Introduction à la logique

6 décembre 2018

1 Introduction

2 Calcul propositionnel informel

3 La formalisation du calcul propositionnel

4 Calcul informel des prédicats

4.1 Langage du premier ordre

DÉFINITION 4.1 *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 4.2 *Soit $\mathcal{L}$ un langage du premier ordre. Une* formule atomique *de $\mathcal{L}$ est définie comme $A_i^k(t_1, \ldots, t_k)$, où A_i^n est un symbole de prédicat de $\mathcal{L}$ et $t_1, \ldots, t_n$ sont des termes de $\mathcal{L}$.*

DÉFINITION 4.3 *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).

DÉFINITION 4.4 *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.

DÉFINITION 4.5 *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 4.6 *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 l'interprétation de* a_i*),*
— *une collection de fonctions* $\bar{f}_i^n$, $i > 0$, $n > 0$ *(*$\bar{f}_i^n$ *est l'interprétation de* f_i^n*),*
— *une collection de relations* $\bar{A}_i^n$, $i > 0$, $n > 0$ *(*$\bar{A}_i^n$ *est l'interprétation de* A_i^n*).*

4.3 Satisfaction d'une formule bf dans une interprétation

DÉFINITION 4.7 *Soit* I *une* interprétation I *d'un langage* $\mathcal{L}$. *Une* valuation *est une fonction* v *de l'ensemble des termes de* $\mathcal{L}$ *dans* D_I *avec les propriétés suivantes*

(i) $v(a_i) = \bar{a}_i$ *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* $v(f_i^n(t_1, \ldots t_n)) = \bar{f}_i^n(v(t_1), \ldots, v(t_n))$

DÉFINITION 4.8 *Deux valuations* v *et* v' *sont* i*-équivalentes si* $v(x_j) = v'(x_j)$ *pour toute variable* x_j, *où* $j \neq i$.

DÉFINITION 4.9 *Soit* $\mathcal{A}$ *une formule bf de* $\mathcal{L}$ *et* I *une interprétation de* L. *Une valuation* v *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) v *satisfait à la formule atomique* $A_j^n(t_1, \ldots t_n)$ *si* $\bar{A}_i^n(v(t_i), \ldots, v(t_n))$ *est vraie dans* D_I.

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

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

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

PROPOSITION 4.10 *Soit* $\mathcal{A}(x_i)$ *une formule bf dans laquelle* x_i *est libre, et soit* t *une terme qui est libre pour* x_i *dans* $\mathcal{A}(x_i)$. *Soit* v *une valuation et* v' *la valuation* i*-équivalente à* v *dans laquelle* $v'(x_i) = v(t)$. *Alors,* v *satisfait à* $\mathcal{A}(t)$ *si et seulement si* v' *satisfait à* $\mathcal{A}(x_i)$.

DÉFINITION 4.11 *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* $\mathcal{A}$.

PROPOSITION 4.12 *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 4.13 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$ et* I *une interprétation de $\mathcal{L}$. Alors,* $\mathrm{I} \models \mathcal{A}$ *si et seulement si, pour toute variable* x_i, $\mathrm{I} \models (\forall x_i)\mathcal{A}$.

COROLLAIRE 4.14 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$,* I *une interprétation de $\mathcal{L}$. Alors,* $\mathrm{I} \models \mathcal{A}$ *si et seulement si, pour toute suite de variables* $y_1, \dots y_n$ *de $\mathcal{L}$,* $\mathrm{I} \models (\forall y_1) \dots (\forall y_n)\mathcal{A}$.

PROPOSITION 4.15 *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 $\mathcal{A}$.*

DÉFINITION 4.16 *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 4.17 *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 4.18 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ qui est une tautologie est vraie dans toute interprétation de $\mathcal{L}$.*

DÉFINITION 4.19 *Une formule bf $\mathcal{A}$ de $\mathcal{L}$ est* fermée *si elle ne contient pas de variables libres.*

PROPOSITION 4.20 *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 varaible libre de $\mathcal{A}$, alors ν satisfait à $\mathcal{A}$ si et seulement si w satisfait à $\mathcal{A}$.*

COROLLAIRE 4.21 *Soit* I *une interprétation de $\mathcal{L}$ et $\mathcal{A}$, une formule bf fermée de $\mathcal{L}$. Alors* $\mathrm{I} \models \mathcal{A}$ *ou bien* $\mathrm{I} \models (\sim\mathcal{A}$.

DÉFINITION 4.22 *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

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* $\mathcal{L}$. *On déduit* $\mathcal{B}$ *de* $\mathcal{A}$ *et* $\mathcal{A} \to \mathcal{B}$.

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

DÉFINITION 5.2 1. *Une* preuve 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* $\mathcal{A}_i$ *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 formuels 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 dans $K_{\mathcal{L}}$ *de* Γ.

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.

PROPOSITION 5.4 *Tout axiome obtenu à partir des schémas d'axiomes (K4), (K5) et (K6) est logiquement valide.*

THÉORÈME 5.5 *(Théorème de sûreté ou Soudness theorem) Pour toute formule bf* $\mathcal{A}$ *de* $\mathcal{L}$, *si* $\underset{K}{\vdash} \mathcal{A}$, *alors* $\mathcal{A}$ *est logiquement valide. On en déduit que* K *est cohérent.*

THÉORÈME 5.6 *(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* $\Gamma \cup \{\mathcal{A}\} \underset{K}{\vdash} \mathcal{B}$, *et la déduction ne contient aucun pas de généralisation avec une variable qui est libre dans* $\mathcal{A}$, *alors* $\Gamma \underset{K}{\vdash} (\mathcal{A} \to \mathcal{B})$.

COROLLAIRE 5.7 *Si* $\Gamma \cup \{\mathcal{A}\} \underset{K}{\vdash} \mathcal{B}$ *et si* $\mathcal{A}$ *est fermée, alors* $\Gamma \underset{K}{\vdash} (\mathcal{A} \to \mathcal{B})$.

COROLLAIRE 5.8 *Pour toutes formules bf,* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *de* $\mathcal{L}$,

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

PROPOSITION 5.9 *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *des formules bf de* $\mathcal{L}$, *et* Γ *un ensemble de formules bf de* $\mathcal{L}$. *Si* $\Gamma \underset{K}{\vdash} (\mathcal{A} \to \mathcal{B})$, *alors* $\Gamma \cup \{\mathcal{A}\} \underset{K}{\vdash} \mathcal{B}$.

5.1 Équivalence, substitution

PROPOSITION 5.10 *Soient $\mathcal{A}$ et $\mathcal{B}$ des formules bf de $\mathcal{L}$. Alors,* $\vdash_K (\mathcal{A} \leftrightarrow \mathcal{B})$ *si et seulement si* $\vdash_K (\mathcal{A} \rightarrow \mathcal{B})$ *et* $\vdash_K (\mathcal{B} \rightarrow \mathcal{A})$.

DÉFINITION 5.11 *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 5.12 *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 5.13 *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* $\vdash_K ((\forall x_i)\mathcal{A}(x_i) \leftrightarrow (\forall x_j)\mathcal{A}(x_j))$.

PROPOSITION 5.14 *Soit $\mathcal{A}$ une formule bf de $\mathcal{L}$ dont les variables libres sont $y_1, \ldots, y_n$. Alors* $\vdash_K \mathcal{A}$ *si et seulement si* $\vdash_K (\forall x_1) \ldots (\forall x_n)\mathcal{A}$.

DÉFINITION 5.15 *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 5.16 *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,*

$$\vdash_K ((\mathcal{A} \leftrightarrow \mathcal{B})' \rightarrow (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)).$$

COROLLAIRE 5.17 *Soit $\mathcal{A}, \mathcal{B}, \mathcal{A}_0, \mathcal{B}_0$ comme dans la proposition ci-dessus. Si* $\vdash_K (\mathcal{A} \leftrightarrow \mathcal{B})$, *alors* $\vdash_K (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)$.

COROLLAIRE 5.18 *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* $\vdash_K (\mathcal{A}_0 \leftrightarrow \mathcal{B}_0)$.

5.2 Forme prénexe

PROPOSITION 5.19 *Soient $\mathcal{A}$ et $\mathcal{B}$ des formules bf de $\mathcal{L}$.*

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

$$\vdash_K ((\forall x_i)(\mathcal{A} \rightarrow \mathcal{B}) \leftrightarrow (\mathcal{A} \rightarrow (\forall x_i)\mathcal{B})),$$

et

$$\vdash_K ((\exists x_i)(\mathcal{A} \rightarrow \mathcal{B}) \leftrightarrow (\mathcal{A} \rightarrow (\exists x_i)\mathcal{B})).$$

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

$$\vdash_K ((\forall x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow ((\exists x_i)\mathcal{A} \to \mathcal{B})),$$

et

$$\vdash_K ((\exists x_i)(\mathcal{A} \to \mathcal{B}) \leftrightarrow ((\forall x_i)\mathcal{A} \to \mathcal{B})).$$

LEMME 5.20 *Soient $\mathcal{A}$ et $\mathcal{B}$ des formules bf de $\mathcal{L}$, et x_i une variable. Alors,*

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

DÉFINITION 5.21 *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 5.22 *Pour toute formule bf $\mathcal{A}$ de $\mathcal{L}$, il existe une formule $\mathcal{B}$ sous forme prénexe qui est équivente de manière prouvable à $\mathcal{A}$.*

DÉFINITION 5.23 *(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.

5.3 Le théorème d'adéquation pour K

DÉFINITION 5.24 *Une* extension *de* K *est un système formel obtenue 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 5.25 *Un* système du premier ordre *est une extension de $K_{\mathcal{L}}$ pour un langage du premier ordre $\mathcal{L}$.*

DÉFINITION 5.26 *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 5.27 *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 cohérent.*

DÉFINITION 5.28 *Un système du premier ordre* S *est* complet *si, pour toute formule fermée bf* $\mathcal{A}$*, soit* $\vdash_{S} \mathcal{A}$*, soit* $\vdash_{S} (\sim\mathcal{A})$.

PROPOSITION 5.29 *Soit* S *un système cohérent du premier ordre. Alors, il existe une extension cohérente de* S *qui est complète.*

PROPOSITION 5.30 *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 5.31 *(Théorème d'adéquation) Si* $\mathcal{A}$ *est une formule bf de* $\mathcal{L}$ *qui est logiquement valide, alors* A *est un théorème de* $K_{\mathcal{L}}$.

5.4 Modèles

DÉFINITION 5.32 *(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 5.33 *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 5.34 *Un système du premier ordre* S *est cohérent si et seulement si il a un modèle.*

PROPOSITION 5.35 *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 5.36 *(Théorème de Löwenheim-Skolem) Si un système du premier ordre a un modèle, alors il a un modèle dénombrable.*

THÉORÈME 5.37 *(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 5.38 *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.*

6 Quelques systèmes formels du premier ordre

6.1 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 6.1 *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 6.2 *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 6.3 *Soit* S, *un système du premier ordre cohérent avec égalité. Alors,* S *a un modèle dans lequel l'interprétation de* $\mathcal{A}_1^2$ *est* $=$. *Un tel modéle est appelé* modèle normal *de* S.

6.2 La théorie des groupes

Le langage du premier ordre, $\mathcal{L}_G$, approprié à la théorie des groupes a les symboles particuliers suivants :

— 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 $=$.

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

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

(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)

6.3 L'arithmétique du premier ordre

Le langage du premier ordre, $\mathcal{L}_N$, approprié à l'arithmétique a les symboles particuliers suivants :

— 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 $=$.

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

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

6.4 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 les symboles particuliers suivants :

— 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.

NOTATION 6.4 — *On introduit le symbole $\subseteq$ comme abbréviation : ainsi,* $(t_1 \subseteq t_2)$ *signifie* $(\forall x_1)(x_1 \in t_1 \to x_1 \in t_2)$.

— *On introduit $\exists_1$ comme abbréviation signifiant « Il existe un et un seul ». Ainsi* $(\exists_1 x_1)\mathcal{A}(x_1$ *signifie* $((\exists x_1)\mathcal{A}(x_1)) \wedge ((\forall x_2)A(x_2) \to (x_2 = x_1)))$.

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

(ZF1) $(x_1 = x_2 \leftrightarrow (\forall x_3)(x_3 \in x_1 \leftrightarrow x_3 \in x_2))$. (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) $(\forall x_1)(\exists_1 x_2)\mathcal{A}(x_1, x_2) \to (\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathcal{A}(x_6, x_5)))$, 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 remplacement : l'ensemble x_4 est formé des images de tous les éléments de x_3 par la fonction déterminée par $\mathcal{A}$.)

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

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

On 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 6.5 *(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.*

PROPOSITION 6.6 *L'axiome (ZF2) et le schéma d'axiome de remplacement (ZF6) permettent de montrer que le schéma d'axiomes de compréhension (aussi appelé schéma d'axiomes de séparation) est un théorème de ZF : si $\mathcal{A}$ est une formule bf de $\mathcal{L}_{ZF}$ contenant une variable libre, alors*

$$\vdash_{ZF} (\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (x_3 \in x_1 \wedge \mathcal{A}(x_3)).$$

7 Fonctions et relations récursives, ensembles récursifs

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 7.1 *L'ensemble des fonctions* récursives *est l'ensemble des fonctions obtenues des fonctions de base par un nombre fini d'applications des trois opération 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 *: si* $g : \mathbb{N}^{k+1} \to \mathbb{N}$ *est 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 $f(n_1, \ldots, n_k) = \mu n[g(n_1, \ldots, n_k, n) = 0]$.
   On a une définition équivalente :soit R *une relation à* k *entrées telle que pour tout* $n_1, \ldots, n_k \in \mathbb{N}$ *il existe* $n \in \mathbb{N}$ *tel que* $R(n_1, \ldots, n_k, n)$ *est vrai. Alors, la fonction* $f : \mathbb{N}^k \to \mathbb{N}$ *obtenue de* g *par l'opérateur plus petit nombre est définie ainsi*

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

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

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

DÉFINITION 7.2 *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 7.3 *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 7.4 *Une relation sur* $\mathbb{N}$ *à* k *entrées est* récursive *si sa fonction caractéristique est récursive. Un sous-ensemble de* $\mathbb{N}^k$ *est récursif si sa fonction caractéristique est récursive.*

PROPOSITION 7.5 *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 7.6 *Tout singleton de* $\mathbb{N}$ *est un sous-ensemble récursif de* $\mathbb{N}$*.*

Les fonctions suivantes sont récursives :

$$\begin{aligned}
\mathrm{add}(m,n) &= m+n,\\
\mathrm{mult}(m,n) &= mn,\\
\exp(m,n) &= m^n,\\
\mathrm{sous}(m,n) &= \max(m-n,0),\\
\mathrm{sgn}(m) &= \begin{cases} 0, & m=0,\\ 1, & m\neq 0,\end{cases}\\
\mathrm{cosgn}(m) &= \begin{cases} 1, & m=0,\\ 0, & m\neq 0,\end{cases}\\
\mathrm{rest}(m,n) &= \begin{cases} 0, & n=0,\\ \text{reste de la division de } m \text{ par } n, & n\neq 0.\end{cases}
\end{aligned}$$

Soient $R_1(x,y)$, $R_2(x,y)$ et $R_3(x,y)$ les trois relations primitives récursives $\ll x=y\gg$, $\ll x<y\gg$et $\ll x>y\gg$ respectivement. Leurs fonctions caractéristiques sont :

$$\begin{array}{lcl}
\mathrm{eg}(x,y) := C_{R_1}(x,y) &=& \mathrm{sgn}(\mathrm{sous}(x,y)+\mathrm{sous}(y,x)),\\
\mathrm{pp}(x,y) := C_{R_2}(x,y) &=& \mathrm{cosgn}(\mathrm{sous}(y,x)),\\
\mathrm{pg}(x,y) := C_{R_3}(x,y) &=& \mathrm{cosgn}(\mathrm{sous}(x,y)).
\end{array} \tag{7.1}$$

8 Vers le théorème d'incomplétude de Gödel

Nombre de Gödel d'un symbole de $\mathcal{L}$: ce sera un nombre impair

- $g(() = 3$,
- $g()) = 5$,
- $g(,) = 7$,
- $g(\sim) = 9$,
- $g(\rightarrow) = 11$,
- $g(\forall) = 13$,
- $g(x_k) = 7+8k, \quad k=1,2,\ldots,$
- $g(a_k) = 9+8k, \quad k=1,2,\ldots,$
- $g(f_k^n) = 11+8\times(2^n\times 3^k), \quad n=1,2,\ldots,k=1,2,\ldots$
- $g(A_k^n) = 13+8\times(2^n\times 3^k), \quad n=1,2,\ldots,k=1,2,\ldots$

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 *exprimables* dans $\mathcal{N}$.

8.1 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 8.1 *Si* $m, n \in \mathbb{N}$, *alors*

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

DÉFINITION 8.2 *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* $\vdash_{\mathcal{N}} \mathcal{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$ *;*
2. *si* $R(n_1, \ldots, n_k)$ *est fausse dans* $\mathbb{N}$, *alors* $\vdash_{\mathcal{N}} \sim \mathcal{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$.

REMARQUE 8.3 *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 8.4 *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* $n_1, \ldots, n_k$

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

PROPOSITION 8.5 *Une fonction ou une relation sur les nombres naturels est expressible dans* $\mathcal{N}$ *si et seulement si elle est récursive.*

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

THÉORÈME 8.6 (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 8.7 *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. Prf *:* $\mathrm{Prf}(n)$ *est vraie si et seulement si* n *est le nombre de Gödel d'une preuve dans* $\mathcal{N}$ *;*
5. Pf *:* $\mathrm{Prf}(m,n)$ *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* $\mathcal{A}(0^{(m)})$.

COROLLAIRE 8.8 *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* $\vdash_{\mathcal{N}} \mathcal{W}((0)^{(m)}),(0)^{(n)})$ *;*
2. *si* $W(m,n)$ *est fausse dans* $\mathbb{N}$*, alors* $\vdash_{\mathcal{N}} \sim\mathcal{W}((0)^{(m)}),(0)^{(n)})$.

DÉFINITION 8.9 *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 8.10 *Ni* $\mathcal{U}$*, ni* $\sim\mathcal{U}$ *ne sont des théorèmes de* $\mathcal{N}$.