Introduction à la logique

4 septembre 2018

1 Introduction

Qu'est-ce qu'une preuve mathématique ? Si l'on se donne des axiomes de base, que peut-on prouver à l'aide de ces axiomes ? Peut-on trouver un ensemble d'axiomes qui permettent de prouver tous les théorèmes des mathématiques ? Il est naturel de commencer par la sous-question : Peut-on trouver un ensemble d'axiomes qui permettent de prouver tous les théorèmes de l'arithmétique. Ceci nous amène à d'autres questions de base. Qu'est-ce qu'un énoncé mathématique ?

Avant de se mettre à définir ce qu'est un énoncé mathématique, et par là, on veut dire un énoncé qui a un contenu mathématique, on peut s'intéresser à la pure déduction logique : on se donne des énoncés (ou propositions) qui peuvent être, soit justes, soit faux, et on s'intéresse à établir cette véracité ou fausseté à partir de règles de base. Dans le langage courant, nos énoncés sont des phrases. À partir d'énoncés de base, on peut consruire des énoncés plus complexes en utilisant les opérations $\wedge$ (ET), $\vee$ (OU) et $\sim$ (NON), aussi noté $\neg$ dans d'autres références. À partir de ces opérations de base, on pourra définir d'autres opérations comme l'implication, $\rightarrow$ (IMPLIQUE), et l'équivalence, $\leftrightarrow$ (ÉQUIVALENT). Cette partie de la logique s'appelle le *calcul propositionnel*.

On traitera le calcul propositionnel de deux façons. D'un côté on pourra utiliser des tables de vérité pour vérifier si un énoncé est une *tautologie*, c'est-à-dire qu'il est toujours vrai, quelles que soient les valeurs de vérité que l'on donne aux variables propositionnelles. C'est le point de vue *sémantique*. De l'autre côté, on se donnera une infinité d'axiomes de base qui seront des tautologies, et on s'intéressera à l'ensemble des formules que l'on pourra déduire de ces axiomes en utilisant la règle du *modus ponens* : ces formules seront appelées *théorèmes* du système formel. C'est le point de vue

syntaxique. On montrera que les deux points de vue se rejoignent, et que les tautologies sont exactement les théorèmes du système formel.

Tout cela plafonne très vite si on ne met pas de contenu mathématique dans ces propositions. Faisons le parallèle entre une proposition et une phrase. La phrase a un sens lorsqu'elle est écrite dans un langage. Dans un langage, on a des mots de base et des règles pour les agencer de manière à faire des phrases. On voudra, de même, définir un *langage mathématique*, dont les phrases seront appelées *formules bien formées* (abbréviation formules bf), parce que conformes à la grammaire du langage. Les éléments de base seront des constantes et des variables et on pourra les combiner en utilisant des symboles de fonctions et de relations, aussi appelées *prédicats*. On verra qu'une fonction est un cas particulier de prédicat et on parlera donc de *calcul des prédicats*. On pourra également utiliser les quantificateurs : le quantificateur universel $\forall$ (POUR TOUT), et le quantificateur existentiel $\exists$ (IL EXISTE). On parle de *logique du premier ordre* quand les quantificateurs ne peuvent être appliqués qu'aux variables et pas aux prédicats. Les grands résultats de la logique concernent la logique du premier ordre.

Comme précédemment, on traitera le calcul des prédicats de deux points de vue. Dans le point de vue sémantique, on interprétera les symboles du langages dans des modèles ou interprétations, et on s'intéressera aux formules qui seront vraies dans toute interprétation.

Du point de vue syntaxique, on voudra définir la notion de preuve dans ce langage. Pour cela on se donnera des axiomes de base qui comprennent les axiomes de base du langage propositionnelle et deux règles de déduction : le modus ponens et la *généralisation*. Les formules seront divisées en deux groupes : celles qui contiennent des *variables libres*, comme $\ll$ x=2 $\gg$, et celles dont toutes les variables sont précédées d'un quantificateur (ou *variables liées*), comme $\ll \forall x(x = 0 \vee x = 1) \gg$. Dans le deuxième cas, il est naturel de se demander si la formule est vraie ou fausse, et ceci dépendra de l'interprétation que l'on fera de la formule. Une formule bf dont toutes les variables sont liées est un théorème du langage si elle peut être obtenue à partir des axiomes de base et des règles de déduction du langage. On fera le lien entre les formules qui sont vérifiées dans nos modèles et les théorèmes de notre langage. Le théorème d'adéquation nous dira que ce sont les mêmes à condition de regarder **tous** les modèles du langage.

On construira ensuite des théories du premier ordre en ajoutant de nouveaux axiomes qui ne seront vrais que dans certains contextes. Ainsi, $(\forall x)(\forall y)((x = y) \rightarrow (x = y))$ est un axiome logique, alors que $(\forall x)(\forall y)(x \cdot$

$y = y \cdot x$) est vrai dans $\mathbb{N}$, mais pas dans l'ensemble des matrices $n \times n$ à coefficients réels. On pourra le prendre comme axiome de la théorie de l'arithmétique.

On étudiera quelques théories du premier ordre. Un prédicat très important sera l'égalité, pour lequel on introduit des axiomes. Les exemples de théorie du premier ordre que nous considérerons seront toutes des théories avec égalité : la théorie des groupes, l'arithmétique de Peano, la théorie des ensembles.

On terminera en énonçant et expliquant le théorème d'incomplétude de Gödel qui affirme qu'il est impossible de trouver un système complet d'axiomes pour la théorie de l'arithmétique et on expliquera brièvement l'idée de la preuve.

2 Calcul propositionnel informel

Dans ce contexte, on considère des *propositions* que l'on notera $A, B, C, \ldots$. Par exemple, la proposition A pourrait être la proposition $1 + 1 = 2$. Une proposition donnée est vraie V (T dans le livre) ou fausse F. Lorsqu'on veut mentionner une proposition arbitraire, on utilisera les lettres $p, q, r, \ldots$, de la même manière qu'on utilise par exemple la lettre x pour désigner une variable qui peut prendre comme valeur un nombre quelconque. Les lettres $p, q, r, \ldots$ sont appelées *variables propositionnelles*. Ces variables peuvent prendre deux valeurs $\{V, F\}$ appelées *valeurs de vérité*.

À partir de propositions, on peut construire de nouvelles propositions en itérant les règles de construction suivantes :

- La *négation* d'une proposition A est la proposition $\sim A$. Elle est vraie si et seulement si A est fausse.
- La *conjonction* de deux propositions A et B est la proposition $A \wedge B$ (on lit « A et B »). Elle est vraie si et seulement si A et B sont simultanément vraies.
- La *disjonction* de deux propositions A et B est la proposition $A \vee B$ (on lit « A ou B »). Elle est vraie si et seulement si au moins une des propositions A et B est vraie.
- Si A et B sont deux propositions, on construit la proposition $A \to B$ (on lit « A implique B », ou encore « si A, alors B »). Elle est vraie dès que B est vraie ou A est fausse.
- Si A et B sont deux propositions, on construit la proposition $A \leftrightarrow B$ (on lit « A équivalent à B »). Elle est vraie si et seulement si A et B sont simultanément vraies et simultanément fausses.

Ces nouvelles propositions sont des *propositions composées*. En appliquant de manière itérative ces règles à des variables propositionnelles, on construira des *formules propositionnelles*. On les notera $\mathcal{A}, \mathcal{B}, \mathcal{C}$, etc.

2.1 Fonctions de vérité et tables de vérité

On peut associer une *fonction de vérité* à une formule construite à partir des règles précédentes. Ces fonctions de vérité seront notées respectivement $f^{\sim}$, $f^{\wedge}$, $f^{\vee}$, $f^{\rightarrow}$, $f^{\leftrightarrow}$. La première fonction $f^{\sim}$est une fonction d'une variable, alors que les autres sont des fonctions de deux variables. Les variables ne peuvent prendre que les deux valeurs V et F. Donc, on donne les valeurs de la fonction dans une table, appelée *table de vérité*.

Table de vérité de $f^{\sim}$.

p	$\sim$p
V	F
F	V

Tables de vérité de $f^{\wedge}$, $f^{\vee}$, $f^{\rightarrow}$, $f^{\leftrightarrow}$.

p	q	p $\wedge$ q
V	V	V
V	F	F
F	V	F
F	F	F

p	q	p $\vee$ q
V	V	V
V	F	V
F	V	V
F	F	F

p	q	p $\rightarrow$ q
V	V	V
V	F	F
F	V	V
F	F	V

p	q	p $\leftrightarrow$ q
V	V	V
V	F	F
F	V	F
F	F	V

DÉFINITION 2.1 *1. Une formule propositionnelle est une* tautologie *si sa fonction de vérité ne prend que la valeur* V.

2. *Une formule propositionnelle est une* contradiction *si sa fonction de vérité ne prend que la valeur* F.

DÉFINITION 2.2 *1. Si $\mathcal{A}$ et $\mathcal{B}$ sont deux formules propositionnelles, on dit que $\mathcal{A}$* implique logiquement *$\mathcal{B}$ si $(\mathcal{A} \rightarrow \mathcal{B})$ est une* tautologie.

2. *Si $\mathcal{A}$ et $\mathcal{B}$ sont deux formules propositionnelles, on dit que $\mathcal{A}$* est logiquement équivalent à *$\mathcal{B}$ si $(\mathcal{A} \leftrightarrow \mathcal{B})$ est une* tautologie.

2.2 Règles de manipulation et de substitution

Elles sont résumées dans le théorème suivant.

THÉORÈME 2.3 *1. Si $\mathcal{A}$ et $\mathcal{A} \rightarrow \mathcal{B}$ sont des tautologies, alors $\mathcal{B}$ est une tautologie.*

2. *Soit $\mathcal{A}$ est une formule propositionnelle dans laquelle des variables propositionnelles $p_1, \ldots, p_n$ apparaissent et soient $\mathcal{A}_1, \ldots, \mathcal{A}_n$ des formules propositionnelles. Si $\mathcal{A}$ est une tautologie, alors la formule propositionnelle $\mathcal{B}$ obtenue de $\mathcal{A}$ en remplaçant chaque occurrence de p_i par $\mathcal{A}_i$ est aussi une tautologie.*
3. *Pour toutes formules propositionnelles $\mathcal{A}$ et $\mathcal{B}$, $(\sim(\mathcal{A} \wedge \mathcal{B}))$ est logiquement équivalent à $((\sim \mathcal{A}) \vee (\sim \mathcal{B}))$, et $(\sim (\mathcal{A} \vee \mathcal{B}))$ est logiquement équivalent à $(\sim(\mathcal{A}) \wedge (\sim\mathcal{B}))$.*
4. *Si $\mathcal{B}_1$ est une formule propositionnelle obtenue de la formule propositionnelle $\mathcal{A}_1$ en substituant la formule propositionnelle $\mathcal{B}$ à quelques occurrences de $\mathcal{A}$ dans $\mathcal{A}_1$ et si $\mathcal{B}$ est logiquement équivalent à $\mathcal{A}$, alors $\mathcal{B}_1$ est logiquement équivalent à $\mathcal{A}_1$.*
5. *Soit $\mathcal{A}$ une formule propositionnelle ne contenant que les connecteurs $\sim$, $\wedge$ et $\vee$ (on dit que $\mathcal{A}$ est* restreinte*). Soit $\mathcal{A}^*$ la formule propositionnelle obtenue de $\mathcal{A}$ en échangeant $\wedge$ et $\vee$ et en changeant chaque variable propositionnelle par sa négation. Alors, $\mathcal{A}^*$ est logiquement équivalente à $\sim\mathcal{A}$.*
6. *Soient $\mathcal{A}_1, \ldots, \mathcal{A}_n$ des formules propositionnelles. Alors, $(\bigvee_{i=1}^{n}(\sim \mathcal{A}_i))$ est logiquement équivalente à $(\sim(\bigwedge_{i=1}^{n} \mathcal{A}_i))$. Aussi, $(\bigwedge_{i=1}^{n}(\sim\mathcal{A}_i))$ est logiquement équivalente à $(\sim(\bigvee_{i=1}^{n} \mathcal{A}_i))$.*

2.3 Formes normales

DÉFINITION 2.4 *Une formule propositionnelle ne contenant que les connecteurs $\sim$, $\wedge$ et $\vee$ est appelée* formule propositionnelle restreinte.

THÉORÈME 2.5 *Toute fonction de vérité définie sur un ensemble de n variables propositionnelles $p_1, \ldots, p_n$ est la fonction de vérité $f : \{V, F\}^n \to \{V, F\}$ d'une formule propositionnelle.*

THÉORÈME 2.6 *Toute formule propositionnelle contenant des variables propositionnelles $p_1, \ldots, p_n$ et qui n'est pas une contradiction est logiquement équivalente à une formule propositionnelle de la forme $(\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n} Q_{ij}))$, où chaque Q_{ij} est, soit p_j, soit $\sim p_j$. Cette forme est appelée* forme normale disjonctive.

COROLLAIRE 2.7 *Toute formule propositionnelle contenant des variables propositionnelles $p_1, \ldots, p_n$ et qui n'est pas une tautologie est logiquement équivalente à une formule propositionnelle de la forme $(\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n} Q_{ij}))$, où chaque Q_{ij} est, soit p_j, soit $\sim p_j$. Cette forme est appelée* forme normale conjonctive.

Les formes normales disjonctives ou conjonctives sont très utiles en informatique lorsqu'on veut construire des algorithmes de vérification. Mais, si la formule est grosse, la ramener à une forme normale devient vite fastidieux pour un ordinateur.

2.4 Ensembles adéquats de connecteurs

DÉFINITION 2.8 *Un* ensemble adéquat de connecteurs *est un ensemble de connecteurs tel que toute fonction de vérité peut être représentée comme la fonction de vérité d'une formule propositionnelle ne contenant que des connecteurs de cet ensemble.*

DÉFINITION 2.9 *1. Le connecteur* NOR*, noté « $\downarrow$ », a pour table de vérité :*

p	q	$p \downarrow q$
V	V	F
V	F	F
F	V	F
F	F	V

Il est tel que $(p \downarrow q)$ *est logiquement équivalent à* $(\sim(p \vee q))$.

2. Le connecteur NAND*, noté « $\mid$ », a pour table de vérité :*

p	q	$p \mid q$
V	V	F
V	F	V
F	V	V
F	F	V

Il est tel que $(p \mid q)$ *est logiquement équivalent à* $(\sim(p \wedge q))$.

THÉORÈME 2.10 *Les ensembles suivants de connecteurs sont adéquats :*

1. $\{\sim, \wedge\}$,
2. $\{\sim, \vee\}$,
3. $\{\sim, \rightarrow\}$,
4. $\{\downarrow\}$,
5. $\{\mid\}$.

2.5 Règles de déduction

EXEMPLE 2.11 *Voici une règle de déduction de base :*

$$(p \rightarrow q), p; \quad \therefore \quad q$$

On peut l'interpréter ainsi : Si $(p \to q)$ *prend la valeur* V *et si* p *prend la valeur* V*, alors* q *prend la valeur* V*.*

On généralise l'exemple précédent dans la définition.

DÉFINITION 2.12 *La* règle de déduction

$$\mathcal{A}_1, \ldots \mathcal{A}_n; \quad \therefore \quad \mathcal{A}$$

est invalide *s'il est possible d'assigner des valeurs de vérité aux variables propositionnelles de telle sorte que* $\mathcal{A}_1, \ldots \mathcal{A}_n$ *prennent la valeur* V *et* $\mathcal{A}$*, la valeur* F*. Dans le cas contraire, la règle de déduction est dite* valide*.*

THÉORÈME 2.13 *La règle de déduction*

$$\mathcal{A}_1, \ldots \mathcal{A}_n; \quad \therefore \quad \mathcal{A}$$

est valide si et seulement si la formule propositionnelle

$$((\mathcal{A}_1 \wedge \cdots \wedge \mathcal{A}_n) \to \mathcal{A})$$

est une tautologie.

3 La formalisation du calcul propositionnel

Nous formalisons maintenant le contexte précédent pour introduire la notion de *système formel*, défini comme la réunion d'un alphabet de symboles, d'un ensemble de formules bien formées (formules bf), d'axiomes et de règles de déduction. On s'intéresse aux formules que l'on pourra déduire des axiomes, qui seront les théorèmes du système formel.

DÉFINITION 3.1 *Un* système formel L *du calcul propositionnel est défini comme :*

1. *Un alphabet infini de symboles :*

$$\sim, \to, (,), p_1, p_2, p_3, \ldots$$

2. *Un ensemble de formules bien formées (formules bf) défini inductivement comme suit :*

   (i) Pour tout i, p_i *est une formule bf ;*

   (ii) Si $\mathcal{A}$ *et* $\mathcal{B}$ *sont des formules bf, alors* $(\sim \mathcal{A})$ *et* $(\mathcal{A} \to \mathcal{B})$ *sont des formules bf.*

(iii) Toute formule bf est obtenue en appliquant les règles (i) et (ii) un nombre fini de fois.

3. *Un ensemble infini d'axiomes obtenu à partir des 3 schémas suivants : pour toutes formules bf $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$, les formules bf suivantes sont des axiomes :*

   (L1) $(\mathcal{A} \to (\mathcal{B} \to \mathcal{A}))$ *;*

   (L2) $((\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})))$

   (L3) $(((\sim\mathcal{A}) \to (\sim\mathcal{B})) \to (\mathcal{B} \to \mathcal{A}))$

4. *Une règle de déduction, le* modus ponens*, qui dit que $\mathcal{B}$ est une conséquence directe de $\mathcal{A}$ et $(\mathcal{A} \to \mathcal{B})$.*

DÉFINITION 3.2 *Une* preuve *dans* L *est une suite finie de formules bf, $\mathcal{A}_1, \ldots, \mathcal{A}_n$, telles que, pour tout $i \in \{1, \ldots, n\}$, soit $\mathcal{A}_i$ est un axiome de* L*, soit $\mathcal{A}_i$ se déduit de deux éléments précédents, $\mathcal{A}_j$ et $\mathcal{A}_k$, $j, k < i$, par utilisation du modus ponens. On dira que cette suite représente une* preuve de $\mathcal{A}_n$ dans L*, et on dira que $\mathcal{A}_n$ est un* théorème *de* L.

Plus généralement on peut s'intéresser dans L aux déductions d'un ensemble Γ de formules bf qui ne sont pas nécessairement des théorèmes de L.

DÉFINITION 3.3 *Soit Γ un ensemble de formules bf de* L*. Une suite finie de formules bf, $\mathcal{A}_1, \ldots, \mathcal{A}_n$, est une* déduction de Γ *si pour tout $i \in \{1, \ldots, n\}$ on a une des situations suivantes :*

(a) $\mathcal{A}_i$ est un axiome de L *;*

(b) $\mathcal{A}_i$ est dans Γ ;

(c) $\mathcal{A}_i$ se déduit de deux éléments précédents, $\mathcal{A}_j$ et $\mathcal{A}_k$, $j, k < i$, par utilisation du modus ponens.

On dit que $\mathcal{A}_n$ se déduit de Γ dans L*, ou encore que $\mathcal{A}_n$ est une* conséquence de Γ dans L*. On écrira* $\Gamma \underset{L}{\vdash} \mathcal{A}_n$.

REMARQUE 3.4 *Si $\mathcal{A}$ est un théorème de* L*, alors* $\emptyset \underset{L}{\vdash} \mathcal{A}$.

Le théorème de déduction suivant permet de simplifier la preuve de théorèmes dans L :

THÉORÈME 3.5 *(Théorème de déduction) Soit Γ un ensemble de formules bf de* L *possiblement vide, et $\mathcal{A}$ et $\mathcal{B}$ deux formules bf de* L*. Si* $\Gamma \cup \{\mathcal{A}\} \underset{L}{\vdash} \mathcal{B}$*, alors* $\Gamma \underset{L}{\vdash} (\mathcal{A} \to \mathcal{B})$.

La réciproque est aussi vraie :

PROPOSITION 3.6 *Si* $\Gamma \underset{\mathrm{L}}{\vdash} (\mathcal{A} \to \mathcal{B})$, *alors* $\Gamma \cup \{\mathcal{A}\} \underset{\mathrm{L}}{\vdash} \mathcal{B}$.

Le théorème de déduction a pour conséquence l'important corollaire suivant :

COROLLAIRE 3.7 *Soient* $\mathcal{A}$, $\mathcal{B}$ *et* $\mathcal{C}$ *des formules bf de* L. *Alors,*

$$\{(\mathcal{A} \to \mathcal{B}), (\mathcal{B} \to \mathcal{C})\} \underset{\mathrm{L}}{\vdash} (\mathcal{A} \to \mathcal{C}).$$

Nous terminons par un résultat technique qui sera utile plus tard.

PROPOSITION 3.8 *Pour toutes formules bf,* $\mathcal{A}$ *et* $\mathcal{B}$, *de* L, *les formules suivantes sont des théorèmes de* L *:*

(a) $(\sim\mathcal{B} \to (\mathcal{B} \to \mathcal{A}))$,

(b) $((\sim\mathcal{A} \to \mathcal{A}) \to \mathcal{A})$.

3.1 Le théorème d'adéquation

Dans le meilleur des mondes, les théorèmes de L devraient être exactement les tautologies. Le théorème d'adéquation montre que c'est bien le cas. Pour cela il faut pouvoir assigner des valeurs de vérité aux formules bf de L.

DÉFINITION 3.9 *Une* valuation *de* L *est une fonction* ν *dont le domaine est l'ensemble des formules bf de* L *et l'image est l'ensemble* $\{\mathsf{V}, \mathsf{F}\}$ *et qui satisfait, pour toutes formules bf* $\mathcal{A}$ *et* $\mathcal{B}$ *de* L, *aux deux conditions :*

(i) $\nu(\mathcal{A}) \neq \nu(\sim\mathcal{A})$ *;*

(ii) $\nu(\mathcal{A} \to \mathcal{B}) = \mathsf{F}$ *si et seulement si* $\nu(\mathcal{A}) = \mathsf{V}$ *et* $\nu(\mathcal{B}) = \mathsf{F}$.

DÉFINITION 3.10 *Une formule bf* $\mathcal{A}$ *de* L *est une* tautologie *si pour toute valuation* ν *de* L, $\nu(\mathcal{A}) = \mathsf{V}$.

THÉORÈME 3.11 *(Théorème de sûreté (Soundness Theorem)) Tout théorème de* L *est une tautologie.*

Soit $\mathcal{A}$ un théorème de L. La preuve se fait par induction sur la longueur n de la suite de formules qui constitue une preuve de $\mathcal{A}$.
Cas $n = 1$**.** La formule est un axiome. On vérifie par les tables de vérité et le théorème 2.3, 2. des notes que tout axiome est une tautologie.
Étape d'induction. On suppose que la preuve de $\mathcal{A}$ est de longueur n et que le théorème est prouvé pour toute formule dont la preuve est de longueur inférieure à n. Si $\mathcal{A}$ est un axiome, on a fini. Sinon, $\mathcal{A}$ s'obtient par modus ponens de deux formules $\mathcal{B}$ et $\mathcal{B} \to \mathcal{A}$, dont la preuve est de longueur inférieure à n et qui sont donc des tautologies. On a déjà montré au théorème 2.3, 1. que si $\mathcal{B}$ et $\mathcal{B} \to \mathcal{A}$ sont des tautologies, alors $\mathcal{A}$ est une tautologie. □

La réciproque nous demandera d'introduire de nouveaux outils : il faudra ajouter de nouveaux axiomes à L de manière cohérente jusqu'à obtenir une extension complète de L.

DÉFINITION 3.12 *Une* extension *de* L *est un système formel* L^* *dans lequel on a altéré les axiomes et/ou on en a ajouté de nouveaux, de telle sorte que tous les théorèmes de* L *demeurent des théorèmes de* L^* *(et* L^* *contient possiblement de nouveaux théorèmes).*

DÉFINITION 3.13 *Une extension* L^* *de* L *est* cohérente *(ou* consistante*) si pour toute formule bf* $\mathcal{A}$ *de* L*,* $\mathcal{A}$ *et* $\sim\mathcal{A}$ *ne sont pas simultanément des théorèmes de* L^**.*

PROPOSITION 3.14 L *est cohérent.*

PREUVE Supposons le contraire : il existe une formule bf $\mathcal{A}$ telle que $\underset{L}{\vdash} \mathcal{A}$ et $\underset{L}{\vdash} (\sim\mathcal{A})$ Par le thórème de sûreté, $\mathcal{A}$ et $(\sim\mathcal{A})$ sont des tautologies. Ceci est impossible car si $\mathcal{A}$ est une tautologie, alors $(\sim \mathcal{A})$ est une contradiction et si $(\sim \mathcal{A})$ est une tautologie, alors $\mathcal{A}$ est une contradiction. Donc L est cohérent. □

PROPOSITION 3.15 *Une extension* L^* *de* L *est cohérente si et seulement si il existe une formule bf* $\mathcal{A}$ *qui n'est pas un théorème de* L^**.*

PREUVE Si L^* est cohérente alors, pour toute formule $\mathcal{A}$, soit $\mathcal{A}$, soit $(\sim\mathcal{A})$ n'est pas un théorème.

Réciproquement, supposons que L^* n'est pas cohérente, et montrons que toute formule bf $\mathcal{A}$ de L est un théorème de L^*. On sait qu'il existe une

formule $\mathcal{B}$ telle que $\underset{L^*}{\vdash} \mathcal{B}$ et $\underset{L^*}{\vdash} (\sim\mathcal{B})$. Par la proposition 3.8(a) des notes on a

$$\underset{L}{\vdash} (\sim\mathcal{B} \to (\mathcal{B} \to \mathcal{A})).$$

Comme L^* est une extension de L, $\underset{L^*}{\vdash} (\sim\mathcal{B} \to (\mathcal{B} \to \mathcal{A}))$. Par modus ponens deux fois, on tire $\underset{L^*}{\vdash} (\mathcal{B} \to \mathcal{A})$ et, finalement, $\underset{L^*}{\vdash} A$. □

PROPOSITION 3.16 *Soit* L^* *une extension cohérente de* L, *et* $\mathcal{A}$ *une formule bf de* L *qui n'est pas un théorème de* L^*. *Alors l'extension* L^{**}*de* L *obtenue en ajoutant à* L^* *l'axiome* $(\sim\mathcal{A})$ *est cohérente.*

PREUVE Soit $\mathcal{A}$ une formule bf de L qui n'est pas un théorème de L^*. Supposons que L^{**} est incohérente. Par la preuve de la proposition 3.15 des notes, on sait que $\underset{L^{**}}{\vdash} \mathcal{A}$. Mais, L^{**} diffère de L^* par le seul axiome supplémentaire $(\sim\mathcal{A})$. Donc, $(\sim\mathcal{A}) \underset{L^*}{\vdash} \mathcal{A}$. Par le théorème de déduction, on en conclut que $\underset{L^*}{\vdash} (\sim\mathcal{A} \to \mathcal{A})$. On a aussi par la proposition 3.8 (b)

$$\underset{L}{\vdash} (((\sim\mathcal{A}) \to \mathcal{A}) \to \mathcal{A}),$$

et donc, $\underset{L^*}{\vdash} (((\sim\mathcal{A}) \to \mathcal{A}) \to \mathcal{A})$. Par modus ponens, on tire $\underset{L^*}{\vdash} \mathcal{A}$ et on contredit le fait que $\mathcal{A}$ n'est pas un théorème de L^*. Donc, L^{**} est cohérente. □

DÉFINITION 3.17 *Une extension* L^* *de* L *est* complète *si pour toute formule bf* $\mathcal{A}$ *de* L, $\mathcal{A}$ *ou* $\sim\mathcal{A}$ *est un théorème de* L^*.

THÉORÈME 3.18 *Soit* L^* *une extension cohérente de* L. *Alors, il existe une extension cohérente et complète de* L^*.

Ce théorème a une preuve un peu longue que l'on présentera plus tard.

PROPOSITION 3.19 *Soit* L^* *une extension cohérente de* L. *Alors, il existe une valuation* v *qui prend la valeur* V *sur chaque théorème de* L^*.

PREUVE On considère une extension, J, cohérente et complète de L. Soit $\mathcal{A}$ une formule bf de L. On pose $v(\mathcal{A}) = V$ si $\mathcal{A}$ est un théorème de J, et $v(\mathcal{A}) = F$ sinon.

Commençons par montrer que v est une valuation.

(i) Comme exactement une des formules $\mathcal{A}$ et $\sim\mathcal{A}$ est un théorème de J, on a bien $\nu(\mathcal{A}) \neq \nu(\sim\mathcal{A})$.

(ii) On doit aussi montrer que $\nu(\mathcal{A} \to \mathcal{B}) = \mathsf{F}$ si et seulement si $\nu(\mathcal{A}) = \mathsf{V}$ et $\nu(\mathcal{B}) = \mathsf{F}$. Soient $\mathcal{A}$ et $\mathcal{B}$ tels que $\nu(\mathcal{A}) = \mathsf{V}$ et $\nu(\mathcal{B}) = \mathsf{F}$, et supposons que $\nu(\mathcal{A} \to \mathcal{B}) = \mathsf{V}$. Alors, $\underset{\mathsf{J}}{\vdash} \mathcal{A}$ et $\underset{\mathsf{J}}{\vdash} (\mathcal{A} \to \mathcal{B})$. Donc, par modus ponens, $\underset{\mathsf{J}}{\vdash} \mathcal{B}$. Contradiction.

Réciproquement supposons que $\nu(\mathcal{A} \to \mathcal{B}) = \mathsf{F}$ et que, soit $\nu(\mathcal{A}) = \mathsf{F}$ ou $\nu(\mathcal{B}) = \mathsf{V}$. Puisque J est complète, alors $\underset{\mathsf{J}}{\vdash} (\sim(\mathcal{A} \to \mathcal{B}))$ et $\underset{\mathsf{J}}{\vdash} (\sim\mathcal{A})$ ou $\underset{\mathsf{J}}{\vdash} \mathcal{B}$.

— Si $\underset{\mathsf{J}}{\vdash} (\sim\mathcal{A})$, on a aussi par (L1)

$$\underset{\mathsf{J}}{\vdash} (\sim\mathcal{A} \to (\sim\mathcal{B} \to \sim\mathcal{A})).$$

Alors, par modus ponens, on a $\underset{\mathsf{J}}{\vdash} (\sim\mathcal{B} \to \sim\mathcal{A})$. En utilisant (L3) et le syllogisme hypothétique, on obtient $\underset{\mathsf{J}}{\vdash} (\mathcal{A} \to \mathcal{B})$. Contradiction.

— Si $\underset{\mathsf{J}}{\vdash} \mathcal{B}$, on a aussi $\underset{\mathsf{J}}{\vdash} (\mathcal{B} \to (\mathcal{A} \to \mathcal{B}))$ par (L2). On obtient encore une contradiction par modus ponens.

Donc, ν est une valuation.

Soit $\mathcal{A}$ un théorème de L^*. ALors, $\mathcal{A}$ est un théorème de J. Donc, $\nu(A) = \mathsf{V}$. □

THÉORÈME 3.20 *(Théorème d'adéquation) Si $\mathcal{A}$ est une formule bf de* L *et si $\mathcal{A}$ est une tautologie, alors* $\underset{\mathsf{L}}{\vdash} \mathcal{A}$.

PREUVE Soit $\mathcal{A}$ une formule bf de L qui est une tautologie. Supposons que $\mathcal{A}$ n'est pas un théorème de L. Alors, l'extension L^* de L obtenue en ajoutant $\sim\mathcal{A}$ comme axiome est cohérente. Soit ν une valuation qui prend la valeur V sur chaque théorème de L^*. Alors, $\nu(\sim\mathcal{A}) = \mathsf{V}$. Contradiction, car A est une tautologie et donc, $\nu(\mathcal{A}) = \mathsf{V}$. Donc, $\mathcal{A}$ est un théorème de L. □

PROPOSITION 3.21 L *est décidable, c'est-à-dire qu'il existe une méthode effective pour décider si une formule bf quelconque de* L *est un théorème de* L.

PREUVE Il suffit de décider si la formule est une tautologie en utilisant la méthode des tables de vérité. □

4 Calcul informel des prédicats

Il est maintenant grand temps de mettre un peu de contenu mathématique dans nos formules. Pour cela on va introduire des *quantificateurs* :

— le quantificateur universel $\forall$,

— le quantificateur existentiel $\exists$.

On introduira aussi des symboles de relations, aussi appelées *prédicats*.

4.1 Langage du premier ordre

Dans un *langage du premier ordre* $\mathcal{L}$, on ne donne un alphabet de symboles :

— des variables $x_1, x_2, \ldots,$

— un ensemble (possiblement vide) de constantes individuelles $a_1, a_2, \ldots,$

— un ensemble (possiblement vide) de symboles représentant des prédicats, A_i^n, où n représente le nombre d'entrées du prédicat,

— un ensemble (possiblement vide) de symboles représentant des fonctions f_i^n, où n représente le nombre d'entrées de la fonction,

— les symboles de ponctuation $\ll (\gg, \ll) \gg, \ll , \gg,$

— les connecteurs $\sim$ et $\rightarrow$,

— le quantificateur $\forall$.

REMARQUE 4.1 *On a déjà vu que* $\{\sim, \rightarrow\}$ *forme un ensemble adéquat de connecteurs. On peut aussi remarquer que le quantificateur existentiel se déduit du quantificateur universel et de la négation. En effet,* $(\exists x)A(x)$ *est équivalent à* $\sim(\forall x) \sim A(x)$.

EXEMPLE 4.2 **Langage de l'artihmétique du premier ordre.** *On se donne :*

— *la constante* a_1 *représentant* 0,

— *le symbole de prédicat* A_1^2 *représentant* $=$ *(ainsi* $A_1^2(x_1, x_2)$ *représente* $x_1 = x_2$*),*

— f_1^1*, représentant la fonction successeur (ainsi* $f_1^1(x)$ *représente* $x + 1$*),*

— f_1^2*, représentant la fonction* $+$ *(ainsi* $f_1^2(x_1, x_2)$ *représente* $x_1 + x_2$*),*

— f_2^2*, représentant la fonction* $\times$ *(ainsi* $f_2^2(x_1, x_2)$ *représente* $x_1 x_2$*),*

DÉFINITION 4.3 *Soit* $\mathcal{L}$ *un langage du premier ordre. Un* terme *de* $\mathcal{L}$ *est défini comme suit :*

(i) Une variable ou une constante individuelle est un terme.

(ii) Si f_i^n *est un symbole de fonction dans* $\mathcal{L}$ *et* $t_1, \ldots, t_n$ *sont des termes de* $\mathcal{L}$*, alors* $f_i^n(t_1, \ldots, t_n)$ *est un terme de* $\mathcal{L}$*.*

(iii) L'ensemble des termes de $\mathcal{L}$ est généré par (i) et (ii).

DÉFINITION 4.4 *Soit $\mathcal{L}$ un langage du premier ordre. Une* formule atomique *de $\mathcal{L}$ est définie comme $A_i^n(t_1, \ldots, t_n)$, où A_i^n est un symbole de prédicat de $\mathcal{L}$ et $t_1, \ldots, t_n$ sont des termes de $\mathcal{L}$.*

On peut maintenant définir les formules bf de $\mathcal{L}$.

DÉFINITION 4.5 *Une formule bf de $\mathcal{L}$ est définie par :*

(i) Toute formule atomique de $\mathcal{L}$ est une formule bf de $\mathcal{L}$.

(ii) Si $\mathcal{A}$ et $\mathcal{B}$ sont des formules bf de $\mathcal{L}$ et x_i est une variable, alors $(\sim\mathcal{A})$, $\mathcal{A} \to \mathcal{B}$ et $(\forall x_i)\mathcal{A}$ sont des formules bf de $\mathcal{L}$.

(iii) L'ensemble des formules bf de $\mathcal{L}$ est généré par (i) et (ii).

NOTATION 4.6 *On utilisera les abbréviations*
— $(\exists x)\mathcal{A}(x)$ *pour* $(\sim((\forall x)(\sim\mathcal{A}(x))))$,
— $(\mathcal{A} \wedge \mathcal{B})$ *pour* $(\sim(\mathcal{A} \to (\sim\mathcal{B})))$,
— $(\mathcal{A} \vee \mathcal{B})$ *pour* $((\sim\mathcal{A}) \to \mathcal{B})$.
On se permettra d'omettre les parenthèses lorsque le sens sera clair.

Si l'on considère une formule du type $x_1 = 0$, elle n'est en général ni juste, ni fausse, alors que dans $\mathbb{N}$, la formule $(\forall x_1)(x_1 = 0)$ est fausse. La différence entre les deux est que dans la première la variable est *libre*, alors qu'elle est *liée* dans la seconde. Nous allons formaliser cette différence.

DÉFINITION 4.7 *Dans la formule bf $(\forall x_i)\mathcal{A}$, on dit que $\mathcal{A}$ est le* champ d'action *du quantificateur. Plus généralement, si $(\forall x_i)\mathcal{A}$ apparait comme sous-formule d'une formule bf $\mathcal{B}$, on dit que le champ d'action du quantificateur dans $\mathcal{B}$ est $\mathcal{A}$. Une occurrence de la variable x_i dans une formule bf est dite* liée *si elle apparait, soit dans le champ d'action d'un $(\forall x_i)$ dans la formule ou si elle est le x_i du $(\forall x_i)$. Dans le cas contraire, elle est* libre.

On aura besoin de savoir quand on peut remplacer des variables par des termes. Pour cela il faut distinguer les termes libres et liés.

DÉFINITION 4.8 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$. Un terme t est dit libre pour x_i dans $\mathcal{A}$ si pour toute variable x_j apparaissant dans t, x_i n'apparait pas libre dans le champ d'action d'un $(\forall x_j)$.*

4.2 Interprétations

DÉFINITION 4.9 *Une* interprétation I *d'un langage $\mathcal{L}$ est la donnée de :*

- *un ensemble non vide* D_I, *appelé* domaine *de* I,
- *une collection d'éléments distingués* $\{\bar{a}_1, \bar{a}_2, \ldots\}$ *($\bar{a}_i$ est appelé l'interprétation de a_i),*
- *une collection de fonctions* $\bar{f}_i^n$, $i > 0$, $n > 0$ *($\bar{f}_i^n$ est appelée l'interprétation de f_i^n),*
- *une collection de relations* $\bar{A}_i^n$, $i > 0$, $n > 0$ *($\bar{A}_i^n$ est appelée l'interprétation de A_i^n).*

EXEMPLE 4.10 *Le langage de l'arithmétique peut être interprété dans $\mathbb{N}$, mais aussi dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Les mêmes formules ne seront pas vraies dans toutes les interprétations.*

4.3 Satisfaction d'une formule bf dans une interprétation

DÉFINITION 4.11 *Soit* I *une* interprétation *d'un langage $\mathcal{L}$. Une* valuation *est une fonction ν de l'ensemble des termes de $\mathcal{L}$ dans* D_I *avec les propriétés suivantes*

(i) $\nu(a_i) = \bar{a}_i$ *pour chaque constante individuelle* a_i *de* $\mathcal{L}$.

(ii) Si f_i^n *est un symbole de fonction dans* $\mathcal{L}$ *et* $t_1, \ldots, t_n$ *sont des termes de* $\mathcal{L}$, *alors* $\nu(f_i^n(t_1, \ldots t_n)) = \bar{f}_i^n(\nu(t_1), \ldots, \nu(t_n))$.

DÉFINITION 4.12 *Deux valuations ν et ν' sont i-équivalentes si $\nu(x_j) = \nu'(x_j)$ pour toute variable x_j, où $j \neq i$.*

DÉFINITION 4.13 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$, et* I *une interprétation de $\mathcal{L}$. Une valuation ν dans* I *satisfait à $\mathcal{A}$ si on peut montrer par induction qu'elle satisfait à $\mathcal{A}$ en utilisant les pas d'induction suivants :*

(i) ν satisfait à la formule atomique $A_j^n(t_1, \ldots t_n)$ si $\bar{A}_i^n(\nu(t_i), \ldots, \nu(t_n))$ est vraie dans D_I.

(ii) ν satisfait à $(\sim\mathcal{B})$ si ν ne satisfait pas à $\mathcal{B}$.

(iii) ν satisfait à $(\mathcal{B} \to \mathcal{C})$ si ν satisfait à $(\sim\mathcal{B})$ ou ν satisfait à $\mathcal{C}$.

(iv) ν satisfait à $(\forall x_i)\mathcal{B}$, si pour toute valuation ν' qui est i-équivalente à ν, alors ν' satisfait à $\mathcal{B}$.

PROPOSITION 4.14 *Soit $\mathcal{A}(x_i)$ une formule bf dans laquelle x_i est libre, et soit t un terme qui est libre pour x_i dans $\mathcal{A}(x_i)$. Soit ν une valuation, et ν' la valuation i-équivalente à ν dans laquelle $\nu'(x_i) = \nu(t)$. Alors, ν satisfait à $\mathcal{A}(t)$ si et seulement si ν' satisfait à $\mathcal{A}(x_i)$.*

DÉFINITION 4.15 *Une formule bf $\mathcal{A}$ est* vraie *dans une interprétation* I *si toute valuation dans* I *satisfait à $\mathcal{A}$. On notera* $I \models \mathcal{A}$ *si $\mathcal{A}$ est vraie dans* I. *La formule $\mathcal{A}$ est* fausse *si aucune valuation dans* I *ne satisfait à $\mathcal{A}$.*

REMARQUE 4.16 *Il existe des formules $\mathcal{A}$ qui ne sont ni vraies, ni fausses dans une interprétation* I. *C'est le cas de la formule $x_1 = 0$ dans le langage de l'arithmétique.*

PROPOSITION 4.17 *Si les formules bf $\mathcal{A}$ et $(\mathcal{A} \to \mathcal{B})$ sont vraies dans une interprétation* I, *alors $\mathcal{B}$ est vraie dans* I.

PROPOSITION 4.18 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$, et* I *une interprétation de $\mathcal{L}$. Alors,* $I \models \mathcal{A}$ *si et seulement si, pour toute variable* x_i, $I \models (\forall x_i)\mathcal{A}$.

COROLLAIRE 4.19 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$,* I *une interprétation de $\mathcal{L}$. Alors,* $I \models \mathcal{A}$ *si et seulement si, pour toute suite de variables* $y_1, \ldots y_n$ *de $\mathcal{L}$,* $I \models (\forall y_1) \ldots (\forall y_n)\mathcal{A}$.

PROPOSITION 4.20 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$ et* I *une interprétation de $\mathcal{L}$. Alors, ν satisfait à la formule $(\exists x_i)\mathcal{A}$ si et seulement si il existe au moins une valuation ν' qui est i-équivalente à ν et qui satisfait à $\mathcal{A}$.*

Il est maintenant le temps de faire le lien entre notre système formel L et les formules du langage du premier ordre $\mathcal{L}$. Dans ce cadre, il est naturel de remplacer les variables propositionnelles de L par des formules bf de $\mathcal{L}$.

DÉFINITION 4.21 *On considère une formule bf, $\mathcal{A}_0$, du langage formel* L. *Une formule $\mathcal{A}$ obtenue en remplaçant chaque variable propositionnelle de $\mathcal{A}_0$ par une formule bf de $\mathcal{L}$ est dite une* matérialisation par substitution *de $\mathcal{A}_0$ dans $\mathcal{L}$.*

DÉFINITION 4.22 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ est une* tautologie *si c'est la matérialisation par substitution d'une tautologie $\mathcal{A}_0$ de* L.

PROPOSITION 4.23 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ qui est une tautologie est vraie dans toute interprétation de $\mathcal{L}$.*

DÉFINITION 4.24 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ est* fermée *si elle ne contient pas de variables libres.*

PROPOSITION 4.25 *Soit* I *une interprétation de $\mathcal{L}$ et $\mathcal{A}$, une formule bf de $\mathcal{L}$. Si ν et w sont deux valuations de $\mathcal{L}$ qui prennent la même valeur pour toute variable libre de $\mathcal{A}$, alors ν satisfait à $\mathcal{A}$ si et seulement si w satisfait à $\mathcal{A}$.*

COROLLAIRE 4.26 *Soit* I *une interprétation de* $\mathcal{L}$ *et* $\mathcal{A}$*, une formule bf fermée de* $\mathcal{L}$*. Alors* $I \models \mathcal{A}$ *ou bien* $I \models (\sim\mathcal{A})$.

DÉFINITION 4.27 *Une formule bf* $\mathcal{A}$ *de* $\mathcal{L}$ *est* logiquement valide *si* $\mathcal{A}$ *est vraie dans toute interprétation de* $\mathcal{L}$*. Elle est dite* contradictoire *si elle est fausse dans toute interprétation.*

5 Calcul des prédicats formel

Dans cette section nous allons définir et étudier la notion de preuve dans un système formel déductif $K_{\mathcal{L}}$ construit à partir d'un langage du premier ordre $\mathcal{L}$.

DÉFINITION 5.1 *Soit* $\mathcal{L}$ *un langage du premier ordre. On définit un* système formel déductif *par les axiomes et règles de déduction suivantes :*

Axiomes. *Soient* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *des formules bf de* $\mathcal{L}$*. Alors, les formules bf suivantes sont des axiomes de* $K_{\mathcal{L}}$.

(K1) $(\mathcal{A} \to (\mathcal{B} \to \mathcal{A}))$.

(K2) $(\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C}))$.

(K3) $(\sim\mathcal{A} \to \sim\mathcal{B}) \to (\mathcal{B} \to \mathcal{A})$.

(K4) $((\forall x_i)\mathcal{A} \to \mathcal{A})$*, si* x_i *n'est pas libre dans* $\mathcal{A}$.

(K5) $((\forall x_i)\mathcal{A}(x_i) \to \mathcal{A}(t))$*, si* $\mathcal{A}(x_i)$ *est une formule bf dans* $\mathcal{L}$ *et* t *est un terme de* $\mathcal{L}$ *qui est libre pour la variable* x_i *dans* $\mathcal{A}(x_i)$.

(K6) $((\forall x_i)(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\forall x_i)\mathcal{B})$*, si* $\mathcal{A}$ *ne contient pas d'occurrence libre de la variable* x_i.

Règles.

(1) Modus ponens *: Si* $\mathcal{A}$ *et* $\mathcal{B}$ *des formules bf de* $\mathcal{L}$*, alors on déduit* $\mathcal{B}$ *de* $\mathcal{A}$ *et* $(\mathcal{A} \to \mathcal{B})$.

(2) Généralisation *: Si* $\mathcal{A}$ *est une formule de* $\mathcal{L}$ *et* x_i *est une variable, on déduit* $(\forall x_i)\mathcal{A}$ *de* $\mathcal{A}$.

Ceci nous permet de définir la notion de preuve.

DÉFINITION 5.2 *1. Une* preuve dans $K_{\mathcal{L}}$ *est une suite finie* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *de formules bf de* $\mathcal{L}$ *telles que pour tout* i*, soit* $\mathcal{A}_i$ *est un axiome de* $K_{\mathcal{L}}$*, soit* $\mathcal{A}_i$ *découle des* $\mathcal{A}_j$*,* $j < i$ *par modus ponens ou généralisation. On dira que* $\mathcal{A}_n$ *est un* théorème *de* $K_{\mathcal{L}}$.

2. *Si* Γ *est un ensemble de formules bf de* $\mathcal{L}$*, une* déduction de Γ dans $K_{\mathcal{L}}$ *est une suite de formules bf* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *de* $\mathcal{L}$ *telles que pour tout* i*, soit* $\mathcal{A}_i$ *est un axiome de* $K_{\mathcal{L}}$*, soit* $\mathcal{A}_i$ *est dans* Γ*, soit* $\mathcal{A}_i$ *découle des* $\mathcal{A}_j$*,* $j < i$ *par modus ponens ou généralisation. On dira que* $\mathcal{A}_n$ *est une* conséquence de Γ dans $K_{\mathcal{L}}$*.*

PROPOSITION 5.3 *Soit* $\mathcal{A}$ *une formule bf de* $\mathcal{L}$*. Si* $\mathcal{A}$ *est une tautologie, alors* $\mathcal{A}$ *est un théorème de* $K_{\mathcal{L}}$*.*

Attention ! La réciproque ne sera plus vraie.

NOTATION 5.4 *Pour alléger la notation, nous noterons* $K_{\mathcal{L}}$ *par* K*.*

PROPOSITION 5.5 *Tout axiome obtenu à partir des schémas d'axiomes (K4), (K5) et (K6) est logiquement valide.*

THÉORÈME 5.6 *(Théorème de sûreté ou Soudness theorem) Soit* $\mathcal{A}$ *une formule bf de* $\mathcal{L}$*. Si* $\vdash_K \mathcal{A}$*, alors* $\mathcal{A}$ *est logiquement valide. On en déduit que* K *est cohérent.*

THÉORÈME 5.7 *(Théorème de déduction pour* K*) Soient* A *et* B *deux formules bf de* $\mathcal{L}$*, et* Γ *un ensemble (possiblement vide) de formules bf de* $\mathcal{L}$*. Si* $\Gamma \cup \{\mathcal{A}\} \vdash_K \mathcal{B}$*, et si la déduction ne contient aucun pas de généralisation avec une variable qui est libre dans* $\mathcal{A}$*, alors* $\Gamma \vdash_K (\mathcal{A} \to \mathcal{B})$*.*

COROLLAIRE 5.8 *Si* $\Gamma \cup \{\mathcal{A}\} \vdash_K \mathcal{B}$ *et si* $\mathcal{A}$ *est fermée, alors* $\Gamma \vdash_K (\mathcal{A} \to \mathcal{B})$*.*

COROLLAIRE 5.9 *Pour toutes formules bf,* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *de* $\mathcal{L}$*,*

$$\{(\mathcal{A} \to \mathcal{B}), (\mathcal{B} \to \mathcal{C})\} \vdash_K (\mathcal{A} \to \mathcal{C}).$$

PROPOSITION 5.10 *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *des formules bf de* $\mathcal{L}$*, et* Γ *un ensemble de formules bf de* $\mathcal{L}$*. Si* $\Gamma \vdash_K (\mathcal{A} \to \mathcal{B})$*, alors* $\Gamma \cup \{\mathcal{A}\} \vdash_K \mathcal{B}$*.*

5.1 Équivalence, substitution

PROPOSITION 5.11 *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *des formules bf de* $\mathcal{L}$*. Alors,* $\vdash_K (\mathcal{A} \leftrightarrow \mathcal{B})$ *si et seulement si* $\vdash_K (\mathcal{A} \to \mathcal{B})$ *et* $\vdash_K (\mathcal{B} \to \mathcal{A})$*.*

DÉFINITION 5.12 *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *des formules bf de* $\mathcal{L}$*. On dit que* $\mathcal{A}$ *et* $\mathcal{B}$ *sont* démontrablement équivalentes *si* $\vdash_K (\mathcal{A} \leftrightarrow \mathcal{B})$*.*

COROLLAIRE 5.13 *Soient $\mathcal{A}, \mathcal{B}, \mathcal{C}$ des formules bf de $\mathcal{L}$. Si $\mathcal{A}$ et $\mathcal{B}$ sont démontrablement équivalentes, et $\mathcal{B}$ et $\mathcal{C}$ sont démontrablement équivalentes, alors $\mathcal{A}$ et $\mathcal{C}$ sont démontrablement équivalentes.*

PROPOSITION 5.14 *Si x_i apparait libre dans $\mathcal{A}(x_i)$ et x_j est une variable qui n'est ni libre, ni liée dans $\mathcal{A}(x_i)$, alors $\underset{K}{\vdash} ((\forall x_i)\mathcal{A}(x_i) \leftrightarrow (\forall x_j)\mathcal{A}(x_j))$.*

PROPOSITION 5.15 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$ dont les variables libres sont $y_1, \ldots, y_n$. Alors $\underset{K}{\vdash} \mathcal{A}$ si et seulement si $\underset{K}{\vdash} (\forall x_1) \ldots (\forall x_n)\mathcal{A}$.*

DÉFINITION 5.16 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$ dont les variables libres sont $y_1, \ldots, y_n$. Alors la formule bf $(\forall y_1) \ldots (\forall y_n)\mathcal{A}$ est appelée* fermeture universelle *de $\mathcal{A}$ et notée $\mathcal{A}'$.*

PROPOSITION 5.17 *Soit $\mathcal{A}$ et $\mathcal{B}$ deux formules de $\mathcal{L}$. Supposons que $\mathcal{B}_0$ est obtenue d'une formule $\mathcal{A}_0$ en substituant $\mathcal{B}$ à une occurrence ou plus de $\mathcal{A}$ dans $\mathcal{A}_0$. Alors,*

$$\underset{K}{\vdash} ((\mathcal{A} \leftrightarrow \mathcal{B})' \rightarrow (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)).$$

COROLLAIRE 5.18 *Soit $\mathcal{A}, \mathcal{B}, \mathcal{A}_0, \mathcal{B}_0$ comme dans la proposition ci-dessus. Si $\underset{K}{\vdash} (\mathcal{A} \leftrightarrow \mathcal{B})$, alors $\underset{K}{\vdash} (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)$.*

COROLLAIRE 5.19 *Si la variable x_j n'apparait pas (ni libre, ni liée) dans une formule bf $\mathcal{A}(x_i)$, et si $\mathcal{B}_0$ est obtenue d'une formule $\mathcal{A}_0$ en substituant $(\forall x_j)\mathcal{A}(x_j)$ à une occurrence ou plus de $(\forall x_i)\mathcal{A}(x_i)$ dans $\mathcal{A}_0$, alors $\underset{K}{\vdash} (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)$.*

6 Forme prénexe

On veut ici définir une forme normale pour les formules contenant des quantificateurs. On va montrer qu'on peut envoyer tous les quantificateurs au début.

PROPOSITION 6.1 *Soient $\mathcal{A}$ et $\mathcal{B}$ des formules bf de $\mathcal{L}$.*

(i) Si x_i n'apparait pas libre dans $\mathcal{A}$, alors

$$\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \rightarrow \mathcal{B}) \leftrightarrow (\mathcal{A} \rightarrow (\forall x_i)\mathcal{B})),$$

(ii) Si x_i n'apparait pas libre dans $\mathcal{A}$, alors

$$\underset{K}{\vdash} ((\exists x_i)(\mathcal{A} \rightarrow \mathcal{B}) \leftrightarrow (\mathcal{A} \rightarrow (\exists x_i)\mathcal{B})).$$

(iii) Si x_i n'apparait pas libre dans $\mathcal{B}$, alors

$$\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow ((\exists x_i)\mathcal{A} \to \mathcal{B})),$$

(iv) Si x_i n'apparait pas libre dans $\mathcal{B}$, alors

$$\underset{K}{\vdash} ((\exists x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow ((\forall x_i)\mathcal{A} \to \mathcal{B})).$$

LEMME 6.2 *Soient $\mathcal{A}$ et $\mathcal{B}$ des formules bf de $\mathcal{L}$, et x_i une variable. Alors,*

1. $\underset{K}{\vdash} (\mathcal{A} \to \mathcal{B})$ *si et seulement si* $\underset{K}{\vdash} (\sim\mathcal{B} \to \sim\mathcal{A})$.
2. $\underset{K}{\vdash} \sim(\mathcal{A} \to \mathcal{B})$ *si et seulement si* $\underset{K}{\vdash} \mathcal{A}$ *et* $\underset{K}{\vdash} \sim\mathcal{B}$.
3. $\underset{K}{\vdash} \mathcal{A} \to (\exists x_i)\mathcal{A}$.

PREUVE

1. Exercice en utilisant (K3).
2. Supposons que $\underset{K}{\vdash} \sim(\mathcal{A} \to \mathcal{B})$. Comme $\underset{K}{\vdash} \sim(\mathcal{A} \to \mathcal{B}) \to \mathcal{A}$ et $\underset{K}{\vdash} \sim(\mathcal{A} \to \mathcal{B}) \to \sim\mathcal{B}$ sont des tautologies (exercice), on en tire $\underset{K}{\vdash} \mathcal{A}$ et $\underset{K}{\vdash} \sim\mathcal{B}$. Réciproquement, supposons que $\underset{K}{\vdash} \mathcal{A}$ et $\underset{K}{\vdash} \sim\mathcal{B}$. On en tire que $\underset{K}{\vdash} \sim(\mathcal{A} \to \mathcal{B})$ en utilisant que $\underset{K}{\vdash} \mathcal{A} \to (\sim B \to \sim(\mathcal{A} \to \mathcal{B}))$ est une tautologie.
3. Exercice en utilisant (K3) et (K6). □

PREUVE DE LA PROPOSITION 6.1 On doit traiter les quatre cas et chaque fois il y a 2 directions à traiter. Certaines étapes très élémentaires ont été sautées.

(i) On a $\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\forall x_i)\mathcal{B}))$, car $(\forall x_i)(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\forall x_i)\mathcal{B})$ est simplement l'axiome (K6). Montrons maintenant $\underset{K}{\vdash} ((\mathcal{A} \to (\forall x_i)\mathcal{B}) \to (\forall x_i)(\mathcal{A} \to \mathcal{B}))$ Par le théorème de déduction, il suffit de montrer que $\{(\mathcal{A} \to (\forall x_i)\mathcal{B})\} \underset{K}{\vdash} (\forall x_i)(\mathcal{A} \to \mathcal{B})$.

(1)	$\mathcal{A} \to (\forall x_i)\mathcal{B}$	Hyp.
(2)	$(\forall x_i)\mathcal{B} \to B$	(K4) ou (K5)
(3)	$\mathcal{A} \to \mathcal{B}$	SH
(4)	$(\forall x_i)(\mathcal{A} \to \mathcal{B})$	Gen.

(ii) Par le lemme 6.2(1), il suffit de montrer

$$\underset{K}{\vdash} \sim(\exists x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow \sim(\mathcal{A} \to (\exists x_i)\mathcal{B}).$$

Par le théorème de déduction, pour montrer $\underset{K}{\vdash} \sim(\exists x_i)(\mathcal{A} \to \mathcal{B}) \to \sim(\mathcal{A} \to (\exists x_i)\mathcal{B})$, il suffit de montrer $\{\sim(\exists x_i)(\mathcal{A} \to \mathcal{B})\} \underset{K}{\vdash} \sim(\mathcal{A} \to (\exists x_i)\mathcal{B})$, et par le lemme 6.2(2), il suffit de montrer $\{\sim(\exists x_i)(\mathcal{A} \to \mathcal{B})\} \underset{K}{\vdash} \mathcal{A}$ et $\{\sim(\exists x_i)(\mathcal{A} \to \mathcal{B})\} \underset{K}{\vdash} \sim(\exists x_i)\mathcal{B}$.

(1)	$\sim(\exists x_i)(\mathcal{A} \to \mathcal{B})$	Hyp.
(2)	$\sim\sim(\forall x_i) \sim(\mathcal{A} \to \mathcal{B})$	def de $\exists$
(3)	$(\forall x_i) \sim(\mathcal{A} \to \mathcal{B})$	
(4)	$(\forall x_i) \sim(\mathcal{A} \to \mathcal{B}) \to \sim(\mathcal{A} \to \mathcal{B})$	(K4) ou (K5)
(5)	$\sim(\mathcal{A} \to \mathcal{B})$	MP (3)(4)
(6)	$\mathcal{A}$	Lemme 6.2(2)
(7)	$\sim\mathcal{B}$	Lemme 6.2(2)
(8)	$(\forall x_i) \sim\mathcal{B}$	Gen
(9)	$\sim(\exists x_i)$B	def de $\exists$

Dans l'autre direction, pour montrer $\underset{K}{\vdash} \sim(\mathcal{A} \to (\exists x_i)\mathcal{B}) \to \sim(\exists x_i)(\mathcal{A} \to \mathcal{B})$, il suffit de montrer $\{\sim(\mathcal{A} \to (\exists x_i)\mathcal{B})\} \underset{K}{\vdash} \sim(\exists x_i)(\mathcal{A} \to \mathcal{B})$.

(1)	$\sim(\mathcal{A} \to (\exists x_i)\mathcal{B})$	Hyp.
(2)	$\mathcal{A}$	Lemme 6.2(2)
(3)	$\sim(\exists x_i)\mathcal{B}$	Lemme 6.2(2)
(4)	$(\forall x_i) \sim\mathcal{B}$	def de $\exists$
(5)	$(\forall x_i) \sim\mathcal{B} \to \sim\mathcal{B}$	(K4) ou (K5)
(6)	$\sim\mathcal{B}$	MP (4)(5)
(7)	$\sim(\mathcal{A} \to \mathcal{B})$	Lemme 6.2(2)
(8)	$(\forall x_i) \sim(\mathcal{A} \to \mathcal{B})$	Gen.
(9)	$\sim(\exists x_i)(\mathcal{A} \to \mathcal{B})$	def de $\exists$

(iii) Par (i) on a $\underset{K}{\vdash} ((\forall x_i)(\sim\mathcal{B} \to \sim\mathcal{A}) \leftrightarrow (\sim\mathcal{B} \to (\forall x_i) \sim\mathcal{A}))$. Par le corollaire 5.18 appliqué plusieurs fois on a successivement,

$$\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow (\sim\mathcal{B} \to (\forall x_i) \sim\mathcal{A})),$$

$$\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow (\sim\mathcal{B} \to \sim(\exists x_i)\mathcal{A})),$$

et finalement

$$\underset{K}{\vdash} ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow ((\exists x_i)\mathcal{A} \to \mathcal{B})).$$

(iv) Exercice en utilisant (ii). □

DÉFINITION 6.3 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ est sous* forme prénexe *si elle est de la forme*

$$(Q_1 x_{i_1})(Q_2 x_{i_2}) \dots (Q_n x_{i_n})\mathcal{D},$$

où $\mathcal{D}$ est une formule bf sans quantificateur et chaque Q_j est soit $\forall$, soit $\exists$.

PROPOSITION 6.4 *Pour toute formule bf $\mathcal{A}$ de $\mathcal{L}$, il existe une formule $\mathcal{B}$ sous forme prénexe qui est démontrablement équivente à $\mathcal{A}$.*

DÉFINITION 6.5 *(i) Soit $n > 0$. Une formule bf sous forme prénexe est une Π_n-formule si elle commence par un quantificateur universel et a $n-1$ alternances de type de quantificateurs.*

(ii) Soit $n > 0$. Une formule bf sous forme prénexe est une Σ_n-formule si elle commence par un quantificateur existentiel et a $n-1$ alternances de type de quantificateurs.

6.1 Le théorème d'adéquation pour K

Le but de cette section est de montrer que si $\mathcal{A}$ est une formule bf logiquement valide de $\mathcal{L}$, alors $\mathcal{A}$ est un théorème de $K_{\mathcal{L}}$.

DÉFINITION 6.6 *Une* extension *de* K *est un système formel obtenu en changeant et/ou augmentant l'ensemble des axiomes de telle sorte que tout théorème de* K *soit un théorème de l 'extension de* K. *On peut de même définir une extension d'une extension de* K.

DÉFINITION 6.7 *Un* système du premier ordre *est une extension de $K_{\mathcal{L}}$ pour un langage du premier ordre $\mathcal{L}$.*

DÉFINITION 6.8 *Un système du premier ordre* S *est* cohérent *s'il n'existe pas de formule bf $\mathcal{A}$ telle que $\mathcal{A}$ et $(\sim\mathcal{A})$ soient simultanément des théorèmes de* S.

PROPOSITION 6.9 *Soit* S *un système cohérent du premier ordre et $\mathcal{A}$ une formule bf* fermée *qui n'est pas un théorème de* S. *Alors, l'extension S^* de* S *obtenue en ajoutant $(\sim\mathcal{A})$ comme axiome additionnel est cohérente.*

DÉFINITION 6.10 *Un système du premier ordre* S *est* complet *si, pour toute formule bf fermée $\mathcal{A}$, soit $\vdash_S \mathcal{A}$, soit $\vdash_S (\sim\mathcal{A})$.*

PROPOSITION 6.11 *Soit S un système cohérent du premier ordre. Alors, il existe une extension de S qui est complète.*

PROPOSITION 6.12 *Soit S un système cohérent du premier ordre. Alors, il existe une interprétation de $\mathcal{L}$ dans laquelle chaque théorème de S est vrai.*

THÉORÈME 6.13 *(Théorème d'adéquation) Si $\mathcal{A}$ est une formule bf de $\mathcal{L}$ qui est logiquement valide, alors A est un théorème de $K_{\mathcal{L}}$.*

6.2 Modèles

DÉFINITION 6.14 *(i) Soit Γ un ensemble de formules bf de $\mathcal{L}$. Une interprétation de $\mathcal{L}$ dans laquelle chaque formule de Γ est vraie est appelée un* modèle *de Γ.*

(ii) Soit S un système du premier ordre. Un modèle *de S est une interprétation de $\mathcal{L}$ dans laquelle chaque théorème de S est vrai.*

PROPOSITION 6.15 *Soit S un système du premier ordre et I une interprétation de L dans laquelle chaque axiome de S est vrai. Alors, I est un modèle de S.*

PROPOSITION 6.16 *Un système du premier ordre S est cohérent si et seulement si il a un modèle.*

PROPOSITION 6.17 *Soit S, un système du premier ordre cohérent, et $\mathcal{A}$ une formule bf qui est vraie dans tout modèle de S. Alors $\mathcal{A}$ est un théorème de S.*

THÉORÈME 6.18 *(Théorème de Löwenheim-Skolem) Si un système du premier ordre a un modèle, alors il a un modèle dénombrable.*

THÉORÈME 6.19 *(Théorème de compacité) Si chaque sous-ensemble fini de l'ensemble des axiomes d'un système du premier ordre S a un modèle, alors S lui-même a un modèle.*

COROLLAIRE 6.20 *Soit Γ un ensemble infini de formules bf de $K_{\mathcal{L}}$. Alors, Γ a un modèle dès que chaque sous-ensemble fini de Γ a un modèle.*

7 Quelques systèmes formels du premier ordre

La quasi-totalité des systèmes formels du premier ordre importants en mathématiques ont un symbole de prédicat représentant l'égalité. Nous prendrons donc le temps de détailler les axiomes auxquels satisfait ce prédicat. Nous regarderons ensuite les systèmes du premier ordre de la théorie des groupes (car c'est l'un des plus simples), de l'arithmétique et de la théorie des ensembles.

7.1 Systèmes du premier ordre avec égalité

L'égalité est un prédicat à deux entrées. Nous le noterons A_1^2. Une fois que nous aurons pris l'habitude de manipuler les axiomes, nous nous permettrons aussi de noter $A_1^2(x, y)$ par $x = y$.

Dans un système du premier ordre avec égalité, nous ajoutons aux axiomes (K1)-(K6) les axiomes (E7), (E8) et (E9) définis comme suit :

DÉFINITION 7.1 *Toute extension de $K_{\mathcal{L}}$ qui inclut dans ses axiomes les axiomes (E7), (E8) et (E9) définis ci-dessous est appelé* système du premier ordre avec égalité*. Les axiomes suivants sont appelés* axiomes de l'égalité *:*

(E7) $A_1^2(x_1, x_1)$.

(E8) $A_1^2(t_k, u) \to A_1^2(f_i^n(t_1, \ldots, t_k, \ldots, t_n), f_i^n(t_1, \ldots, u, \ldots, t_n))$, *où* $t_1, \ldots, t_n, u$ *sont des termes quelconques et* f_i^n *est un symbole de fonction de* $\mathcal{L}$.

(E9) $A_1^2(t_k, u) \to (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \to A_i^n(t_1, \ldots, u, \ldots, t_n))$, *où* $t_1, \ldots, t_n, u$ *sont des termes quelconques et* A_i^n *est un symbole de prédicat de* $\mathcal{L}$.

PROPOSITION 7.2 *Soit S, un système du premier ordre avec égalité. Alors, les formules bf suivantes sont des théorèmes de S :*

(i) $(\forall x_i)A_1^2(x_1, x_1)$,

(ii) $\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$,

(iii) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)))$.

PROPOSITION 7.3 *Soit S, un système du premier ordre cohŕent avec égalité. Alors, S a un modèle dans lequel l'interprétation de $\mathcal{A}_1^2$ est $=$. Un tel modèle est appelé* modèle normal *de S.*

7.2 La théorie des groupes

Le langage du premier ordre, $\mathcal{L}_G$, approprié à la théorie des groupes a l'alphabet suivant de symboles :

— des variables $x_1, x_2, \ldots$;
— une constante a_1 correspondant à l'identité ;
— des symboles de fonctions : f_1^1 correspond à l'inverse et f_1^2 au produit ;
— un symbole de prédicat : A_1^2 que l'on notera aussi $=$;
— des symboles de ponctuation : $\ll (\gg, \ll) \gg, \ll , \gg$;
— des symboles logiques : $\forall$, $\sim$, $\rightarrow$.

On définit $\mathcal{G}$, l'extension de $L_{\mathcal{L}_G}$ dont les axiomes propres sont (E7), (E8), (E9) et

(G1) $f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3))$. (Associativité)

(G2) $f_1^2(a_1, x_1) = x_1$. (Élément neutre à gauche)

(G3) $f_1^2(f_1^1(x_1), x_1) = a_1$. (Inverse à gauche)

EXEMPLE 7.4 *Vérifions que a_1 est aussi élément neutre à droite et que $f_1^1(x_1)$ est aussi inverse à droite. Pour simplifier, on va noter $f_1^2(x_1, x_2)$ par x_1x_2, et $f_1^1(x_1) = x_1^{-1}$. Commençons par montrer que x_1^{-1} est inverse à droite, c'est-à-dire $x_1x_1^{-1} = a_1$. Pour cela, on va utiliser que x_1^{-1} a lui-même un inverse à gauche $(x_1^{-1})^{-1}$ qui satisfait à $(x_1^{-1})^{-1}x_1^{-1} = a_1$. On a*

$$\begin{aligned}
x_1x_1^{-1} &= a_1(x_1x_1^{-1}), && \text{(G2)}\\
&= ((x_1^{-1})^{-1}x_1^{-1})(x_1x_1^{-1}), && \text{(G3)}\\
&= (x_1^{-1})^{-1}(x_1^{-1}(x_1x_1^{-1})), && \text{(G1)}\\
&= (x_1^{-1})^{-1}((x_1^{-1}x_1)x_1^{-1}), && \text{(G1)}\\
&= (x_1^{-1})^{-1}(a_1x_1^{-1}), && \text{(G3)}\\
&= (x_1^{-1})^{-1}x_1^{-1}, && \text{(G2)}\\
&= a_1. && \text{(G3)}
\end{aligned}$$

Il nous reste à prouver que $x_1a_1 = x_1$. En effet,

$$\begin{aligned}
x_1a_1 &= x_1(x_1^{-1}x_1), && \text{(G3)}\\
&= (x_1x_1^{-1})x_1, && \text{(G1)}\\
&= a_1x_1, && \text{démontré ci-dessus}\\
&= x_1. && \text{(G2)}
\end{aligned}$$

7.3 L'arithmétique du premier ordre

C'est l'exemple le plus important de la logique, et celui où ont été obtenus les résultats les plus spectaculaires.

Le langage du premier ordre, $\mathcal{L}_N$, approprié pour l'arithmétique, a l'alphabet suivant de symboles :

— des variables $x_1, x_2, \ldots$;
— une constante a_1 correspondant à 0 ;
— des symboles de fonctions : f_1^1 correspond à la fonction successeur (on notera aussi $t' = f_1^1(t)$), et f_1^2, f_2^2 correspondant à la somme et au produit et pour lesquels on utilisera aussi la notation usuelle $+$ et $\times$;
— un symbole de prédicat : A_1^2 que l'on notera aussi $=$;
— des symboles de ponctuation : $\ll (\gg, \ll) \gg, \ll , \gg$;
— des symboles logiques : $\forall$, $\sim$, $\rightarrow$.

On définit $\mathcal{N}$, l'extension de $K_{\mathcal{L}_N}$ dont les axiomes propres sont (E7), (E8), (E9) et les sept axiomes ou schémas d'axiomes suivants

(N1) $(\forall x_1) \sim (f_1^1(x_1) = a_1)$.

(N2) $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2) \rightarrow x_1 = x_2)$.

(N3) $(\forall x_1)(f_1^2(x_1, a_1) = x_1)$.

(N4) $(\forall x_1)(\forall x_2)(f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2)))$.

(N5) $(\forall x_1)(f_2^2(x_1, a_1) = a_1)$.

(N6) $(\forall x_1)(\forall x_2)(f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1))$.

(N7) $\mathcal{A}(a_1) \rightarrow ((\forall x_1)(\mathcal{A}(x_1) \rightarrow \mathcal{A}(f_1^1(x_1))) \rightarrow (\forall x_1)\mathcal{A}(x_1))$, pour toute formule $\mathcal{A}(x_1)$ de $\mathcal{L}_N$ dans laquelle x_1 est libre.

Dans la notation usuelle, ces axiomes deviennent

(N1*) $(\forall x_1) \sim (x_1' = a_1)$.

(N2*) $(\forall x_1)(\forall x_2)(x_1' = x_2' \rightarrow x_1 = x_2)$.

(N3*) $(\forall x_1)(x_1 + 0 = x_1)$.

(N4*) $(\forall x_1)(\forall x_2)(x_1 + x_2' = (x_1 + x_2)')$.

(N5*) $(\forall x_1)(x_1 \times 0 = 0)$.

(N6*) $(\forall x_1)(\forall x_2)(x_1 \times x_2' = (x_1 \times x_2) + x_1)$.

(N7*) $\mathcal{A}(0) \rightarrow ((\forall x_1)(\mathcal{A}(x_1) \rightarrow \mathcal{A}(f_1^1(x_1))) \rightarrow (\forall x_1)\mathcal{A}(x_1))$, pour toute formule $\mathcal{A}(x_1)$ de $\mathcal{L}_N$ dans laquelle x_1 est libre.

Historiquement, les grandes questions du domaine ont été les suivantes :

(Q1) Est-ce que l'ensemble des entiers naturels $\mathbb{N}$ est le seul modèle normal du système $\mathcal{N}$?

(Q2) Le système formel $\mathcal{N}$ est-il complet ?

Dans les deux cas on s'attendait à des réponses positives. Les deux ont eu des réponses négatives. Pour la question (Q1) on s'attendait à une réponse positive parce que les axiomes de Peano caractérisent l'ensemble $\mathbb{N}$. La réponse négative à la question (Q2) est le célèbre théorème d'incomplétude de Kurt Gödel en 1931. En particulier, en lien avec la question (Q2), on peut trouver une formule $\mathcal{A}$ dans le langage $\mathcal{L}_N$ telle que $\mathcal{A}$ est vraie dans $\mathbb{N}$ mais $\mathcal{A}$ n'est pas un théorème de $K_{\mathcal{L}_N}$.

7.4 La théorie des ensembles formelle

Le système formel associé est appelé *système de Zermelo-Fraenkel* et noté ZF.

Le langage du premier ordre, $\mathcal{L}_{ZF}$, approprié à la théorie des ensembles a l'alphabet suivant de symboles :

— des variables $x_1, x_2, \dots$;
— aucune constante ;
— aucun symbole de fonction ;
— deux symboles de prédicat : A_1^2 et A_2^2 correspondant à l'égalité et à l'appartenance (on notera $t_1 \in t_2$ pour $A_2^2(t_1, t_2)$, où t_1, t_2 sont des termes ;
— des symboles de ponctuation : $\ll (\gg$, $\ll) \gg$, $\ll , \gg$;
— des symboles logiques : $\forall$, $\sim$, $\rightarrow$.

NOTATION 7.5 — *On introduit le symbole $\subseteq$ comme abbréviation : ainsi,* $(t_1 \subseteq t_2)$ *signifie* $(\forall x_1)(x_1 \in t_1 \rightarrow x_1 \in t_2)$.
— *On introduit $\exists_1$ comme abbréviation signifiant $\ll$ Il existe un et un seul $\gg$. Ainsi* $(\exists_1 x_1)\mathcal{A}(x_1)$ *signifie* $((\exists x_1)\mathcal{A}(x_1)) \wedge ((\forall x_2)A(x_2) \rightarrow (x_2 = x_1)))$.

On définit ZF, l'extension de $K_{\mathcal{L}}$ dont les axiomes propres sont (E7), (E8), (E9) et les huit axiomes suivants

(ZF1) $(x_1 = x_2 \leftrightarrow (\forall x_2)(x_2 \in x_1 \leftrightarrow x_3 \in x_2))$. (Axiome d'extensionnalité)

(ZF2) $(\exists x_1)(\forall x_2) \sim (x_2 \in x_1)$. (Existence de l'ensemble vide)

(ZF3) $(\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2)$. (Axiome des paires)

(ZF4) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (\exists x_4)(x_4 \in x_1 \wedge x_3 \in x_4)$. (Axiome de l'union des éléments de x_1). On notera $\bigcup x_1$ l'ensemble x_2 obtenu et on utilisera l'abbréviation $(t_1 \cup t_2)$ pour $\bigcup\{t_1, t_2\}$.

(ZF5) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_3 \subseteq x_1)$. (Axiome de l'ensemble des parties d'un ensemble)

(ZF6) $(\forall x_1)(\exists_1 x_2)\mathcal{A}(x_1, x_2) \rightarrow (\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathcal{A}(x_6, x_5)))$, pour toute formule $\mathcal{A}$ dans laquelle x_1 et x_2 sont libres et dans laquelle les quantificateurs $(\forall x_5)$ et $(\forall x_6)$ n'apparaissent pas. (Axiome de replacement : l'ensemble x_4 est formé des images de tous les éléments de x_3 par la fonction déterminée par $\mathcal{A}$.)

(ZF7) $(\exists x_1)(\emptyset \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \rightarrow x_2 \cup \{x_2\} \in x_1))$. (Axiome de l'existence d'un ensemble infini) Note : on définit le singleton $\{x_2\}$ comme la paire $\{x_2, x_2\}$.

(ZF8) $(\forall x_1)(\sim x_1 = \emptyset \rightarrow (\exists x_2)(x_2 \in x_1 \wedge \sim (\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$ (Axiome de fondation : tout ensemble non-vide x_1 contient un élément qui est disjoint de x_1.)

On ne sait pas montrer que ZF est cohérent. Mais, l'axiome de fondation élimine le paradoxe de Russell. La bonne nouvelle est que ZF tient la route depuis plus d'un siècle et que toutes les tentatives pour montrer sa non cohérence ont échoué.

On travaille en mathématiques avec ZF auquel on ajoute un ou deux axiomes, soit l'axiome du choix et l'hypothèse du continu.

Axiome du choix

(AC) Pour tout ensemble x non vide, il existe un ensemble y qui a précisément un élément en commun avec chaque élément de x.

Hypothèse du continu

(HC) Chaque sous-ensemble non vide des nombres réels est soit fini, ou dénombrable, ou a la même cardinalité que les nombres réels (c'est-à-dire est en bijection avec les nombres réels).

PROPOSITION 7.6 *(AC) et (HC) sont indépendants de ZF et indépendants entre eux. En particulier, si ZF est cohérent, alors ZF + (AC) + (HC), ZF + (AC) + (∼ HC), ZF + (∼AC) + (HC) et ZF + (∼AC) + (∼HC) sont cohérents.*

8 Fonctions et relations récursives, ensembles récursifs

Ici, on parle de fonctions et de relations sur les entiers naturels $\mathbb{N}$ et de sous-ensembles de $\mathbb{N}^k$.

DÉFINITION 8.1 *Une fonction arithmétique est une fonction de la forme*

$$f : \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \to \mathbb{N}.$$

Les fonctions primitives récursives et récursives sont générées à partir des fonctions de base suivantes.

Fonctions récusives de base

1. La fonction zéro $z : \mathbb{N} \to \mathbb{N}$, définie par $z(n) = 0$ pour tout $n \in \mathbb{N}$.
2. La fonction successeur $s : \mathbb{N} \to \mathbb{N}$, définie par $s(n) = n + 1$ pour tout $n \in \mathbb{N}$.
3. Les fonctions projections $p_i^k : \mathbb{N}^k \to \mathbb{N}$, définies par $p_i^k(n_i, \ldots, n_k) = n_i$ pour tout $n_1, \ldots, n_k \in \mathbb{N}$.

DÉFINITION 8.2 *L'ensemble des fonctions* récursives *est l'ensemble des fonctions obtenues des fonctions de base par un nombre fini d'applications des trois opérations suivantes :*

1. *La* composition *de* $g : \mathbb{N}^j \to \mathbb{N}$ *avec* $(h_1, \ldots h_j)$*, où* $h_i : \mathbb{N}^k \to \mathbb{N}$*, est la fonction* $f = g \circ (h_1, \ldots, h_j) : \mathbb{N}^k \to \mathbb{N}$ *définie par*

$$f(n_1, \ldots, n_k) = (g(h_1(n_1, \ldots, n_k), \ldots, h_j(n_1, \ldots, n_k)).$$

2. *La* récurrence *de base* $g : \mathbb{N}^k \to \mathbb{N}$ *et de pas* $h : \mathbb{N}^{k+2} \to \mathbb{N}$ *donnant une fonction* $f : \mathbb{N}^{k+1} \to \mathbb{N}$ *définie par*

$$\begin{cases} f(n_1, \ldots, n_k, 0) = g(n_1, \ldots, n_k), \\ f(n_1, \ldots, n_k, n+1) = h(n_1, \ldots, n_k, n, f(n_1, \ldots, n_k, n)). \end{cases}$$

3. *L'*opérateur plus petit nombre *: soit* $g : \mathbb{N}^{k+1} \to \mathbb{N}$ *une fonction telle que pour tout* $n_1, \ldots, n_k \in \mathbb{N}$ *il existe* $n \in \mathbb{N}$ *tel que* $g(n_1, \ldots, n_k, n) = 0$*. Alors, la fonction* $f : \mathbb{N}^k \to \mathbb{N}$ *obtenue de* g *par l'opérateur plus petit nombre est définie ainsi*

$$f(n_1, \ldots, n_k) = \min\{n \mid g(n_1, \ldots, n_k, n) = 0\}.$$

On note $f(n_1, \ldots, n_k) = \mu n[g(n_1, \ldots, n_k, n) = 0]$.

Une fonction obtenue des fonctions de base en utilisant seulement les opérations de composition et de récurrence est dite primitive-récursive.

EXEMPLE 8.3 *Soient* $h(x_1, x_2) = s(x_1) + x_2$, $g_1(x) = x^3$ *et* $g_2(x) = x^2 + 9$. *Soit* $f(x) = h \circ (g_1, g_2)(x)$ *pour* $x \geq 0$. *Alors,* f *peut s'écrire de manière simplifiée*

$$f(x) = x^3 + x^2 + 10.$$

EXEMPLE 8.4 **(la fonction** add**)** *Nous pouvons définir l'addition,* $\mathrm{add}(m, n) = m + n$, *à partir de la fonction successeur, des fonctions projection* $p_1^{(1)}$ *et* $p_3^{(3)}$ *et d'une récurrence de base* $g(x) = p_1^{(1)}(x) = x$ *et de pas* $h(x, y, z) = s \circ p_3^{(3)}(x, y, z) = s(p_3^{(3)}(x, y, z)) = s(z)$.

$$\begin{cases} \mathrm{add}(m, 0) = g(m) = m, \\ \mathrm{add}(m, n + 1) = h(m, n, \mathrm{add}(m, n)) = s(\mathrm{add}(m, n)). \end{cases}$$

EXEMPLE 8.5 **(la fonction** mult**)** *À partir de la fonction addition précédemment définie, des fonctions projection* $p_1^{(3)}$ *et* $p_3^{(3)}$, *et d'une récurrence de base* $g(x) = 0$ *et de pas* $h(x, y, z) = \mathrm{add}(p_1^{(3)}(x, y, z), p_3^{(3)}(x, y, z)) = \mathrm{add}(x, z)$, *nous pouvons définir la multiplication.*

$$\begin{cases} \mathrm{mult}(m, 0) = g(m) = 0, \\ \mathrm{mult}(m, n + 1) = h(m, n, \mathrm{mult}(m, n)) = \mathrm{add}(m, \mathrm{mult}(m, n)). \end{cases}$$

EXEMPLE 8.6 **(la fonction** exp**)** *De façon similaire on peut définir la fonction exponentielle* $\exp(m, n) = m^n$. *Il suffit de choisir* $g(x) = 1$ *et* $h(x, y, z) = \mathrm{mult}(x, z)$. *Notons ici que, dans le but d'alléger la notation, nous n'utilisons plus la fonction projection. Nous avons alors :*

$$\begin{cases} \exp(m, 0) = 1, \\ \exp(m, n + 1) = \mathrm{mult}(m, \exp(m, n)). \end{cases}$$

EXEMPLE 8.7 *Pour définir la récursion* $\mathrm{add}(m, n+1)$, *nous avons utilisé la fonction successeur. Pour* $\mathrm{mult}(m, n+1)$, *nous avons utilisé* add *et pour* $\exp(m, n+1)$, *nous avons utilisé* mult. *La prochaine fonction qui est formée en suivant le même processus est une tour d'exponentielles. Notons* $\mathrm{add}(m, n) = f_1(m, n)$, $\mathrm{mult}(m, n) = f_2(m, n)$, $\exp(m, n) = f_3(m, n)$. *On définit* f_4 *par*

$$\begin{cases} f_4(m, 0) = 1 \\ f_4(m, n + 1) = f_3(m, f_4(m, n)). \end{cases}$$

On a alors

$$f_4(m,n) = \underbrace{m^{m^{m^{\cdots^{m}}}}}_{n \textit{ fois}}.$$

La fonction f_4 est appelée tétration ou tour de puissance.

Similairement, pour $i > 4$, on peut définir $f_i(m,n)$ par

$$\begin{cases} f_i(m,0) = 1, \\ f_i(m,n+1) = f_{i-1}(m, f_i(m,n)). \end{cases}$$

Ces fonctions sont appelées puissances itérées de Knuth. Chaque fonction f_{i+1} croît inimaginablement plus vite que f_i.

EXEMPLE 8.8 *La fonction factorielle est une fonction primitive récursive. On définit la fonction factorielle comme suit :*

$$\begin{cases} \text{fact}(0) = 1, \\ \text{fact}(n+1) = \text{mult}(n+1, \text{fact}(n)). \end{cases}$$

Après avoir montré que l'addition est une fonction primitive récursive, on peut se demander s'il en est de même pour la soustraction. La soustraction usuelle n'est pas une fonction totale dans $\mathbb{N}$. En effet, si on prend $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ telle que $f(x,y) = x - y$, on remarque que, par exemple, $f(3,5)$ n'est pas définie. Il faut donc définir un autre type de soustraction pour avoir une fonction totale sur $\mathbb{N} \times \mathbb{N}$. Nous allons appeler cette fonction la *soustraction propre*.

DÉFINITION 8.9 *La soustraction propre est définie comme suit :*

$$\begin{cases} \text{sous}(x,y) = x - y & \textit{si} \quad x \geq y, \\ \text{sous}(x,y) = 0 & \textit{si} \quad x < y. \end{cases}$$

EXEMPLE 8.10 *La soustraction propre est une fonction primitive récursive. Pour le démontrer, il faut procéder en deux étapes. On commence par démontrer que la fonction prédécesseur est une fonction primitive récursive et on s'en sert pour construire la soustraction propre.*

DÉFINITION 8.11 *La fonction prédécesseur se définit par récurrence :*

$$\begin{cases} \text{pred}(0) = 0, \\ \text{pred}(y+1) = y. \end{cases}$$

Nous pouvons maintenant construire la soustraction propre en utilisant la récurrence et la composition.

$$\begin{cases} \text{sous}(m, 0) = m, \\ \text{sous}(m, n+1) = \text{pred}(\text{sous}(m, n)). \end{cases}$$

Pour pouvoir parler de relations primitives récursives et récursives, on introduit les deux fonctions suivantes

$$\begin{cases} \text{sgn}(0) = 0, \\ \text{sgn}(y+1) = 1; \end{cases} \qquad \begin{cases} \text{cosgn}(0) = 1, \\ \text{cosgn}(y+1) = 0. \end{cases}$$

DÉFINITION 8.12 *Soit* R *une relation sur* $\mathbb{N}$ *à* k *entrées. La fonction caractéristique de* R*, notée* C_R*, est définie par*

$$C_R(n_1, \ldots, n_k) = \begin{cases} 0, & \textit{si } R(n_1, \ldots, n_k) \textit{ est vraie}, \\ 1, & \textit{sinon}. \end{cases}$$

DÉFINITION 8.13 *Soit* A *un sous ensemble de* $\mathbb{N}^k$*. La fonction caractéristique de* A*, notée* C_A*, est définie par*

$$C_A(n_1, \ldots, n_k) = \begin{cases} 0, & \textit{si } (n_1, \ldots, n_k) \in A, \\ 1, & \textit{sinon}. \end{cases}$$

DÉFINITION 8.14 *Une relation sur* $\mathbb{N}$ *à* k *entrées est* primitive récursive *(resp. récursive) si sa fonction caractéristique est primitive récursive (resp. récursive). Un sous-ensemble de* $\mathbb{N}^k$ *est primitif récursif (resp. récursif) si sa fonction caractéristique est primitive récursive (resp. récursive).*

EXEMPLE 8.15 *Soient* $R_1(x, y)$*,* $R_2(x, y)$ *et* $R_3(x, y)$ *les trois énoncés* $\ll x = y \gg$*,* $\ll x < y \gg$*, et* $\ll x > y \gg$ *respectivement.* R_1*,* R_2 *et* R_3 *sont des relations binaires. Nous pouvons définir de façon primitive récursive leurs fonctions caractéristiques des trois prédicats binaires introduits dans l'exemple 8.15 précédent. Il est commode de leur donner un nom qu'on peut utiliser par la suite.*

$$\begin{array}{lcl} \text{eg}(x, y) := C_{R_1}(x, y) & = & \text{sgn}(\text{sous}(x, y) + \text{sous}(y, x)), \\ \text{pp}(x, y) := C_{R_2}(x, y) & = & \text{cosgn}(\text{sous}(y, x)), \\ \text{pg}(x, y) := C_{R_3}(x, y) & = & \text{cosgn}(\text{sous}(x, y)), \end{array} \tag{8.1}$$

où, par abus de notation, nous écrivons $\text{sous}(x, y) + \text{sous}(y, x)$ *plutôt que*

$$\text{add} \circ (\text{sous}, \text{sous} \circ (p_2^2, p_1^2))(x, y)).$$

Ces relations $\ll x < y \gg$, $\ll x > y \gg$ et $\ll x = y \gg$ de l'exemple 8.15 sont primitives récursives. Nous avons en effet construit leurs fonctions caractérisques en (8.1) *par composition de fonctions primitives récursives.*

PROPOSITION 8.16 *Soient R et S deux relations récursives à k entrées. Alors, les relations $\sim R$, $R \vee S$ et $R \wedge S$ sont récusives.*

PROPOSITION 8.17 *Tout singleton de $\mathbb{N}$ est un sous-ensemble récursif de $\mathbb{N}$.*

EXEMPLE 8.18 *La fonction d'Ackermann définie par*

1. $A(0, y) = y + 1$,
2. $A(x + 1, 0) = A(x, 1)$,
3. $A(x + 1, y + 1) = A(x, A(x + 1, y))$,

n'est pas primitive récursive, mais elle est ceendant calculable. La fonction d'Ackermann a la propriété de $\ll$ croître plus rapidement $\gg$ que toutes les fonctions primitives récursives, d'où son attrait. Mais puisqu'elle croît plus rapidement que toute fonction primitive récursive, elle ne peut en être une. Les preuves de ces propriétés sont arides, nous nous abstiendrons de les faire ici.

PROPOSITION 8.19 *La fonction d'Ackermann définie dans l'exemple 8.18 est récursive.*

9 Vers le théorème d'incomplétude de Gödel

Gödel a montré l'existence d'une formule bien formée fermée $\mathcal{A}$ telle que ni $\mathcal{A}$, ni $\sim A$ ne sont des théorèmes de $\mathcal{N}$. On va sauter des étapes de sa preuve et se concentrer sur les idées. Dans ce contexte, il a introduit les fonctions récursives, pour lesquelles Turing a montré que ce sont exactement les fonctions calculables par une machine de Turing.

L'idée de la preuve de Gödel est qu'on peut coder des formules bien formées du langage $\mathcal{L}_N$ et des preuves dans le système $\mathcal{N}$ à l'intérieur de $\mathcal{N}$. En fait, on peut le faire pour n'importe quel langage $\mathcal{L}$ du premier ordre, et n'importe quel système du premier ordre S. On associe des *nombres de Gödel* à chaque symbole de $\mathcal{L}$, à chaque formule bien formée de $\mathcal{L}$, et à chaque preuve de S. On le fait via une fonction g. Le domaine de g est l'ensemble des symboles de $\mathcal{L}$, des formules bien formées de $\mathcal{L}$, et des preuves de S. C'est une fonction injective à valeurs dans $\mathbb{N}$. Elle utilise l'idée que la décomposition d'un nombre entier en facteurs premiers est

unique si les facteurs premiers sont rangés en ordre croissant. On aura besoin d'énumérer les nombres premiers : $p_1, p_2, \ldots, p_n, \ldots$. Ainsi $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.

Nombre de Gödel d'un symbole de $\mathcal{L}$: ce sera un nombre impair
- $g(() = 3$,
- $g()) = 5$,
- $g(,) = 7$,
- $g(\sim) = 9$,
- $g(\to) = 11$,
- $g(\forall) = 13$,
- $g(x_k) = 7 + 8k, \quad k = 1, 2, \ldots,$
- $g(a_k) = 9 + 8k, \quad k = 1, 2, \ldots,$
- $g(f_k^n) = 11 + 8 \times (2^n \times 3^k), \quad n = 1, 2, \ldots, k = 1, 2, \ldots$
- $g(A_k^n) = 13 + 8 \times (2^n \times 3^k), \quad n = 1, 2, \ldots, k = 1, 2, \ldots$

Nombre de Gödel d'une formule bf de $\mathcal{L}$: ce sera un nombre pair, dont l'exposant de 2 dans la décomposition en nombres premiers sera impair. Une formule bien formée $\mathcal{A}$ de $\mathcal{L}$ est une suite $u_1 \ldots u_n$ de symboles $u_1, \ldots, u_n$. Son nombre de Gödel est

$$G(\mathcal{A}) = G(u_1 \ldots u_n) = 2^{g(u_1)} 3^{g(u_2)} \ldots p_n^{g(u_n)}.$$

Nombre de Gödel d'une preuve dans S **:** ce sera un nombre pair, dont l'exposant de 2 dans la décomposition en nombres premiers sera pair. Une preuve dans S est une suite $\mathcal{A}_1, \ldots, \mathcal{A}_n$ de formules bf de $\mathcal{L}$. Son nombre de Gödel est

$$G(\mathcal{A}_1, \ldots, \mathcal{A}_n) = 2^{g(\mathcal{A}_1)} 3^{g(\mathcal{A}_2)} \ldots p_n^{g(\mathcal{A}_n)}.$$

Les fonctions et relations récursives sont précisément celles qui sont *expressibles* dans $\mathcal{N}$.

9.1 Fonctions et relations expressibles dans $\mathcal{N}$

Le système $\mathcal{N}$ contient une copie des nombres naturels. Ainsi 0 est représenté par le terme ferme a_1 que l'on notera 0 ou encore $0^{(0)}$. Par induction on représentera $n + 1$ par le terme $(0^{(n)})'$.

PROPOSITION 9.1 *Si* $m, n \in \mathbb{N}$, *alors*

1. *si* $m \neq n$, *alors* $\underset{\mathcal{N}}{\vdash} \sim (0^{(m)} = 0^{(n)})$;
2. *si* $m = n$, *alors* $\underset{\mathcal{N}}{\vdash} (0^{(m)} = 0^{(n)}$.

DÉFINITION 9.2 *Une relation* R *à* k *entrées sur les nombres naturels est* expressible dans $\mathcal{N}$ *(ou* représentable dans $\mathcal{N}$*) s'il existe une formule bien formée* $\mathcal{A}(x_1, \ldots, x_k)$ *à* k *variables libres telle que pour tous* $n_1, \ldots n_k \in \mathbb{N}$

1. *si* $R(n_1, \ldots, n_k)$ *est vraie dans* $\mathbb{N}$, *alors* $\underset{\mathcal{N}}{\vdash} \mathcal{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$;
2. *si* $R(n_1, \ldots, n_k)$ *est fausse dans* $\mathbb{N}$, *alors* $\underset{\mathcal{N}}{\vdash} \sim \mathcal{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$.

REMARQUE 9.3 *Une fonction* f *de* k *variables à valeurs dans* $\mathbb{N}$ *est donnée par une relation* R *à* $k+1$ *variables telle que* $R(n_1, \ldots, n_{k+1})$ *est vraie si et seulement si* $f(n_1, \ldots, n_k) = n_{k+1}$.

DÉFINITION 9.4 *Une fonction* f *de* k *variables à valeurs dans* $\mathbb{N}$ expressible dans $\mathcal{N}$ *(ou* représentable dans $\mathcal{N}$*) si sa relation associée est représentable dans* $\mathcal{N}$*, par une formule bien formée* $\mathcal{A}(x_1, \ldots, x_{k+1})$ *à* $k+1$ *variables libres telle que pour tous* $n_1, \ldots, n_k$

$$\underset{\mathcal{N}}{\vdash} (\exists_1 x_{k+1}) \mathcal{A}(0^{(n_1)}, \ldots, 0^{(n_k)}, x_{k+1}).$$

PROPOSITION 9.5 *Une fonction ou une relation sur les nombres naturels est expressible dans* $\mathcal{N}$ *si et seulement si elle est récursive.*

9.2 Les idées de la preuve du théorème d'incomplétude de Gödel

THÉORÈME 9.6 (THÉORÈME D'INCOMPLÉTUDE DE GÖDEL) $\mathcal{N}$ *n'est pas complet. Il existe une formule bf* $\mathcal{U}$ *fermée telle que ni* $\mathcal{U}$, *ni* $\sim\mathcal{U}$ *ne sont des théorèems de* $\mathcal{N}$.

PROPOSITION 9.7 *Les relations suivantes sur* $\mathbb{N}$ *sont récursives, et donc, expressibles dans* $\mathcal{N}$:

1. Wf : $\mathrm{Wf}(n)$ *est vraie si et seulement si* n *est le nombre de Gödel d'une formule bf de* $\mathcal{L}_N$;
2. Lax : $\mathrm{Lax}(n)$ *est vraie si et seulement si* n *est le nombre de Gödel d'un axiome logique de* $\mathcal{N}$ *(c'est-à-dire un axiome de* K*)* ;
3. Prax : $\mathrm{Prax}(n)$ *est vraie si et seulement si* n *est le nombre de Gödel d'un axiome spécifique de* $\mathcal{N}$*, incluant les axiomes de l'égalité* ;

4. $\mathtt{Prf}$ *:* $\mathtt{Prf}(n)$ *est vraie si et seulement si* n *est le nombre de Gödel d'une preuve dans* $\mathcal{N}$ *;*
5. $\mathtt{Pf}$ *:* $\mathtt{Prf}(m, n)$ *est vraie si et seulement si* m *est le nombre de Gödel de la preuve dans* $\mathcal{N}$ *d'une formule de nombre de Gödel* n *;*
6. W *:* $W(m, n)$ *est vraie si et seulement si* m *est le nombre de Gödel d'une formule bien formée* $\mathcal{A}(x_1)$ *dans laquelle* x_1 *est libre, et* n *est le nombre de Gödel d'une preuve dans* $\mathcal{N}$ *de* $\mathcal{A}(0^{(m)})$ *;*
7. $\mathtt{D}$ *:* $\mathtt{D}(m, n)$ *est vraie si et seulement si* m *est le nombre de Gödel d'une formule bien formée* $\mathcal{A}(x_1)$ *dans laquelle* x_1 *est libre, et* n *est le nombre de Gödel de la formule* $\mathcal{A}(0^{(m)})$.

COROLLAIRE 9.8 *Comme* W *est expressible dans* $\mathcal{N}$*, il existe une formule bf* $\mathcal{W}(x_1, x_2)$ *aux deux variables libres* x_1, x_2*, telle que*

1. *si* $W(m, n)$ *est vraie dans* $\mathbb{N}$*, alors* $\underset{\mathcal{N}}{\vdash} \mathcal{W}((0)^{(m)}), (0)^{(n)})$ *;*
2. *si* $W(m, n)$ *est fausse dans* $\mathbb{N}$*, alors* $\underset{\mathcal{N}}{\vdash} {\sim}\mathcal{W}((0)^{(m)}), (0)^{(n)})$.

DÉFINITION 9.9 *On définit une formule bf fermée* $\mathcal{U}$ *en deux étapes. Soit* p *le nombre de Gödel de la formule*

$$(\forall x_2)\ {\sim}\mathcal{W}(x_1, x_2)$$

à une variable libre x_1*. Alors la formule* $\mathcal{U}$ *est la formule*

$$(\forall x_2)\ {\sim}\mathcal{W}((0)^{(p)}, x_2).$$

Le théorème de Gödel suit de la proposition suivante.

PROPOSITION 9.10 *Ni* $\mathcal{U}$*, ni* ${\sim}\mathcal{U}$ *ne sont des théorèmes de* $\mathcal{N}$.

Regardons l'interprétation de $\mathcal{U}$:

≪ *Pour tout* $n \in \mathbb{N}$*, ce n'est pas le cas que* p *est le nombre de Gödel d'une formule bf* $\mathcal{A}(x_1)$ *dans laquelle* x_1 *est libre et que* n *est le nombre de Gödel d'une preuve de* $\mathcal{A}(0^{(p)})$ *dans* $\mathcal{N}$. ≫

Mais, $\mathcal{A}(0^{(p)})$ est la formule $\mathcal{U}$. Donc, l'interprétation de $\mathcal{U}$ est :

≪ *Pour tout* $n \in \mathbb{N}$*, ce n'est pas le cas que* n *est le nombre de Gödel d'une preuve de* $\mathcal{U}$ *dans* $\mathcal{N}$. ≫

Donc, finalement, l'interprétation de $\mathcal{U}$ est :

Je ne suis pas démontrable dans $\mathcal{N}$.

On voit donc que $\mathcal{U}$ ne peut être un théorème de $\mathcal{N}$ parce qu'alors elle serait démontrable. On voit aussi que ${\sim}\mathcal{U}$ ne peut être un théorème de $\mathcal{N}$ parce que la négation de $\mathcal{U}$ dit que $\mathcal{U}$ est démontrable dans $\mathcal{N}$.