $+_R$, et plus tard une opération de multiplication $\cdot_R$, compatibles avec celles sur $\mathbb{Q}$ au travers de l'injection naturelle ϕ de $\mathbb{Q}$ dans $\mathbb{R}_{\mathrm{D}}$. On s'intéresse d'abord à la somme. Notre contrainte est donc la suivante : en supposant l'opération $+_R$ donnée, pour tous rationnels r et s on veut pouvoir vérifier l'égalité suivante

$$\phi(r) +_R \phi(s) = \phi(r + s).$$

où, par définition,

$$\phi(r) = \Big\{q \in \mathbb{Q} \;\Big|\; q < r\Big\},$$
$$\phi(s) = \Big\{q \in \mathbb{Q} \;\Big|\; q < s\Big\}$$

et

$$\phi(r + s) = \Big\{q \in \mathbb{Q} \;\Big|\; q < r + s\Big\}.$$

Or, exiger $q < r$ est équivalent à exiger $q \in \phi(r)$; cela nous permet d'écrire nos conditions non plus par rapport au rationnel r mais bien par rapport au réel $\phi(r)$ qui lui est associé. Ensuite, on souhaite traduire la condition qui définit l'ensemble $\phi(r + s)$.

Lemme 7.3.1. *Soient deux rationnels r et s. Alors un rationnel q est tel que $q < r + s$ si et seulement si il existe deux rationnels q_r et q_s tels que $q_r < r$ et $q_s < s$ et $q = q_r + q_s$.*

Démonstration. Si q s'écrit $q_r + q_s$ où $q_r < r$ et $q_s < s$, les propriétés de la somme vis-à-vis de l'ordre dans $\mathbb{Q}$ garantissent que $q < r + s$. Réciproquement, si $q < r + s$, alors il existe $q' \in \mathbb{Q}$ tel que $q < q' < r + s$. On écrit alors

$$q = (q' - s) + (s + q - q')$$

où $q' - s < r$ car $q' < r + s$ et où $s + q - q' < s$ car $q < q'$. □

À l'aide de cette description, $\phi(r + s)$ peut être réexprimé comme suit :

$$\phi(r + s) = \{q_r + q_s \mid q_r \in \phi(r) \text{ et } q_s \in \phi(s)\}.$$

On peut alors généraliser à $\mathbb{R}_{\mathrm{D}}$ tout entier.

Définition 7.3.2. *On définit comme opération d'addition sur* $\mathbb{R}_{\mathrm{D}}$ *l'application suivante :*

$$+_R : \mathbb{R}_{\mathrm{D}} \times \mathbb{R}_{\mathrm{D}} \to \mathbb{R}_{\mathrm{D}} \ : \ (x, y) \mapsto x +_R y = \{p + q | p \in x \ et \ q \in y\}.$$

Il est naturel de vérifier que l'opération "somme" est bien définie, c'est-à-dire à valeurs dans $\mathbb{R}_{\mathrm{D}}$. On s'intéresse ensuite à ses propriétés.

Proposition 7.3.3. *Pour tous* $x, y \in \mathbb{R}_{\mathrm{D}}$ *la somme* $x +_R y$ *est bien une coupure de Dedekind. De plus, la somme est associative et commutative et on a*

$$\phi(r + s) = \phi(r) + \phi(s)$$

pour tous $r, s \in \mathbb{Q}$.

Démonstration. Passons en revue toutes les conditions.

- On montre que $x +_R y$ est une coupure en vérifiant les conditions de la définition 7.1.1.

  C1 : En effet, si $x, y \in \mathbb{R}_{\mathrm{D}}$ alors $x +_R y \neq \emptyset$ vu que

  $$x +_R y = \{r + s | r \in x \ et \ s \in y\}$$

  et que chacun des ensembles x, y est non-vide. De plus, vu que $x, y \in \mathbb{R}_{\mathrm{D}}$, il existe $r_0 \notin x$ et $s_0 \notin y$. On obtient alors

  $$r + s < r_0 + s_0$$

  pour tous $r \in x, s \in y$. Il vient alors $x +_R y \neq \mathbb{Q}$.

  C2 : Soient $r \in x +_R y$ et $s < r$. Par définition, il existe $p \in x$ et $q \in y$ tels que $r = p + q$. Dès lors $s - q < r - q = p$ et donc $s - q \in x$ (voir remarque 7.1.2). Ainsi, s est bien un élément de $x +_R y$ car il se décompose en la somme d'un élément de x et d'un élément de y :

  $$s = \underbrace{(s - q)}_{\in x} + \underbrace{q}_{\in y} \in x +_R y.$$

  C3 : Soit $s \in x +_R y$; par la définition 7.3.2 de la somme, on a alors que s est de la forme $s = s_x + s_y$, avec $s_x \in x$ et $s_y \in y$. Comme x et y sont des réels, on sait d'une part que chacun d'eux est majoré ; disons par M_x et M_y respectivement. Dès lors, $s = s_x + s_y < M_x + M_y$. La coupure $x +_R y$ est donc bien majorée. D'autre part, on sait qu'il existe $s'_x \in x$ et $s'_y \in y$ tels que $s_x < s'_x$ et $s_y < s'_y$. Donc, $s_x + s_y < s'_x + s'_y \in x +_R y$ et on conclut que $x +_R y$ n'a pas de plus grand élément.

- La somme est associative : $\forall x, y, z \in \mathbb{R}_{\mathrm{D}}[(x +_R y) +_R z = x +_R (y +_R z)]$. En développant chacun des termes suivant la définition 7.3.2 on obtient d'une part

  $$\begin{aligned}(x +_R y) +_R z &= \{q + r \mid q \in x +_R y \text{ et } r \in z\} \\ &= \{(s + t) + r \mid s \in x, \ t \in y \text{ et } r \in z\}\end{aligned}$$

et d'autre part,

$$\begin{aligned} x +_R (y +_R z) &= \{s + q \mid s \in x \text{ et } q \in (y +_R z)\} \\ &= \{s + (t + r) \mid s \in x,\ t \in y \text{ et } r \in z\}. \end{aligned}$$

L'égalité découle alors par double inclusion, directement de l'associativité de la somme dans $\mathbb{Q}$.

- La somme est commutative : $\forall x, y \in \mathbb{R}_{\mathrm{D}}[x +_R y = y +_R x]$.
  C'est une conséquence directe de la commutativité de la somme dans $\mathbb{Q}$: on doit démontrer
  $$\{r + s \mid r \in x \textit{ et } s \in y\} = \{s + r \mid s \in y \textit{ et } r \in x\}.$$
  L'égalité découle alors par double inclusion, de la commutativité de la somme dans $\mathbb{Q}$.
- Si r, s sont rationnels, alors on a
  $$\phi(r + s) = \{q \in \mathbb{Q} \,|q < r + s\}$$
  et
  $$\phi(r) + \phi(s) = \{q_r + q_s | q_r \in \phi(r) \text{ et } q_s \in \phi(s)\}.$$
  On montre que ces deux ensembles sont égaux par double inclusion en utilisant le lemme 7.3.1. □

Ayant à disposition une somme associative et commutative, il est naturel de chercher à définir un neutre. D'une part, on souhaitera que $\phi : \mathbb{Q} \to \mathbb{R}_{\mathrm{D}}$ soit un morphisme, et donc $\phi(0)$ semble un bon candidat comme neutre pour la somme. D'autre part, vu le dernier point de la proposition 7.3.3, on a

$$\phi(r) +_R \phi(0) = \phi(r + 0) = \phi(r)$$

pour tout $r \in \mathbb{Q}$. Si finalement $(\mathbb{R}_{\mathrm{D}}, +_R, 0_R)$ est un groupe, on doit donc avoir $0_R = \phi(0)$. Il n'est donc pas surprenant d'avoir le résultat suivant.

Proposition 7.3.4. *L'élément $0_R = \phi(0)$ est neutre pour l'addition $+_R$.*

Démonstration. Vu la commutativité de $+_R$, pour montrer que 0_R est le neutre, il suffit de montrer que $0_R +_R x = x$ pour tout $x \in \mathbb{R}_{\mathrm{D}}$. On procède par double inclusion :

- $x \subseteq 0_R +_R x$: soit $r \in x$, vu *C3* on sait qu'il existe et $r' \in x$ tel que $r < r'$. Dès lors $r = r' + (r - r') \in x +_R 0_R$.
- $0_R +_R x \subseteq x$: comme tout élément de $x +_R 0_R$ est de la forme $r + s$, avec $r \in x$ et $s < 0$, on a bien $r + s < r \in x$ donc $r + s \in x$ vu *C2*. □

On souhaite maintenant définir une structure de groupe sur $\mathbb{R}_{\mathrm{D}}$. Il est naturel de demander que l'opposé réel soit compatible avec le plongement ϕ de $\mathbb{Q}$ dans $\mathbb{R}$. En fait, vu le dernier point de la proposition 7.3.3, on n'a pas le choix puisque

$$\phi(r) + \phi(-r) = \phi(0) = 0_R\,.$$

Donc le passage à l'opposé $-_R$ doit vérifier la propriété suivante :

$$-_R\phi(r) = \phi(-r),$$

pour tout rationnel r.

Cependant, cette définition ne s'adapte pas directement à une coupure quelconque. Analysons la situation en étudiant la condition qui définit un opposé.

Lemme 7.3.5. *Soit $x \in \mathbb{R}_{\mathrm{D}}$. Alors on a $x +_R y \leq_{\mathbb{R}_{\mathrm{D}}} 0_R$ (pour $y \in \mathbb{R}_{\mathrm{D}}$) si et seulement si y est un minorant de $A = \{\phi(-r)|r \in x\}$.*

Démonstration. Par définition, la condition $x +_R y \leq_{\mathbb{R}_{\mathrm{D}}} 0_R$ est équivalente à

$$\forall r \in x, \forall s \in y, r + s < 0,$$

ou encore à

$$\forall r \in x, \forall s \in y, s < -r.$$

Cette condition est encore équivalente à

$$\forall r \in x, y \subseteq \phi(-r),$$

ou encore au fait que y soit un minorant de l'ensemble A de l'énoncé. □

D'un point de vue intuitif, le lemme précédent montre qu'une des inégalités nécessaires pour que y définisse un opposé de x impose que y soit un minorant d'un ensemble. On peut penser que pour avoir l'autre inégalité, il est raisonnable (voire nécessaire et suffisant) de choisir le plus grand des minorants. Ce choix est en fait imposé, comme le montre le résultat suivant.

Lemme 7.3.6. *Soit $x \in \mathbb{R}_{\mathrm{D}}$. Alors on a $x + y \geq_{\mathbb{R}_{\mathrm{D}}} 0_R$ (pour $y \in \mathbb{R}_{\mathrm{D}}$) si et seulement pour tout minorant w de $A = \{\phi(-r)|r \in x\}$, on a $w \leq_{\mathbb{R}_{\mathrm{D}}} y$.*

Démonstration. Supposons d'abord $x+y \geq_{\mathbb{R}_{\mathrm{D}}} 0_R$, considérons un minorant w de $\{\phi(-r)|r \in x\}$ et $t \in w$. Montrons alors que t appartient à y. Puisque w est une coupure, il existe t' tel que $t' \in w$ et $t < t'$. Alors $t - t' < 0$. Par hypothèse, il existe $x_1 \in x$ et $y_1 \in y$ tels que $x_1 + y_1 = t - t'$. On a alors $t = (t' + x_1) + y_1$. Puisque $t' \in w$, $t' \in \phi(-x_1)$, on a $t' + x_1 < 0$, et donc $t < y_1$, puis finalement $t \in y$.

Réciproquement, supposons que pour tout minorant w de $A = \{\phi(-r)|r \in x\}$, on a $w \leq_{\mathbb{R}_{\mathrm{D}}} y$ et montrons $x + y \geq_{\mathbb{R}_{\mathrm{D}}} 0_R$. Pour cela on considère $t \in \phi(0)$. Il existe $t' \in \mathbb{Q}$ tel que $t < t' < 0$ (car $\phi(0)$ est une coupure). Il existe ensuite $x_1 \in x$ tel que $x_1 - t' \notin x$, par la proposition 7.2.6. On a alors

$$\forall u \in x[x_1 - t' > u].$$

On a donc $-x_1 + t' < -u$ (ou $\phi(-x_1 + t') \leq_{\mathbb{R}_{\mathrm{D}}} \phi(-u)$) pour tout $u \in x$. L'hypothèse fournit alors $\phi(-x_1 + t') \leq_{\mathbb{R}_{\mathrm{D}}} y$, donc $-x_1 + t \in y$. Il existe donc $y_1 \in y$ tel que $-x_1 + t = y_1$, et finalement $t \in x + y$. □

Cela conduit naturellement à la définition de l'opposé.

Définition 7.3.7. *Pour tout $x \in \mathbb{R}_{\mathrm{D}}$, l'opposé de x est défini par*

$$-_R x = \inf\{\phi(-r) | r \in x\}.$$

Le résultat suivant résume les propriétés de l'opposé.

Proposition 7.3.8. *Soit $x \in \mathbb{R}_{\mathrm{D}}$. L'opposé $-_R x$ définit bien une coupure de Dedekind. De plus on a $x +_R (-_R x) = 0_R$. En particulier, $(\mathbb{R}_{\mathrm{D}}, +_R, 0_R)$ est un groupe commutatif.*

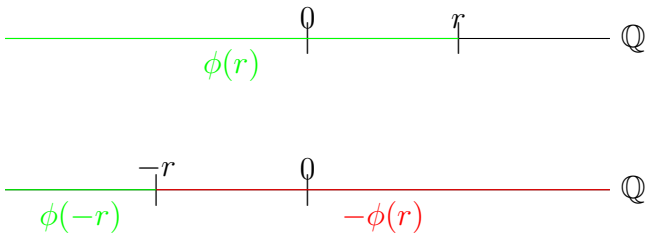
Démonstration. L'opposé $-_R x$ est bien une coupure parce que c'est une borne inférieure (voir le théorème 7.2.5). Le deuxième point découle alors directement des lemmes 7.3.5 et 7.3.6 et le dernier des propriétés de la somme $+_R$. □

À ce stade, nous avons bien défini sur $\mathbb{R}_{\mathrm{D}}$ une structure de groupe commutatif, dont l'addition est $+_R$ et le neutre 0_R. Mentionnons maintenant une autre construction de l'opposé proposée par Enderton [14] et qui semble plus basée sur une intuition géométrique de la "droite réelle".

Définissons pour tout sous-ensemble A de $\mathbb{Q}$ l'ensemble $-A = \{-r | r \in A\}$. Il apparaît alors que $\phi(-r) \neq -\phi(r)$:

$$\begin{aligned} -\phi(r) &= -\{s \in \mathbb{Q} \,|\, s < r\} \\ &= \{-s \in \mathbb{Q} \,|\, -(-s) < r\} \\ &= \{s \in \mathbb{Q} \,|\, s > -r\}. \end{aligned}$$

Ce n'est donc pas aussi simple mais cette première constatation, représentée schématiquement ci-dessous nous donne un premier (petit) pas vers la solution.



Le schéma nous souffle une première intuition : poser

$$-_R \phi(r) = \Big(-\phi(r) \Big)^c.$$

Cependant, l'ensemble $\Big(-\phi(r) \Big)^c$ possède un plus grand élément. La condition *C3* de la définition 7.1.1 d'une coupure n'est donc pas respectée. En effet,

- notons d'abord que comme il n'est pas possible d'avoir $-r < -r$ on a que $-r$ est un élément de $(-\phi(r))^c$;
- ensuite, comme par définition de $-\phi(r)$ et puisque l'ordre dans $\mathbb{Q}$ est total, il apparaît clairement que pour tout $q \in (-\phi(r))^c$ on a $q \leq -r$.

Dès lors, il faut à $\Big(-\phi(r)\Big)^c$ ajouter une contrainte pour s'assurer que pour tout élément q de $-_R\phi(r)$, il existe un élément q' dans $-_R\phi(r)$ tel que l'on ait $q < q'$. On propose alors pour $-_R\phi(r)$ l'ensemble des rationnels q tels que $-q \geq r$ (intuition première) et tels qu'il existe $q' > q$ tel que $-q' \geq r$ (pour vérifier (*C3*)). On remarque qu'on peut résumer les conditions, étant donné que

$$\Big[(-q \geq r) \wedge (q' > q) \wedge (-q' \geq r)\Big] \;\leftrightarrow\; \Big[(q' > q) \wedge (-q' \geq r)\Big].$$

Enfin, il faut arriver à généraliser la définition à un $x \in \mathbb{R}_{\mathrm{D}}$ quelconque. Pour cela, on remarque qu'exiger que $-q' \geq r$ revient à exiger que $-q' \notin \phi(r)$. On arrive alors à la définition suivante.

Définition 7.3.9. *Soit $x \in \mathbb{R}_{\mathrm{D}}$, on pose*

$$-_R x = \{r \in \mathbb{Q} \mid \exists q > r[-q \notin x]\}$$

et on dit que $-_R x$ est l'opposé de x.

Évidemment, on ne peut pas définir deux fois l'opposé. Si on veut suivre la démarche d'Enderton, on est amené à démontrer que $-_R x$, associé à $x \in \mathbb{R}_{\mathrm{D}}$ selon la définition 7.3.9, est bien défini, et qu'il est réellement l'opposé de x. C'est ce qui est fait dans la proposition suivante. Mais on peut aussi se contenter de montrer que l'opposé tel que défini selon la définition 7.3.9 coïncide avec l'opposé de la définition 7.3.7, c'est ce que nous ferons par la suite.

Proposition 7.3.10. *Le nombre $-_R x$ défini en 7.3.9 est une coupure. De plus, pour tout $x \in \mathbb{R}_{\mathrm{D}}$, on a $x +_R (-_R x) = 0_R$.*

Démonstration. On utilise la définition pour montrer que $-_R x$ est bien une coupure.

- *C1* : d'abord, on montre que $-_R x$ est non vide. Comme x est une coupure, on sait qu'il existe au moins un rationnel q qui ne soit pas dans x. Soit alors r un rationnel tel que $r < -q$. On a donc $-q > r$ et $-(-q) \notin x$. Ainsi, on a bien que r est un élément de $-_R x$. On montre ensuite que $-_R x \neq \mathbb{Q}$. Soit r un élément de x, alors, pour tout rationnel q tel que $q > -r$, on a $-q \in x$ (car $-q < r$). Dès lors, $-r$ ne peut appartenir à $-_R x$. Notons qu'ici on vient en particulier de montrer qu'on a

$$r \in x \to -r \notin -_R x.$$

- *C2* : si r est un élément de $-_R x$ et $s \leq r$, alors il existe $q > r$ tel que $-q \notin x$, donc on obtient $q > s$ et $-q \notin x$, qui implique $s \in -_R x$;
- *C3* : soit $s \in -_R x$, et donc t tel que $t > s$ et $-t \notin x$. On sait qu'il existe toujours $q \in \mathbb{Q}$ tel que $s < q < t$. On a alors $q > s$ et $q \in -_R x$. Cela montre que -$_R x$ n'a pas de plus grand élément.

Ensuite, montrons qu'alors $x +_R (-_R x) = 0_R$. On procède par double inclusion.

- On a $x +_R (-_R x) \subseteq 0_R$: tout élément de $x +_R (-_R x)$ est de la forme $s + s'$ où $s \in x$ et $s' \in -_r x$. En particulier, il existe $t > s'$ tel que $-t \notin x$ et donc tel que $s < -t$. Dès lors, $s + s' < s' - t < 0$.
- On a enfin $0_R \subseteq x +_R (-_R x)$: soit $p \in 0_R$. On a par définition $-p > 0$, donc $\frac{-p}{2} > 0$. Par la proposition 7.2.6, il existe $q \in x$ tel que

$$q + (\frac{-p}{2}) \notin x.$$

Donc, si on pose $s = \frac{p}{2} - q$, on a bien $-s \notin x$ et donc par définition de $-_R x$, tout rationnel r strictement inférieur à s appartient à $-_R x$. Alors on a

$$p = q + (p - q),$$

où $q \in x$ et $(p - q) \in -_R x$ vu que $p - q < s$. Et donc $p \in x +_R (-_R x)$. □

Bien sûr, sachant que les deux définitions de $-_R x$ que nous avons formulées conduisent toutes deux à un opposé de x pour $+_{\mathbb{Z}}$, on sait qu'elles coïncident. Mais pour que le propos soit complet, terminons cette section, comme nous l'avons annoncé, en montrant que les deux opposés coïncident, sans utiliser la proposition 7.3.10.

Proposition 7.3.11. *Pour tout $x \in \mathbb{R}_{\mathrm{D}}$, on a*

$$\inf\{\phi(-r) | r \in x\} = \{s \in \mathbb{Q} \mid \exists q > s [-q \notin x]\}.$$

Démonstration. On procède comme d'habitude par double inclusion.

- Soient $s \in \mathbb{Q}$ et $q > s$ tel que $-q \notin x$ et montrons que s appartient à $\inf\{\phi(-r) | r \in x\}$. Pour tout $r \in x$, on a alors $r < -q$ car $-q \notin x$. Donc on a $q < -r$, et finalement $\phi(q) \leq_{\mathbb{R}_{\mathrm{D}}} \phi(-r)$. Donc $\phi(q)$ est un minorant de $\inf\{\phi(-r) | r \in x\}$ et on a donc $\phi(q) \leq_{\mathbb{R}_{\mathrm{D}}} \inf\{\phi(-r) | r \in x\}$, c'est-à-dire $\phi(q) \subseteq \inf\{\phi(-r) | r \in x\}$. On conclut puisque $s \in \phi(q)$.
- Soit maintenant $s \in \inf\{\phi(-r) | r \in x\}$. Par le théorème 7.2.5, il existe $y \in \mathbb{R}_{\mathrm{D}}$ tel que $y \subseteq \phi(-r)$ pour tout $r \in x$ et $s \in y$. Puisque y est une coupure, il existe $q \in y$ tel que $s < q$. Mais alors on a $q \in \phi(-r)$ pour tout $r \in x$, ce qui donne $q < -r$, ou encore $-q > r$, pour tout $r \in x$. On a donc $-q \notin x$ et cela suffit. □

7.4 La multiplication dans $\mathbb{R}_{\mathrm{D}}$

Dans la continuité de la section précédente, on définit un produit $\cdot_R$ sur $\mathbb{R}_{\mathrm{D}}$ de sorte que la fonction ϕ soit un morphisme multiplicatif de $(\mathbb{Q}, .)$ dans $(\mathbb{R}, \cdot_R)$. La définition du produit ne peut être une transposition de la définition de la somme. En effet, soit r et s deux rationnels tels que $r > 0$ et $s > 0$ et soit $P_{r,s}$ un sous-ensemble de $\mathbb{Q}$ défini comme suit :

$$P_{r,s} = \{p.q \mid p \in \phi(r) \text{ et } q \in \phi(s)\}.$$

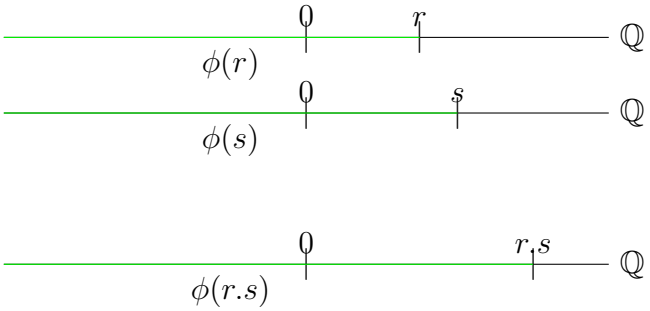
On sait que l'on peut trouver deux rationnels $p < 0$ et $q < 0$ (donc tels que $p \in \phi(r)$ et $q \in \phi(s)$) qui vérifient $p.q > r.s$. Comme on voudrait que $\phi(r) \cdot_R \phi(s) = \phi(r.s)$, l'ensemble $P_{r,s}$ n'est pas adéquat. De plus cet ensemble n'est pas une coupure car il contient tous les rationnels positifs. En effet, si $a \in \mathbb{Q}$ et $a > 0$, on a $a = (-1).(-a)$ où $-1 < r$ et $-a < s$. Il n'est donc pas majoré.

Or, comme r et s sont tels que $0_R <_{\mathbb{R}_D} \phi(r)$ et $0_R <_{\mathbb{R}_D} \phi(s)$, on peut réexprimer $\phi(r.s)$ comme suit :

$$\phi(r.s) = 0_R \cup \{p.q \mid 0 \leq p < r \text{ et } 0 \leq q < s\}.$$

En effet, d'une part, si p et q sont positifs et tels que $p < r$ et $q < s$, alors $p.q < r.s$ par les propriétés de la multiplication dans $\mathbb{Q}$, et 0_R est aussi inclus dans $\phi(r.s)$. Réciproquement, tout nombre négatif dans $\phi(r.s)$ appartient à 0_R, et pour tout nombre positif $t < r.s$, il existe $t' \in \mathbb{Q}$ tel que $t < t' < r.s$. Alors $t = \frac{t'}{s}.(s\frac{t}{t'})$ où le premier facteur est inférieur à r et le second inférieur à s.

Voici une représentation de cette situation.



On généralise alors pour deux réels x et y tels que $0 <_{\mathbb{R}_D} x$ et $<_{\mathbb{R}_D} y$.

Définition 7.4.1 (Produit de nombres positifs)**.** *Pour tous $x, y \in \mathbb{R}_D$ tels que $0_R \leq_{\mathbb{R}_D} x$ et $0_R \leq_{\mathbb{R}_D} y$, on pose*

$$x \cdot_R y = 0_R \cup \{p.q \mid 0 \leq p \in x \text{ et } 0 \leq q \in y\}.$$

Proposition 7.4.2. *Si deux réels $x, y \in \mathbb{R}_D$ sont tels que $0_R \leq_{\mathbb{R}_D} x$ et $0_R \leq_{\mathbb{R}_D} y$ alors l'ensemble défini par*

$$x \cdot_R y = 0_R \cup \{p.q \mid 0 \leq p \in x \text{ et } 0 \leq q \in y\}$$

est une coupure de $\mathbb{Q}$. En d'autres termes, l'opération définie en 7.4.1 est bien à image dans $\mathbb{R}_D$.

Démonstration. Soient $x, y \in \mathbb{R}_D$ tels que $0 <_{\mathbb{R}_D} x$ et $<_{\mathbb{R}_D} y$, on montre que $x \cdot_R y$ est une coupure.

- *C1* : D'une part, pour tout rationnel $r < 0$ on a par définition que $r \in 0_R \subseteq x \cdot_R y$. Dès lors $x \cdot_R y \neq \emptyset$. D'autre part, puisque x et y sont majorés, il existe des rationnels (strictement positifs) m_x et m_y tels que $p < m_x$ et $q < m_y$ pour tous $p \in x$ et $q \in y$. On constate alors que $m_x.m_y \notin x \cdot_R y$, donc l'ensemble $x \cdot_R y$ est bien distinct de $\mathbb{Q}$.

- *C2* : Soient $r \in x \cdot_R y$ et $s < r$. On distingue trois cas.
  - (i) si $r < 0$ alors, par transitivité de $<$ d'une part et par définition de 0_R d'autre part on a bien $s \in 0_R$ et donc $s \in x \cdot_R y$;
  - (ii) si $0 \leq r$ et $s < 0$, on a par définition que $s \in 0_R$ et donc $s \in x \cdot_R y$;
  - (iii) si $0 < r$ et $0 < s$, comme $r \in x \cdot_R y$, alors par définition de $\cdot_R$, r peut être exprimé comme le produit de deux rationnels positifs p et q appartenant à x et à y respectivement :
    $$r = p.q \text{ où } 0 < p \in x \text{ et } 0 < q \in y.$$
    Il s'ensuit que l'on a
    $$s < p.q$$
    avec s, p et q positifs. Mais alors, on a
    $$s = \tfrac{s}{p}.p, \text{ avec } 0 \leq p \in x \text{ et } 0 \leq \tfrac{s}{p} \in y \text{ (car } \tfrac{s}{p} < q).$$
    Ainsi, s est bien un élément de $x \cdot_R y$.
- *C3* : si m_x et m_y sont des majorants (strictement positifs) pour x et y respectivement, alors $m_x.m_y$ est un majorant de $x \cdot_R y$. On montre ensuite que $x \cdot_R y$ ne possède pas de plus grand élément. Soit donc $r \in x \cdot_R y$, si $r < 0$ alors il est évident qu'il existe $s \in x \cdot_R y$ tel que $r < s$ (tout rationnel s tel que $r < s < 0$ convient). On suppose donc que $0 \leq r$. Soient alors $p \in x$ et $q \in y$ tels p, q sont positifs et tels que $r = p.q$. En particulier, comme x et y sont des coupures, on sait qu'il existe p' (resp q') tels que $p < p'$ et $p' \in x$ (resp. $q < q'$ et $q' \in y$). Dès lors, $p'.q' \in x \cdot_R y$ et $r = p.q \leq p'.q'$. □

Pour généraliser le produit à $\mathbb{R}_{\mathrm{D}}$ tout entier, on se ramène au produit de deux réels positifs. Pour ce faire, on introduit la notion de valeur absolue.

Définition 7.4.3. *La valeur absolue de x, notée $|x|$, est définie par*

$$|x| = \begin{cases} x & \text{si } x \geq 0_R \text{ ;} \\ -_R x & \text{si } x < 0_R. \end{cases}$$

Proposition 7.4.4. *Pour tout réel x on a*

$$|x| \geq 0_R \,.$$

Démonstration. Si $x \geq 0_R$ c'est évident. Soit donc $x < 0_R$ et soit r un élément de 0_R. On montre que $r \in -_R x$. Comme 0_R est une coupure, on est assuré de l'existence d'un rationnel q tel que $r < q < 0$. Mais alors, par définition 7.2.1 de l'ordre dans $\mathbb{R}_{\mathrm{D}}$, on a $x \subseteq 0_R$ et donc $-q \notin x$. En d'autres termes, on a

$$\exists q > r[-q \notin x].$$

Vu la définition 7.3.9 de l'opposé, il apparaît clairement que $r \in -_R x$. □

Passons maintenant à la définition générale du produit.

Définition 7.4.5. *Le produit sur* $\mathbb{R}_{\mathrm{D}}$ *est l'opération*

$$\cdot_R : \mathbb{R}_{\mathrm{D}} \times \mathbb{R}_{\mathrm{D}} \to \mathbb{R}_{\mathrm{D}} \ : \ (x, y) \mapsto x \cdot_R y$$

définie par

$$x \cdot_R y = \begin{cases} 0_R \cup \{p.q | 0 \leq p \in x \text{ et } 0 \leq q \in y\} & \text{si } 0_R \leq x \text{ et } 0_R \leq y\,; \\ |x| \cdot_R |y| & \text{si } x < 0_R \text{ et } y < 0_R\,; \\ -_R(|x| \cdot_R |y|) & \text{si } x < 0_R \text{ xor } y < 0_R. \end{cases}$$

Remarque 7.4.6. *Si* x *et* y *sont du même signe, il apparaît que le produit* $x \cdot_R y$ *est positif.*

Nous nous intéressons maintenant aux propriétés habituelles du produit. Les preuves consistent en de simples vérifications, mais on ne peut éviter la multiplication des cas, vu la définition qui a été adoptée.

Proposition 7.4.7. *Ainsi défini, le produit* $\cdot_R$ *est associatif et commutatif.*

Démonstration.

- Le produit est associatif : $\forall x, y, z \in \mathbb{R}_{\mathrm{D}}\ x \cdot_R (y \cdot_R z) = (x \cdot_R y) \cdot_R z$.
  Soient $x, y, z \in \mathbb{R}_{\mathrm{D}}$, on traite alors chacun des cas selon le signe de x, y et z.

  (*i*) si $x > 0_R$ *et* $y > 0_R$ *et* $z > 0_R$, comme chacun des termes est du même signe on a d'une part

  $$\begin{aligned} x \cdot_R (y \cdot_R z) &= 0_R \cup \{p.q \mid 0 \leq p \in x \text{ et } 0 \leq q \in (y \cdot_R z)\} \\ &= 0_R \cup \{p.(r.s) \mid 0 \leq p \in x,\ 0 \leq r \in y,\ 0 \leq s \in z\} \end{aligned}$$

  et d'autre part,

  $$\begin{aligned} (x \cdot_R y) \cdot_R z &= 0_R \cup \{p.s \mid 0_R \leq p \in (x \cdot_R y) \text{ et } 0 \leq s \in z\} \\ &= 0_R \cup \{(p.r).s \mid 0 \leq p \in x,\ 0 \leq r \in y,\ 0 \leq s \in z\} \end{aligned}$$

  la conclusion découle alors directement de l'associativité du produit dans $\mathbb{Q}$.

  (*ii*) si $x < 0_R$ *xor* $y < 0_R$ *xor* $z < 0_R$, on a alors

  (a) si $x < 0_R$, alors on a d'une part

  $$\begin{aligned} x \cdot_R (y \cdot_R z) &= -(|x| \cdot_R (y \cdot_R z)) \\ &= -((|x| \cdot_R y) \cdot_R z)) \end{aligned}$$

  et d'autre part

  $$\begin{aligned} (x \cdot_R y) \cdot_R z &= -(|x| \cdot_R y) \cdot_R z \\ &= -((|x| \cdot_R y) \cdot_R z)) \end{aligned}$$

  (b) si $y < 0$ alors $x \cdot_R y = -x \cdot_R |y|$ et $y \cdot_R z = -|y| \cdot_R z$. Donc

$$\begin{aligned} x \cdot_R (y \cdot_R z) &= -(x \cdot_R (|y| \cdot_R z)) \\ &= -(x \cdot_R y \cdot_R z) \\ &= -(x \cdot_R |y|) \cdot_R z)) \\ &= -((x \cdot_R |y|) \cdot_R z)) \end{aligned}$$

(c) on procède pareillement qu'en (a) ou (b).

(*iii*) Si $x > 0_R$ *xor* $y > 0_R$ *xor* $z > 0_R$: vu la remarque 7.4.6, si $x > 0_R$, alors $x \cdot_R y < 0_R$ et $y \cdot_R z > 0_R$, et donc

$$(x \cdot_R y) \cdot_R z = |x| \cdot_R |y| \cdot_R |z| = x \cdot_R (y \cdot_R z).$$

On utilise les mêmes arguments pour les deux autres cas.

(*iv*) Si $x < 0_R$ *et* $y < 0_R$ *et* $z < 0_R$, comme le produit de x par y et de y par z sont positifs on a

$$(x \cdot_R y) \cdot_R z = (|x| \cdot_R |y|) \cdot_R z = -(|x| \cdot_R |y| \cdot_R |z|) = x \cdot_R (y \cdot_R z).$$

- Le produit est commutatif : $\forall x, y \in \mathbb{R}_{\mathrm{D}}\ x \cdot_R y = y \cdot_R x$.
  Soient $x, y \in \mathbb{R}_{\mathrm{D}}$. Si $x, y > 0_R$, alors comme le produit est commutatif dans $\mathbb{Q}$ on a successivement

$$\begin{aligned} x \cdot_R y &= 0_R \cup \{p.q |\ 0 \leq p \in x \text{ et } 0 \leq q \in y\} \\ &= 0_R \cup \{q.p |\ 0 \leq p \in x \text{ et } 0 \leq q \in y\} \\ &= y \cdot_R x. \end{aligned}$$

  La commutativité étant établie pour le produit de deux nombres positifs, elle suit pour les deux autres cas de la définition 7.4.5 du produit, comme ci-dessus. □

Montrons maintenant que le plongement de $\mathbb{Q}$ dans $\mathbb{R}_{\mathrm{D}}$ a les propriétés souhaitées.

Proposition 7.4.8. *On a*

$$\phi(p.q) = \phi(p) \cdot_R \phi(q)$$

pour tous $p, q \in \mathbb{Q}$.

Démonstration. On remarque d'abord qu'on a $\phi(r) \geq_{\mathbb{R}_{\mathrm{D}}} 0_R$ si et seulement si $r \geq 0$, par la proposition 7.2.2. On traite alors plusieurs cas en fonction du signe de p et q.

- Si $0 < p$ et $0 < q$, alors on a

$$\phi(p) \cdot_R \phi(q) = 0_R \cup \{r.s | 0 \leq r < p \text{ et } 0 \leq s < q\}$$

  et nous avons montré en introduction de cette section que cet ensemble est $\phi(p.q)$.

- Si p ou q est nul, l'autre étant positif ou nul, alors on constate que par définition $\phi(p) \cdot_R \phi(q) = 0_R = \phi(p.q)$.

- Si $p < 0$ et $q < 0$, alors on a par définition

$$\phi(p) \cdot_R \phi(q) = |\phi(p)| \cdot_R |\phi(q)| = (-_R \phi(p)) \cdot_R (-_R \phi(q)$$

Par la proposition 7.3.3, on obtient $-_R \phi(p) = \phi(-p) = -_R \phi(q) = \phi(-q)$ et donc, en utilisant le premier cas

$$\phi(p) \cdot_R \phi(q) = \phi(-p) \cdot_R \phi(-q) = \phi((-p).(-q)) = \phi(p.q).$$

- Le dernier cas $p < 0$ *xor* $q < 0$ se traite de la même façon. □

Ensuite, on montre que le produit admet un neutre. Vu la proposition 7.4.8, le nombre $\phi(1)$ est un bon candidat.

Définition 7.4.9. *On pose* $1_R = \phi(1)$.

Proposition 7.4.10. *L'élément* 1_R *est neutre pour* $\cdot_R$ *: on a*

$$x \cdot_R 1_R = 1_R$$

pour tout réel x.

Démonstration. D'abord, on établit la propriété pour $x \geq 0_R$. On procède par double inclusion.

- $x \subseteq x \cdot_R 1_R$: il suffit de traiter le cas $x \geq 0_R$, soit $s \in x$. Si $s < 0$, vu la définition 7.4.5 du produit pour deux éléments positifs, il est clair que s est un élément du produit $x \cdot_R 1_R$. Si $0 \leq s$ alors il existe $s' \in x$ tel que $s < s'$. On a alors $s = s'.\frac{s}{s'}$ où $s' \in x$ et $\frac{s}{s'} \in 1_R$.
- $x \cdot_R 1_R \subseteq x$: soit $s \in x \cdot_R 1_R$, si $s < 0$, il est clair que $s \in x$ (car $x \geq 0_R$). Si $0 \leq s$, alors $s = p.q$ avec $0 \leq p \in x$ et $0 \leq q \in 1_R$. Dès lors, $s < p \in x$ donc $s \in x$.

Si à présent $x \leq 0_R$, vu la définition 7.4.5 du produit, on a

$$x \cdot_R 1_R = -_R(-_R x \cdot_R 1_R).$$

Par la propriété 7.4.4, on a $-_R x \geq 0$. Par le premier point de la preuve, on sait donc que l'on a $-_R x \cdot_R 1_R = -_R x$, de sorte que

$$x \cdot_R 1_R = -_R(-_R x) = x.$$ □

On montre maintenant que le produit est distributif par rapport à la somme.

Théorème 7.4.11. *Pour tout réel* x, y *et* z, *on a*

$$(x +_R y) \cdot_R z = x \cdot_R z +_R y \cdot_R z.$$

Démonstration. On établit d'abord la propriété pour $x, y, z \geq 0_R$. Si un des trois réels est nul, la propriété est immédiate. Dans le cas contraire, on a d'une part :

$$\begin{aligned}(x +_R y) \cdot_R z &= 0_R \cup \{t.q \mid 0 \leq q \in z \text{ et } 0 \leq t \in (x +_R y)\} \\ &= 0_R \cup \{(p+r).q | 0 \leq q \in z \text{ et } p \in x \text{ et } r \in y \text{ et } 0 \leq p+r\}\end{aligned}$$

Et d'autre part

$$x \cdot_R z +_R y \cdot_R z = \{u + v \mid u \in x \cdot_R z \text{ et } v \in y \cdot_R z\}$$

où finalement

$$u \in x \cdot_R z \leftrightarrow u < 0 \quad \text{ou} \quad u = p.q \text{ avec } 0 \leq p \in x \text{ et } 0 \leq q \in z$$

et

$$v \in y \cdot_R z \leftrightarrow v < 0 \quad \text{ou} \quad v = r.q \text{ avec } 0 \leq r \in y \text{ et } 0 \leq q \in z.$$

Procédons alors par double inclusion et distinguons les cas.

- On a $(x +_R y) \cdot_R z \subseteq x \cdot_R z +_R y \cdot_R z$: soit $t \in (x +_R y) \cdot_R z$.
  - (i) Si $t < 0$, alors $t \in x \cdot_R z +_R y \cdot_R z$, car t se décompose en la somme de deux nombres strictement négatifs (on a $\phi(0) \subseteq \phi(0) + \phi(0)$).
  - (ii) Si $t \geq 0$, alors il existe p, q, r tels que $t = (p + r).q$ et $0 \leq q \in z$, $p \in x$, $r \in y$ et $0 \leq p + r$. On a alors $t = p.q + r.q$ et $p.q \in x \cdot_R z$ et $p.r \in y \cdot_R z$.
- On a $x \cdot_R z +_R y \cdot_R z \subseteq (x +_R y) \cdot_R z$: soit $t \in x \cdot_R z +_R y \cdot_R z$. Il existe $u \in x \cdot_R z$ et $v \in y \cdot_R z$ tels que $t = u + v$. Alors les cas suivants peuvent se produire :
  - (i) Si $u < 0$, alors on remarque que $v \in y \cdot_R z$ implique $v \in (x +_R y) \cdot_R z$ car $0 \in x$. Alors $t = u + v < v$, donc $t \in (x +_R y) \cdot_R z$;
  - (ii) Si $v < 0$, on procède de la même façon ;
  - (iii) Si $u \geq 0$ et $v \geq 0$, alors il existe $p, q, p', q' \geq 0$ tels que $q, q' \in z$, $p \in x$ et $q \in y$ et $u = p.q$, $v = p'q'$. Si $q = q'$, alors on a $t = u+v = (p+p').q$, et on conclut. Si $q \neq q'$, on peut supposer $q > q'$, et on a $t = u + v = (p + p'\frac{q'}{q}).q$, où $p \in x$ et $p'\frac{q'}{q} < p' \in y$.

Pour les autres cas, on se ramène à chaque fois au cas précédent grâce à la valeur absolue :

$$(x +_R y) \cdot_R z = \begin{cases} (x +_R y) \cdot_R z & \text{si } 0_R \leq (x +_R y) \text{ et } 0_R \leq z\,; \\ |x +_R y| \cdot_R |z| & \text{si } (x +_R y) < 0_R \text{ et } z < 0_R\,; \\ -_R(|x +_R y| \cdot_R |z|) & \text{si } (x +_R y) < 0_R \text{ xor } z < 0_R. \end{cases}$$

et en notant que $-(x + y) = -x - y$. □

Étant donné un réel x, on souhaite à présent pouvoir lui associer un réel, que l'on notera x^{-1}, qui soit tel que

$$x \cdot_R x^{-1} = 1_R \ .$$

En utilisant l'associativité du produit $\cdot_R$ et l'existence d'un neutre, on montre facilement qu'un tel élément, s'il existe, est unique. Bien sûr, puisque ϕ est un morphisme pour $\cdot_R$ (voir proposition 7.4.8), on a

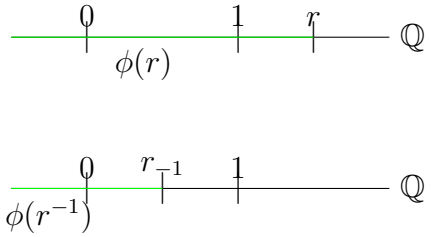
$$\phi(r) \cdot_R \phi(r^{-1}) = \phi(r.r^{-1}) = \phi(1) = 1_R,$$

et on doit donc avoir $(\phi(r))^{-1} = \phi(r^{-1})$ pour tout $r \in \mathbb{Q}\setminus\{0\}$.

Remarquons enfin que ${0_R}^{-1}$ ne peut exister, car on montre à partir de la définition que $0_R \cdot_R y = 0_R \neq 1_R$, pour tout $y \in \mathbb{R}_{\mathrm{D}}$.

En d'autres termes, on va établir que tout élément non-nul admet un inverse. Comme pour la définition de l'opposé, on a le choix de "résoudre l'équation" posée ci-dessus, ou d'effectuer une discussion minutieuse basée sur l'intuition géométrique. C'est cette deuxième méthode que nous suivons.

Pour aider l'intuition, on considère d'abord le cas où $x > 0_R$. Si $x = \phi(r)$ avec $0 < r \in \mathbb{Q}$, on a $(\phi(r))^{-1} = \phi(r^{-1})$:



Donc,

$$\begin{aligned}(\phi(r))^{-1} &= \{s \in \mathbb{Q} \,|\, s < r^{-1}\} \\ &= \{s \in \mathbb{Q} \,|\, s \leq 0 \text{ } ou \text{ } \tfrac{1}{s} > r\}.\end{aligned}$$

Ici, une difficulté subsiste. En effet, l'expression dépend de r, et cela entrave la généralisation à un $x \in \mathbb{R}_{\mathrm{D}}$ quelconque (pour lequel on a pas de r). Or, on a l'implication suivante :

$$\frac{1}{s} > r \to \frac{1}{s} \notin \phi(r).$$

Cependant, on ne peut accepter $\frac{1}{s} = r$ pour vérifier *C3*. Ainsi, porté par l'intuition et l'analogie avec la définition de l'opposé, on propose la définition (intermédiaire) suivante.

Définition 7.4.12. *Pour tout réel x tel que $0_R < x$ on pose*

$$x^{-1} = 0_R \cup \{s \in \mathbb{Q} \,|\, \exists t > s[\frac{1}{t} \notin x]\}.$$

On dit que x^{-1} est l'inverse de x. Par la suite, on pourra également le noter $\frac{1}{x}$.

On vérifie alors que la définition est pertinente.

Proposition 7.4.13. *Si $x \in \mathbb{R}_{\mathrm{D}}$ est tel que $0_R < x$ alors on a $x^{-1} \in \mathbb{R}_{\mathrm{D}}$ et $x \cdot_R x^{-1} = 1_R$.*

Démonstration.

(*i*) D'abord on montre que $x^{-1} \in \mathbb{R}_{\mathrm{D}}$. On vérifie donc chacun des points de la définition 7.1.1 d'une coupure de Dedekind.

- *C1* : par définition, $x^{-1} \neq \emptyset$. On montre que $x^{-1} \neq \mathbb{Q}$. Soit $s \in x$ tel que $0 < s$, alors pour tout $t \in \mathbb{Q}$ on a l'implication suivante
$$t > \frac{1}{s} \rightarrow \frac{1}{t} < s.$$
Mais alors, vu le point *C2* de la définition 7.1.1 d'une coupure on a
$$\forall t > \frac{1}{s}[\frac{1}{t} \in x],$$
et donc $\frac{1}{s} \notin x^{-1}$ (par définition).
- *C2* : soit $s \in x^{-1}$ et $p < s$. Si $s < 0$, alors $p < 0$ et $p \in x^{-1}$. Sinon, par définition 7.4.12 de l'inverse, on sait qu'il existe $t > s$ tel que $t^{-1} \notin x$. Par transitivité de la relation d'ordre, on a aussi $t > p$ et dès lors on a $p \in x^{-1}$.
- *C3* : soit $s \in x^{-1}$. Si $s < 0$, il existe $s' \in \mathbb{Q}$ tel que $s < s' < 0$. Alors $s' \in x^{-1}$, par définition. Sinon, on sait qu'il existe $t, p \in \mathbb{Q}$ tel que $t > p > s$ et $t^{-1} \notin x$, donc par définition de x^{-1}, on a $p \in x^{-1}$ et $s < p$.

(*ii*) On montre ensuite que x^{-1} est bien l'inverse de x : $x \cdot_R x^{-1} = 1_R$. Pour ce faire, on procède par double inclusion.

- On a $1_R \subseteq x \cdot_R x^{-1}$: soit $s \in 1_R$. Vu la définition du produit (pour deux éléments positifs), si $s < 0$, alors il est clair que s est un élément du produit $x \cdot_R x^{-1}$. Si $s \geq 0$, alors il existe s' rationnel tel que $s < s' < 1$. On a alors $\frac{1}{s'} > 1$. Puisque $\mathbb{Q}$ est archimédien et $x > 0_R$, il existe alors $u \in x$ tel que $\frac{1}{s'}u = \frac{u}{s'} \notin x$. Alors par définition de x^{-1}, tout rationnel positif q tel que $q < \frac{s'}{u}$ appartient à x^{-1}. Donc $\frac{s}{u} \in x^{-1}$ et $s = u.\frac{s}{u}$.
- On a $x \cdot_R x^{-1} \subseteq 1_R$: si $s \in x \cdot_R x^{-1}$ alors soit $s < 0$ et donc $s \in 0_R$ soit $s = p.q$ avec $0 \leq p \in x$ et $0 \leq q \in x^{-1}$. Par définition 7.4.12 de l'inverse on sait qu'il existe $t > q$ tel que $t^{-1} \notin x$. En particulier, pour un tel t, on a $t^{-1} > p$ vu le point *C2* pour la coupure x. Ainsi, on a $p.q < t^{-1}.t = 1$ ce qui prouve bien que $s \in 1_R$. □

Comme pour le produit, on généralise la notion d'inverse à $\mathbb{R}_D$ tout entier (sauf 0_R) grâce à la valeur absolue.

Définition 7.4.14. *Pour tout $x \in \mathbb{R}_D$ non nul, on définit l'inverse de x, noté x^{-1} par*[4]
$$x^{-1} = \begin{cases} x^{-1} & \text{si } x > 0_R\,; \\ -_R(|x|)^{-1} & \text{si } x < 0_R. \end{cases}$$

On montre comme plus haut, en utilisant les propriétés de la valeur absolue, que le nombre ainsi défini est un inverse de x, quel que soit x non nul.

Comme résultat final pour ce chapitre, on montre que $\mathbb{R}_D$ est complet. Ainsi, en plus d'avoir étendu $\mathbb{Q}$, la nouvelle structure obtenue, $\mathbb{R}_D$ est bien plus riche car, toute partie majorée de $\mathbb{R}_D$ possède une borne supérieure (voir 7.2.5) et (en corollaire de cela) toute suite de Cauchy converge.

4. La définition n'est pas circulaire : il s'agit, à droite de l'égalité ci-dessous, de l'inverse défini pour les réels positifs.

Lemme 7.4.15. *Dans $\mathbb{R}_{\mathrm{D}}$, toute suite croissante (resp. décroissante) et majorée (resp. minorée) converge.*

Démonstration. Soit $(x_j)_j$ une suite croissante et majorée de $\mathbb{R}_{\mathrm{D}}$, on sait qu'alors $(x_j)_j$ possède une borne Sup M (cf. 7.2.5). On montre qu'alors, $(x_j)_j$ converge vers M. En effet, par définition de la borne Sup, on sait que pour tout $\epsilon > 0$ il existe $x_J \in \mathbb{N}$ tel que

$$|x_J - M| \leq \epsilon.$$

En particulier, comme la suite est croissante, on a alors

$$j \geq J \to |x_j - M| \leq \epsilon.$$

Le cas de la suite décroissante se résout immédiatement en considérant la suite $-(x_j)_j$. □

Lemme 7.4.16. *Si d'une suite de Cauchy on peut extraire une sous-suite qui converge, alors la suite est convergente.*

Démonstration. Soit $(x_j)_j$ une suite de Cauchy et $(x_{j_k})_k$ une sous-suite de $(x_j)_j$ qui converge vers x. Pour tout $\epsilon > 0$, il existe alors M_1 et M_2 tels que

$$\begin{aligned} &k > M_1 \ \to \ |x_{j_k} - x| \leq \epsilon/2, \\ &p, q > M_2 \ \to \ |x_i - x_j| \leq \epsilon/2. \end{aligned}$$

Mais alors, pour $M = \sup\{M_1, M_2\}$, on a

$$k > M \ \to \ |x_k - x| \leq |x_k - x_{j_k}| + |x_{j_k} - x| \leq \epsilon.$$

Et donc la suite $(x_j)_j$ est bien convergente. □

Pour les besoins du théorème, on introduit aussi deux nouvelles notions : la partie positive x_+ et la partie négative x_- d'un nombre réel x.

Définition 7.4.17. *Pour tout réel x, on définit la partie positive x_+ (resp. négative x_-) de x par*

$$(i) \ x_+ = \begin{cases} x & \text{si } x \geq 0 \\ 0 & \text{sinon} \end{cases}$$

$$(ii) \ x_- = \begin{cases} -x & \text{si } x < 0 \\ 0 & \text{sinon} \end{cases}$$

On notera, par exemple, que $x = x_+ - x_-$ et que $|x| = x_+ + x_-$. On pourra au besoin considérer les "opérations" $\cdot_+$ et $\cdot_-$ comme des fonctions de $\mathbb{R}_{\mathrm{D}}$ dans $\mathbb{R}_{\mathrm{D}}$.

Théorème 7.4.18. *L'espace $(\mathbb{R}_{\mathrm{D}}, \leq)$ est complet ; c'est à dire que toute suite de Cauchy converge.*

Démonstration. Soit $(x_j)_j$ une suite de Cauchy. On va extraire de $(x_j)_j$ une sous-suite convergente. Pour tout $k \in \mathbb{N}$, il existe un plus petit indice j_k à partir duquel tous les éléments suivants de la suite sont situés les uns par rapport aux autres à une distance inférieure à $(\frac{1}{2})^k$. On définit ainsi $(x_{j_k})_k$ une sous-suite de $(x_j)_j$. Mais alors, si l'on considère la suite $(S_{k+})_k$ définie par

$$S_{k+} = (x_{j_k} - x_{j_{k-1}})_+ + (x_{j_{k-1}} - x_{j_{k-2}})_+ + ... + (x_{j_2} - x_{j_1})_+ + (x_{j_1})_+$$

Cette suite est croissante et majorée par $(x_{j_1})_+ + 2$, donc elle converge. Semblablement, on définit la suite S_{k-} par

$$S_{k-} = (x_{j_k} - x_{j_{k-1}})_- + (x_{j_{k-1}} - x_{j_{k-2}})_- + ... + (x_{j_2} - x_{j_1})_+ + (x_{j_1})_-$$

qui est donc aussi convergente car croissante et majorée (par $(x_{j_1})_- + 2$). Mais alors la suite $S_{k+} - S_{k-}$ est aussi convergente. Or $S_{k+} - S_{k-} = (x_{j_k})_k$. On a donc bien exhibé une sous-suite convergente de la suite de Cauchy. Dès lors, par le lemme 7.4.16, $(x_j)_j$ converge. □

Chapitre 8

Les réels à la Cantor

Comme Dedekind, Cantor cherche à construire les réels comme extensions de $\mathbb{Q}$; comme $\mathbb{Z}$ est une extension de $\mathbb{N}$, et $\mathbb{Q}$ une extension de $\mathbb{Z}$: "Les nombres rationnels constituent le fondement [indispensable] à l'établissement du concept plus étendu de grandeur numérique" [1]. Bien que Cantor n'ait pas à sa connaissance le concept de corps développé par Dedekind, il apparaît dans ses travaux qu'il considère comme acquises les propriétés suivantes [2] de $\mathbb{Q}$:

1. la somme et le produit dans $\mathbb{Q}$ sont internes (ainsi que la différence et la division) ;
2. $\mathbb{Q}$ possède un ordre ;
3. $\mathbb{Q}$ est dense (dans l'ensemble à construire).

Le souhait de faire des suites de Cauchy l'objet générateur pour construire les réels tient du fait que Cantor estime que : "Elle [cette construction de $\mathbb{R}$] présente l'avantage d'être celle qui se prête le mieux aux calculs analytiques" [3]. Il considère que la définition des réels comme étant les coupures de $\mathbb{Q}$ peut être au contraire une difficulté car les réels se présentent rarement sous cette forme.

On considère ici l'ensemble $\mathscr{A}$ des suites rationnelles de Cauchy. On montre d'abord que $\mathscr{A}$ est un anneau commutatif avec unité, qu'il contient un idéal I bien particulier qui fait de l'anneau quotient $\mathscr{A}/I$ un corps commutatif. On identifiera alors ce dernier à $\mathbb{R}_C$, les réels à la Cantor.

8.1 L'anneau des suites de Cauchy

On note $\mathscr{A}$ l'ensemble des suites de Cauchy de nombres rationnels. Il se fait que les opérations usuelles d'addition et de multiplication composante à composante en font un anneau commutatif avec unité. Pour justifier cette assertion, nous avons d'abord besoin de quelques préparatifs élémentaires qui sont par ailleurs bien connus.

1. [4] p. 126
2. Id.
3. Id.

Définition 8.1.1. *L'ensemble des suites de Cauchy à valeurs dans $\mathbb{Q}$ est noté $\mathscr{A}$.*

On note que l'ensemble des suites de Cauchy dans $\mathbb{Q}$ est bien défini. En effet, une suite à valeurs dans $\mathbb{Q}$ est, par définition, un sous-ensemble du produit cartésien $\mathbb{N} \times \mathbb{Q}$. Donc, $\mathscr{A}$ est un sous-ensemble de $\mathscr{P}(\mathbb{N} \times \mathbb{Q})$.

Définition 8.1.2. *Sur $\mathscr{A}$ on définit deux opérations, la somme notée $+_A$ et le produit noté $._A$: si $(r_j)_j$ et $(s_j)_j$ sont deux suites, alors*

$$(r_j)_j +_A (s_j)_j = (r_j + s_j)_j;$$

et

$$(r_j)_j \cdot_A (s_j)_j = (r_j \,.\, s_j)_j$$

On dit que la somme (resp. le produit) se fait composante à composante.

Nous conserverons les notations indicées par A dans les premières utilisations, puis il arrivera qu'on les omette si aucune confusion n'est possible.

Avant de démontrer la légitimité de cette définition, on établit un lemme.

Lemme 8.1.3. *Toute suite de Cauchy est bornée.*

Démonstration. Soit $(r_j)_j$ une suite de Cauchy ; on sait que pour tout $\epsilon > 0$ il existe un naturel N tel que pour tous indices i et j plus grands que N on a $|\, r_j - r_i| < \epsilon$. Pour $\epsilon = 1$, soit N_ϵ tel que

$$\forall i, j \geq N_\epsilon [|\, r_j - r_i| < 1].$$

Alors, pour tout indice $j > N_\epsilon$,

$$|\, r_j \,| \leq |\, r_j - r_{N_\epsilon}| + |r_{N_\epsilon}|.$$

c'est à dire

$$|\, r_j \,| \leq |r_N| + 1.$$

Ainsi, pour $C_N = max\{|r_1|, |r_2|, ..., |r_{N-1}|, |r_N|\}$, on a $r_j \leq C_N + 1, \quad \forall j \in \mathbb{N}$. □

Proposition 8.1.4. *Si $(r_j)_j$ et $(s_j)_j$ sont deux suites de Cauchy, alors $(r_j + s_j)_j$ et $(r_j \,.\, s_j)_j$ sont deux suites de Cauchy. En d'autre termes, les applications définies en 8.1.2 sont bien des opérations internes et partout définies.*

Démonstration. D'abord on vérifie que la somme de deux suites de Cauchy est encore une suite de Cauchy. Soient donc $(r_j)_j$ et $(s_j)_j$ deux suites de Cauchy, pour tout $\epsilon > 0$ on sait qu'il existe respectivement $M \in \mathbb{N}$ et $N \in \mathbb{N}$ tels que

$$i, j \geq M \rightarrow \ |\, r_j - r_i| < \epsilon/2$$

et

$$i, j \geq N \rightarrow \ |s_i - s_j| < \epsilon/2.$$

Donc, si $R = sup\{M, N\}$, on a successivement

$$\begin{aligned} |r_i + s_i - r_j - s_j| &\leq |r_i - r_j| + |s_i - s_j| \\ &= \epsilon \end{aligned}$$

dès que $i, j > R$.

On montre à présent que le produit de deux suites de Cauchy est encore une suite de Cauchy. En effet, soient $(r_j)_j$ et $(s_j)_j$ deux éléments de $\mathscr{A}$. Comme toute suite de Cauchy est bornée (voir 8.1.3), on sait qu'il existe un rationnel C qui est un majorant de $(r_j)_j$ et de $(s_j)_j$. De plus, pour tout $\epsilon > 0$ on peut trouver un indice N tel que, pour tous indices i et j plus grand que N, on a

$$\begin{aligned} |r_i - r_j| &< \epsilon/2C\,; \\ |s_i - s_j| &< \epsilon/2C. \end{aligned}$$

Ainsi, on a successivement, $\forall i, j > N$

$$\begin{aligned} |r_i s_i - r_j s_j| &= |r_i s_i - r_i s_j + r_i s_j - r_j s_j| \\ &\leq |r_i||s_i - s_j| + |s_j||r_i - r_j| \\ &\leq \epsilon. \end{aligned}$$

□

Théorème 8.1.5. *L'ensemble $\mathscr{A}$ des suites de Cauchy à valeurs dans $\mathbb{Q}$, doté des opérations $+_A$ et $._A$, est un anneau commutatif intègre dont $(0)_j$ est le neutre pour l'addition et $(1)_j$ le neutre pour le produit.*

Démonstration. On montre que chacune des propriétés qui définit un anneau commutatif est vérifiée.

- La somme $+_A$ est associative : soient donc $(r_j)_j$, $(s_j)_j$ et $(t_j)_j$ trois éléments de $\mathscr{A}$. Vu la définition de $+_A$ on a d'une part

$$\begin{aligned} \Big((r_j)_j +_A (s_j)_j \Big) +_A (t_j)_j &= (r_j + s_j)_j +_A (t_j)_j \\ &= \Big((r_j + s_j) + t_j \Big)_j \end{aligned}$$

  et d'autre part

$$\begin{aligned} (r_j)_j +_A \Big((t_j)_j +_A (s_j)_j \Big) &= (r_j)_j +_A (s_j + t_j)_j \\ &= \Big(r_j + (s_j + t_j) \Big)_j. \end{aligned}$$

  La conclusion découle directement de l'associativité de la somme dans $\mathbb{Q}$.

- Existence d'un neutre pour $+_A$: vu la définition de $+_A$, il apparaît que la suite nulle $(0)_j$ convient car c'est une suite de Cauchy et dans $\mathbb{Q}$, l'élément 0 est le neutre pour la somme :

$$(r_j)_j + (0)_j = (r_j + 0)_j.$$

- Existence d'un opposé : avec les mêmes arguments qu'au point précédent, on déduit que définir l'opposé d'un élément $(r_j)_j$ par $-(r_j)_j = (-r_j)_j$ convient. En effet, d'abord on remarque que $(-r_j)_j = (-1)_j \cdot_A (r_j)_j$, de sorte que $-(r_j)_j$ est bien une suite de Cauchy. Ensuite, on a bien
$$(r_j)_j +_A (-(r_j)_j) = 0.$$
- La somme $+_A$ est commutative : on procède comme pour l'associativité. La commutativité de $+_A$ est donc assurée par le fait que la somme sur $\mathbb{Q}$ est commutative.
- L'opération $\cdot_A$ est associative : on transpose la démonstration faite pour l'associativité de $+_A$: soient donc $(r_j)_j$, $(s_j)_j$ et $(t_j)_j$ trois éléments de $\mathscr{A}$. On a d'une part
$$\begin{aligned}\Big((r_j)_j \cdot_A (s_j)_j\Big) \cdot_A (t_j)_j &= (r_j \,.\, s_j)_j \cdot_A (t_j)_j \\ &= \Big((r_j \,.\, s_j).t_j\Big)_j\end{aligned}$$
et d'autre part
$$\begin{aligned}(r_j)_j \cdot_A \Big((t_j)_j \cdot_A (s_j)_j\Big) &= (r_j)_j \cdot_A (s_j \,.t_j)_j \\ &= \Big(\, r_j \,.(s_j \,.t_j)\Big)_j.\end{aligned}$$
La conclusion découle directement de l'associativité du produit dans $\mathbb{Q}$.
- Existence d'un neutre pour $\cdot_A$: vu la définition du produit $\cdot_A$, on a
$$(r_j)_j \cdot_A (s_j)_j = (r_j)_j \;\leftrightarrow\; \forall j[r_j \,.\, s_j = r_j]$$
La suite $(1)_j$ vérifie cette propriété (et c'est la seule).
- Distributivité du produit sur la somme : à nouveau, il suffit de développer les expressions ; on conclut grâce à la distributivité du produit sur la somme dans $\mathbb{Q}$. □

8.2 Construction de $\mathbb{R}_{\mathrm{C}}$

Ayant à disposition l'anneau $\mathscr{A}$ des suites de Cauchy dans $\mathbb{Q}$, on introduit la notion d'idéal d'anneau.

Définition 8.2.1. *Soit A un anneau, un idéal I d'un anneau est un sous-ensemble de A tel que*

- *I1 : si $u, v \in I$, alors $u + v \in I$;*
- *I2 : si $u \in I$ et $v \in \mathscr{A}$, alors $u.v \in I$.*

Proposition 8.2.2. *L'ensemble I des suites de Cauchy qui convergent vers 0 est un idéal de $\mathscr{A}$.*

Démonstration. On vérifie que chacun des deux points de la définition 8.2.1 est satisfait.

- *I1* : I est fermé pour l'addition : soient $(r_j)_j$ et $(s_j)_j$ deux éléments de I, on montre en fait que si deux suites convergent vers 0 alors la somme de ces deux suites converge aussi vers 0. Soit donc $\epsilon > 0$, on sait donc qu'il existe un indice M à partir duquel on a

$$\begin{cases} j \geq M \rightarrow |\, r_j \,| \leq \epsilon/2 \\ j \geq M \rightarrow |\, s_j \,| \leq \epsilon/2, \end{cases}$$

  de sorte que l'on a

$$|\, r_j + s_j \,| \leq |\, r_j \,| + |\, s_j \,| \leq \epsilon.$$

  Donc, la suite $(r_j + s_j)_j$ converge vers 0 [4].
- *I2* : si $u \in I$ et $v \in \mathscr{A}$, alors $u.v \in I$: soient $(r_j)_j \in I$ et $(s_j)_j \in \mathscr{A}$, on montre qu'alors $(r_j)_j \cdot_A (s_j)_j$ converge vers 0. Comme $(s_j)_j$ est une suite de Cauchy, on sait que l'ensemble de ses éléments est borné (voir le lemme 8.1.3). Soit alors R un majorant pour $(s_j)_j$. Pour tout $\epsilon > 0$, on sait qu'il existe $M \in \mathbb{N}$ tel que

$$j \geq M \rightarrow |\, r_j \,| \leq \epsilon/R$$

  et donc

$$j \geq M \rightarrow |\, r_j \,.\, s_j \,| \leq \frac{\epsilon}{R}.R = \epsilon.$$

□

Pour rappel, la construction de Cantor repose sur l'idée que tout nombre réel est limite d'une suite de rationnels. Cependant, comme deux suites distinctes peuvent avoir la même limite (on peut considérer comme exemple trivial les suites $(1/j)_j$ et $(-1/j)_j$), il serait plus adéquat de considérer un réel non pas comme une limite mais comme la classe d'équivalence des suites de Cauchy ayant la même limite. Cette définition n'est néanmoins pas encore satisfaisante. En effet, seule la convergence dans $\mathbb{Q}$ a du sens pour l'instant. Pour pallier à ce problème et sans s'éloigner de l'intuition première, on considère comme équivalentes les suites de Cauchy dont la différence converge vers 0.

Définition 8.2.3. *On définit la relation $\sim$ sur $\mathscr{A}$ par*

$$\forall\, (r_j)_j, (s_j)_j \in \mathscr{A}[(r_j)_j \sim (s_j)_j \;\leftrightarrow\; (r_j - s_j)_j \in I].$$

Lemme 8.2.4. *La relation $\sim$ est une relation d'équivalence sur $\mathscr{A}$.*

Démonstration.

- Réflexivité : il est évident que $(r_j)_j \sim (r_j)_j$ vu que pour tout indice j on a $r_j - r_j = 0$;
- Symétrie : si $(r_j - s_j)_j \in I$, alors, comme $(s_j - r_j)_j = (-1_j)_j.(r_j - s_j)_j$ où $(-1_j)_j \in \mathscr{A}$ et $(r_j - s_j)_j \in I$, on a bien que $(s_j - r_j)_j \in I$, vu *I2*, et donc $(s_j)_j \sim (r_j)_j$;

4. Notons qu'il n'est pas difficile de généraliser cette preuve pour la somme de deux suites $(r_j)_j$ et $(s_j)_j$ qui convergent vers r et s respectivement.

- Transitivité : si $(r_j)_j \sim (s_j)_j$ et $(s_j)_j \sim (t_j)_j$, alors, comme par définition $(r_j)_j - (s_j)_j \in I$ et $(s_j)_j - (t_j)_j \in I$, on a $((r_j)_j - (s_j)_j) + ((s_j)_j - (t_j)_j) = (r_j)_j - (t_j)_j \in I$ car I est un idéal. Ainsi, on a bien $(r_j)_j \sim (t_j)_j$. □

On remarque que cette définition aurait un sens (i.e. définirait une relation d'équivalence) quel que soit l'idéal considéré. La relation d'équivalence énoncée juste avant étant licite, on peut alors, comme à l'accoutumée, considérer l'espace quotient. L'usage veut qu'on note l'espace ainsi obtenu $\mathscr{A}/I$.

Définition 8.2.5. *On définit $\mathbb{R}_C$ comme l'espace quotient $\mathscr{A}/I$.*

Conformément au souhait de faire de $\mathbb{R}_C$ une extension de $\mathbb{Q}$, on montre qu'il existe une injection (naturelle) de $\mathbb{Q}$ dans $\mathbb{R}_C$.

Proposition 8.2.6. *L'application ϕ définie par*

$$\phi : \mathbb{Q} \to \mathbb{R}_C : \ r \mapsto [(r)_j]$$

est injective.

Démonstration. Soient r et s deux rationnels tels que $r \neq s$, on sait qu'alors il existe un rationnel $\epsilon > 0$ tel que $|r - s| > \epsilon$. Dès lors, il apparaît clairement que $\phi(r) \neq \phi(s)$. □

Comme lorsque l'on a étudié les réels à la Dedekind, et semblablement au passage de $\mathbb{N}$ à $\mathbb{Z}$ et de $\mathbb{Z}$ à $\mathbb{Q}$, les contraintes liées au désir de faire de ϕ un morphisme vont nous dicter une définition pour les opérations sur $\mathbb{R}_C$.

En d'autre termes, une fois les opérations $+_R$ et $\cdot_R$ données, on veut que la fonction ϕ vérifie, pour tous $r, s \in \mathbb{Q}$

$$\phi(r) +_R \phi(s) = \phi(r + s),$$

et

$$\phi(r) \cdot_R \phi(s) = \phi(r.s).$$

L'intuition est aussi guidée par le fait que $\mathbb{R}_C$ est un espace quotient. On a donc tendance à définir les opérations qui font du passage au quotient un morphisme d'anneau. La définition pour $+_R$ et $\cdot_R$ la plus naturelle semble donc être la suivante.

Définition 8.2.7.

- *La somme $+_R$ est la fonction définie par*

$$+_R \ : \ \mathbb{R}_C \times \mathbb{R}_C \to \mathbb{R}_C \ : \ ([u], [v]) \mapsto [u] +_R [v] = [u + v].$$

- *Le produit $\cdot_R$ est la fonction définie par*

$$\cdot_R \ : \ \mathbb{R}_C \times \mathbb{R}_C \to \mathbb{R}_C \ : \ ([u], [v]) \mapsto [u] \cdot_R [v] = [u.v].$$

Lemme 8.2.8. *Les opérations introduites à la définition 8.2.7 sont bien définies.*

Démonstration. Comme d'habitude, on vérifie que les définitions données sont indépendantes du choix des représentants. Soit donc $u' \sim u$ et $v' \sim v$.

- La somme est indépendante du choix des représentants : en effet, on a
$$(u'+v')-(u+v) = \underbrace{(u'-u)}_{\in I} + \underbrace{(v'-v)}_{\in I} \in I,$$
donc $[u+v] = [u'+v']$.
- Le produit est indépendant du choix des représentants : on procède semblablement en écrivant
$$u.v - u'.v' = u.v - u.v' + u.v' - u'.v' = \underbrace{u.(v-v')}_{\in I} + \underbrace{v'.(u-u')}_{\in I} \in I. \qquad \square$$

Notons que dans cette preuve, nous n'avons pas utilisé la forme particulière de l'idéal. Elle s'adapte à des contextes bien plus généraux.

Théorème 8.2.9. *L'ensemble $\mathbb{R}_C$ muni des deux opérations $+_R$ et $\cdot_R$ définies en 8.2.7 est un anneau dont $1_R = \phi(1)$ est le neutre pour la somme et $0_R = \phi(0)$ le neutre pour le produit.*

Démonstration. Il n'y a dans cette démonstration, ni artifice, ni idée astucieuse. De plus, les arguments sont semblables aux précédents. Aussi, l'on se permet de ne pas mener à leurs termes les différents calculs.

- L'opération $+_R$ est associative : soient $[u]$, $[v]$ et $[w]$ des éléments de $\mathbb{R}_C$, par définition de $+_R$ on a d'une part
$$\begin{aligned}([u]+_R[v])+_R[w] &= [u+v]+_R[w] \\ &= [(u+v)+w]\end{aligned}$$
et d'autre part
$$\begin{aligned}[u]+_R([v]+_R[w]) &= [u]+_R[v+w] \\ &= [u+(v+w)]\end{aligned}$$
Aussi, l'associativité de $+_R$ découle directement de l'associativité de la somme dans $\mathscr{A}$.
- L'élément $\phi(0) = [(0)_j]$ est le neutre pour $+_R$: cela tient du fait que 0 est le neutre pour la somme dans $\mathscr{A}$
- Existence d'un opposé : comme d'habitude, le plus opportun est de définir l'opposé par $-[u] = [-u]$. Cette définition est bien licite car d'une part $-u$ est toujours défini de par la nature d'anneau de $\mathscr{A}$. Et d'autre part, $-[u]$ est indépendant du représentant car, par définition 8.2.2
$$u - u' \in I \to -(u-u') \in I.$$
On vérifie alors immédiatement que l'on a
$$\forall [u] \in \mathbb{R}_C \Big(\ [u]+_R([-u]) = [0] \ \Big).$$

- Commutativité de $+_R$: on procède comme pour établir l'associativité de $+_R$. Ce résultat est assuré par le caractère commutatif de la somme dans $\mathscr{A}$.
- Associativité de $\cdot_R$: soient $[u]$, $[v]$ et $[w]$ des éléments de $\mathbb{R}_C$. Par définition de $\cdot_R$ on a d'une part

$$\begin{aligned}([u]\cdot_R[v])\cdot_R[w] &= [u.v]\cdot_R[w]\\ &= [(u.v).w]\end{aligned}$$

et d'autre part

$$\begin{aligned}[u]\cdot_R([v]\cdot_R[w]) &= [u]\cdot_R[v.w]\\ &= [u\cdot_R(v.w)].\end{aligned}$$

Aussi, l'associativité de $\cdot_R$ découle directement de l'associativité du produit dans $\mathscr{A}$.
- L'élément $[(1)_j] = \phi(1)$ est le neutre pour $\cdot_R$: cela tient du fait que 1 est le neutre pour le produit dans $\mathscr{A}$.
- Distributivité de $\cdot_R$ sur $+_R$: cela tient du fait que dans $\mathscr{A}$ le produit est distributif par rapport à la somme. En effet,

$$\begin{aligned}([u]+_R[v])\cdot_R[w] &= [u+v]\cdot_R[w]\\ &= [(u+v).w]\end{aligned}$$

et

$$\begin{aligned}([u]\cdot_R[w])+_R([v]\cdot_R[w]) &= [u.w]+_R[v.w]\\ &= [(u.w+v.w)].\end{aligned}$$

□

Remarque 8.2.10. *Le théorème 8.2.9 est en fait un exemple d'un théorème classique*[5]*. Soit A un anneau et I un idéal de A. Si on définit sur A/I les opérations $+_{A/I}$ et $._{A/I}$ par*

$$[a]+_{A/I}[b] = [a+_A b],$$

et

$$[a].{}_{A/I}[b] = [a._A b],$$

alors les opérations sont bien définies, A/I est un anneau et l'application $\pi : A \to A/I$ de passage au quotient est un morphisme d'anneaux.

Pour faire de $\mathbb{R}_C$ un corps, il reste à définir l'opération d'inverse. Soit donc $[(r_j)_j] \in \mathbb{R}_C$ un élément non nul. Pour rappel, cela signifie que $(r_j)_j$ ne converge pas vers 0. Dès lors, on sait qu'il existe $\alpha > 0$ tel que, quel que soit l'indice J considéré, il existe un terme r_j de la suite d'indice supérieur à J qui est plus grand en module que α :

$$\exists\alpha\ \Big[\ (\ \forall J\in\mathbb{N},\ \exists j>J\ :\ |\,r_j\,|>\alpha)\ \Big].$$

5. Voir [17, p. 42].

Mais comme $(r_j)_j$ est une suite de Cauchy, on sait aussi que quel que soit la précision exigée, par exemple $\epsilon = \alpha/2$, il existe un indice M à partir duquel tous les éléments suivants de la suite sont à une distance inférieure à ϵ :

$$\exists M \in \mathbb{N} \ \Big[\ i, j > M \to |r_i - r_j| < \alpha/2 \Big].$$

Donc pour cet indice M, on sait d'une part qu'il existe un élément r_j de module plus grand que α ; c'est à dire que r_j est éloigné de 0 d'une distance plus grande que α. Et d'autre part, tous les autres éléments suivant r_M sont à une distance de r_j inférieure à $\alpha/2$. Il en résulte que tous les termes d'indice plus grand que M sont non nuls (ils ont une valeur absolue plus grande que $\frac{\alpha}{2}$). Ces développements permettent de poser la définition suivante.

Définition 8.2.11. *Pour tout élément non nul $[(r_j)_j] \in \mathbb{R}_{\mathrm{C}}$, on définit (avec les notations ci-dessus) l'élément $[(r_j)_j]^{-1}$ par $[(r_j)_j]^{-1} = [(s_j)_j]$ où*

$$s_j = \begin{cases} 0 & si\ j \leq M\ ; \\ \frac{1}{r_j} & si\ j > M. \end{cases}$$

Il reste alors à faire les vérifications d'usage.

Proposition 8.2.12. *Pour tout élément non nul $[(r_j)_j] \in \mathbb{R}_{\mathrm{C}}$, l'élément $[(r_j)_j]^{-1}$ est bien défini. De plus on a $[(r_j)_j] \cdot_R [(r_j)_j]^{-1} = [(1)_j]$.*

Démonstration.
On montre que la suite $(s_j)_j$ introduite à la définition 8.2.11 est de Cauchy. En effet, en procédant comme ci-dessus, on montre qu'il existe $\alpha > 0$ tel que $\forall \epsilon > 0, \exists J \in \mathbb{N}$ tel que

$$i, j > J \Rightarrow |r_i - r_j| < \epsilon\alpha^2 \ et \ |r_i|, |r_j| \geq \alpha.$$

Dès lors on a bien, pour $i, j > J$,

$$|\frac{1}{r_i} - \frac{1}{r_j}| = |\frac{r_i - r_j}{r_i r_j}| < \epsilon.$$

De plus on a $[(r_j)_j] \cdot_R [(r_j)_j{}^{-1}] = 1$ car, vu la construction de $(s_j)_j$, on a, à partir d'un certain indice, $r_j \,.\, s_j = 1$. Enfin, on note que si on construit une suite $(s_j)_j$ à partir d'un autre représentant de $[(r_j)_j]$, cela fournit également un inverse de $[(r_j)_j]$. La construction est donc indépendante du représentant choisi, vu l'unicité de l'inverse. □

On peut résumer les résultats de cette section en un théorème.

Théorème 8.2.13. *Le quintuple $(\mathbb{R}_{\mathrm{C}}, +_R, 0_R, \cdot_R, 1_R)$ est un corps commutatif.*

8.3 Ordre sur $\mathbb{R}_C$

Soit deux éléments $(r_j)_j$ et $(s_j)_j$ de $\mathscr{A}$, comme ces suites sont de Cauchy, on sait que quelle que soit la précision ϵ donnée, il existe un indice M à partir duquel tous les éléments suivants de la suite $(r_j)_j$ et $(s_j)_j$ respectivement se trouvent dans des intervalles fixes, de rayon ϵ. L'espoir est alors que pour un certain ϵ ces intervalles soient disjoints, et qu'ils puissent ainsi définir un ordre entre les suites :

Ainsi, on pourrait convenir que "$(r_j)_j < (s_j)_j$" s'il existe un ϵ pour lequel on a un indice M tel que

$$j \geq M \to r_j \leq r_M + \epsilon < s_M - \epsilon \leq s_j,$$

où l'existence de l'indice M est assurée par le fait que les suites considérées sont de Cauchy. On arrive alors naturellement à la définition, où on élimine le recours à ϵ en introduisant deux rationnels.

Définition 8.3.1 (Ordre sur $\mathbb{R}_C$)**.** *Soient $[(r_j)_j]$ et $[(s_j)_j]$ deux éléments de $\mathbb{R}_C$, on pose $[(r_j)_j] \leq_R [(s_j)_j]$ si une des deux propriétés est vérifiée*

$$[(r_j)_j] = [(s_j)_j]$$

ou

$$\exists M \in \mathbb{N}\ \exists p, q \in \mathbb{Q}\ \forall j \left[\ j \geq M\ \to\ [r_j \leq p < q \leq s_j]\ \right].$$

Il faut maintenant s'assurer que la relation définie en 8.3.1 est bien licite, en faisant les vérifications habituelles.

Proposition 8.3.2. *La relation $\leq_R$ définie en 8.3.1 est un ordre sur $\mathbb{R}_C$ et est indépendante des représentants.*

Démonstration.
D'abord, on vérifie que la relation est réflexive, transitive et antisymétrique.

- Réflexivité : la réflexivité de l'égalité implique la réflexivité de $\leq_R$;
- Transitivité : soient $[(r_j)_j]$, $[(s_j)_j]$ et $[(t_j)_j]$ trois éléments de $\mathbb{R}_C$ tels que

$$[(r_j)_j] \leq [(s_j)_j] \text{ et } [(s_j)_j] \leq [(t_j)_j].$$

Si au moins deux représentants des trois réels sont équivalents, la transitivité est assurée. Sinon, cela signifie qu'il existe des naturels M_1 et M_2 tels que respectivement

$$\exists p_1, q_1 \in \mathbb{Q}\ [j > M_1\ \to\ r_j \leq p_1 < q_1 \leq s_j],$$

et

$$\exists p_2, q_2 \in \mathbb{Q}\ [j > M_2 \ \rightarrow \ s_j \leq p_2 < q_2 \leq t_j].$$

On en déduit que pour $M \geq sup\{M_1, M_2\}$, grâce à la transitivité de l'ordre dans $\mathbb{Q}$, on a

$$j > M \ \rightarrow \ r_j \leq p_1 < q_1 \leq t_j.$$

- Antisymétrie : soient $[(r_j)_j]$ et $[(s_j)_j]$ deux éléments de $\mathbb{R}_C$ tels que $[(r_j)_j] \leq_R [(s_j)_j]$ et $[(s_j)_j] \leq_R [(r_j)_j]$. On montre qu'alors il n'est pas possible que $[(r_j)_j] \neq [(s_j)_j]$. En effet, si tel n'est pas le cas, vu la définition 8.3.1 de $\leq_R$ il existe M_1 et M_2 tels que respectivement

$$\exists p_1, q_1 \in \mathbb{Q}\ [j > M_1 \ \rightarrow \ r_j \leq p_1 < q_1 \leq s_j],$$

et

$$\exists p_2, q_2 \in \mathbb{Q}\ [j > M_2 \ \rightarrow \ s_j \leq p_2 < q_2 \leq r_j].$$

On en déduit que pour $M \geq sup\{M_1, M_2\}$, grâce à la transitivité de l'ordre dans $\mathbb{Q}$, on a

$$r_j < s_j < r_j$$

ce qui est contradictoire.

On montre à présent que la définition 8.3.1 de $\leq_R$ est indépendante des représentants. Soient alors $[(r_j)_j]$ et $[(s_j)_j]$ deux éléments de $\mathbb{R}_C$ tels que $[(r_j)_j] \leq_R [(s_j)_j]$ et soit $(r'_j)_j$ une suite de Cauchy équivalente à $(r_j)_j$. Évidemment, si $(r_j)_j \sim (s_j)_j$ il n'y a rien à démontrer, on suppose donc que $[(r_j)_j] \neq [(s_j)_j]$. Dès lors, vu la définition de $\leq_R$ on sait qu'il existe un indice K et deux rationnels p et q tels que

$$\forall j \ \Big[\ j > K \ \rightarrow \ [r_j \leq p < q \leq s_j] \ \Big].$$

Puisque $(r_j)_j$ est de Cauchy et puisque $(r_j)_j$ et $(r'_j)_j$ sont des suites équivalentes, il existe des indices $L, M \in \mathbb{N}$ tels que

$$\begin{aligned} i, j > L \rightarrow |r_i - r_j\,| &< (q-p)/3 \\ j > M \rightarrow |\,r_j - r'_j| &< (q-p)/3, \end{aligned}$$

Dès lors, pour $J > \sup\{K, L, M\}$ on a d'une part

$$j \geq J \rightarrow |r_j - r'_j| < (q-p)/3,$$

et d'autre part

$$j \geq J \rightarrow |\,r_j - r_J| < (q-p)/3.$$

Donc, au total, on a

$$j \geq J \rightarrow |r_J - r'_j| < 2(q-p)/3.$$

Enfin, puisque $r_J \leq p$, on a

$$j \geq J \rightarrow r'_j < p + 2(q-p)/3 < q \leq s_j,$$

c'est-à-dire $[(r'_j)_j] \leq [(s_j)_j]$. On procède de la même manière pour le cas $(s_j)_j \sim (s_j)_j{}'$. □

Remarque 8.3.3. *Vu la définition 8.3.1 de $\leq_R$ il apparaît assez clairement que l'injection ϕ définie en 8.2.6 préserve la relation d'ordre. En effet, pour $r, s \in \mathbb{Q}$ tels que $r \leq s$, si $r = s$ alors $\phi(r) = \phi(s)$ sinon, on on sait qu'il existe des rationnels p, q tels que $r < p < q < s$ et comme par définition $\phi(r) = (r)_j$ et $\phi(s) = (s)_j$, on vérifie trivialement que $\phi(r) \leq_R \phi(s)$:*

$$\forall j \Big[r < p < r < s \Big]$$

Enfin, on montre que l'ordre défini sur $\mathbb{R}_C$ est total.

Proposition 8.3.4. *Si $(r_j)_j$ et $(s_j)_j$ sont deux suites de Cauchy non-équivalentes, alors une et une seule des propositions suivantes est vérifiée*

(a) $\exists M \in \mathbb{N} \ \exists p, q \in \mathbb{Q} \ [\ j > M \to r_j \leq p < q \leq s_j]$;

(b) $\exists M \in \mathbb{N} \ \exists p, q \in \mathbb{Q} \ [\ j > M \to s_j \leq p < q \leq r_j]$.

Démonstration.
Comme on considère deux suites de Cauchy $(r_j)_j$ et $(s_j)_j$ qui ne sont pas équivalentes, on sait que, par définition, $(r_j - s_j)_j$ ne converge pas vers 0. Dès lors, il existe un rationnel $\epsilon > 0$ tel que $\forall M \in \mathbb{N}$ il existe au moins un indice $j_M > M$ tel que $|r_{j_M} - s_{j_M}| \geq \epsilon$. Puisque les suites $(r_j)_j$ et $(s_j)_j$ sont de Cauchy, il existe $K \in \mathbb{N}$ tel que

$$\begin{aligned} i, j > K \ &\to \ |r_i - r_j| < \epsilon/3 \ ; \\ i, j > K \ &\to \ |s_i - s_j| < \epsilon/3. \end{aligned}$$

Vu la première condition ci-dessus, on a alors $j_K > K$ tel que

$$|r_{j_K} - s_{j_K}| \geq \epsilon.$$

On peut supposer sans perte de généralité $s_{j_K} > r_{j_K}$ (quitte par exemple à renommer les suites). On a alors

$$s_{j_K} \geq r_{j_K} + \epsilon$$

et simultanément, puisque $j_K > K$,

$$j > j_K \to (|\, r_j - r_{j_K}| < \epsilon/3 \text{ et } |\, s_j - s_{j_K}| < \epsilon/3).$$

Cette dernière condition implique

$$j > j_K \to (r_j < r_{j_K} + \epsilon/3 \text{ et } s_{j_K} - \epsilon/3 < s_j).$$

La condition (a) de l'énoncé est donc satisfaite pour les rationnels $p = r_{j_K} + \epsilon/3$ et $q = s_{j_K} - \epsilon/3$, qui sont tels que $p < q$ parce que $s_{j_K} \geq r_{j_K} + \epsilon$. On a donc montré que si $[(r_j)_j]$ et $[(s_j)_j]$ ne sont pas équivalents, alors on a soit $[(r_j)_j] \leq_R [(s_j)_j]$ soit $[(s_j)_j] \leq_R [(r_j)_j]$. □

Chapitre 9

Théorème d'isomorphie

Nous avons expliqué dans les chapitres précédents deux constructions possibles des nombres réels, à savoir celle de Dedekind et celle de Cantor. Une question naturelle est alors de savoir à quel point ces constructions diffèrent. Il s'avère que l'on peut construire un isomorphisme entre $\mathbb{R}_{\mathrm{C}}$ et $\mathbb{R}_{\mathrm{D}}$, donc ces structures ne sont pas différentes. Toute personne intéressée par la construction d'un isomorphisme concret pourra consulter [27, p. 233]. On se concentre ici sur un théorème d'isomorphie plus général, concernant les corps commutatifs archimédiens complets, dont on peut également trouver l'explication dans [27, p. 177]. On détaille ici cette approche. Ce théorème plus général nous permettra de comparer les corps commutatifs (non triviaux) $\mathbb{R}_{\mathrm{C}}$ et $\mathbb{R}_{\mathrm{D}}$. Aussi, l'on énoncera les résultats de ce chapitre dans le contexte de corps commutatifs non réduits à $\{0\}$, même si ces hypothèses ne sont pas toujours nécessaires.

Enfin, la première étape du théorème général dont il est question ici consiste à montrer que l'on peut "plonger" le corps $\mathbb{Q}$ dans tout corps commutatif totalement ordonné $\mathbb{K}$ (dont la définition est donnée ci-dessous), à l'aide d'une application qui va préserver la somme, le produit, et l'ordre. On montre en fait d'abord qu'une telle application (un morphisme) existe de $\mathbb{N}$ dans $\mathbb{K}$, puis on la prolonge successivement de $\mathbb{N}$ à $\mathbb{Z}$, puis de $\mathbb{Z}$ à $\mathbb{Q}$, en utilisant les définitions mêmes de $\mathbb{Z}$ et $\mathbb{Q}$.

9.1 Quelques morphismes

Proposition 9.1.1. *Si $(\mathbb{K}, +, .)$ est un corps (commutatif, non trivial), alors il existe un unique morphisme (de structures additive et multiplicative) $f_{\mathbb{N}}$ de $\mathbb{N}$ dans $\mathbb{K}$.*

Démonstration. Démontrons d'abord l'unicité. Si f est un morphisme de $\mathbb{N}$ dans $\mathbb{K}$, alors on a[1] $f(0) = 0_{\mathbb{K}}$ et $f(1) = 1_K$, et par suite $f(n+1) = f(n) +_{\mathbb{K}} f(1) = f(n) +_{\mathbb{K}} 1_{\mathbb{K}}$, pour tout $n \in \mathbb{N}$. Par le théorème 4.2.2 de la récursion, on sait qu'il existe exactement une

1. Remarquons que si on n'impose pas ces conditions dans la définition de morphisme, en choisissant une définition plus faible, on a tout de même $f(0) = 0_{\mathbb{K}}$ car f préserve la somme, mais on a deux choix pour $f(1)$, à savoir 1_K ou $0_{\mathbb{K}}$. Dans le deuxième cas, f est alors identiquement nul.

application ayant ces propriétés. Passons à l'existence. On utilise donc le théorème 4.2.2 où, avec les notations du théorème, on pose

$$a = 0_{\mathbb{K}} \text{ et } F : k \in \mathbb{K} \mapsto k +_{\mathbb{K}} 1_{\mathbb{K}}$$

L'application $f_{\mathbb{N}}$ cherchée est alors définie par

(i) $f_{\mathbb{N}}(0) = 0_{\mathbb{K}}$;

(ii) $f_{\mathbb{N}}(n+1) = F(f_{\mathbb{N}}(n)) = f_{\mathbb{N}}(n) +_{\mathbb{K}} 1_{\mathbb{K}}$.

On prouve ensuite qu'il s'agit d'un morphisme.

D'abord, par définition on a $f_{\mathbb{N}}(0) = 0_{\mathbb{K}}$, et $f_{\mathbb{N}}(1) = 0_{\mathbb{K}} + 1_{\mathbb{K}} = 1_{\mathbb{K}}$. On montre ensuite que la somme est préservée :

$$f_{\mathbb{N}}(m+n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n).$$

Pour ce faire, on procède par récurrence sur n. Soit donc T l'ensemble défini par

$$T = \Big\{ n \in \mathbb{N} \;\Big|\; \forall m \in \mathbb{N}\ [f_{\mathbb{N}}(m+n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n)] \Big\}.$$

- $0 \in T$: c'est immédiat vu que, par définition de $f_{\mathbb{N}}$, on a successivement

$$\begin{aligned} f_{\mathbb{N}}(m+0) &= f_{\mathbb{N}}(m) \\ &= f_{\mathbb{N}}(m) + f_{\mathbb{N}}(0). \end{aligned}$$

- Induction : soit $n \in T$, comme alors, par hypothèse sur n, on a

$$\forall m \in \mathbb{N}\ [f_{\mathbb{N}}(m+n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n)]$$

il s'ensuit que

$$\begin{aligned} f_{\mathbb{N}}(m+n+1) &= f_{\mathbb{N}}(m+n) + f_{\mathbb{N}}(1) \\ &= f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n) + f_{\mathbb{N}}(1) \\ &= f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n+1). \end{aligned}$$

On procède de la même manière pour établir que $f_{\mathbb{N}}(m.n) = f_{\mathbb{N}}(m).f_{\mathbb{N}}(n)$. □

Notons que l'on peut étudier, si $\mathbb{K}$ a les bonnes propriétés, le caractère injectif ou croissant du morphisme $f_{\mathbb{N}}$. Rappelons pour ce faire que la caractéristique d'un corps $\mathbb{K}$ est soit le plus petit naturel n tel que

$$1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}} = 0_{\mathbb{K}},$$

où la somme contient n termes, si un tel nombre existe, soit 0 dans le cas contraire. La somme apparaissant dans cette définition n'est autre que $f_{\mathbb{N}}(n)$. On obtient donc naturellement le résultat suivant.

Proposition 9.1.2. *Soit $\mathbb{K}$ un corps (commutatif, non trivial). Alors la caractéristique de $\mathbb{K}$ est nulle si et seulement si $f_{\mathbb{N}}$ est injectif.*

Démonstration. Si $f_{\mathbb{N}}$ est injectif, alors pour tout $n \neq 0$ on a $f_{\mathbb{N}}(n) \neq f_{\mathbb{N}}(0)$ et donc $f_{\mathbb{N}}(n) \neq 0_{\mathbb{K}}$. Vu l'interprétation de $f_{\mathbb{N}}$, on en déduit que la caractéristique de $\mathbb{K}$ est nulle.

Réciproquement, si $\mathbb{K}$ est de caractéristique nulle et si $m, n \in \mathbb{N}$ sont tels que $f_{\mathbb{N}}(m) = f_{\mathbb{N}}(n)$, alors, comme l'ordre sur $\mathbb{N}$ est total, on a $m \leq n$ ou $n \leq m$. Traitons le premier cas. Comme $m \leq n$, vu 4.4.14 on a $n = m + (n - m)$ de sorte que

$$f_{\mathbb{N}}(n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n - m) = f_{\mathbb{N}}(m)$$

Comme $\mathbb{K}$ est un corps, on en déduit que $f_{\mathbb{N}}(n - m) = 0_{\mathbb{K}}$ et, vu l'interprétation de $f_{\mathbb{N}}$ on a

$$\underbrace{1_{\mathbb{K}} + ... + 1_{\mathbb{K}}}_{(n-m)fois} = 0_{\mathbb{K}}.$$

Dès lors, $n - m = 0$ car la caractéristique de $\mathbb{K}$ est nulle, donc finalement $m = n$. □

Nous avons montré, dans le chapitre consacré à $\mathbb{Q}$, et celui consacré à $\mathbb{R}_{\mathrm{D}}$, que l'ordre était compatible avec la somme et le produit. Ces constatations interviennent comme définition d'un corps totalement ordonné, que nous donnons maintenant.

Définition 9.1.3. *Un corps $\mathbb{K}$ est dit totalement ordonné s'il est muni d'une relation d'ordre $\leq$ telle que*

(i) Pour tous $a, b, c \in \mathbb{K}$, on a $a \leq b \to a + c \leq b + c$;

(ii) Pour tous $a, b \in \mathbb{K}$ tels que $a \geq 0$ et $b \geq 0$, on a $a.b \geq 0$.

Remarquons que puisque dans un corps, tout élément admet un opposé, la première condition implique aussi $a + c < b + c \to a < b$ pour tous $a, b, c \in \mathbb{K}$. On montre également facilement que dans tout corps totalement ordonné non trivial, on a $0_{\mathbb{K}} < 1_{\mathbb{K}}$.

Proposition 9.1.4. *Soit $\mathbb{K}$ un corps (commutatif, non trivial) totalement ordonné. Alors $f_{\mathbb{N}}$ est strictement croissant. En particulier, tout corps totalement ordonné est de caractéristique nulle.*

Démonstration. On montre d'abord par récurrence que pour tout naturel n non nul, on a $f_{\mathbb{N}}(n) > 0_{\mathbb{K}}$. On procède par récurrence. Soit l'ensemble T définit par

$$T = \{n \in \mathbb{N} \mid f_{\mathbb{N}}(n^+) > 0\}.$$

- $0 \in T$: c'est immédiat car $0_{\mathbb{K}} < 1_{\mathbb{K}}$;
- Induction : si n appartient à T alors, vu 4.4.12, on a successivement

$$f_{\mathbb{N}}(n^+) = f_{\mathbb{N}}(n) + 1_{\mathbb{K}} > 1_{\mathbb{K}} > 0_{\mathbb{K}}.$$

Cela étant établi, soit $m, n \in \mathbb{N}$ tels que $m < n$. Par le théorème 4.4.14, on peut écrire $n = m + (n - m)$, avec $n - m \neq 0$. On a alors

$$f_{\mathbb{N}}(n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n - m) > f_{\mathbb{N}}(m),$$

où l'inégalité est assuré d'une part grâce au fait que, comme $n - m \neq 0$, on a montré que $f_{\mathbb{N}}(n^+) > 0$, et d'une part vu la condition (i) de la définition 9.1.3. Enfin, le cas particulier résulte de la proposition 9.1.2. □

Remarquons que cette proposition stipule de manière formelle le fait évident que dans un corps totalement ordonné, en ajoutant 1_K à un élément, on obtient un élément plus grand, et que l'on peut répéter cette opération un certain nombre de fois.

On prolonge maintenant $f_{\mathbb{N}}$ à $\mathbb{Z}$ pour disposer alors d'un morphisme d'anneaux. Pour tous $k, l \in \mathbb{K}$, on écrira naturellement $k -_{\mathbb{K}} l$ pour $k +_{\mathbb{K}} (-_{\mathbb{K}} l)$, comme il est d'usage.

Proposition 9.1.5. *Soit $\mathbb{K}$ un corps (commutatif, non trivial) totalement ordonné.*
L'application $f_{\mathbb{Z}}$ définie par

$$f_{\mathbb{Z}} \ : \ \mathbb{Z} \to \mathbb{K} : \ [a, b] \mapsto f_{\mathbb{Z}}([a, b]) = f_{\mathbb{N}}(a) -_{\mathbb{K}} f_{\mathbb{N}}(b)$$

est un morphisme strictement croissant d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$.

Démonstration. D'abord, on montre que la définition ne dépend pas du représentant et que $f_{\mathbb{Z}}$. Par définition, on a

$$(a, b) \sim (a', b') \leftrightarrow a + b' = a' + b.$$

Comme $f_{\mathbb{N}}$ est un morphisme, on a

$$(a, b) \sim (a', b') \to f_{\mathbb{N}}(a + b') = f_{\mathbb{N}}(a' + b) \to f_{\mathbb{N}}(a) +_{\mathbb{K}} f_{\mathbb{N}}(b') = f_{\mathbb{N}}(a') +_{\mathbb{K}} f_{\mathbb{N}}(b).$$

Puisque $\mathbb{K}$ est un anneau, on obtient

$$(a, b) \sim (a', b') \to f_{\mathbb{N}}(a) -_{\mathbb{K}} f_{\mathbb{N}}(b) = f_{\mathbb{N}}(a') -_{\mathbb{K}} f_{\mathbb{N}}(b').$$

Enfin, par définition de $f_{\mathbb{Z}}$, on a

$$(a, b) \sim (a', b') \to f_{\mathbb{Z}}([a, b]) = f_{\mathbb{Z}}([a', b']).$$

On montre de manière similaire que $f_{\mathbb{Z}}$ est croissant. En effet, par la définition 5.3.2, on a dans $\mathbb{Z}$

$$[a, b] < [c, d] \leftrightarrow a + d < b + c.$$

On a donc successivement, puisque $f_{\mathbb{N}}$ est un morphisme strictement croissant

$$[a, b] < [c, d] \to a + d < b + c \to f_{\mathbb{N}}(a + d) < f_{\mathbb{N}}(b + c) \to f_{\mathbb{N}}(a) + f_{\mathbb{N}}(d) < f_{\mathbb{N}}(b) + f_{\mathbb{N}}(c).$$

Puisque $\mathbb{K}$ est un corps totalement ordonné, on obtient, en "soustrayant" $f_{\mathbb{N}}(d) +_{\mathbb{K}} f_{\mathbb{N}}(b)$:

$$[a, b] < [c, d] \to f_{\mathbb{N}}(a) -_{\mathbb{K}} f_{\mathbb{N}}(b) < f_{\mathbb{N}}(c) -_{\mathbb{K}} f_{\mathbb{N}}(c)$$

et on conclut par définition de $f_{\mathbb{Z}}$. On montre ensuite que $f_{\mathbb{Z}}$ préserve les opérations.

- On a $f_{\mathbb{Z}}(z+z') = f_{\mathbb{Z}}(z) +_{\mathbb{K}} f_{\mathbb{Z}}(z')$: si $z = [a,b]$ et $z' = [c,d]$, alors

$$\begin{aligned} f_{\mathbb{Z}}([a,b]+[c,d]) &= f_{\mathbb{Z}}([a+c,b+d]) = f_{\mathbb{N}}(a+c) -_{\mathbb{K}} f_{\mathbb{N}}(b+d) \\ &= f_{\mathbb{N}}(a) +_{\mathbb{K}} f_{\mathbb{N}}(c) +_{\mathbb{K}} -_{\mathbb{K}}(f_{\mathbb{N}}(b) +_K f_{\mathbb{N}}(d)) \\ &= (f_{\mathbb{N}}(a) -_{\mathbb{K}} f_{\mathbb{N}}(b)) +_{\mathbb{K}} (f_{\mathbb{N}}(c) - f_{\mathbb{N}}(d)) \\ &= f_{\mathbb{Z}}(z) +_{\mathbb{K}} f_{\mathbb{Z}}(z'). \end{aligned}$$

- On a $f_{\mathbb{Z}}(z.z') = f_{\mathbb{Z}}(z).{}_{\mathbb{K}} f(z')$: si $z = [a,b]$ et $z' = [c,d]$, alors

$$\begin{aligned} f_{\mathbb{Z}}(z.z') &= f_{\mathbb{Z}}([a,b].[c,d]) = f_{\mathbb{Z}}([ac+bd, ad+bc]) \\ &= f_{\mathbb{N}}(ac+bd) -_{\mathbb{K}} (f_{\mathbb{N}}(ad+bc)) \\ &= f_{\mathbb{N}}(a).{}_{\mathbb{K}} f_{\mathbb{N}}(c) +_{\mathbb{K}} f_{\mathbb{N}}(b).{}_{\mathbb{K}} f_{\mathbb{N}}(d) -_{\mathbb{K}} \left(f_{\mathbb{N}}(a).{}_{\mathbb{K}} f_{\mathbb{N}}(d) +_{\mathbb{K}} f_{\mathbb{N}}(b).{}_{\mathbb{K}} f_{\mathbb{N}}(c)\right) \\ &= f_{\mathbb{N}}(a).{}_{\mathbb{K}}(f_{\mathbb{N}}(c) - f_{\mathbb{N}}(d)) +_{\mathbb{K}} f_{\mathbb{N}}(b).{}_{\mathbb{K}}(f_{\mathbb{N}}(d) -_{\mathbb{K}} f_{\mathbb{N}}(c)) \\ &= (f_{\mathbb{N}}(a) -_{\mathbb{K}} f_{\mathbb{N}}(b)).{}_{\mathbb{K}}((f_{\mathbb{N}}(c) - f_{\mathbb{N}}(d)) = f_{\mathbb{Z}}(z).{}_{\mathbb{K}} f(z'). \end{aligned}$$

Enfin, on a directement par définition que $f_{\mathbb{Z}}(0) = 0_{\mathbb{K}}$ et $f_{\mathbb{Z}}(1) = 1_{\mathbb{K}}$. □

De la même manière, on prolonge $f_{\mathbb{Z}}$ à $\mathbb{Q}$ pour avoir un morphisme de corps.

Proposition 9.1.6. *Soit $\mathbb{K}$ un corps (commutatif, non trivial) totalement ordonné. L'application $f_{\mathbb{Q}}$ définie par*[2]

$$f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{K} : [a,b] \mapsto f_{\mathbb{Q}}([a,b]) = f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b)$$

est un morphisme de corps de $\mathbb{Q}$ dans $\mathbb{K}$, strictement croissant.

Démonstration. On procède en tout point comme pour la proposition précédente, et on montre d'abord que la définition de $f_{\mathbb{Q}}$ est indépendante des représentants. Pour tous $a, b, a', b' \in \mathbb{Z}$ tels que $b, b' \neq 0$, on a

$$(a,b) \sim (a',b') \leftrightarrow a.b' = a'.b.$$

Comme $f_{\mathbb{Z}}$ est et est un morphisme, on a par la définition 6.1.1

$$(a,b) \sim (a',b') \to f_{\mathbb{Z}}(a.b') = f_{\mathbb{Z}}(a'.b) \to f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}(b') = f_{\mathbb{Z}}(a').{}_{\mathbb{K}} f_{\mathbb{Z}}(b).$$

Par le caractère strictement croissance de $f_{\mathbb{Z}}$, les éléments $f_{\mathbb{Z}}(b)$ et $f_{\mathbb{Z}}(b')$ sont strictement positifs. Puisque $\mathbb{K}$ est un corps, on obtient, en multipliant par les inverses de ces éléments, également strictement positifs[3]

$$(a,b) \sim (a',b') \to f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b) = f_{\mathbb{Z}}(a').{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b').$$

2. Pour garder la notation compacte, on se permet d'écrire $f_{\mathbb{Z}}^{-1}(b)$ au lieu de $(f_{\mathbb{Z}}(b))^{-1}$, l'exposant -1 désignant l'inverse dans le corps $\mathbb{K}$.

3. C'est une propriété immédiate des corps totalement ordonnés.

Enfin, par définition de $f_{\mathbb{Q}}$, on a

$$(a,b) \sim (a',b') \to f_{\mathbb{Q}}([a,b]) = f_{\mathbb{Q}}([a',b']).$$

On démontre de la même manière que $f_{\mathbb{Q}}$ est strictement croissant : par la définition 6.2.1, pour $[a,b],[c,d] \in \mathbb{Q}$ tels que $c > 0$ et $d > 0$, on a

$$[a,b] < [c,d] \leftrightarrow a.d < b.c.$$

Comme $f_{\mathbb{Z}}$ est un morphisme strictement croissant, on a successivement

$$[a,b] < [c,d] \to a.d < b.c \to f_{\mathbb{Z}}(a.d) < f_{\mathbb{Z}}(b.c) \to f_{\mathbb{Z}}(a).f_{\mathbb{Z}}(d) < f_{\mathbb{Z}}(b).f_{\mathbb{Z}}(c).$$

Puisque $\mathbb{K}$ est un corps totalement ordonné, en "divisant" par l'élément strictement positif $f_{\mathbb{N}}(d).f_{\mathbb{N}}(b)$, on obtient

$$[a,b] < [c,d] \to f_{\mathbb{Z}}(a).f_{\mathbb{Z}}^{-1}(b) < f_{\mathbb{Z}}(c).f_{\mathbb{Z}}^{-1}(c)$$

et on conclut par définition de $f_{\mathbb{Q}}$.

On montre ensuite que les opérations sont préservées.

- $f_{\mathbb{Q}}(r+s) = f_{\mathbb{Q}}(r) +_{\mathbb{K}} f_{\mathbb{Q}}(s)$: à nouveau, il s'agit simplement d'appliquer les propriétés de $f_{\mathbb{Z}}$ aux définitions considérées. Si $r = [a,b]$ et $s = [c,d]$, alors

$$\begin{aligned} f_{\mathbb{Q}}([a,b]+[c,d]) &= f_{\mathbb{Q}}([a.d. + b.c, b.d]) \\ &= f_{\mathbb{Z}}(a.d. + b.c) \cdot_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b.d) \\ &= \Big(f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}(d) +_{\mathbb{K}} f_{\mathbb{Z}}(b).{}_{\mathbb{K}} f_{\mathbb{Z}}(c)\Big).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b) \cdot_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(d) \\ &= f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b) +_{\mathbb{K}} f_{\mathbb{Z}}(c).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(d) \\ &= f_{\mathbb{Q}}([a,b]) +_{\mathbb{K}} f_{\mathbb{Q}}([c,d]). \end{aligned}$$

- $f_{\mathbb{Q}}(r.s) = f_{\mathbb{Q}}(r) \cdot_{\mathbb{K}} f_{\mathbb{Q}}(s)$:
  On procède comme au point précédent. Si $r = [a,b]$ et $s = [c,d]$, alors

$$\begin{aligned} f_{\mathbb{Q}}([a,b].[c,d]) &= f_{\mathbb{Q}}([a.c, b.d]) \\ &= f_{\mathbb{Z}}(a.c).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b.d) \\ &= f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}(c).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(d) \\ &= (f_{\mathbb{Z}}(a).{}_{\mathbb{K}}.{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(b))(f_{\mathbb{Z}}(c).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(d)) \\ &= f_{\mathbb{Q}}([a,b]).{}_{\mathbb{K}} f_{\mathbb{Q}}([c,d]). \end{aligned}$$

Enfin, on a encore par définition que $f_{\mathbb{Q}}(0) = 0_{\mathbb{K}}$ et $f_{\mathbb{Q}}(1) = 1_{\mathbb{K}}$. □

Remarque 9.1.7. *On vérifie que les morphismes définis ci-dessus sont compatibles avec les plongements successifs de $\mathbb{N}$ dans $\mathbb{Z}$ et de $\mathbb{Z}$ dans $\mathbb{Q}$: on a $f_{\mathbb{N}} = f_{\mathbb{Z}} \circ \phi$, où ϕ est*

le plongement canonique de $\mathbb{N}$ *dans* $\mathbb{Z}$ *et* $f_{\mathbb{Z}} = f_{\mathbb{Q}} \circ \phi$ *où, cette fois,* ϕ *est le plongement canonique de* $\mathbb{Z}$ *dans* $\mathbb{Q}$. *En effet, pour* $n \in \mathbb{N}$, *on a*

$$f_{\mathbb{Z}} \circ \phi(n) = f_{\mathbb{Z}}([n, 0]) = f_{\mathbb{N}}(n) -_{\mathbb{K}} f_{\mathbb{N}}(0) = f_{\mathbb{N}}(n),$$

puisque $f_{\mathbb{N}}(0) = 0_{\mathbb{K}}$. *De même, pour tout* $a \in \mathbb{Z}$, *on a*

$$f_{\mathbb{Q}} \circ \phi(a) = f_{\mathbb{Q}}([a, 1]) = f_{\mathbb{Z}}(a).{}_{\mathbb{K}} f_{\mathbb{Z}}^{-1}(1) = f_{\mathbb{Z}}(a),$$

car, puisque $f_{\mathbb{Z}}$ *est un morphisme d'anneaux, on a* $f_{\mathbb{Z}}(1) = 1_{\mathbb{K}}$.

On peut représenter ces égalités à l'aide de diagrammes commutatifs :

On aura besoin dans la suite de la définition de la valeur absolue dans un corps totalement ordonné quelconque. Nous l'avons déjà rencontrée dans $\mathbb{Q}$ ou $\mathbb{R}_{\mathrm{D}}$. La définition est évidemment similaire.

Définition 9.1.8. *Si* $\mathbb{K}$ *est un corps totalement ordonné, on définit la valeur absolue d'un élément* $x \in \mathbb{K}$ *par*

$$|x| = \begin{cases} x & si\ x \geq 0_{\mathbb{K}}\ ; \\ -_{\mathbb{K}} x & si\ x \leq 0_{\mathbb{K}}. \end{cases}$$

Proposition 9.1.9. *Si* $\mathbb{K}$ *est un corps (commutatif, non trivial) totalement ordonné, alors pour tous rationnels* r *et* s, *on a*

$$|f_{\mathbb{Q}}(r) - f_{\mathbb{Q}}(s)| = f_{\mathbb{Q}}(|r - s|)$$

Démonstration. Cela vient d'une part de la définition de la valeur absolue, et d'autre part du caractère strictement croissant de $f_{\mathbb{Q}}$ (établi en 9.1.6). En effet, on a

$$|f_{\mathbb{Q}}(r - s)| = \begin{cases} f_{\mathbb{Q}}(r - s) & \text{si } f_{\mathbb{Q}}(r - s) \geq 0_{\mathbb{K}} \\ -f_{\mathbb{Q}}(r - s) & \text{si } f_{\mathbb{Q}}(r - s) < 0_{\mathbb{K}}. \end{cases}$$

Or, comme $f_{\mathbb{Q}}$ est strictement croissant, on peut réexprimer les conditions comme suit

$$|f_{\mathbb{Q}}(r - s)| = \begin{cases} f_{\mathbb{Q}}(r - s) & \text{si } r - s \geq 0 \\ f_{\mathbb{Q}}(s - r) & \text{si } r - s < 0. \end{cases}$$

En d'autres termes, on a

$$|f_{\mathbb{Q}}(r) - f_{\mathbb{Q}}(s)| = f_{\mathbb{Q}}(|r - s|).$$

□

9.2 Théorème d'isomorphie

À l'aide des morphismes définis dans la section précédente, et après un lemme, on montre un théorème d'isomorphie général qui a pour corollaire que les constructions des réels à la Dedekind et à la Cantor sont équivalentes.

Définition 9.2.1. *Un corps totalement ordonné $\mathbb{K}$ est archimédien si pour tout élément k de $\mathbb{K}$ il existe un naturel n tel que*

$$f_{\mathbb{N}}(n) > k.$$

Vu la remarque 9.1.7, on peut dans la définition précédente considérer que n est un élément de $\mathbb{Q}$, et écrire $f_{\mathbb{Q}}(n)$ au lieu de $f_{\mathbb{N}}(n)$. C'est ce que nous ferons par la suite.

Lemme 9.2.2. *Si $\mathbb{K}$ est un corps (complet) archimédien, alors une suite de rationnels $(r_j)_j$ est de Cauchy si et seulement si la suite $(f_{\mathbb{Q}}(r_j))_j$ est de Cauchy.*

Démonstration.
Soit $(r_j)_j$ une suite de Cauchy dans $\mathbb{Q}$. Comme $\mathbb{K}$ est archimédien, pour tout $\epsilon > 0$ on peut trouver un naturel n tel que $1 < f_{\mathbb{Q}}(n)\epsilon$ i.e.

$$f_{\mathbb{Q}}(1/n) < \epsilon$$

Vu que $(r_j)_j$ est de Cauchy, on sait qu'il existe alors $N \in \mathbb{N}$ tel que

$$i, j > N \to |r_i - r_j| < 1/n.$$

Ainsi, on a, vu la croissance stricte de $f_{\mathbb{Q}}$ (voir proposition 9.1.6)

$$|f_{\mathbb{Q}}(r_i) - f_{\mathbb{Q}}(r_j)| = f_{\mathbb{Q}}(|r_i - r_j|) < f_{\mathbb{Q}}(1/n) < \epsilon$$

et donc on a bien que $(f_{\mathbb{Q}}(r_j))_j$ est une suite de Cauchy. On montre maintenant la réciproque. Soit une suite $(r_j)_j$ telle que $(f_{\mathbb{Q}}(r_j))_j$ soit suite de Cauchy et soit $\epsilon > 0$ et $n \in \mathbb{N}$ tels que $1 < n.\epsilon$ (un tel n existe car $\mathbb{Q}$ est archimédien). Par définition,

$$\exists N \in \mathbb{N} \ : \ i, j > N \ \Rightarrow \ |f_{\mathbb{Q}}(r_i) - f_{\mathbb{Q}}(r_j)| < f_{\mathbb{Q}}(1/n)$$

Dès lors, comme $|f_{\mathbb{Q}}(r_i) - f_{\mathbb{Q}}(r_j)| = f_{\mathbb{Q}}(|r_i - r_j|)$ vu la proposition 9.1.9, et comme $f_{\mathbb{Q}}$ est strictement croissant, on a bien

$$|r_i - r_j| < 1/n < \epsilon,$$

ce qui termine la preuve. □

On arrive maintenant au théorème d'isomorphie visé.

Théorème 9.2.3. *Si $\mathbb{K}$ est un corps commutatif archimédien complet, alors il existe un isomorphisme g de $\mathbb{R}_{\mathrm{C}}$ dans $\mathbb{K}$ tel que*

$$f_{\mathbb{Q}} = g \circ \phi,$$

où ϕ est l'injection canonique de $\mathbb{Q}$ dans $\mathbb{R}_C$ définie en 8.2.6.

Démonstration. Soit l'application g définie par :

$$g \ : \ \mathbb{R}_C \to \mathbb{K} \ : \ [(r_j)_j] \mapsto \lim_j f_{\mathbb{Q}}(r_j).$$

On montre tour à tour que g est bien défini, qu'il est un morphisme de corps de $\mathbb{R}_C$ dans $\mathbb{K}$, qu'il est bijectif et enfin qu'il vérifie $f_{\mathbb{Q}} = g \circ \phi$.

- L'application g est bien définie. Tout d'abord, on montre que l'expression qui définit g a bien un sens, c'est-à-dire que pour toute suite de Cauchy $(r_j)_j$, la suite $(f_{\mathbb{Q}}(r_j))_j$ converge. Mais par le lemme 9.2.2, c'est une suite de Cauchy. Puisque $\mathbb{K}$ est complet, cette suite converge.

  On montre que la définition de g est indépendante des représentants. Soient en effet deux suites équivalentes $(r_j)_j$ et $(s_j)_j$ de $\mathscr{A}$, comme ces suites sont de Cauchy, les suites $(f_{\mathbb{Q}}(r_j))_j$ et $(f_{\mathbb{Q}}(s_j))_j$ sont alors des suites de Cauchy, et donc ces deux suites convergent. Notons r et s leurs limites respectives. De plus, comme $(r_j)_j$ et $(s_j)_j$ sont équivalentes, on a, par définition de l'équivalence

  $$(r_j - s_j) \to 0.$$

  Soit donc $0 < \epsilon \in \mathbb{K}$. Comme $\mathbb{K}$ est archimédien, on sait qu'il existe une naturel n tel que $1 < n\epsilon$. Il existe alors $N \in \mathbb{N}$ tel que

  $$j > N \to |\, r_j - s_j \,| < \frac{1}{n}.$$

  Et donc, vu le corollaire 9.1.9 on a

  $$|f_{\mathbb{Q}}(r_j) - f_{\mathbb{Q}}(s_j)| = f_{\mathbb{Q}}(|\, r_j - s_j \,|) < f_{\mathbb{Q}}(\frac{1}{n}) < \epsilon$$

  On en conclut que $r = s$, c'est à dire

  $$\lim_j (f_{\mathbb{Q}}(r_j)) = \lim_j (f_{\mathbb{Q}}(s_j)),$$

  ce qui montre bien que la définition de g est indépendante du représentant.
- L'application g est un morphisme d'anneaux.

  (i) Pour tout $[(r_j)_j]$ et $[(s_j)_j]$ dans $\mathbb{R}_C$, on a

  $$g([(r_j)_j] + [(s_j)_j]) = g([(s_j)_j]) +_{\mathbb{K}} g([(s_j)_j]).$$

  En effet, en utilisant uniquement les définitions, on note qu'on a successivement

  $$\begin{aligned} g((r_j)_j + (s_j)_j) &= g((r_j + s_j)_j) \\ &= \lim_j f_{\mathbb{Q}}(r_j + s_j) \\ &= \lim_j (f_{\mathbb{Q}}(r_j) + f_{\mathbb{Q}}(s_j)). \end{aligned}$$

  Or, on sait que les suites $(f_{\mathbb{Q}}(r_j))_j$ et $(f_{\mathbb{Q}}(s_j))_j$ convergent. On a alors finalement

  $$\begin{aligned} \lim_j (f_{\mathbb{Q}}(r_j) + f_{\mathbb{Q}}(s_j)) &= \lim_j f_{\mathbb{Q}}(r_j) +_{\mathbb{K}} \lim_j f_{\mathbb{Q}}(s_j) \\ &= g((r_j)_j) +_{\mathbb{K}} g((s_j)_j). \end{aligned}$$

(*ii*) Pour tout $[(r_j)_j]$ et $[(s_j)_j]$ dans $\mathbb{R}_{\mathrm{C}}$, on a

$$g([(r_j)_j].[(s_j)_j]) = g([(s_j)_j]) \cdot_{\mathbb{K}} g([(s_j)_j]).$$

Avec les mêmes arguments qu'au point précédent, on a

$$\begin{aligned} g((r_j)_j \,.\, (s_j)_j) &= g((r_j \,.\, s_j)_j) \\ &= \lim_j f_{\mathbb{Q}}(r_j \,.\, s_j) \\ &= (\lim_j f_{\mathbb{Q}}(r_j)).{}_{\mathbb{K}}(\lim_j f_{\mathbb{Q}}(s_j)) \\ &= g((r_j)_j) \cdot_{\mathbb{K}} g((s_j)_j). \end{aligned}$$

- L'application g est une bijection.

(*i*) On établit d'abord que g est injectif. Soient donc $[(r_j)_j]$ et $[(s_j)_j]$ deux éléments de $\mathbb{R}_{\mathrm{C}}$ tels que tels que $[(r_j)_j] \neq [(s_j)_j]$. Comme $\mathbb{R}_{\mathrm{C}}$ est totalement ordonné (et quitte à renommer les éléments) on a $[(r_j)_j] < [(s_j)_j]$; c'est à dire, selon la définition consacrée 8.3.1

$$\exists p, q \in \mathbb{Q},\ J \in \mathbb{N} \left[j \geq J \ \rightarrow \ r_j < p < q < s_j \right].$$

Autrement dit, pour $j \geq J$, on a $\mid r_j - s_j \mid > |p-q|$ de sorte que pour $\epsilon < f_{\mathbb{Q}}(|p-q|)$ on sait qu'alors il existe $J \in \mathbb{N}$ tel que

$$j > J \ \rightarrow \ |f_{\mathbb{Q}}(r_j) - f_{\mathbb{Q}}(s_j)| > f_{\mathbb{Q}}(|p-q|) > \epsilon \ ;$$

ce qui montre bien que $g((r_j)_j) \neq g((s_j)_j)$. On remarque que les mêmes arguments impliquent que g est strictement croissant.

(*ii*) On montre à présent que g est surjectif. Soit $k \in \mathbb{K}$, si $k = 0_{\mathbb{K}}$, alors $0 \in \mathbb{R}_{\mathrm{C}}$ vérifie $g(0) = 0$. On suppose donc $k \neq 0$, et quitte à considérer $-k$, on suppose aussi que $k > 0$. Pour tout naturel j non nul, on note p_j le plus petit entier naturel n tel que $f_{\mathbb{Q}}(n) \geq f_{\mathbb{Q}}(j)k$. Par définition on a alors $f_{\mathbb{Q}}(p_j - 1) < f_{\mathbb{Q}}(j)k$, puis successivement

$$\begin{aligned} f_{\mathbb{Q}}(p_j - 1) < f_{\mathbb{Q}}(j)k &\rightarrow f_{\mathbb{Q}}(p_j - 1)(f_{\mathbb{Q}}(j))^{-1} < k \\ &\rightarrow f_{\mathbb{Q}}(p_j)(f_{\mathbb{Q}}(j))^{-1} - f_{\mathbb{Q}}(1)(f_{\mathbb{Q}}(j))^{-1} < k \\ &\rightarrow f_{\mathbb{Q}}(\frac{p_j}{j}) < k + (f_{\mathbb{Q}}(j))^{-1}. \end{aligned}$$

Dès lors, on a

$$k < f_{\mathbb{Q}}(\frac{p_j}{j}) < k + f_{\mathbb{Q}}(\frac{1}{j}).$$

On en conclut que la suite $(f_{\mathbb{Q}}(\frac{p_j}{j}))_j$ est de Cauchy et converge vers k. Vu le lemme 9.2.2, la suite $(\frac{p_j}{j})_j$ est une suite de Cauchy dans $\mathbb{Q}$ et, par construction, elle est telle que $g((\frac{p_j}{j})_j) = k$.

- On a $f_{\mathbb{Q}} = g \circ \phi$.
  Soit $r \in \mathbb{Q}$, comme $\phi(r) = (r)_j$, on a

$$\begin{aligned} g(\phi(r)) &= \lim_j f_{\mathbb{Q}}((r)_j) \\ &= f_{\mathbb{Q}}(r). \end{aligned}$$

□

On a établi que $\mathbb{R}_{\mathrm{D}}$ est un corps, qu'il est complet et qu'il est muni d'un ordre total. On montre aussi assez facilement que c'est un corps totalement ordonné archimédien complet. On termine donc le corollaire suivant

Proposition 9.2.4. *Les corps totalement ordonnés $\mathbb{R}_{\mathrm{C}}$ et $\mathbb{R}_{\mathrm{D}}$ sont isomorphes.*

Quatrième partie

Logique intuitionniste

Introduction

Il est un fait qu'au XX^{e} siècle, une crise des fondements en mathématiques a exigé de repenser ces bases. Comme on l'a vu, une solution a été le développement de la logique classique et la formulation des mathématiques dans celle-ci. Il s'agit du formalisme, initié par Hilbert et défendu par Bourbaki. Par exemple, on peu lire dans [7], dans son mode d'emploi que "Le traité prend les mathématiques à leur début" et que "Le mode d'exposition suivi est axiomatique". D'ailleurs, Bourbaki s'autoproclame comme référence absolue : "Le texte étant consacré à l'exposé dogmatique d'une théorie[...]" (p VII).

Ce n'est cependant pas la seule réponse possible. Dans [22] il est présenté d'autres courant de pensées, à savoir :

1. l'intuitionnisme (aussi appelé constructivisme [4]) : ce mouvement est dû à Brouwer et Heyting. L'idée est que les objets mathématiques sont des créations mentales, immédiatement appréhendées par l'esprit du ou de la mathématicien.ne. Faire des mathématiques ne se résume pas en un jeu formel de manipulation de symboles. Aussi, en mathématique constructive, est considéré comme dénué de sens le fait de parler de la "véracité" ou de la "fausseté" d'une proposition indépendamment des connaissances que l'on possède son sujet ;
2. le constructivisme à la Bishop : il se place dans la continuité du constructivisme à la Brouwer. Il y a en réalité peu de considérations philosophiques. La volonté première est de donner à tout énoncé mathématique une signification "numérique" voir [5, p. ix] : "Notre programme est simple : donner, autant que faire se peut, une signification numérique à l'analyse classique" [5]. On présentera ce courant plus en détail dans la suite ;
3. les mathématiques constructives récursives : développées par Andreï Andreïevitch Markov dans les années 1950. Il s'agit d'un pan du constructivisme. Les objets mathématiques sont des algorithmes (représentés par des mots de longueur arbitraire mais finie, sur un alphabet fini). C'est à lui que l'on doit le principe qui porte son nom, à savoir le principe de Markov : s'il est impossible qu'un algorithme ne s'arrête pas, alors il doit s'arrêter ;

4. On choisira plutôt le terme "constructivisme" car le terme "intuitionnisme" a été employé par la partie adverse pour discréditer le mouvement (c.f. [3]).

5. Our program is simple : to give numerical meaning to as much as possible of classical abstract analysis.

4. le finitisme : seuls les éléments concrètement finiment représentables sont des objets de la théorie. Les notions abstraites d'ensembles, d'opérations, de constructions etc... ne sont pas admises. Kronecker, qui était fortement opposé à l'infini actuel, peut être présenté comme le précurseur du finitisme. Un exemple d'une telle théorie est l'arithmétique récursive primitive ;
5. le prédicativisme : une mention du prédicativisme a déjà été faite. On exige ici qu'aucun objet a ne soit défini en faisant référence à une collection A dont a est un élément. On évite ainsi les définitions circulaires. On reste cependant subordonné à la logique classique.

On peut noter qu'en plus de ces alternatives, des divergences ont aussi lieu dans les mathématiques classiques elles-mêmes. On rappelle par exemple, pour la théorie des ensembles, la théorie de Zermelo-Fraenkel, celle de von Neumann-Bernays et celle de Kelley-Morse. On peut aussi citer l'enjeu de l'axiome du choix.

Ainsi, dans cette partie, on va s'intéresser d'un peu plus près aux mathématiques constructives. On ne distinguera pas, sauf mention contraire explicite, un pan du constructivisme d'un autre.

Chapitre 10

Logique constructiviste

"Qui veut tuer son chien l'accuse de la rage"

Roger Apéry, au sujet des mathématicien.ne.s classiques [3].

Si l'on parle de constructivisme, c'est parce que la notion première et génératrice est la construction. A. Heyting énonce dans [20] que "La notion générale d'une construction possible doit être acceptée comme une notion primitive ; cependant pour une théorie particulière, des règles peuvent être données pour signifier quelles constructions y seront considérées comme possibles". On ne se limite donc pas uniquement à des constructions "réellement effectuées" ; on travaille aussi avec des constructions dont on admet qu'elles sont possibles, sans les donner explicitement.

Cette volonté de remettre la constructibilité au centre de la pratique mathématique vient d'un sentiment de perte de sens avec l'élaboration de nouveaux théorèmes mathématiques, qui affirment l'existence d'objets mathématiques sans pour autant pouvoir les exhiber.

Pour mieux comprendre, on considère l'exemple suivant (tiré de [22]).

Exemple 10.0.1. *Il existe deux nombres irrationnels a et b tels que a^b est rationnel*

Démonstration. Soit $a = \sqrt{2}$, on sait que $\sqrt{2}$ est irrationnel, si l'on suppose que $\sqrt{2}^{\sqrt{2}}$ est rationnel alors on a bien $a = b = \sqrt{2}$ irrationnels et $a^b = \sqrt{2}^{\sqrt{2}}$ est rationnel. Sinon, $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ est bien rationnel. □

Dans le paradigme classique, cette démonstration est licite et l'existence de a et de b est donc établie. Cependant, l'on se rend compte que l'on est, à la fin de cette démonstration, incapable de donner une construction de ces éléments. C'est ce qu'on appelle une démonstration d'existence sans témoin [1]. Il s'avère qu'une telle démonstration est possible

1. Le terme est emprunté à [12].

grâce au tiers exclu[2]. Or, si l'on veut ne pas accepter ce principe, c'est toute la logique qu'il faut revoir.

On introduit ici les symboles logiques $\vee$, $\wedge$, $\rightarrow$ et $\neg$ dont les significations sont établies par Brouwer.

Définition 10.0.1.

1. *prouver que l'on a $p \vee q$ signifie déterminer soit une preuve de p soit une preuve de q soit une preuve de p et de q ;*
2. *prouver que l'on a $p \wedge q$ signifie déterminer une preuve de p et une preuve de q ;*
3. *prouver $p \rightarrow q$ signifie déterminer une preuve qui transforme toute preuve de p en une preuve de q ainsi, la validité de p entraîne la validité de q ;*
4. *prouver $\neg p$ signifie que l'on a une preuve qui transforme toute preuve de p en une preuve de l'absurde (telle que $0 = 1$). En d'autres termes, $\neg p$ signifie qu'il est absurde d'avoir p.*

On peut déjà exhiber un théorème de LPC qui n'est plus vrai ici. Alors que dans LPC les propositions p et $\neg(\neg p)$ sont équivalentes, il n'en est pas de même dans la logique constructiviste. En effet, $\neg(\neg p)$ signifie qu'il est absurde que p soit absurde. Autrement dit, p est possible, mais cela ne procure pas une construction de p pour autant. On n'a donc plus $\neg(\neg p) \rightarrow p$ qui est bien un théorème de LPC.

10.1 Système formel constructiviste

On a déjà introduit les connecteurs de la logique constructive. On peut ensuite énoncer des axiomes et des règles d'inférence pour définir un système formel. Il est cependant important d'insister sur le fait que, alors que la logique formelle est fondamentale et fondatrice en logique classique, elle est seconde dans le constructivisme. Brouwer met donc en garde de ne pas tomber dans les travers du formalisme.

Définition 10.1.1. *Étant donnés les connecteurs logiques $\neg$, $\rightarrow$, $\wedge$ et $\vee$, si p et q sont des preuves alors les énoncés bien formulés sont de la forme*

1. $\neg p$;
2. $p \rightarrow q$;
3. $p \wedge q$;
4. $p \vee q$.

Contrairement à LPC où $\wedge$ et $\vee$ sont des abréviations définies grâce uniquement aux connecteurs $\neg$ et $\rightarrow$, on peut montrer que les quatre connecteurs constructifs sont eux indépendants, voir [25].

2. Notons que la nature du nombre $(\sqrt{2})^{\sqrt{2}}$ est maintenant bien connue en vertu du théorème de Gel'fond-Schneider.

Comme pour LPC, où plusieurs systèmes équivalents peuvent être définis, il existe plusieurs propositions de systèmes axiomatiques pour la logique constructive. On retiendra ici celui proposé par Heyting.

Définition 10.1.2. *Le système axiomatique de Heyting est constitué des axiomes suivants.*

A_1 $p \to (p \wedge p)$
A_2 $(p \wedge q) \to (q \wedge p)$
A_3 $(p \to q) \to ((p \wedge r) \to (q \wedge r))$
A_4 $((p \to q) \wedge (q \to r)) \to (p \to r)$
A_5 $q \to (p \to q)$
A_6 $(p \wedge (p \to q)) \to q$
A_7 $p \to (p \vee q)$
A_8 $(p \vee q) \to (q \vee p)$
A_9 $((p \to r) \wedge (q \to r)) \to ((p \vee q) \to r)$
A_{10} $\neg p \to (p \to q)$
A_{11} $((p \to q) \wedge (p \to \neg q)) \to \neg p$.

Avec enfin le modus ponens et la substitution comme règles d'inférence, on peut définir le système formel constructif.

On prend le temps ici de justifier le choix des axiomes. Celui-ci repose en effet sur le fait que les énoncés traduisent de grandes vérités intuitives.

A_1 $p \to (p \wedge p)$
Une preuve π de $p \to (p \wedge p)$ est une preuve qui transforme toute construction π_p de p en un preuve de $p \wedge p$. Or une preuve de $p \wedge p$ est la donnée d'une construction de p et de p : (π_p, π_p). On peut donc bien établir une preuve π qui transforme toute preuve π_p en une preuve $\pi(\pi_p) = (\pi_p, \pi_p)$ de $p \wedge p$. En d'autres mots, si l'on a une construction de p, alors on peut construire p et construire p ;

A_2 $(p \wedge q) \to (q \wedge p)$
Une preuve π de $(p \wedge q) \to (q \wedge p)$ est donc une construction $\pi_{q \wedge p}$ de $q \wedge p$ à partir d'une construction $\pi_{p \wedge q}$ de $p \wedge q$. Or $\pi_{p \wedge q} = (\pi_p, \pi_q)$ et donc il suffit de considérer que $\pi(\pi_{p \wedge q}) = \pi(\pi_p, \pi_q) = (\pi_q, \pi_p) = \pi_{q \wedge p}$. Autrement dit, si l'on possède une preuve de $p \wedge q$ cela signifie, par définition, que l'on a une construction de p et une construction de q. On peut donc donner (sans difficulté) une démonstration de q et une démonstration de p ;

A_3 $(p \to q) \to ((p \wedge r) \to (q \wedge r))$
Si l'on a une démonstration de $p \to q$: c'est à dire que de toute preuve de p on peut établir une preuve de q, alors si l'on a une preuve de $p \wedge r$, on a en particulier une preuve de p. Donc, on peut fournir une construction de q. Mais on a aussi une preuve de r, de sorte que l'on a une preuve de q et une preuve de r. Ainsi si l'on a $p \to q$ alors si on a $p \wedge r$ on a bien $q \wedge r$;

A_4 $((p \to q) \wedge (q \to r)) \to (p \to r)$
Soit $(\pi_{p\to q}, \pi_{q\to r})$ une preuve de $(p \to q) \wedge (q \to r)$. Dès lors, si l'on a une construction π_p de p, alors $\pi_{q\to r}(\pi_{p\to q}(\pi_p))$ est une construction de r.
Si $(p \to q)$ et $(q \to r)$ admettent des démonstrations, alors si l'on a p il suffit d'appliquer $(p \to q)$ pour obtenir une construction de q puis $(q \to r)$ pour obtenir une construction de r. Ainsi, partant d'une construction de p on obtient bien une construction de r ;

A_5 $q \to (p \to q)$
Soit π_p une preuve de p, alors $\pi_{q\to p} = \pi_p$ est une construction de q à partir de π_p.
Si l'on a une preuve de q, alors, quelle que soit la proposition considérée p il suffit d'appliquer la construction de q.

A_6 $(p \wedge (p \to q)) \to q$
Soit $(\pi_p, \pi_{p\to q})$ une preuve de $p \wedge (p \to q)$. On possède donc une construction de p et une construction de $p \to q$. Il suffit dès lors de considérer $\pi_{p\to q}(\pi_p)$ qui est bien une construction de q à partir de $(\pi_p, \pi_{p\to q})$.
Une preuve de $(p \wedge (p \to q)) \to q$ est une construction qui transforme toute preuve de $p \wedge (p \to q)$ en une preuve de q. Or une preuve de $p \wedge (p \to q)$ est la donnée d'une construction de p et de $p \to q$, où une preuve de $p \to q$ est une construction qui transforme toute preuve de p en une preuve de q. Aussi, si l'on possède une preuve de p et une preuve de $p \to q$ il suffit d'appliquer successivement les deux constructions pour obtenir une preuve de q.

A_7 $p \to (p \vee q)$
Si l'on possède une construction de p, alors on a bien une preuve de $p \vee q$. En effet, une construction de $p \vee q$ exige une construction de p, que l'on possède, ou une construction de q.

A_8 $(p \vee q) \to (q \vee p)$
Un preuve de $p \vee q$ est la donnée d'une construction de p ou d'une construction de q. Si l'on possède une construction de p (et donc une preuve de $p \vee q$), alors on est tout naturellement en mesure de fournir une preuve de $q \vee p$ car on possède une preuve de p. Il en est de même si l'on a une preuve de q.

A_9 $((p \to r) \wedge (q \to r)) \to ((p \vee q) \to r)$
Soit une preuve $\left(\pi_{(p\to r)}, \pi_{(q\to r)}\right)$ de $(p \to r) \wedge (q \to r)$. Cela signifie donc que l'on a une preuve de $p \to r$ et une preuve de $q \to r$, c'est à dire qu'on sait construire r à partir de p, et une preuve de $q \to r$, c'est à dire qu'on peut construire r à partir de q. Dès lors, si l'on a une preuve de $p \vee q$ c'est-à-dire une preuve de p ou une preuve de q, alors il suffit de considérer $\pi_{p\to r}(\pi_p)$ pour obtenir une construction de r à partir de la preuve de $p \vee q$.

A_{10} $\neg p \to (p \to q)$
Soit $\pi_{\neg p}$ une preuve de $\neg p$. C'est-à-dire que toute construction de p mène à une absurdité. Mais alors, de toute construction de p, on peut construire une preuve π_q de q puisqu'il n'y a pas de preuve de p.

A_{11} $((p \to q) \wedge (p \to \neg q)) \to \neg p$
Soit une preuve $\left(\pi_{p\to q}, \pi_{p\to\neg q}\right)$ de $(p \to q) \wedge (p \to \neg q)$. Cela signifie que l'on a une construction qui transforme toute preuve de p en une preuve de q, et une construction qui transforme toute preuve de p en une preuve de $\neg q$. Or, $\neg q$ signifie que toute construction de q mène à une absurdité. Donc de p on peut déduire une preuve de q et une impossibilité de q : $\left(\pi_{p\to q}(\pi_p), \pi_{p\to\neg q}(\pi_p)\right) = (p \wedge \neg p)$; ce qui est une absurdité.

Définition 10.1.3. *Le langage propositionnel constructif (qu'on notera IPC[3]) est le système formel constructif dont les symboles logiques sont définis en 10.0.1, les règles de syntaxe sont données par 10.1.1 et les axiomes sont ceux présentés en 10.1.2.*

Voici deux exemples pour illustrer IPC. Ces résultats seront utilisés dans le méta-théorème de déduction.

Théorème 10.1.4. *Si $IPC \vdash p$ et $IPC \vdash q$, alors $IPC \vdash p \wedge q$.*

Démonstration. On a

1. $IPC \vdash q$
2. $IPC \vdash q \to (p \to q)$
3. $IPC \vdash p \to q$
4. $IPC \vdash (p \to q) \to ((p \wedge p) \to (q \wedge p))$
5. $IPC \vdash (p \wedge p) \to (q \wedge p)$
6. $IPC \vdash p$
7. $IPC \vdash p \to (p \wedge p)$
8. $IPC \vdash p \wedge p$
9. $IPC \vdash q \wedge p$. □

Théorème 10.1.5. *Si p est un énoncé bien formulé, alors $IPC \vdash p \to p$.*

Remarquons que l'on démontre ici ce résultat à l'aide des axiomes et du modus ponens, mais qu'il est évident, puisque prouver $p \to p$ par exemple revient à trouver une preuve qui transforme toute preuve de p en une preuve de p. Il semblerait que ce soit sous la pression des mathématiciens classiques que ce type de preuve a été développé dans IPC.

Démonstration. En partant de A_3 et A_5 on a, par modus ponens

1. $IPC \vdash (p \to (p \to p)) \to ((p \wedge p) \to ((p \to p) \wedge p))$
2. $IPC \vdash p \to (p \to p)$
3. $IPC \vdash (p \wedge p) \to ((p \to p) \wedge p)$
   Or, en appliquant successivement le théorème 10.1.4 puis le modus ponens à A_1 et A_4 il vient

3. Intuitionistic Propositional Calculus, pour ne pas confondre avec LPC.

4. $IPC \vdash p \to (p \wedge p)$
5. $IPC \vdash \Big(\big[p \to (p \wedge p)\big] \wedge \big[(p \wedge p) \to ((p \to p) \wedge p)\big]\Big) \to \Big(p \to ((p \to p) \wedge p)\Big)$
6. $IPC \vdash p \to ((p \to p) \wedge p)$.
   Ensuite vu A_6 et A_4 en appliquant à nouveau successivement le théorème 10.1.5 et le modus ponens on a
7. $IPC \vdash (p \wedge (p \to p)) \to p$
8. $IPC \vdash \Big([p \to ((p \to p) \wedge p)] \wedge [p \wedge (p \to p)) \to p]\Big) \to \Big(p \to p\Big)$
9. $IPC \vdash p \to p$. □

Dans le même ordre d'idées, établissons un théorème de IPC, qui existait déjà en tant qu'axiome dans LPC.

Proposition 10.1.6. *La formule*

$$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$$

est un théorème de IPC.

Démonstration. Une preuve formelle peut être trouvée dans [16]. Utilisons plutôt la signification du connecteur $\to$. La formule est un théorème si on peut trouver une preuve qui transforme toute preuve de $p \to (q \to r)$ en une preuve de $(p \to q) \to (p \to r)$. On se donne donc une preuve π_1 de $p \to (q \to r)$ et une preuve π_2 de $(p \to q)$ et on essaie de transformer cette dernière en une preuve de $(p \to r)$. Partant d'une preuve de p, π_2 la transforme en une preuve de q et π_1 la transforme en une preuve de $(q \to r)$. De ces deux dernières preuves, on tire une preuve de r via l'axiome A_4. □

Dans IPC, on a aussi un métathéorème de la déduction. Il s'établit semblablement que dans LPC.

Définition 10.1.7. *Une formule q est déduite des formules $p_a,\ p_b, \ldots p_m$ si elle est un théorème de IPC, si elle est une des formules p_i ou si elle inférée par modus ponens de formules déduites de $p_a,\ p_b, \ldots p_m$. On note alors*

$$IPC + p_a + p_b + \cdots + p_m \vdash q$$

Théorème 10.1.8 (Méta-théorème de la déduction)**.** *Si quand on ajoute aux axiomes de IPC les formules $p_a,\ p_b,\ \ldots, p_m$ on établit, avec uniquement la règle du modus ponens, que q est un théorème, alors on a*

$$IPC \vdash p_a \to (p_b \to (\ldots (p_m \to q) \ldots)).$$

Démonstration. On montre d'abord que si on a

$$IPC + p_a + p_b + \cdots + p_l + p_m \vdash q$$

alors on a aussi

$$IPC + p_a + p_b + \cdots + p_l \vdash p_m \to q.$$

Le résultat général s'obtient alors sans difficulté en procédant de proche en proche.

D'abord, on montre que la propriété est vérifiée si q est un théorème de IPC ou une des formules parmi $p_a, \ldots p_m$. Ensuite, on prouve que si la propriété est vérifiée pour les formules q et $q \to r$ alors elle est vérifiée pour r.

1. D'abord, si q est un théorème de IPC alors, par la définition 10.1.7, q est déduit de $p_a,\ p_b,\ \ldots, p_l$. La formule $q \to (p_m \to q)$ est un théorème de IPC (obtenu par substitution évidente dans l'axiome **A5**). Donc par modus ponens, la formule $p_m \to q$ est également déduite de $p_a,\ p_b,\ \ldots, p_l$.

   Ensuite, si q est une des formules parmi $p_a, \ldots, p_m$, alors deux cas sont possibles :

   (a) si $q \equiv p_m$: comme $p_m \to p_m$ est un théorème de IPC par la proposition 10.1.5, on a
   $$IPC + p_a + p_b + \cdots + p_l \vdash p_m \to q\ ;$$

   (b) si q est une formule parmi $p_a, \ldots, p_l$: la formule $p_i \to (p_m \to p_i)$ est un théorème de IPC. On a donc, dans $IPC + p_a + p_b + \cdots + p_l$, les théorèmes p_i et $p_i \to (p_m \to p_i)$. En appliquant le modus ponens, on a donc bien $IPC + p_a + p_b + \cdots + p_l \vdash p_m \to q$. Formellement, on écrit

   $$\begin{aligned} IPC + p_a + p_b + \cdots + p_l &\vdash p_i \\ &\vdash p_i \to (p_m \to pi) \\ &\vdash p_m \to p_i. \end{aligned}$$

2. On suppose à présent que la propriété est vérifiée pour les formules déduites q et $q \to r$. Dès lors, $p_m \to q$ et $p_m \to (q \to r)$ sont déduits de $IPC + p_a + p_b + \cdots + p_l$. Comme la formule $\Big(p_m \to (q \to r)\Big) \to \Big((p_m \to q) \to (p_m \to r)\Big)$ est un théorème dans IPC, elle est déduite de $p_a, p_b, \ldots, p_l$. Il suffit alors d'appliquer le modus ponens :

   $$\begin{aligned} IPC + p_a + p_b + \cdots + p_l &\vdash p_m \to q \\ &\vdash p_m \to (q \to r) \\ &\vdash \Big(p_m \to (q \to r)\Big) \to \Big((p_m \to q) \to (p_m \to r)\Big) \\ &\vdash (p_m \to q) \to (p_m \to r) \\ &\vdash p_m \to r. \end{aligned}$$

La preuve est alors complète. □

Nous n'irons pas plus loin dans l'étude de la logique constructiviste. En effet, nous ne ferions que rejouer au même jeux que dans le premier chapitre. On peut d'ailleurs mentionner le fait que Gödel (en 1933) à réussi à faire coexister les deux logiques sous une même bannière : "traduction négative" [4]. Mais la raison est aussi idéologique. Comme déjà mentionné, l'intention première de Bishop et Brouwer était de s'éloigner d'un formalisme jugé déconnecté de l'intuition et de l'activité mathématique pour rester concentrer sur l'établissement de propriétés à la signification numérique indéniable.

4. [12, pp. 119-120]

Chapitre 11

Théorie des ensembles

"Alors que vous pensez en termes d'axiomes et de déductions, nous pensons en termes d'évidences"

A. Heyting [19]

Contrairement à la théorie Z-F, dans laquelle un ensemble est un objet de la théorie, et donc peut n'avoir qu'une existence idéale, un ensemble dans le paradigme constructif n'est considéré que si l'on donne (au moins implicitement) la construction de ses éléments et que l'on précise comment vérifier que deux éléments de cet ensemble sont égaux. Semblablement, pour définir une fonction d'un ensemble A à un ensemble B, il faut décrire la construction qui permet de passer d'un élément de A à un élément de B, et montrer que deux éléments de A qui sont égaux fournissent deux éléments égaux de B.

Tout comme pour les symboles $\neg$, $\wedge$, $\vee$ et $\rightarrow$, les significations de $\exists$ et $\forall$ doivent être rediscutées.

Pour Bishop [1], un énoncé universel, $\forall x[p(x)]$, a une signification semblable à l'interprétation classique : tout élément d'un ensemble A vérifie la propriété p. En d'autres termes, on signifie qu'on a une preuve qui transforme toute construction de x en une construction de $p(x)$. Heyting cependant insiste sur la nuance qu'il y a entre les deux interprétations. Si dans l'ensemble A on établit la proposition $\forall x p(x)$, on signifie que la propriété est vérifiée pour un x quelconque, et non pas que la propriété est vérifiée pour la totalité des éléments de A ([19, p. 179]).

Définition 11.0.1. *Dans un ensemble, on notera $\forall x[p(x)]$ pour signifier que quelque soit l'élément x de A, on peut vérifier que $p(x)$ est vrai.*

Comme déjà mentionné en 10.0.1, l'existence constructiviste est plus stricte, et donc bien distincte de l'existence classique.

Définition 11.0.2. *Asserter qu'il existe un élément qui vérifie une propriété p, $\exists x p(x)$, signifie que l'on peut construire un x et vérifier $p(x)$.*

1. [5, p. 8].

Définition 11.0.3. *Un ensemble A est défini quand (i) on décrit comment construire ses éléments à partir d'objets dont l'existence est antérieure à A, et quand (ii) il est expliqué ce que signifie être égaux pour deux éléments (quelconques) de A.*

Définition 11.0.4. *L'égalité $=$ dans un ensemble A est une relation d'équivalence. C'est à dire que pour tous éléments a, b et c de A, on vérifie que*

1. $a = a$;
2. *si* $(a = b)$ *alors* $(b = a)$;
3. *si* $(a = b)$ *et* $b = c$, *alors* $a = c$.

Exemple 11.0.1. *Si l'on considère que l'ensemble des naturels est donné, la définition classique des entiers convient au paradigme constructivisme. En effet, l'ensemble les entiers $\mathbb{Z}$ est l'ensemble des couples de naturels (a, b) et l'égalité est définie par*

$$(a, b) =_{\mathbb{Z}} (c, d) \leftrightarrow a + d =_{\mathbb{N}} b + c$$

En fait, les nombres naturels sont considérés par les constructivistes comme donnés a priori ; il n'y a donc pas lieu de proposer une construction de ceux-ci, ni même de donner un système axiomatique. Ainsi, Bishop dans ([5, p. 2]) écrit que : "Les entiers positifs et leur arithmétique sont présupposés par la nature même de notre intelligence." C'est aussi le parti pris par D. Bridges et F. Richman dans "Varieties of Constructive Mathematics" ([8, p. 6]), autre ouvrage de référence pour la construction des nombres réels.

Certain.ne.s cependant, se donnent la peine d'en donner une interprétation ; à l'aide de bâtons par exemple. C'est le cas de Heyting qui, dans ([19, p. 178]) explique que : " (...) dans la théorie des nombres naturels (concrétisés par des barres), | est constructible ; si n désigne un nombre constructible, $n|$ est considéré comme constructible."

On a donc à disposition l'ensemble des naturels, noté $\mathbb{N}$, et son arithmétique. On construit $\mathbb{Z}$ et $\mathbb{Q}$ de la même façon que dans le paradigme classique.

Définition 11.0.5. *L'ensemble des entiers, noté $\mathbb{Z}$ est l'ensemble des couples (a, b) où a et b sont des naturels et où deux éléments (a, b) et (c, d) sont égaux si $a + d = b + c$.*

Il en est de même pour les rationnels.

Définition 11.0.6. *L'ensemble des rationnels, noté $\mathbb{Q}$, est défini comme l'ensemble des couples d'entiers $\mathbb{Z} \times \mathbb{N}_0$ dont l'égalité est*

$$(a, b) = (c, d) \quad si\ ad = bc.$$

Pour un ensemble, on peut aussi définir une relation binaire symétrique et transitive mais non réflexive. On parle alors de relation d'inégalité [2]. On pourrait s'étonner de devoir spécifier la nature d'une inégalité et de ne pas se satisfaire d'une définition négative : $x \neq y$ si et seulement si $\neg(x = y)$. Cela tient de la nature de la négation. Aussi, Bishop préfère, autant que faire se peut, user de définitions positives qui ont, dit-il dans [5, p. 8], une valeur numérique plus significative.

2. Traduit littéralement de l'anglais "inequality" utilisé par [5] et [8].

Définition 11.0.7. *Une inégalité sur un ensemble A, notée $\neq$ est une relation binaire telle que*

(*i*) *si $a \neq b$ alors $b \neq a$;*

(*ii*) *il est impossible que $a \neq a$.*

Si l'inégalité vérifie aussi la condition

$$x \neq y \ \rightarrow \ \forall z\Big((x \neq z) \vee (y \neq z)\Big)$$

on dit que $\neq$ est une séparation [3].

Si en plus la séparation vérifie $x = y \leftrightarrow \neg(x \neq y)$, alors on dit que la séparation est stricte [4].

Étant donné un ensemble A, pour définir l'ensemble des parties de A il faut donc expliciter comment vérifier qu'un élément donné est un sous-ensemble de A et définir la notion d'égalité de deux sous-ensembles de A.

Définition 11.0.8. *Un sous-ensemble S de A est un ensemble dont les éléments sont déterminés par $(x \in A) \wedge P(x)$ où P est une propriété, et où deux éléments de S sont égaux s'ils sont égaux dans A. On notera alors $S = \{x \in A \mid P(x)\}$. De plus on notera $S \subseteq A$ pour signifier que S est un sous-ensemble de A.*

On notera qu'ici on suppose implicitement que si x vérifie P et si $x = y$ alors y vérifie P. En d'autres termes, l'on ne s'intéressera qu'aux propositions qui vérifient le principe d'extensionnalité.

Définition 11.0.9. *Si S et T sont deux sous-ensembles de A, on dit que $S = T$ si on a $S \subseteq T$ et $T \subseteq S$.*

On vérifie que l'égalité ainsi définie est bien une relation d'équivalence.

Proposition 11.0.10. *La relation $S = T$ définie par $(S \subseteq T) \wedge (T \subseteq S)$ est une relation d'équivalence.*

Démonstration.

1. $S = S$, en effet, $(S \subseteq S) \wedge (S \subseteq S)$ vu que tout élément de T est un élément de T ;
2. si $S = T$ alors $T = S$ c'est évident vu A_2 ;
3. si $S = T$ et $T = U$ alors $S = U$ vu le théorème 10.1.4 et A_8, on a

$$\Big(S \subseteq T \wedge T \subseteq U\Big) \wedge \Big(U \subseteq T \wedge T \subseteq S\Big).$$

Ainsi, vu A_4 on a bien $(S \subseteq U) \wedge (U \subseteq S)$. □

3. Traduit du mot "apartness" utilisé par [8].
4. Traduit du mot "tight" utilisé par [8].

Définition 11.0.11. *L'union de deux sous-ensembles S et T de A est l'ensemble donné par*

$$S \cup T \;=\; \{x \in A \mid (x \in S) \vee (x \in T)\},$$

l'égalité sur $S \cup T$ étant l'égalité de A.

Définition 11.0.12. *Soient deux sous-ensembles S et T d'un ensemble A. L'intersection de S et T est le sous-ensemble*

$$S \cap T \;=\; \{x \in A \mid (x \in S) \wedge (x \in T)\},$$

l'égalité sur $S \cap T$ étant l'égalité de A.

Définition 11.0.13. *Étant donnés des ensembles S_1, $S_2, \ldots,$ S_n, on définit l'ensemble produit cartésien $S_1 \times S_2 \times \cdots \times S_n$ comme l'ensemble des n-uples $(x_1, \ldots, x_n)$ tels que $x_i \in S_i$. pour tout i.*

L'égalité sur $S_1 \times S_2 \times \ldots \times S_n$ est alors défini par

$$(x_1, \ldots, x_n) \;=\; (y_1, \ldots, y_n) \text{ si } x_i = y_i \text{ pour tout } i.$$

Définition 11.0.14. *Une application f d'un ensemble A dans un ensemble B est un procédé*[5] *qui permet, à partir d'un élément a de A, de déterminer un élément b de B, noté $f(b)$, en un nombre fini d'étapes.*

5. Dans [8, p. 8], c'est le terme "algorithme" qui est utilisé. Mais à son tour, le terme "algorithme" renvoie à la notion primitive et intuitive de construction.

Chapitre 12

Construction de R

On procède de manière très semblable que dans le paradigme classique. D'abord on définit **R** comme étant l'ensemble des suites numériques régulières (des suites de Cauchy particulières) et on montre qu'il existe une injection ϕ de $\mathbb{Q}$ dans **R**. Ensuite, l'on dote **R** d'une structure additive (qui en fait un groupe) et multiplicative et l'on vérifie que ϕ préserve ces structures. On complète en montrant qu'avec les opérations définies **R** est un corps commutatif. Enfin, on présente quelque propriétés relatives à l'ordre. Les définitions présentées dans ce chapitre sont celles de [8]. La présentation a été adaptée et détaillée pour coïncider avec ce qui a été proposé dans la partie classique.

12.1 Définition des Réels Constructifs

La définitions des réels dans le paradigme constructiviste correspond peu ou prou à la définition qui préside à la construction de Cantor, à ceci près que l'on spécifie la vitesse à laquelle la différence des termes de la suite converge vers 0.de convergence vers 0.

Définition 12.1.1. *Une suite $(r_j)_j$ à valeurs dans $\mathbb{Q}$*[1] *est régulière si pour tous indices j, k dans $\mathbb{N}_0$, on a*

$$|\, r_j \; - \; r_k| \leq j^{-1} + \; k^{-1}.$$

Exemple 12.1.1. *Les suites constantes sont régulières. En effet, soit $q \in \mathbb{Q}$, la suite $(q)_j$ définie par $q_j = q$ est régulière car on*

$$|q_i - q_j| = |q - q| = 0 \leq i^{-1} + \; j^{-1}$$

On définit alors l'égalité entre deux suites numériques régulières.

Définition 12.1.2. *Si $(r_j)_j$ et $(s_j)_j$ sont deux suites numériques régulières, alors on dit que $(r_j)_j = (s_j)_j$ si pour tout naturel j, $|\, r_j - s_j \,| \leq 2/j$.*

1. On appellera ces suites des suites numériques.

Exemple 12.1.2. *Les suites* $(0)_j$ *et* $(\frac{1}{j})_j$ *sont égales. En effet, pour tout indice* j *on a*

$$|0 - \frac{1}{j}| = \frac{1}{j} \leq \frac{2}{j}$$

On vérifie évidement que la définition est licite. Le caractère symétrique et réflexif se fait sans difficulté. Pour déterminer la transitivité, il faut d'abord établir le lemme suivant.

Lemme 12.1.3. *Deux suites régulières* $(r_j)_j$ *et* $(s_j)_j$ *sont égales si et seulement si pour tout naturel* m *il existe un naturel* N *tel que pour tout indice* $j \geq N$ *on a*

$$| r_j - s_j | \leq m^{-1}.$$

Démonstration. D'abord, si l'on suppose que $(r_j)_j = (s_j)_j$ alors pour le naturel m considéré, $N = 2m$ convient :

$$j \geq 2m \Rightarrow | r_j - s_j | \leq \frac{2}{j} \leq \frac{1}{m}.$$

Réciproquement, si l'on suppose que pour tout naturel m il existe un naturel N tel que pour tout indice $j \geq N$ on a

$$| r_j - s_j | \leq m^{-1},$$

alors, pour $k \geq \max\{m, N\}$ on a

$$\begin{aligned} |r_j - s_j| &\leq |r_j - r_k| + |r_k - s_k| + |s_k - s_j| \\ &\leq j^{-1} + k^{-1} + m^{-1} + j^{-1} + k^{-1} \\ &< 2j^{-1} + 3k^{-1}. \end{aligned}$$

Comme l'inégalité est vérifiée pour tout k, on en déduit qu'on a bien

$$|r_j - s_j| \leq 2/j.$$ □

Le lemme exprime le fait que deux suites $(r_j)_j$ et $(s_j)_j$ régulières sont égales si et seulement si $| r_j - s_j |$ peut être rendu arbitrairement petit, pour tout j suffisamment grand.

Proposition 12.1.4. *La relation définie en 12.1.2 est une relation d'équivalence.*

Démonstration.

(*i*) réflexivité : on a $(r_j)_j = (r_j)_j$ car pour tout j on a $| r_j - r_j | = 0 \leq 2/j$;

(*ii*) symétrie : si $(r_j)_j = (s_j)_j$, alors par définition on a, pour tout naturel j,

$$| r_j - s_j | = | s_j - r_j | \leq 2/j,$$

et donc on a bien $(s_j)_j = (r_j)_j$;

(*iii*) transitivité : soient $(r_j)_j$, $(s_j)_j$ et $(t_j)_j$ trois suites numériques régulières telles que $(r_j)_j = (s_j)_j$ et $(s_j)_j = (t_j)_j$. Vu le lemme 12.1.3, on sait alors que pour tout $m \in \mathbb{N}$ il existe N_1 et N_2 tels que

$$\forall j \geq N_1,\ |\, r_j - s_j \,| \leq 1/2m$$

et

$$\forall j \geq N_2,\ |t_j - s_j \,| \leq 1/2m$$

ainsi, pour tout $m \in \mathbb{N}$ on a

$$\forall j \geq \max\{N_1, N_2\}\ |\, r_j - t_j| \leq |\, r_j - s_j \,| + |t_j - s_j \,| \leq 1/m.$$

On conclut alors grâce au lemme 12.1.3. □

On définit les réels comme étant l'ensemble des suites numériques régulières.

Définition 12.1.5. *L'ensemble des réels, noté* **R**, *est l'ensemble des suites numériques régulières, où l'égalité est définie en 12.1.2.*

On montre alors qu'il existe une injection de $\mathbb{Q}$ dans **R**. Sans surprise, elle est analogue au plongement défini dans le contexte de la construction de Cantor.

Proposition 12.1.6. *L'application ϕ définie par*

$$\phi \ :\ r \in \mathbb{Q} \mapsto (r)_j \in \mathbf{R}$$

est bien définie et injective.

Démonstration. L'application vérifie les exigences de la définition 11.0.14. En effet, pour un rationnel r quelconque on lui attribue la suite régulière $(r)_j$. On montre ensuite que si $\phi(r) = \phi(s)$ alors $r = s$. En effet, par définition 12.1.2 de l'égalité dans **R** on a

$$|(\phi(r))_j - (\phi(s))_j| = |r - s| \leq 2/j,$$

on conclut alors grâce au caractère archimédien de $\mathbb{Q}$. □

12.2 La structure additive sur R

Dans cette section, on commence par une définition de la somme sur **R** et on étudie ses propriétés.

Définition 12.2.1. *Soit $x \equiv (r_j)_j$ et $y \equiv (s_j)_j$ deux réels, on définit la somme sur* **R** *comme suit :*

$$x +_R y \ =\ (r_{2j} + s_{2j})_j$$

On vérifie ensuite que l'opération est licite ; c'est-à-dire que le résultat obtenu est un réel.

Proposition 12.2.2. *Si $x \equiv (r_j)_j$ et $y \equiv (r_j)_j$ sont deux réels alors $x +_R y$ est aussi un réel.*

Démonstration. Soit $x \equiv (r_j)_j$ et$y \equiv (s_j)_j$ deux réels, conformément à la définition 12.1.1 d'une suite régulière, tout revient à vérifier que pour tous indices i et j on a

$$|(r_{2i} + s_{2i}) \ - \ (r_{2j} + s_{2j})| \leq \ i^{-1} + j^{-1}.$$

Or, comme $(r_j)_j$ et $(s_j)_j$ sont deux suites régulières on a successivement

$$\begin{aligned} |(r_{2i} + s_{2i}) \ - \ (r_{2j} + s_{2j})| &\leq |r_{2i} + s_{2i} - r_{2j} + s_{2j}| \\ &\leq |r_{2i} - r_{2j}| + |s_{2i} - s_{2j}| \\ &\leq 2((2i)^{-1} + (2j)^{-1}) \\ &= \ i^{-1} + j^{-1}. \end{aligned}$$

□

Proposition 12.2.3. *La somme définie sur l'ensemble des suites numériques régulières est commutative, associative et admet un neutre.*

Démonstration.
Soient $x \equiv (r_j)_j$, $y \equiv (s_j)_j$ et $z \equiv (t_j)_j$ trois suites numériques régulières ;

(*i*) Commutativité : la commutativité de la somme s'établit sans difficulté par simple application des définitions. En effet, pour tout naturel j on a

$$(x +_R y)_j = (r_{2j} + s_{2j}) = (s_{2j} + r_{2j}) = (y +_R x)_j.$$

(*ii*) Associativité : en appliquant la définition de la somme, on a

$$\begin{aligned} ((x +_R y) +_R z)_j &= (x +_R y)_{2j} + t_{2j} \\ &= r_{4j} + s_{4j} + t_{2j} \end{aligned}$$

et

$$\begin{aligned} (x +_R (y +_R z))_j &= r_{2j} + (y +_R z)_{2j} \\ &= r_{2j} + s_{4j} + t_{4j}. \end{aligned}$$

Ainsi, conformément à la définition 12.1.2 de l'égalité dans **R**, on montre qu'on a

$$|((x +_R y) +_R z)_j - (x +_R (y +_R z))_j| \leq 2/j$$

En effet, vu les égalités établies au début de la preuve, et comme x, y et z sont des suites régulières, on a successivement

$$\begin{aligned} |((x +_R y) +_R z)_j - (x +_R (y +_R z))_j| &= |r_{4j} + s_{4j} + t_{2j} - r_{2j} - s_{4j} - t_{4j}| \\ &\leq |r_{4j} - r_{2j}| + |t_{2j} - t_{4j}| \\ &\leq \frac{1}{4j} + \frac{1}{2j} + \frac{1}{2j} + \frac{1}{4j} \\ &= \frac{3}{2j} < \frac{2}{j}. \end{aligned}$$

(*iii*) Existence d'un neutre : il suffit d'appliquer la définition à $\phi(0)$ pour se convaincre. Pour tout réel $x \equiv (r_j)_j$

$$x +_R \phi(0) = (r_{2j} + 0)_j.$$

□

Proposition 12.2.4. *Pour tout réel $x \equiv (r_j)_j$ on peut construire un réel $y \equiv (s_j)_j$ tel que*

$$x + y = 0.$$

Démonstration. On constate immédiatement que la définition

$$-((r_j)_j) = (-r_j)_j$$

convient. □

Pour finir cette section, on vérifie que l'application ϕ définie en 12.1.6 préserve la somme.

Proposition 12.2.5. *Pour tous rationnels r et s on a*

$$\phi(r) +_R \phi(s) = \phi(r + s).$$

Démonstration. On applique simultanément la définition de la somme et la définition 12.1.2 de l'égalité sur $\mathbb{R}$:

$$\begin{aligned} |[\phi(r) +_R \phi(s)]_j \ - \ [\phi(r+s)]_j| &= |r + s - (r + s)| \\ &= 0 \end{aligned}$$

□

12.3 L'anneau R

On définit ensuite le produit sur **R**. Pour ce faire, on établit d'abord le lemme suivant.

Proposition 12.3.1. *Si $x \equiv (r_j)_j$ est une suite numérique régulière, alors le plus petit entier positif plus grand que $|r_1| + 2$, est tel que pour tout élément r_j de la suite on a $|\, r_j \,| \leq K_x$.*

Démonstration. On a successivement

$$\begin{aligned} |\, r_j \,| &= |\, r_j \ - r_1 \ + \ r_1| \\ &\leq \ |\, r_j \ - r_1| \ + \ |r_1| \, . \end{aligned}$$

Or $(r_j)_j$ est une suite numérique régulière donc, par définition, $|\, r_j \ - r_1| \leq j^{-1} + 1$. Il en résulte donc

$$|\, r_j \,| \leq j^{-1} + 1 + |r_1| \leq |r_1| + 2.$$

□

Définition 12.3.2. *La borne canonique*[2] *d'une suite numérique régulière $(r_j)_j$ est le plus petit entier positif plus grand que $|r_1|+2$. On le note K_x.*

Proposition 12.3.3. *Si $x \equiv (r_j)_j$ et $y \equiv (r_j)_j$ sont deux réels, alors la suite définie par*

$$x \cdot_R y \;=\; (r_{2kj}\ s_{2kj})_j \quad \textit{avec} \quad k = \max\{K_x, K_y\}$$

est un réel.

Démonstration. Soient donc $x \equiv (r_j)_j$ et $y \equiv (r_j)_j$ deux suites régulières et $k = \max\{K_x, K_y\}$. On a successivement

$$\begin{aligned}
|(x \cdot_R y)_i - (x \cdot_R y)_j| &= |r_{2ki}s_{2ki} - r_{2kj}s_{2kj}| \\
&\leq |r_{2ki}s_{2ki} - r_{2ki}s_{2kj}| + |r_{2ki}s_{2kj} - r_{2kj}s_{2kj}| \\
&\leq |r_{2ki}||s_{2ki} - s_{2kj}| + |s_{2kj}||r_{2ki} - r_{2kqj}| \\
&\leq |r_{2ki}|((2ki)^{-1} + (2kj)^{-1}) + |s_{2kj}|((2ki)^{-1} + (2kj)^{-1}) \\
&= (2k)^{-1}(i^{-1} + j^{-1})(|r_{2ki}| + |s_{2kj}|) \\
&\leq i^{-1} + j^{-1}
\end{aligned}$$

où la dernière inégalité est justifiée par le fait que $k \geqslant |r_j|$ et $k \geqslant |s_j|$, pour tout j. □

L'injection ϕ définie en 12.1.6 préserve le produit.

Proposition 12.3.4. *Pour tous rationnels r et s on a*

$$\phi(r) \cdot_R \phi(s) = \phi(r.s).$$

Démonstration. Par définition de ϕ, les suites $\phi(r)$ et $\phi(s)$ sont constantes ; c'est-à-dire que pour tout indice j, on a

$$(\phi(r))_j = r \quad \text{et} \quad (\phi(s))_j = s.$$

Dès lors on vérifie sans peine que

$$\phi(r) \cdot_R \phi(s) - \phi(r.s) = 0$$ □

Proposition 12.3.5. *Le produit défini sur l'ensemble des suites numériques régulières est commutatif et associatif et le réel $1_R = \phi(1)$ est le neutre pour la multiplication.*

Démonstration.

- Commutativité du produit : la commutativité s'établit par simple application des définitions. En effet, si $x \equiv (r_j)_j$, $y \equiv (r_j)_j$ sont des réels, pour tout naturel j on a successivement

$$\begin{aligned}
(x \cdot_R y)_j &= r_{2kj}s_{2kj} \\
&= s_{2kj}r_{2kj} \\
&= (y \cdot_R x)_j
\end{aligned}$$

  où $k = \max\{K_x, K_y\}$.

2. Terme emprunté à [8].

- Associativité du produit : ici, on utilise le lemme 12.1.3 et les définitions. Soient $x \equiv (r_j)_j$, $y \equiv (r_j)_j$ et $z \equiv (t_j)_j$ des réels. Pour appliquer la définition, on pose $k_1 = \max\{K_{x \cdot_R y}, K_z\}$, $k_2 = \max\{K_x, K_y\}$, $k_3 = \max\{K_x, K_{y \cdot_R z}\}$ et enfin $k_4 = \max\{K_y, K_z\}$. Par définition, on a alors d'une part

$$((x \cdot_R y) \cdot_R z)_j = (x \cdot_R y)_{2k_1 j} t_{2k_1 j} = r_{4k_1k_2j} s_{4k_1k_2j} t_{2k_1 j},$$

et d'autre part

$$(x \cdot_R (y \cdot_R z))_j = r_{2k_3 j} (y \cdot_R z)_{2k_3 j} = r_{2k_3 j} s_{4k_3k_4j} t_{4k_3k_4j}.$$

Par le lemme 12.1.3, réels $((x \cdot_R y) \cdot_R z)$ et $(x \cdot_R (y \cdot_R z))$ sont égaux si et seulement si

$$|r_{4k_1k_2j} s_{4k_1k_2j} t_{2k_1 j} - r_{2k_3 j} s_{4k_3k_4j} t_{4k_3k_4j}|$$

peut être rendu arbitrairement petit, pour j suffisamment grand. Mais on a

$$\begin{aligned} |r_{4k_1k_2j} s_{4k_1k_2j} t_{2k_1 j} - r_{2k_3 j} s_{4k_3k_4j} t_{4k_3k_4j}| \leq\ & |r_{4k_1k_2j}||s_{4k_1k_2j}||t_{2k_1 j} - t_{4k_3k_4j}| \\ & + |r_{4k_1k_2j}||t_{4k_3k_4j}||s_{4k_1k_2j} - s_{4k_3k_4j}| \\ & + |s_{4k_3k_4j}||t_{4k_3k_4j}||r_{4k_1k_2j} - r_{2k_3 j}|. \end{aligned}$$

Vu les définitions de K_x, K_y et K_z, le membre de droite de cette inégalité est majoré par

$$K_x K_y (\frac{1}{2k_1 j} + \frac{1}{4k_3k_4j}) + K_x K_z (\frac{1}{4k_1k_2j} + \frac{1}{4k_3k_4j}) + K_y K_z (\frac{1}{4k_1k_2j} + \frac{1}{2k_3 j}).$$

À son tour, vu les définitions de $k_1, \ldots, k_4$, cette expression est majorée par

$$\frac{4}{4j} + \frac{K_x K_y}{2k_1 j} + \frac{K_y K_z}{2k_3 j}.$$

Cette expression est inférieure ou égale à m^{-1} dès que j est supérieur ou égal au plus petit entier J supérieur à

$$m(1 + \frac{K_x K_y}{2k_1} + \frac{K_y K_z}{2k_3}).$$

- Existence d'un neutre pour le produit : comme 1 est le neutre pour le produit dans $\mathbb{Q}$, on vérifie sans peine que $\phi(1)$ convient : pour tout réel $x \equiv (r_j)_j$ on a

$$(x \cdot_R \phi(1))_j = r_{2kj},$$

où $k = \max\{K_x, K_1\}$. Et donc, comme $(r_j)_j$ est une suite régulière on a bien

$$|(x \cdot_R \phi(1))_j - r_j| = |r_{2kj} - r_j| \leq \frac{1}{2kj} + \frac{1}{j} \leq \frac{2}{j}.$$ □

Enfin, on montre que le produit est distributif par rapport à la somme, ainsi $(\mathbf{R}, +_R, 0_R, \cdot_R, 1_R)$ est un anneau.

Proposition 12.3.6. *Le produit dans* **R** *distribue la somme.*

Démonstration. Soient $x \equiv (r_j)_j$, $y \equiv (r_j)_j$ et $z \equiv (t_j)_j$ des réels. Il s'agit de montrer qu'on a

$$(x +_R y) \cdot_R z = (x \cdot_R z) +_R (y \cdot_R z).$$

On définit $k_1 = \max\{K_{x+y}, K_z\}$, $k_2 = \max\{K_x, K_z\}$, et $k_3 = \max\{K_y, K_z\}$ et on calcule

$$((x +_R y) \cdot_R z)_j = (x +_R y)_{2k_1 j} t_{2k_1 j} = (r_{4k_1 j} + s_{4k_1 j}) t_{2k_1 j}.$$

D'autre part, on a

$$((x \cdot_R z) +_R (y \cdot_R z))_j = (x \cdot_R z)_{2j} + (y \cdot_R z)_{2j} = r_{4k_2 j} t_{4k_2 j} + s_{4k_3 j} t_{4k_3 j}.$$

Par le lemme 12.1.3, les réels $(x +_R y) \cdot_R z$ et $(x \cdot_R z) +_R (y \cdot_R z)$ sont donc égaux si l'expression

$$|r_{4k_1 j} t_{2k_1 j} + s_{4k_1 j} t_{2k_1 j} - r_{4k_2 j} t_{4k_2 j} - s_{4k_3 j} t_{4k_3 j}|$$

peut être rendue arbitrairement petite, pour j suffisamment grand. Mais on a

$$|r_{4k_1 j} t_{2k_1 j} + s_{4k_1 j} t_{2k_1 j} - r_{4k_2 j} t_{4k_2 j} - s_{4k_3 j} t_{4k_3 j}| \leq |r_{4k_1 j} t_{2k_1 j} - r_{4k_2 j} t_{4k_2 j}| + |s_{4k_1 j} t_{2k_1 j} - s_{4k_3 j} t_{4k_3 j}|.$$

La manipulation classique des valeurs absolues (dans $\mathbb{Q}$) montre que le membre de droite est majoré par

$$|r_{4k_1 j}||t_{2k_1 j} - t_{4k_2 j}| + |t_{4k_2 j}||r_{4k_1 j} - r_{4k_2 j}| + |s_{4k_1 j}||t_{2k_1 j} - t_{4k_3 j}| + |t_{4k_3 j}||s_{4k_1 j} - s_{4k_3 j}|.$$

Vu les définitions de K_x, K_y et K_z et par régularité des suites considérées, cette expression est majorée par

$$K_x(\frac{1}{2k_1 j} + \frac{1}{4k_2 j}) + K_z(\frac{1}{4k_1 j} + \frac{1}{4k_2 j}) + K_y(\frac{1}{2k_1 j} + \frac{1}{4k_3 j}) + K_z(\frac{1}{4k_1 j} + \frac{1}{4k_3 j}).$$

Vu les définitions de k_1, k_2, k_3, cette expression est majorée par

$$\frac{1}{j}(\frac{K_x + K_y}{2k_1} + \frac{6}{4}).$$

Cette expression est inférieure ou égale à m^{-1} dès que j est supérieur ou égal au plus petit entier J supérieur à

$$m(\frac{K_x + K_y}{2k_1} + \frac{6}{4}).$$

□

Pour pouvoir faire de **R** un corps, il faut encore expliquer comment obtenir un inverse pour un élément donné. Pour se faire, il faut définir sur $\mathbb{R}$ la notion d'ordre.

12.4 Inégalité et Ordre sur R

Pour définir l'inverse de tout nombre non nul, on passe ici par la définition de l'ordre sur **R**. Mentionnons le fait interpellant que ni [5] ni [8] ne donnent de définition de relation d'ordre.

Pour pouvoir construire sur **R** les relations d'inégalité et d'ordre, on définit d'abord les opérations suivantes.

Définition 12.4.1. *Soient $x \equiv (r_j)_j$ et $y \equiv (s_j)_j$ deux réels, alors*

- $\max_{\mathbf{R}}\{(r_j)_j, (s_j)_j\} = (\max\{r_j, s_j\})_j$;
- $\min_{\mathbf{R}}\{(r_j)_j\ , (s_j)_j\} = (\min\{r_j, s_j\})_j$;
- $|\,(r_j)_j\,|_{\mathbf{R}} = (|\,r_j\,|_j)$.

Comme pour la somme et le produit, on vérifie que les définitions sont licites.

Proposition 12.4.2. *Soient deux réels $x \equiv (r_j)_j$ et $y \equiv (r_j)_j$. Les suites* $\max\{x, y\}$ *et* $\min\{x, y\}$ *sont des suites régulières.*

Démonstration. Soient $x \equiv (r_j)_j$ et $y \equiv (s_j)_j$ deux réels. On montre d'abord que $\max\{x, y\}$ est une suite régulière, c'est à dire

$$|(\min\{r, s\})_i - (\min\{r, s\})_j| \leq i^{-1} + j^{-1}.$$

Pour chaque couple d'entiers naturels (i, j) quatre cas sont possibles.

1. Si $\max\{r_i, s_i\} = r_i$ et $\max\{r_j, s_j\} = r_j$, alors
$$|\max\{r_i, s_i\} - \max\{r_j, s_j\}| \leq i^{-1} + j^{-1}.$$
2. Il en est de même si $\max\{r_i, s_i\} = s_i$ et $\max\{r_j, s_j\} = s_j$.
3. Si maintenant on a $\max\{r_i, s_i\} = r_i$ et $\max\{r_j, s_j\} = s_j$, en particulier on a $s_i \leq r_i$ et $-s_j \leq -r_j$. Dès lors, on a d'une part
$$r_i - s_j \leq r_i - r_j \leq |r_i - r_j| \leq p^{-1} + q^{-1}$$
et d'autre part
$$r_i - s_j \geq s_i - s_j \geq -|s_i - s_j| \geq -(p^{-1} + q^{-1}).$$
Ainsi, on a
$$|r_i - s_j| \leq p^{-1} + q^{-1}.$$
4. Si on a $\max\{r_i, s_i\} = s_i$ et $\max\{r_j, s_j\} = r_j$, on procède comme au point précédent.

On applique le même raisonnement pour $\min\{r, s\}$. □

Proposition 12.4.3. *Si $x \equiv (r_j)_j$ est une suite régulière, alors la suite numérique $|x|$ définie par*

$$|x|_j = |\, r_j \,|$$

est une suite régulière.

Démonstration. Pour montrer que $|x|$ est une suite régulière, il faut montrer, conformément à la définition 12.1.1 que pour tous indices i et j on a

$$\Big||r_i| - |\, r_j \,|\Big| \leq i^{-1} + j^{-1}.$$

En d'autres termes, tout revient à montrer que l'on a $||a|-|b|| \leq |a-b|$, pour tous rationnels a et b. Cette propriété est en fait très classique. D'une part, comme $a = a - b + b$ on a

$$|a| \leq |a - b| + |b|$$

et donc

$$|a| - |b| \leq |a - b|.$$

D'autre part, en échangeant le rôle de a et de b on obtient

$$|b| - |a| \leq |a - b|.$$

Ainsi, $||a| - |b|| \leq |a - b|$.

Dès lors, si r_j est une suite régulière, on a

$$||r|_i - |r|_j| = ||r_i| - |r_j|| \leq |r_i - r_j| \leq i^{-1} + j^{-1}.$$ □

Proposition 12.4.4. *Si $x \equiv (r_j)_j$ est une suite numérique régulière, alors on a*

$$|x| = \max\{x, -x\}.$$

Démonstration. Une fois encore, il suffit d'écrire les définitions pour s'en convaincre. D'une part, vu la définition de la valeur absolue (voir 12.4.3) on a

$$|x|_j = |\, r_j \,|$$

et d'autre part, vu la définition de $\max_{\mathbf{R}}$ (voir 12.4.3) et de l'opposé (voir 12.2.4) on a

$$(\max_{\mathbf{R}}\{x, -x\})_j = \max(r_j, -r_j).$$

Donc, pour tout indice j on a trivialement

$$||x|_j - (\max_{\mathbf{R}}\{x, -x\})_j| = 0 \leq 2/j.$$

□

Proposition 12.4.5. *Soit $(r_j)_j$ une suite régulière, les propositions suivantes sont équivalentes.*

1. *Il existe un indice N tel que $r_N > 1/N$;*
2. *Il existe un rationnel ϵ et un indice J tels que $r_j > \epsilon$ pour tout $j > J$.*

Démonstration.

- 1. $\to$ 2. : l'idée est de montrer que comme la suite est régulière, il existe un indice J à partir duquel tous les termes suivants sont suffisamment proches de r_N et donc plus grands que ϵ.
  Soient[3] $J \in \mathbb{N}$ et $\epsilon > 0$ tels que

$$r_N > \frac{1}{J} + \frac{1}{N} + \epsilon > \frac{1}{J} + \frac{1}{N} > \frac{1}{N},$$

  en particulier, on a

$$\frac{1}{N} < r_N - \frac{1}{J} - \epsilon$$

  Dès lors, comme $(r_j)_j$ est une suite régulière, pour tout indice $j > J$ on a

$$|r_j - r_N| \leq \frac{1}{j} + \frac{1}{N} < \frac{1}{J} + \frac{1}{N} + \epsilon < r_N.$$

  On distingue deux cas :
  (a) si $r_j \geq r_N$ on a immédiatement que $r_j > \epsilon$;
  (b) et si $r_j < r_N$, alors

$$|r_j - r_N| = r_N - r_j < \frac{1}{N} + \frac{1}{J} < r_N - \frac{1}{J} - \epsilon + \frac{1}{J}$$

  et donc

$$r_N - r_j < r_N - \epsilon$$

  c'est à dire, on a pour tout indice $j > J$

$$r_j > \epsilon.$$

- 2. $\to$ 1. :
  La réciproque est directe. S'il existe $\epsilon > 0$ et si il existe un indice J tels que pour tout indice $j > J$ on a $r_j > \epsilon$, alors pour $j > J$ tel que $\frac{1}{j} < \epsilon$. Évidemment, un tel j est constructible. En effet, comme $\epsilon \in \mathbb{Q}$, ϵ est de la forme p/q avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}$. mais alors, on a $0 < \frac{1}{q+1} < \frac{p}{q}$ et donc, pour $j \geq \max\{J, q\}$, $r_j > \epsilon > \frac{1}{j}$.

□

3. Comme on travaille dans $\mathbb{Q}$, un tel J et un tel ϵ sont constructibles. donc

Définition 12.4.6. *On dit qu'un réel $x \equiv (r_j)_j$ est positif s'il existe un indice j tel que $r_j > 1/j$. On note alors $x > 0$.*

Définition 12.4.7. *Si x et y sont deux réels, alors on écrit $x < y$ pour dire que $y - x$ est positif.*

On a alors les propositions suivantes.

Lemme 12.4.8. *Soient deux réels x et y :*

1. *si $x > 0$ et $y > 0$, alors $x + y > 0$;*
2. *$\max\{x, y\} > 0$ si et seulement si $x > 0$ ou $y > 0$;*
3. *si $x + y > 0$, alors $x > 0$ ou $y > 0$.*

Démonstration.

1. Soient deux réels $x \equiv (r_j)_j$ et $y \equiv (s_j)_j$ tels que $x > 0$ et $y > 0$, alors vu la proposition 12.4.5 on sait que pour chacun des réels x et y respectivement il existe un rationnel ϵ_x et ϵ_y et un indice N_x et N_y , tels que $r_j > \epsilon_x$ pour tous $j > N_x$ et $s_j > \epsilon_y$ pour tout $j > N_y$. On pose alors $\epsilon = \min\{\epsilon_x, \epsilon_y\}$ et $N = \max\{N_x, N_y\}$. Ainsi, pour tout naturel $j > N$, on a
$$(x +_R y)_j = r_{2j} + s_{2j} > 2\epsilon.$$
Ainsi, $x + y > 0$.
2. On montre d'abord que si $\max\{x, y\} > 0$ alors $x > 0$ ou $y > 0$ puis après si $x > 0$ ou $y > 0$ alors $\max\{x, y\} > 0$.
   (a) Par définition, si $\max\{x, y\} > 0$ alors cela signifie qu'il existe un indice J tel que
   $$(\max\{x, y\})_J = \max\{r_J, s_J\} > \frac{1}{J}$$
   Donc, on a soit$r_J > \frac{1}{J}$ soit $s_J > \frac{1}{J}$. Ainsi, on a soit $x > 0$ soit $y > 0$.

   (b) La réciproque est évidente. Si l'on a $x > 0$ ou $y > 0$, cela signifie que l'on a effectivement soit $x > 0$ soit $y > 0$ ou les deux. On peut supposer, sans perdre de généralité, que $x > 0$. Par définition, on sait donc qu'il existe une indice J tel que $r_J > \frac{1}{J}$. Dès lors, on a
   $$(\max\{x, y\})_J = \max\{r_J, s_J\} > r_J > \frac{1}{J}$$
   et donc $\max\{x, y\} > 0$.
3. si $x + y > 0$, par définition on a qu'il existe indice J tel que
$$(x + y)_J = r_{2J} + s_{2J} > \frac{1}{J}$$

Or, vu le point précédent, il suffit de montrer que l'on a $\max\{x, y\} > 0$ pour conclure. En fait, il suffit d'observer que l'on a

$$2(\max\{x, y\})_{2J} \geq r_{2J} + s_{2J} > \frac{1}{J}.$$

On a donc bien un indice J tel que $(\max\{x, y\})_{2J} > \frac{1}{2J}$.

□

Proposition 12.4.9. *Si x et y sont deux réels, alors la relation $\sim$ définie par*

$$x \sim y \quad si \quad |x - y| > 0$$

est une relation d'inégalité.

Démonstration. Soient $x \equiv (r_j)_j$ et $y \equiv (s_j)_j$ deux réels, conformément à la définition 11.0.7, on vérifie la symétrie et l'anti-réflexivité de $\sim$.

— si $x \sim y$ alors on a $|x - y| = |y - x| > 0$ et donc on a bien $x \sim y$;
— on a $\neg(x \sim x)$. En effet, si $(x \sim x)$ alors il existe un indice N tel que $(|x-x|)_N > 1/N$. On en déduit alors

$$(|x - x|)_N = \max\{r_{2N} - r_{2N},\ -r_{2N} + r_{2N}\} = 0 > 1/N$$

ce qui est absurde.

□

Ainsi, on a une inégalité sur **R**.

Définition 12.4.10. *On définit sur* **R** *la relation d'inégalité par*

$$x \neq y \quad si \quad |x - y| > 0$$

Proposition 12.4.11. *L'inégalité définie sur* **R** *est une séparation.*

Démonstration. Pour rappel, une inégalité $\neq$ est une séparation quand on vérifie que si deux réels x, y sont tels que $x \neq y$ alors pour tout réel z on a soit $z \neq x$ soit $z \neq y$. Soient donc x et y deux réels tels que $x \neq y$. Alors, par définition 12.4.10 d'une inégalité, on a $x - y > 0$ ou $y - x > 0$. Si l'on suppose que $x - y > 0$, alors, pour tout réel z on a

$$(x + z) + (z - y) > 0$$

et donc, vu le point (iii) du lemme 12.4.8, on a $x - z > 0$ ou $z - y > 0$. □

Définition 12.4.12. *Un réel x est négatif si $-x$ est positif.*
Un réel $x \equiv (r_j)_j$ est non-négatif si, pour tout indice j, on a $r_j > -1/j$.

Exemple 12.4.1. *Le réel* 0 *est non-négatif.*

Définition 12.4.13. *Si x et y sont deux réels, alors on écrit $x \leq y$ pour signifier $y - x$ est non-négatif.*

Proposition 12.4.14. *Soient x et y des réels, la relation $x \leq y$ est une relation d'ordre.*

Démonstration. il faut montrer que la relation est réflexive, antisymétrique et transitive.
Soient donc $x \equiv (r_j)_j$, $y \equiv (s_j)_j$ et $z \equiv (t_j)_j$ trois réels.

(*i*) Réflexivité : on a déjà montré que $x \leq x$ en 12.4.1 ;

(*ii*) Anti-symétrie : on suppose que l'on a $x \leq y$ et $y \leq x$, alors, vu la définition 12.4.13 de $\leq$ on a simultanément

$$s_{2j} - r_{2j} > -1/j$$

et

$$r_{2j} - s_{2j} > -1/j,$$

de sorte que

$$|r_{2j} - s_{2j}| < 1/j$$

Mais alors, pour tout j on a

$$\begin{aligned} |\, r_j - s_j \,| &\leq |\, r_j - r_{2j}| + |r_{2j} - s_{2j}| + |s_{2j} - s_j \,| \\ &\leq \frac{1}{j} + \frac{1}{2j} + \frac{1}{j} + \frac{1}{2j} + \frac{1}{j} \\ &\leq \frac{4}{j}. \end{aligned}$$

Ainsi, pour tout naturel m on peut déterminer un indice N à partir duquel on vérifie

$$|\, r_j - s_j \,| \leq \frac{1}{m}.$$

Grâce au lemme 12.1.3, on en déduit que $x = y$.

(*iii*) Transitivité : si $x \leq y$ et $y \leq z$, on a, par définition

$$\begin{aligned} (z - x)_j &= (t_{2j} - s_{2j}) + (s_{2j} - r_{2j}) \\ &> -1/j. \end{aligned}$$

□

Définition 12.4.15. *Soit r un réel, on dit que r est non nul si $r \neq 0$.*

On est maintenant en mesure de définir l'inverse pour un réel non nul.

Définition 12.4.16. *Pour tout réel $x \equiv (r_j)_j$ non nul on définit le réel $y \equiv (s_j)_j$ comme suit : soit un naturel J tel que pour tout indice $j \geq J$ on a $|\, r_j \,| \geq J^{-1}$, on pose*

$$s_j = \begin{cases} \frac{1}{r_{J^3}} & \text{si } j < J \text{ et} \\ \\ \frac{1}{r_{jJ^2}} & \text{si } j \geq J. \end{cases}$$

On montre que la définition a bien un sens.

Proposition 12.4.17. *L'élément défini en 12.4.16 est un réel et vérifie* $x \cdot_R y = 1$.

Démonstration. Par construction, on a $|\, s_j \,| \leq J$, pour tout j. Soient m et n deux naturels, on pose

$$j = \max\{m, J\} \quad \text{et} \quad k = \max\{n, J\}.$$

Ainsi, on a

$$\begin{aligned} |s_m - s_n| &= |s_m||s_n||r_{jJ^2} - r_{kJ^2}| \\ &\leq J^2\Big((jJ^2)^{-1} + (kJ^2)^{-1}\Big) \\ &= j^{-1} + k^{-1} \\ &\leq m^{-1} + n^{-1}. \end{aligned}$$

La suite $(r_j)_j$ est donc bien régulière.

On montre à présent que $x \cdot_R y = 1$, c'est à dire (vu le lemme 12.1.3), que pour tout $m \in \mathbb{N}_0$, il existe N tel que pour tout indice $j \geq N$ on a

$$|(x \cdot_R y)_j - 1| \leq \frac{1}{m}.$$

Or, pour $j \geq J$ vu la définition 12.3.3 du produit, pour $k = \max\{K_x, K_y\}$ on a successivement

$$\begin{aligned} |(r \cdot_R s)_j - 1| &= |r_{2kj}s_{2kj} - 1| \\ &= |r_{2jkJ^2}|^{-1}|r_{2jk} - r_{2jkJ^2}| \\ &\leq |s_{2jk}|\Big((2jk)^{-1} + (2jkJ^2)^{-1}\Big) \leq \frac{1}{j}K_y\Big(\frac{1}{2k} + \frac{1}{2kJ^2}\Big) \leq \frac{1}{m} \end{aligned}$$

pour j supérieur au plus petit entier supérieur à la fois à J et à $mK_y\Big(\frac{1}{2k} + \frac{1}{2kJ^2}\Big)$. □

Cinquième partie

Appendice

Annexe A

Logique propositionnelle Classique

A.1 Axiomes de Łukasiewicz

A1 : $(\varphi \to \chi) \to \Big((\chi \to \psi) \to (\varphi \to \psi)\Big)$;
A2 : $\varphi \to (\neg\varphi \to \chi)$;
A3 : $(\neg\varphi \to \varphi) \to \varphi$;

A.2 Axiomes de Frege

1. $\varphi \to (\psi \to \varphi)$;
2. $\Big(\varphi \to (\psi \to \chi)\Big) \to \Big((\varphi \to \psi) \to (\varphi \to \chi) \Big)$;
3. $\Big(\varphi \to (\psi \to \chi)\Big) \to \Big(\psi \to (\varphi \to \chi)\Big)$;
4. $\Big(\varphi \to \psi\Big) \to \Big(\neg\psi \to \neg\varphi\Big)$;
5. $\neg\neg\varphi \to \varphi$;
6. $\varphi \to \neg\neg\varphi$;

Annexe B

Théorie des Ensembles

B.1 Axiome de la Logique des Prédicats

En plus des axiomes de LPC on a $\forall x[F(x)] \rightarrow F[y]$

B.2 Axiomes de la Théorie des Ensembles de Zermelo-Fraenkel

1. Axiome de l'ensemble vide : $\exists x \forall z[z \notin x]$;
2. Axiome d'extensionnalité : $\forall x \forall y\Big[\forall z[z \in x \leftrightarrow z \in y] \rightarrow x = y\Big]$;
3. Axiome de l'union : $\forall x \exists y \forall z\Big[z \in y \leftrightarrow \exists t[t \in x \wedge z \in t]\Big]$;
4. Axiome de compréhention : $\forall x \exists y \forall z\Big[z \in y \leftrightarrow (z \in x \wedge F(z))\Big]$;
5. Axiome de la puissance : $\forall x \exists y \forall z[z \in y \leftrightarrow z \subseteq x]$;
6. Axiome de la fondation : $(\forall x \neq \emptyset)(\exists y \in x)[x \cap y = \emptyset]$

Bibliographie

[1] URL : https://www.e-periodica.ch/digbib/view?pid=ens-001:1918:20::322#322.

[2] URL : http://bbi-math.narod.ru/newmann/newmann.html.

[3] Roger APÉRY. « Mathématique constructive ». In : *Penser les mathématiques : séminaire de philosophie et mathématiques de l'École normale supérieure (J. Dieudonné, M. Loi, R. Thom)*. Points. Sciences 29. Éditions du Seuil, 1982, pages 58-72. URL : https://hal.archives-ouvertes.fr/hal-01522168.

[4] Jean-Pierre BELNA. *La notion de nombre chez Dedekind, Cantor, Frege : théories, conceptions et philosophie*. fre. Mathesis. Paris : J. Vrin, 1996. ISBN : 2-7116-1292-9.

[5] Errett BISHOP. *Foundations of constructive analysis*. eng. McGraw-Hill series in higher mathematics. New York : McGraw-Hill book company, 1967.

[6] Laurence BOUQUIAUX. *Logique formelle et argumentation*. fre. 1er édition. L'atelier philosophique. Louvain-la-Neuve : De Boeck Supérieur, 2010. ISBN : 9782804104061.

[7] Nicolas BOURBAKI. *Théorie des ensembles*. fre ;eng. 1st ed. 2006. Eléments de mathématique. Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. ISBN : 1-281-08665-7.

[8] Douglas S. BRIDGES. *Varieties of constructive mathematics*. eng. London Mathematical Society lecture note series ; 97. Cambridge ; Cambridge University Press, 1987. ISBN : 0-521-31802-5.

[9] Georg CANTOR. *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts : [mit erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor-Dedekind]*. ger. Hildesheim : Georg Olms, 1962.

[10] Gérard CHAZAL. *Eléments de logique formelle*. fre. Paris : Hermès, 1996. ISBN : 2866015487.

[11] Richard DEDEKIND. *La création des nombres*. fre. Mathésis. Paris : Vrin, 2008. ISBN : 9782711621460.

[12] Gilles DOWEK. *Les métamorphoses du calcul : une étonnante histoire des mathématiques*. fre. Paris : Ed. du Pommier, 2007. ISBN : 9782746503243.

[13] Heinz-Dieter EBBINGHAUS. *Les nombres : leur histoire, leur place et leur rôle de l'Antiquité aux recherches actuelles*. fre. Paris : Vuibert, 1998 - 1999. ISBN : 2711789012.

[14] Herbert B. Enderton. *Elements of set theory*. eng. New York : Academic Press, 1977. ISBN : 0-12-238440-7.

[15] Gottlob Frege. *Les fondements de l'arithmétique : recherche logico-mathématique sur le concept de nombre*. fre. L'ordre philosophique. Paris : Seuil, 1969. ISBN : 9782020027366.

[16] Anne Gouders. *Regards croisés sur la logique intuitioniste propositionnelle*. fre. S.l, 2007.

[17] Georges Hansoul. *Algèbre II*. Notes de cours Uliège.

[18] Georges Hansoul. *Logique mathematique et theorie des ensembles*. Notes de cours Uliège.

[19] Arend Heyting. *Intuitionism : an introduction*. eng. Studies in logic and the foundations of mathematics, 41. Amsterdam : North-Holland, 1971. ISBN : 0720422396.

[20] Arend Heyting. « Remarques sur le constructivisme ». In : *Logique et Analyse* 3.11/12 (1960), p. 177-182. ISSN : 00245836, 22955836. URL : http://www.jstor.org/stable/44093273.

[21] David Hilbert. *Principles of mathematical logic*. eng. New York : Chelsea, 1950.

[22] Georg Kreisel. « Constructivism in mathematics : an introduction ». In : *Bulletin of the London mathematical society*. 22.5 (1999). ISSN : 0024-6093.

[23] Jan Łukasiewicz. *Elements of mathematical logic*. A Pergamon Press Book. Translated from Polish by Olgierd Wojtasiewicz. The Macmillan Company, New York, 1964, p. xi+124.

[24] Jan Łukasiewicz. « The shortest axiom of the implicational calculus of propositions ». In : *Proc. Roy. Irish Acad. Sect. A* 52 (1948), p. 25-33.

[25] McKinsey. « Proof of the independence of the primitive symbols of Heyting's calculus of propositions ». eng. In : *The Journal of symbolic logic* 4.4 (1939), p. 155-158. ISSN : 0022-4812.

[26] Samuel Nicolay. *Analyse Mathématique. Fonctions définies sur une partie de la droite réelle*. fre. ellipses, 2018.

[27] Samuel Nicolay. *Les nombres*. fre. Hermann, 2015.

[28] Petr Sergeevič Novikov. *Introduction à la logique mathématique*. fre. Collection universitaire de mathématiques, 14. Paris : Dunod, 1964.

[29] Jean-François Pabion. *Logique mathématique*. fre. Collection Méthodes. Paris : Hermann, 1976. ISBN : 2705658300.

[30] Daniel Ponasse. *Logique mathématique*. fre. Orgeval : O.C.D.L. Office Central de Librairie, 1972.

[31] Fulvia Skof, éd. *Giuseppe Peano between Mathematics and Logic*. eng. 1st ed. 2011. Milano : Springer Milan, 2011. ISBN : 88-470-1836-6.

[32] Alfred North Whitehead. *Principia mathematica*. eng. II. T. 1. Cambridge : Cambridge University Press, 1927. isbn : 9780521067911.