

**Faculté des Mathématiques et de l'Informatique
Department of Mathematics.**

polycopié de

Logique mathématique

Auteur | **Dr.kheir.saadaoui- University
de Msila-**

mail | **kheir.saadaoui@univ-msila.dz**

2022/2023

Table des matières

1	Introduction	1
1.1	Introduction	1
1.1.1	Objectifs de l'enseignement	1
1.2	Éléments du langage mathématiques	1
1.3	Rédaction de preuves mathématiques	3
1.3.1	Le raisonnement déductif	3
1.3.2	Le raisonnement par l'absurde	3
1.3.3	Le raisonnement par contra-position	4
1.4	Théories mathématiques	4
1.5	Connecteurs logiques	6
1.6	Quantificateurs logiques	8
1.6.1	Règles de négation	9
1.7	Méthodes de démonstration	9
2	Calcul propositionnel	10
2.1	Alphabet et mot	10
2.2	Syntaxe des formules propositionnelles	11
2.3	Principe d'indication sur l'ensemble des formules	14
2.4	L'interprétation d'une formule logique	15
2.4.1	Arbre de décomposition d'une formule	15
2.4.2	Substitution dans un formule	18
2.5	Sémantique	20
2.6	Tautologie et équivalences logiques	24
2.6.1	Formes normales	28
2.7	Systèmes complets de connecteurs	28

2.7.1	Formes normales	30
2.8	Système complets de connecteur	34
2.8.1	Les théories	34
3	Calcul des prédicats	36
3.1	Syntaxe du calcul des prédicats	36
3.1.1	Alphabet des premier ordre	36
3.1.2	Termes	37
3.1.2.1	Le hauteur d'un terme	38
3.1.3	Formule	38
3.2	Variable libre et lié	39
3.2.1	Portée d'un quantificateur	40
3.2.2	Substitution dans les termes	40
3.2.2.1	Notation	40
3.2.3	Substitution dans les formules	41
3.2.3.1	Notation	41
3.3	Sémantique du calcul des prédicats	41
3.3.1	Définition d'une structure	42
3.3.2	Satisfaction d'une formule dans un structure	45
3.3.2.1	Conséquence et équivalence universelle	47
4	Axiomatique de Z F et AC	50
4.1	Paradoxes, théorie naïve des ensembles	50
4.1.1	Paradoxe de Russel	51
4.1.1.1	Énoncé du paradoxe	51
4.1.1.2	Solutions du paradoxe	51
4.1.2	Paradoxe du coiffeur (barbier)	52
4.1.2.1	Énoncé du paradoxe	52
4.1.3	Paradoxe du menteur	53
4.1.3.1	Énoncé du paradoxe	53
4.1.3.2	Solution du paradoxe	54
4.1.4	Paradoxe de Cantor	55
4.1.4.1	Énoncé du paradoxe	55
4.1.4.2	Paradoxe de Cantor et paradoxe de Russell	56
4.1.5	Paradoxe de Richard	57

4.1.5.1	Énoncé du paradoxe	57
4.1.5.2	Solution du paradoxe	58
4.1.6	Paradoxe de Grelling	59
4.1.6.1	Énoncé du paradoxe	59
4.1.6.2	Solution du paradoxe	60
4.2	Axiomes de Zermelo-Fraenkel (ZF)	60
4.2.1	Axiome d'extentionnalité	61
4.2.2	Axiomes de construction	61
4.2.2.1	Axiome de la paire	61
4.2.2.2	Axiome de la réunion	61
4.2.2.3	Axiome des parties	62
4.2.2.4	Schéma d'axiomes de compréhension	62
4.2.2.5	Axiome de remplacement	63
4.2.2.6	Axiome de l'infini	64
4.2.2.7	Axiome de fondation	65
4.2.3	Théorie de Zermelo	65
4.2.4	Théorie de Zermelo-Fraenkel	65
4.3	Axiome du choix (AC)	66
4.3.1	Axiome du choix	66
4.3.2	Quelques formes équivalentes	66
4.3.3	Lemme de Zorn	67
4.3.4	Applications de l'axiome du choix	69
4.3.5	Indépendance de l'axiome du choix	70
4.4	Exercices	71
5	Bon ordre et preuve par récurrence	73
5.1	Preuve par récurrence	73
5.1.1	Preuve par récurrence simple	73
5.1.2	Schéma de preuve par le principe du bon ordre	74
5.1.3	Preuve par récurrence généralisée	76
5.1.4	Preuve par récurrence forte	77
5.1.5	Cas particulier de preuve par récurrence (récurrence de Cauchy)	78
5.1.6	Preuve de l'inégalité de Cauchy Scwhartz par récurrence.	78
5.2	Ordre bien fondé	78
5.2.1	Ordre et ordre strict	78

5.2.2	Minorants, majorants, minimaux et maximaux	80
Bibliographie		82

Introduction

1.1 Introduction

1.1.1 Objectifs de l'enseignement

Acquérir les fondements du raisonnement mathématique, Acquérir les fondements de la théorie des ensembles et acquérir les éléments de la rédaction des preuves mathématiques.

1.2 Éléments du langage mathématiques

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

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

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

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

Proposition 1.1 (ou assertion ou affirmation). Une proposition est un énoncé pouvant être vrai ou faux. Par exemple, « tout nombre premier est impair » et « tout carré de réel est un réel positif » sont deux propositions. Il est facile de démontrer que la première est fausse et la deuxième est vraie. Le mot proposition est clair : on propose quelque chose, mais cela reste à démontrer.

Théorème 1.1. Un théorème est une proposition vraie (et en tout cas démontrée comme telle). Par abus de langage, le mot proposition désigne souvent, dans la pratique des cours de mathématiques, un théorème intermédiaire ou de moindre importance, et même on a tendance à appeler proposition la plupart des théorèmes pour réserver le mot théorème aux plus grand d'entre eux (théorème de Pythagore, ...). C'est d'ailleurs ce dernier point de vue que nous adopterons dans les chapitres ultérieurs (mais pas dans ce premier chapitre où le mot « proposition » aurait alors deux significations différentes).

Corolaire. Un corolaire à un théorème est un théorème qui est conséquence de ce théorème. Par exemple, dans le chapitre « continuité », le théorème des valeurs intermédiaires dit que l'image d'un intervalle de \mathbb{R} par une fonction continue à valeurs réelles, est un intervalle de \mathbb{R} . Un corollaire de ce théorème affirme alors que si une fonction définie et continue sur un intervalle de \mathbb{R} à valeurs réelles, prend au moins une valeur positive et au moins une valeur négative alors cette fonction s'annule au moins une fois dans cet intervalle.

Lemme 1.1. Un lemme est un théorème préparatoire à l'établissement d'un théorème de plus grande importance.

Conjecture. Une conjecture est une proposition que l'on suppose vraie sans parvenir à la démontrer. Les conjectures sont le moteur du progrès des mathématiques. Tel ou tel mathématicien a eu l'impression que tel ou tel résultat important était vrai et l'a énoncé sans pouvoir le démontrer, laissant à l'ensemble de la communauté mathématique le soin de le confirmer par une démonstration convaincante ou de l'infirmier. Les conjectures suivantes sont célèbres :

- (conjecture de Fermat) Si n est un entier supérieur ou égal à 3, il n'existe pas d'entiers naturels tous non nuls x, y et z tels que $x^n + y^n = z^n$ (cette conjecture date du XVII

siècle et il a été démontré récemment que ce résultat était vrai).

Définition 1.1. Une définition est un énoncé dans lequel on décrit les particularités d'un objet.

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

1.3 Rédaction de preuves mathématiques

1.3.1 Le raisonnement déductif

Le schéma du raisonnement déductif est le suivant :

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

Un résultat connu comme étant vrai (c'est à dire un théorème) ne peut entraîner qu'un autre résultat vrai. Cette règle est connue sous le nom de "modus ponens". C'est le raisonnement de base que vous reproduirez un grand nombre de fois. Et même, vous tiendrez ce raisonnement tellement de fois (ou encore, vous serez tellement souvent dans la situation où l'hypothèse P est vraie) que vous risquez à terme de commettre une confusion entre la phrase simple « $P \Rightarrow Q$ est vraie » et la phrase plus complète « P est vraie et $P \Rightarrow Q$ est vraie ». Seule la deuxième permet d'affirmer que Q est vraie.

Sachant de plus que l'implication est transitive, une démonstration prend très souvent la forme suivante : P est vraie et $P \Rightarrow Q \Rightarrow R \Rightarrow \dots \Rightarrow S \Rightarrow T$ est vraie, et on a donc montré que T est vraie.

1.3.2 Le raisonnement par l'absurde

On veut montrer qu'une proposition P est vraie. On suppose que c'est sa négation \bar{P} qui est vraie et on montre que cela entraîne une proposition fausse. On en conclut que P est vraie (puisque Q est fausse, l'implication $\bar{P} \Rightarrow Q$ ne peut être vraie que si \bar{P} est fausse ou encore si P est vraie). Le schéma du raisonnement par l'absurde est le suivant :

Quand $\bar{P} \Rightarrow Q$ est une proposition vraie, et Q est une proposition fausse, on peut affirmer que

P est une proposition vraie.

Exemple. Montrons que $\sqrt{2}$ est irrationnel. Supposons par l'absurde que $\sqrt{2} \in \mathbb{Q}$. Il existe alors deux entiers naturels non nuls a et b tels que $\sqrt{2} = \frac{a}{b}$ ou encore $a^2 = 2b^2$. Maintenant, dans la décomposition en facteurs premiers de l'entier a^2 (qui est à l'évidence supérieur à 2), le nombre premier 2 apparaît à un exposant pair (si $a = 2^\alpha \dots$ alors, $a^2 = 2^{2\alpha}$) alors qu'il apparaît à un exposant impair dans $2b^2$ (si $b = 2^\beta \dots$ alors, $2b^{2\beta+1} \dots$). Si l'on admet l'unicité de la décomposition en facteurs premiers d'un entier naturel supérieur à 2 (unicité qui sera démontrée plus tard dans ce cours), l'égalité des nombres a^2 et $2b^2$ est donc impossible. Par suite, l'hypothèse faite ($\sqrt{2} \in \mathbb{Q}$) est absurde et on a montré (par l'absurde) que $\sqrt{2} \notin \mathbb{Q}$.

1.3.3 Le raisonnement par contra-position

Le schéma est le suivant :

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

$\bar{Q} \Rightarrow \bar{P}$ est une proposition vraie.

Exemple. Soient k et k' deux entiers naturels non nuls. Montrons que $(kk' = 1 \Rightarrow k = k' = 1)$.

Supposons que $k \neq 1$ ou $k' \neq 1$. Alors, on a $(k \geq 2 \text{ et } k' \geq 1)$ ou $(k \geq 1 \text{ et } k' \geq 2)$. Dans les deux cas, on a $kk' \geq 2$ et en particulier, $kk' \neq 1$. Donc,

$$(k \neq 1 \text{ ou } k' \neq 1) \Rightarrow (kk' \neq 1)$$

- Par contra-position, on a montré que

$$(kk' = 1) \Rightarrow (k = 1 \text{ et } k' = 1)$$

1.4 Théories mathématiques

A la base d'une théorie mathématique il y'a les axiomes et les définitions :

1.4. Théories mathématiques

Définition1.2 (Axiome) Un axiome est un énoncé mathématique que F on admet sans démonstration.

Exemple.

- Axiome d'Euclide sur les droites parallèles.
- Axiome de Pasch sur l'intersection d'un triangle et une droite.
- Axiome de Hilbert de la géométrie euclidienne.
- axiome d'Archimède sur les nombres réels.
- Axiome de Peano sur les entiers naturels.
- Axiome de Zermelo-Fränkel sur la théorie des ensembles.
- Axiome de Zorn (dit axiome de choix).

Définition1.3 On pose une définition de façon arbitraire pre désigner un objet mathématique.

Exemple.

- Les définitions d'un nombre.
- Les définitions d'une application.
- Les définitions d'une dérivée.

Dans une théorie mathématique on trouve des propositions (assertions), des prédicats, des théorèmes, des lemmes et des conjectures :

Définition1.4 (Assertion) Une assertion est un énoncé mathématique on peut attribuer la valeur de vérité : vrai (1) ou faux (0) mais jamais les deux à la fois.

Exemple.

- L'énoncé "Alger est la capitale de l'Algérie" est vrai.
- L'énoncé "24 est un multiple de 2" est vrai.
- L'énoncé "19 est un multiple de 2" est faux.

Définition1.5 (Prédicat) Un prédicat est une assertion contenant des variables.

Exemple.

- L'énoncé suivant : $P(n)$: " n est un multiple de 2 " est un prédicat car il devient une assertion quand on donne une valeur à n ;
- $p(10)$: "10 est un multiple de 2 " est une assertion vraie,
- $p(11)$: "11 est un multiple de 2 " est une assertion fausse.
- $q(x, A)$: " $x \in A$ " est un prédicat à deux variables ; $q(1, \mathbb{N})$ est vraie, $q(\sqrt{2}, \mathbb{Q})$ est fausse.

Définition 1.6 (Lemme) Un lemme est un résultat d'importance malaxeur.

Définition 1.7 (Théorème) Un théorème est un résultat d'une importance majeure.

Définition 1.8 (Conjecture) Une conjecture est une proposition q l'on a vérifiée dans plusieurs cas, mais que l'on a pas encore réussi démontrer.

Exemple.

- La conjecture de Fermat sur l'équation diophantienne suivante d'inconnues x, y et z : $n \in \mathbb{N}, x^n + y^n = z^n$. Il affirme qu' n'existe aucune solution non triviale si le paramètre $n > 2$ Mais il fallut attendre 1996, et le mathématicien anglais Andrem-Wiles, pour trouver une réponse définitive.
- La conjecture de Riemann sur les zéros non triviaux de la fonction Zéta : $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ (conjecture non résolue).
- La conjecture de Bertrand sur les nombres premiers dans les intervalles $[n, 2n]$.

1.5 Conneteurs logiques

Soient P et Q deux propositions :

Énoncé. non P

Notation. $\neg P$

L'assertion $\neg P$ est vraie signifie que P est fausse.

Énoncé. P et Q

Notation. $P \wedge Q$

L'assertion $P \wedge Q$ est vraie si P et Q le sont ; $P \wedge Q$ est fausse arien.

Énoncé. P ou Q

Notation. $P \vee Q$

L'assertion $P \vee Q$ est vraie si l'une (au moins) des deux assertions P su Q est vraie, $P \vee Q$ est fausse si P et Q sont fausses.

Énoncé. $\left\{ \begin{array}{l} \text{si } P, \text{ alors } Q \\ P \text{ implique } Q \\ P \text{ est une condition suffisante de } Q \\ Q \text{ est une condition nécessaire de } P \end{array} \right\}$

Notation. $p \implies q, p \rightarrow q$

L'assertion $P \implies Q$ est vraie signifie qu'il est exclu que P soit sans que Q ne le soit.

Énoncé. $\left\{ \begin{array}{l} P \text{ équivant à } Q \\ P \text{ si et seulement si } Q \end{array} \right\}$

Notation. $P \iff Q, P \longleftrightarrow Q, P \equiv Q$

L'assertion $P \iff Q$ est vraie signifie que :

$(P \implies Q)$ et $(Q \implies P)$ sont vraies.

on résume cela dans les tables de vérité ci-dessous

$\neg P$	P
0	1
1	0

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

Propriétés1.1

1.5. Conneteurs logiques

- $P \wedge (Q \vee Q) \equiv (P \wedge Q) \vee (P \wedge Q)$; double distributivité de "et" et "ou".
- $P \vee (Q \wedge Q) \equiv (P \vee Q) \wedge (P \vee Q)$.
- $(P \implies Q) \equiv (\neg Q \implies \neg P)$; contraposée.
- $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$; loi de De Morgan.
- $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.
- $P \implies Q \equiv \neg P \vee Q$.
- $\neg(P \implies Q) \equiv P \wedge \neg Q$.

1.6 Quantificateurs logiques

Énoncé. Quel que soit ou pour tout.

Notation. $\forall (\forall x p(x))$

Énoncé. Il existe au moins ou il existe.

Notation. $\exists (\exists x p(x))$

Exemple.

- La proposition $\forall x \in [-3, 1], x^2 + 2x - 3 \leq 0$ est vraie.
- La proposition $\forall n \in \mathbb{N}, (n^2 \text{ pair}) \implies (n \text{ pair})$ est vraie.
- La proposition $\exists x \in \mathbb{R}, x^2 = 4$ est vraie.
- La proposition $\exists! x \in \mathbb{R}_+^*, \ln x = 1''$ est vraie.

Remarque.

- La proposition $\exists x \in E, P(x)$ signifie que

$$\exists x((x \in E) \wedge P(x))$$

et se lit comme suit : "Il existe un élément x appartenant tel que $P(x)$ soit vraie".

- La proposition $\forall x \in E, P(x)$ signifie que

$$\forall x(x \in E \implies P(x))$$

et se lit comme suit : "Si pour tout (ou quel que soit) x appartenant à $E, P(x)$ est vraie".

- S'il existe un et un seul x dans E , tel que $P(x)$ soit vraie ; on pourra écrire $\exists!x \in E, P(x)$.
- Si $\forall x \in E, P(x)$ est vraie alors $\exists x \in E, P(x)$ est vraie.

Remarque. (Attention) $\exists!$ ne désigne pas un quantificateur. En effet :

$$(\exists!x \in E, P(x)) \equiv (R_1 \wedge R_2) \text{ où } R_1 \equiv (\exists x \in E, P(x))$$

et

$$R_2 \equiv (\forall x \in E, \forall x' \in E, [(P(x) \wedge P(x')) \implies x = x'])$$

1.6.1 Règles de négation

Soit $P(x)$ un prédicat sur E . De manière évidente on a :

- $\neg(\forall x \in E, P(x)) \equiv \exists x \in E, \neg P(x)$.
- $\neg(\exists x \in E, P(x)) \equiv \forall x \in E, \neg P(x)$.

Exemple.

- La négation de $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}_+, 1 + nx \leq (1 + x)^n$ est $\exists n \in \mathbb{N}, \exists x \in \mathbb{R}_+, 1 + nx > (1 + x)^n$.
- La négation de $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 5$ est $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \neq 5$.

Remarque. (Attention) On vérifie aussi que l'on a :

$$\neg(\exists!x \in E, p(x)) \equiv (\neg R_1 \vee \neg R_2)$$

avec $R_1 =$ existence et $R_2 =$ unicité.

- On peut permuter deux quantificateurs identiques.
- Ne pas permuter deux quantificateurs différents.

1.7 Méthodes de démonstration

Faire une démonstration (preuve ou raisonnement), c'est réaliser - processus qui permet de passer de propositions supposées vraies a comme hypothèse à une proposition appelée conclusion et ce en suivant les règles de logique.

Calcul propositionnel

2.1 Alphabet et mot

Soit A un ensemble quelconque (fini ou infini) les éléments de A seront appelés des lettres et A lui-même sera appelé alphabet.

Définition 2.1. Un mot sur l'alphabet A est une suite finie d'éléments de A

$$U = U_1 U_2 \dots U_n$$

n est la longueur du mot U .

L'ensemble des mots sur A sera noté A^* .

Sur A^* on définit l'opération de concaténation :

$$A^* A^* \longrightarrow A^*$$

$$(U, V) \longmapsto U \cdot V = U_1 \cdot U_2 \dots U_n \cdot V_1 \cdot V_2 \dots V_m$$

Avec : $U = U_1 \dots U_n$ et $V = V_1 \dots V_m$

La longueur d'un mot définit une application :

$$l : A^* \longrightarrow \mathbb{N}$$

$$U \longmapsto l(u) = n = \text{longueur de } u$$

la concaténation est une opération associative et pour élément neutre le mot vide ϵ :

$$u \cdot \epsilon = \epsilon \cdot u = u$$

Autrement dit A^* mono ide.

Définition2.2. On dit que $a \in A$ a une occurrence dans le mot u si a est une lettre de u , i.e :

si $u = u_1u_2 \dots u_n$ donc : $\exists K \in \{1, 2, \dots, n\}$ t.q : $a = u_k$

Remarque. il peut y avoir plusieurs occurrences de a^* dans u .

Exemple.

$$A = \{a, b \dots x, y, z\}$$

$$u = abaab$$

$$l(u) = 5$$

a átrois occurrences dans u et b en a deux

Proprietés2.1

- $l(uv) = l(u) + l(v)$
- $uv = uv \Rightarrow v = w$
- $uv = vw \Rightarrow u = w$

Définition2.3. le mot u est un préfixe du mot v s'il existe un mot de w t.q : $v = uw$. u est un suffixe de v si $\exists w \setminus v = wu$

2.2 Syntaxe des formules propositionnelles

Définition2.4. les connecteur propositionnels sont les symboles :

\neg : Pour la negation (non)

\wedge : pour la conjonction (et)

\vee : pour la disjonction (ou)

\longrightarrow : pour l'implication

\longleftrightarrow : pour l'équivalence

Soit P un ensemble non vide des propositions élément ou atomiques, les éléments de P seront noté : p, q, r, s .

Remarque.

1- En logique élémentaire une proposition est une énoncé qui sera á communiquer des faits : $p = \text{il peut}, q = \text{il fait beau}$

2- P contient pas les connecteurs $\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$; on considère l'alphabet suivante :

$$A = P \cup \{ \neg, \wedge, \vee, \longrightarrow, \longleftrightarrow \} \cup \{ (,) \},$$

Soit A^* l'ensemble des mots sur A

$$(p \longrightarrow q) \in A^*$$

$$(p \in A^*$$

$$p \in A^*$$

$$() \in A^*$$

$$(pq\wedge) \in A^*$$

Définition 2.5. L'ensemble \mathcal{F} des formules propositionnelles est plus petit sous ensemble de A^* qui vérifies :

1- $P \subseteq \mathcal{F}$ (toute proposition élémentaire est une forme).

2- $F \in \mathcal{F} \implies \neg F \in \mathcal{F}$

3- $F, G \in \mathcal{F} \implies (F * G) \in \mathcal{F}$ avec $*$, $=$, \wedge , \vee , \longrightarrow , \longleftrightarrow

Remarque.

1- Les formule sont des mots i.e des suit de symboles sans aucune signification l'attribution d'un sens i.e d'une valeur "vrais " ou "fausse" a une formule constitue le sémantique de formule .

2- Le terme " plus petit" est à prendre au sens de l'inclusion des ensembles de \mathcal{F} est donc l'intersection de toutes les parties de A^* qui vérifient les propriétés 1,2 est cette intersection est non vide puisque A^* lui même vérifie ces propriétés donc : $\mathcal{F} = \bigcap_{Y \subseteq A^*} Y$ et Y vérifie 1,2 et 3 .

Exemples.

- $(\neg p \longrightarrow q)$ est une formule .
- $(p \wedge q \wedge r)$ n'est pas une formule.

2.2. Syntaxe des formules propositionnelles

- $(\neg p \longrightarrow q)$ est une formule .
- p est une formule
- $(p \longrightarrow q \vee r)$ n'est pas une formule.

Définition2.6. La longueur d'une formule F est le nombre des lettres dans $Fl(F) = \#$ lettres dans F

Exemple. $F = (p \wedge q)$ $l(F) = 5, F = p; l(F) = 1.$

Remarque : Il n'y a pas de formule de longueur 0

- Il est possible de donner de l'ensemble \mathcal{F} une description plus explicite : nous allons pour cela définir, par récurrence, une suite $(\mathcal{F}_n)_{n \in \mathbb{N}} \in \mathbb{N}$ de parties de A^* , on pose $\mathcal{F}_0 = p$ et pour chaque n

$$\mathcal{F}_{n+1} = \mathcal{F}_n \cup \{ \lceil F, F \in \mathcal{F}_n \} \cup \{ (F * G); F, G \in \mathcal{F}_n, * \in \{ \wedge, \vee, \longrightarrow, \longleftarrow \} \}$$

On notera que la suite que la suite $(\mathcal{F}_n)_{n \in \mathbb{N}}$ est croissante on a $\mathcal{F}_n \subseteq \mathcal{F}_{n+1}$

(pour $n \leq m$, on a $\mathcal{F}_n \subseteq \mathcal{F}_m$)

Proposition2.1. $\mathcal{F} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$

Preuve. Posons $Z = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$:

Z est une partie de A^* qui vérifie les propriétés 1,2 et 3 donc $\mathcal{F} \subseteq Z$ (car \mathcal{F} est le plus petit sous ensemble de A^* vérifier 1,2 et 3)

$Z \subseteq \mathcal{F}$?

On montre par récurrence que, pour chaque entier n , on a $\mathcal{F}_n \subseteq \mathcal{F}$?

Si $n = 0, p = \mathcal{F}_0 \subseteq \mathcal{F}$ par définition, on suppose (hypotèse de récurrence) $\mathcal{F}_n \subseteq \mathcal{F}$ alors $\mathcal{F}_{n+1} \subseteq \mathcal{F}$ d'après la définition de \mathcal{F}_{n+1} et les propriétés de stabilité de \mathcal{F}

Définition2.7. La hauteur d'une formule $F \in \mathcal{F}$ est le plus petit des entiers n tels que :

$F \in \mathcal{F}_n$. Elle noté $h[F]$

$$h(F) = \min \{ n / F \in \mathcal{F}_n \}$$

Exemple.

- $F = p, h(F) = 0$

- $F = (p \wedge q), \quad h(F) = 1$
- $F = \lceil p, \quad h(F) = 1.$
- $F = (\lceil p \wedge q); \quad h(F) = 2.$

2.3 Principe d'indication sur l'ensemble des formules

Supposons que nous voulions démontrer qu'une certaine proposition $Q(F)$ est vérifiée par toute $F \in \mathcal{F}$. Nous pouvons pour cela faire un raisonnement par récurrence (au sens usuel) sur la hauteur de F : nous serons alors amenés à montrer, d'abord que $Q(F)$ est vraie pour toute formule F appartenant a \mathcal{F}_0 puis que si $Q(F)$ est vraie pour toute $F \in \mathcal{F}_n$, alors $Q(F)$ est également vraie pour toute $F \in \mathcal{F}_{n+1} \forall n \in \mathbb{N}$.

Principe. Si Q vérifie :

- 1) $Q(p)$ vraie $\forall p \in P$ i.e ($Q(F)$ vrais par $F \in \mathcal{F}_n$).
- 2) $Q(F)$ vraie $\Rightarrow Q(\lceil F)$ vraie.
- 3) $Q(F)$ vraie et $Q(G)$ vraie $\Rightarrow Q(F * G)$ vraie $*, \wedge, \vee, \Rightarrow, \Leftarrow$, alors $Q(F)$ est vraie $\forall F \in \mathcal{F}$.

Exemple. $Q(F)$: "F a tout de parenthèses ouvrantes que fermantes " i.e : $Q(F) = 'O(F) = f(F)''$ on montre que $Q(F)$ est vraie, $\forall F \in \mathcal{F}$ pour cela posons : $O(F) = \#$ parenthèses ouvrantes, $f(F) = \#$ parenthèses fermantes.

- 1) Soit $F = p \in P, \quad O(F) = f(F) = 0$, donc : $Q(p)$ est vraie.
- 2) On suppose que $Q(F)$ vraie $\Rightarrow Q(\lceil F)$ vraie.

$$O(F) = f(F)$$

$$O(\lceil F) = O(F) = f(F) = f(\lceil F) \text{ i.e : } O(\lceil F) = f(\lceil F) \text{ i.e : } Q(\lceil F) \text{ est vraie.}$$

- 3) Supposons que :

$$\left. \begin{array}{l} O(F) = f(F) \text{ et } O(G) = f(G) \\ O((F * G)) = O(F) + O(G) + 1 \\ f((F * G)) = f(F) + f(G) + 1 \end{array} \right\} \Rightarrow O((F * G)) = f((F * G)) \text{ donc } Q((F * G)) \text{ est vraie.}$$

Sa formules.

On définit l'ensemble $sf(F)$ des sous formules de F par :

- Si $F = p$, $sf(F) = \{F\}$
- Si $F = \neg G$, $sf(F) = \{sf(G)\} \cup \{F\}$.
- Si $F = (G * H)$, $sf(F) = \{sf(G)\} \cup \{H\} \cup \{F\}$.

Exemple.

$$\begin{aligned}
 F &= \neg \left(\underbrace{((p \Rightarrow q) \wedge r)}_G \iff \underbrace{s}_H \right) \\
 &= \neg \underbrace{(G \iff H)}_K = \neg K \\
 sf(F) &= sf(\neg K) = sf(K) \cup \{F\} \\
 K &= (G \iff H) \\
 sf(K) &= sf(G) \vee sf(H) \cup \{K\} \\
 H &= s, \text{ donc } : sf(H) = \{s\} \\
 G &= \left(\underbrace{(p \Rightarrow q)}_{G_1} \wedge \underbrace{r}_{G_2} \right) = (G_1 \wedge G_2) \\
 sf(G) &= sf(G_1 \wedge G_2) = sf(G_1) \vee sf(G_2) \cup \{G\} \\
 sf(G_2) &= \{r\} \\
 G_1 &= (p \Rightarrow q) \text{ donc, } sf(G_1) = sf(p \Rightarrow q) = \{p, q\} \cup \{p \Rightarrow q\} \\
 sf(F) &= \{p, q, r, s, (p \Rightarrow q), (p \Rightarrow q) \wedge r, ((p \Rightarrow q) \wedge r) \iff s, F\}
 \end{aligned}$$

2.4 L'interprétation d'une formule logique

2.4.1 Arbre de décomposition d'une formule

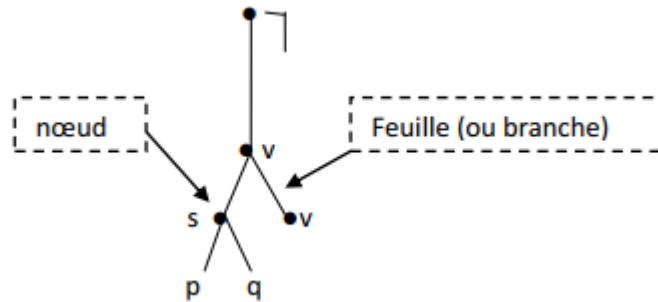
l'arbre A_F de la formule F est définie par récurrence sur F

- Si $F = p$, $A_F = {}^0p$.
- Si $F = \neg G$, $A_F = \neg A_G$.

2.4. L'interprétation d'une formule logique

• Si $F = (G * H)$ $A_F = \bigwedge_{A_G A_H} *$
 Avec : $*$, $=$, \wedge , \vee , \Rightarrow , \Leftrightarrow

Exemple. $F = \neg((p \wedge q) \vee q)$



Exemple. $M = (((A \wedge (\neg B \Rightarrow \neg A)) \wedge (\neg B \vee \neg C)) \Rightarrow (C \Rightarrow \neg A))$

On posons : $M_0 = ((A \wedge (\neg B \Rightarrow \neg A)) \wedge (\neg B \vee \neg C))$ et $M_1 = (C \Rightarrow \neg A)$

il constatera d'abord que M s'écrit $(M_0 \Rightarrow M_1)$

ensuite posons : $M_{00} = (A \wedge (\neg B \Rightarrow \neg A))$, $M_{01} = (\neg B \vee \neg C)$, $M_{10} = c$, $M_{11} = \neg A$ il

écrivra $M_0 = (M_{00} \wedge M_{01})$ et $M_1 = (M_{10} \Rightarrow M_{11})$ pour suivant ainsi, il sera amené à

poser successivement :

$$M_{000} = A, M_{001} = (\neg B \Rightarrow \neg A)$$

$$M_{010} = \neg B, M_{011} = \neg c$$

$$M_{110} = A, M_{0010} = \neg B$$

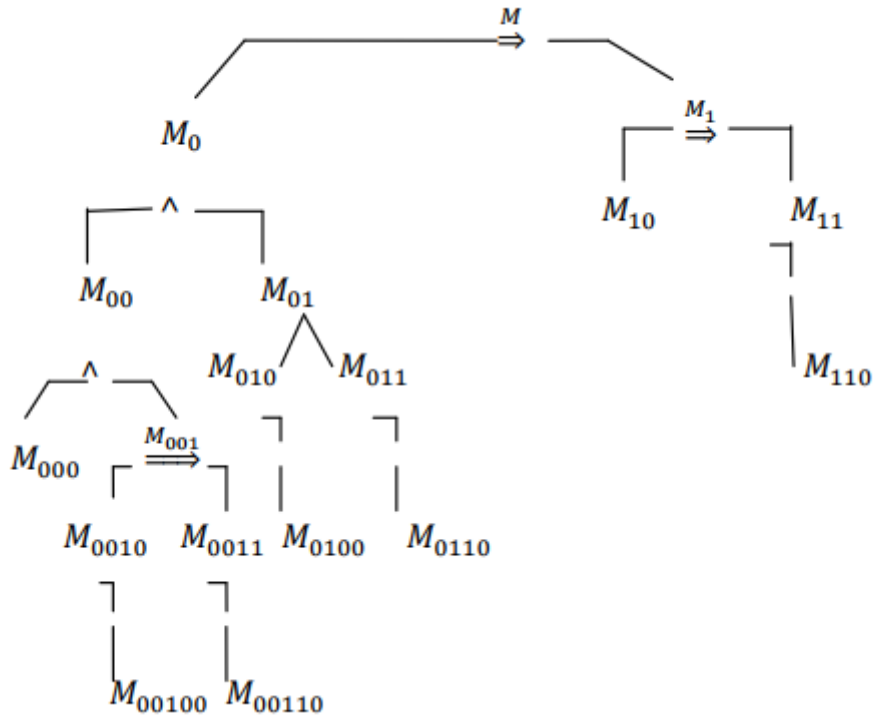
$M_{0011} = \neg A$, $M_{0100} = B$, $M_{0110} = C$, $M_{00100} = B$, $M_{00110} = A$ de telle sorte que :

$$M_{00} = (M_{000} \wedge M_{001}), M_{01} = (M_{010} \vee M_{011}), M_{11} = \neg M_{110}, M_{001} = (M_{0010} \Rightarrow M_{0011}),$$

$$M_{010} = \neg M_{0100}, M_{011} = \neg M_{0110}, M_{0010} = \neg M_{00100} \text{ et } M_{0011} = \neg M_{00110}$$

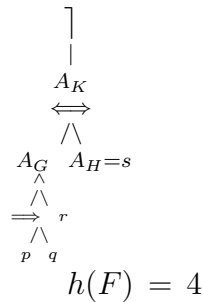
$$h(M) = 5 \text{ i.e. : } M \in \mathcal{F}_s.$$

2.4. L'interprétation d'une formule logique



Définition 2.8. Hauteur d'un arbre est le nombre maximum de feuillets de la racine à une extrémité de l'arbre, dans l'exemple 1 $h(F) = 3$.

Exemple. $F = \lceil ((\underbrace{(p \Rightarrow q)}_G) \wedge r) \Leftrightarrow \underbrace{s}_H) \rceil$
 $F = \lceil (\underbrace{(G \Leftrightarrow H)}_K) = \lceil K$
 $A_F = \lceil \lceil ; K = (G \Leftrightarrow H)$
 $\quad \quad \quad \downarrow$
 $\quad \quad \quad A_K$



Chaque nœud n détermine un sous-arbre A_n qui correspondance à une sous-formule F . Inversement l'arbre de chaque sous-formule est une sous- arbre de l'arbre de la formule Ainsi :

Sous- formules de $F =$ Sous-arbre de A_F

2.4. L'interprétation d'une formule logique

2.4.2 Substitution dans un formule

Soit F une formule et soient p_1, p_2, \dots, p_n des proposition élémentaires.

L'écriture $F[p_1, p_2, \dots, p_n]$ signifie que les lettres de P qui sont dans F sont parmi les $p_i, i = 1, 2, \dots, n$.

Exemple. $F = (p \iff (p \wedge q))$ on écrira $F[p, q]$, soit

$$F = F[p_1, \dots, p_n, q_1, \dots, q_n] \text{ une formule et soient } G_1, G_2, \dots, G_n, n \text{ formules.}$$

Définition2.9. On appelle $F_{\frac{G_1}{p_1}, \frac{G_2}{p_2}, \dots, \frac{G_n}{p_n}}$ le mot obtenu par remplacement (substitution) de G_i à la place de p_i .

Autre notation. $F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} = F[G_1, \dots, G_2, q_1, q_2, \dots, q_n]$

Exemple. $F = (p \iff (p \wedge q)) = F[p, q], G = (q \Rightarrow p)$

$$F_{\frac{G}{p}} = F(G, q) = ((q \Rightarrow p) \iff ((p \Rightarrow q) \wedge q))$$

Proposition. Le mot $F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}$ est aussi une formule.

Preuve. On raisonne par induction sur le formule F

$$* F = p$$

$$- \text{ si } F = p_K \text{ alors } F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} = G_K$$

$$- \text{ si } F = p \neq p_1, p_2, \dots, p_n, F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} = F \text{ dans les deux cas, aux a une formule.}$$

* $F = \lceil G$, on suppose $G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}$ formule. Alors $F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} = \lceil G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}$ est aussi une

formule.

* $F(G * H)$ avec $*$ = $\wedge, \vee, \Rightarrow, \Leftrightarrow$ même raisonnement.

Théorème2.1 (Substitution et valuations). Soit v une valuation, F, G_1, G_2, \dots, G_n des formules et p_1, p_2, \dots, p_n des propositions élémentaires, soit v' la valuation défini par :

$$v'(p) = \begin{cases} v(p) & \text{si } p \neq p_1, p_2, \dots, p_n. \\ \bar{v}(G_i) & \text{si } p = p_i \ (1 \leq i \leq n). \end{cases}$$

$$\text{Alors : } \bar{v}(F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}'(F)$$

Preuve.

2.4. L'interprétation d'une formule logique

1) $* F = p$

$$* \text{ Si } p \neq p_i, \text{ alors : } F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} = F \text{ et } \bar{v}(F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}(F) = v(F) = v'(F) = \bar{v}'(F)$$

$$* \text{ Si } p = p_i \text{ alors, } F_{\frac{G_1}{p_1}, \frac{G_2}{p_2}, \dots, \frac{G_n}{p_n}} = G_i \text{ et : } \bar{v}(F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}(G_i) = v'(p_i) = v'(F) = \bar{v}'(F)$$

2) $F = \lceil G$ et $\bar{v}(G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}'(G)$

$$\bar{v}(F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}(\lceil G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = 1 + \bar{v}(G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = 1 + \bar{v}'(G) = \bar{v}'(\lceil G) = \bar{v}'(F)$$

$$* F = (G * H)$$

$$\text{Si } = 1, F = (G \wedge H) \text{ et } \bar{v}(G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}'(G) \text{ et } \bar{v}(H_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}'(H),$$

$$\bar{v}(F_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}(G_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}} \wedge H_{\frac{G_1}{p_1}, \dots, \frac{G_n}{p_n}}) = \bar{v}(G) \cdot \bar{v}(H) = \bar{v}'(G) \cdot \bar{v}'(H) = \bar{v}'((G_1 H)) = \bar{v}'(F) \text{ même chose pes les autre cas } *, =, \vee, \Rightarrow, \Leftrightarrow .$$

Corolaire. Si F est une autre tautologie alors la forme $F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}$ est aussi une tautologie.

Preuve. Pour tout valuation v on a $\bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}})$

Théorème2.2. Soit F une formule, G une sous-formule de F et H une formule équivalente à G alors : $F' = F_{\frac{H}{G}}$ et logiquement équivalente à F

Preuve. Par indication sur les formules

- Si $F = p, G = F$ et $F' = H$ et donc $F' \sim F$.
- Si $F = \lceil F_1$ alors $G = F$ et donc $H = F'$ et $F \sim F'$ ou G est une sous-formule de F_1 , $F'_1 = F_{1 \frac{H}{G}} \sim F_1$, donc $F' = \lceil F'_1 \sim F$
- Si $F = F_1 * F_2, * = \wedge, \vee, \Rightarrow, \Leftrightarrow . * = \wedge, F = F_1 \wedge F_2$ alors il ya trois possibilités. ou bien $G = F, F' = H$ et on a $F' \sim F$. ou bien G est une sous-formule de F_1 , et par hybothèse d'indication, la formule F'_1 , résultat de la substitution de H à G dans F_1 , et logiquement équivalente à F_1 . La formule F' est alors la formule $(F'_1 \wedge F_2)$ elle est logiquement équivalente à F car, pour toute valuation v , on a $\bar{v}(F') = \bar{v}(F'_1) \cdot \bar{v}(F_2) = \bar{v}(F_1) \cdot \bar{v}(F_2) = \bar{v}((F_1 \wedge F_2)) = \bar{v}(F)$ le raisonnement est tout à fait similaire dans la troisième éventualité, celle où G est une sous-formule de F_2 les cas $F = (F_1 \cup F_2), F = (F_1 \Rightarrow F_2), F = (F_1 \Leftrightarrow F_2)$ se traitent de façon analogue,

2.4. L'interprétation d'une formule logique

en utilisant les propriétés :

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

$$v((F \vee G)) = v(F) + v(G) - v(F).v(G)$$

$$v((F \Rightarrow G)) = 1 - v(F) + v(F).v(G)$$

$$v(F \Rightarrow G) = 1 - v(F) + v(F).v(G).$$

2.5 Sémantique

Définition 2.10. Une distribution de valeurs de vérité ou valuation v est une application :

$v : P \longrightarrow \{0, 1\}$ où P est l'ensemble des propositions élémentaires. On dit que v définit un modèle \mathcal{M} des calculs propositionnels les valeurs 0 et 1 représentent "vrais" et "faux" et peuvent aussi être notées $v, F, 1 = v, 0 = F$. Si P de cardinalité n le nombre de valeurs de vérité différentes est exactement $2^n = 2^{\#P}$.

Exemple. $P = \{p, q\}$ on a donc $2^2 = 4$

1 1

1 0

0 1

0 0

$$v_1 : P \longrightarrow \{0, 1\}$$

$$p \longrightarrow 1$$

$$q \longrightarrow 1$$

$$v_2 : P \longrightarrow \{0, 1\}$$

$$p \longrightarrow 1$$

$$q \longrightarrow 0$$

$$v_3 : P \longrightarrow \{0, 1\}$$

$$p \longrightarrow 0$$

$$q \longrightarrow 1$$

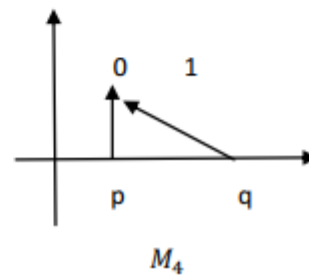
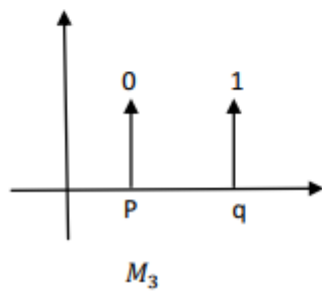
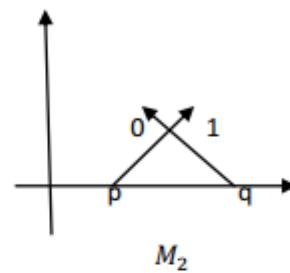
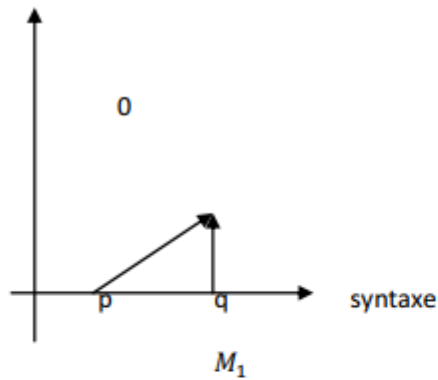
$$v_4 : P \longrightarrow \{0, 1\}$$

$$p \longrightarrow 0$$

$$q \longrightarrow 0$$

Le but de la sémantique est de donner des valeurs de vérité aux formules du calcul des propositions pour les différentes valuations définies sur les propositions élémentaires.

sémantiques



Théorème 2.3. Pour toute valuation $v : P \rightarrow \{0, 1\}$ il existe une unique extension $\bar{v} : \mathcal{F} \rightarrow$

$\{0, 1\}$ (i.e $\bar{v} = v$ sur P) et qui est telle que :

- 1) $\bar{v}(\neg F) = 1 \iff \bar{v}(F) = 0.$
- 2) $\bar{v}((F \wedge G)) = 1 \iff \bar{v}(F) = \bar{v}(G) = 1.$
- 3) $\bar{v}((F \vee G)) = 0 \iff \bar{v}(F) = \bar{v}(G) = 0$
- 4) $\bar{v}((F \Rightarrow G)) = 0 \iff \bar{v}(F) = 1 \text{ et } \bar{v}(G) = 0.$
- 5) $\bar{v}((F \Leftrightarrow G)) = 1 \iff \bar{v}(F) = \bar{v}(G)$

Preuve. Soient \bar{v}_1 et \bar{v}_2 deux extensions de v et soit $Q(F)$ la proposition

“ $\bar{v}_1(F) = \bar{v}_2(F)$ “. On doit montrer que $Q(F)$ est vraie, $\forall F \in \mathcal{F}$

- Si $F = p : \bar{v}_1(F) = \bar{v}_2(F) = v(F)$ donc $Q(F)$ vraie.
- Si $F = \neg G$ et $Q(G)$ vraie.

$$\left. \begin{array}{l} \bar{v}_1(F) = 1 \iff \bar{v}_1(G) = 0 \\ \bar{v}_1(F) = 0 \iff \bar{v}_1(G) = 1 \end{array} \right\} \implies \bar{v}_1(F) = \bar{v}_2(F)$$

2.5. Sémantique

Donc : $Q(F)$ est vraie aussi.

- Môme chose pour $F = (G * H)$, $*$ = $\wedge, \vee, \Rightarrow, \Leftrightarrow$.

Remarque. Si on définit $+ et .$ dans $\frac{\mathbb{Z}}{\mathbb{Z}} = \{0, 1\}$ par

$$0 + 0 = 0 \quad 0 \cdot 0 = 0$$

$$0 + 1 = 1 \quad 0 \cdot 1 = 0$$

$$1 + 0 = 1 \quad 1 \cdot 0 = 0$$

$$1 + 1 = 0 \quad 1 \cdot 1 = 1$$

les conditions 1) et 5) deviennent :

$$1) \bar{v}(\neg F) = 1 + \bar{v}(F).$$

$$2) \bar{v}((F \wedge G)) = \bar{v}(F) \bar{v}(G).$$

$$3) \bar{v}((F \vee G)) = \bar{v}(F) + \bar{v}(G) + \bar{v}(F) \bar{v}(G)$$

$$4) \bar{v}((F \Rightarrow G)) = 1 + \bar{v}(F) + \bar{v}(F) \bar{v}(G).$$

$$5) \bar{v}((F \Leftrightarrow G)) = 1 + \bar{v}(F) + \bar{v}(G)$$

ces conditions sont aussi souvent écrites sous forme de vérité pour les connecteurs $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$

F	$\neg F$
0	1

F	G	$(F \wedge G)$
1	1	1
1	0	0
0	1	0
0	0	0

F	G	$(F \wedge G)$
1	1	1
1	0	0
0	1	0
0	0	0

F	G	$(F \Rightarrow G)$
1	1	1
1	0	0
0	1	1
0	0	1

F	G	$F \Leftrightarrow G$
1	1	1
1	0	0
0	1	0
0	0	1

Exemple. $F = \neg(((p \Leftrightarrow q) \vee (p \Rightarrow q) \wedge (r \Leftrightarrow s)) \Rightarrow (p \Rightarrow q))$

on suppose que $P = \{p, q, r, s\}$

$$v : P \longrightarrow \{0, 1\}$$

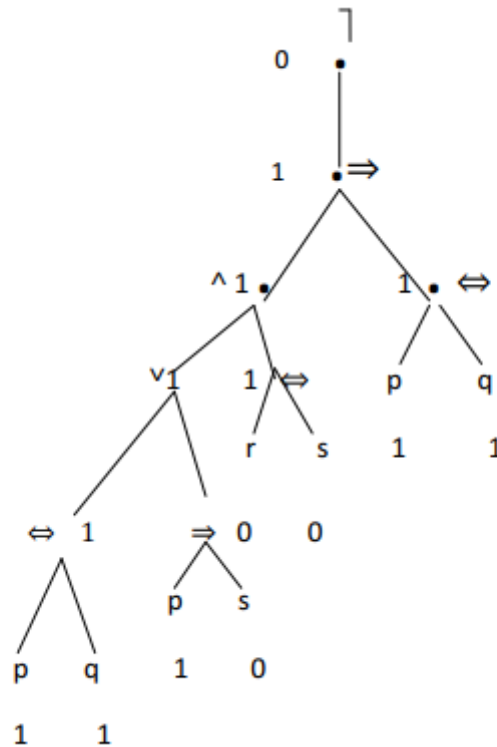
$$p \longrightarrow 1$$

$$q \longrightarrow 1$$

$$r \longrightarrow 0$$

$$s \longrightarrow 0$$

Calculer $\bar{v}(F)$, donc : $\bar{v}(F) = 0$



2.6 Tautologie et équivalences logiques

Soit v une valeur de vérité définissant un modèle \mathcal{M} du calcul propositionnel et soit \bar{v} son extension sur les formules.

Définition 2.11.

- 1) La formule F est dite satisfaite dans le modèle \mathcal{M} si $\bar{v}(F) = 1$, on note $\mathcal{M} \models F$ si non elle est dite non satisfaite $\bar{v}(F) = 0$, on note $\mathcal{M} \not\models F$.
- 2) F est une tautologie si pour tout modèle \mathcal{M} , on a $\mathcal{M} \models F$, on note $\models F$.

Exemple. $F = (p \vee \neg p)$, $P = \{p\}$ a valeur de vérité $\bar{v}_2(F) = 1$ F est une anti tautologie si pour tout modèle \mathcal{M} , on a $\mathcal{M} \not\models F$, on note $\not\models F$.

Exemple. $F = (p \wedge \neg q)$, $P = \{p\}$, $v_1 : p \rightarrow 1$, $\bar{v}_1(F) = 0$,
 $v_2 : p \rightarrow 0$, $\bar{v}_2(F) = 0$.

- Une tautologie est donc une formule toujours vraie (\forall la valuation).
- Une anti tautologie est une formule toujours fausse.

3) est logiquement équivalente à G si $(F \Leftrightarrow G)$ est une tautologie, on note $F \sim G$.

Autrement dit $\bar{v}(F) = \bar{v}(G)$ pour toute valuation v .

Exemple. $F = p, F \sim G, \text{ car } (p \Leftrightarrow \lceil \lceil p)$ est une tautologie $G = \lceil \lceil p$.

Remarque.

1) En terme de table de vérité, une tautologie est une formule qui a des 1 par tout dans sa dernière colonne.

- Une anti-tautologie a des 0 par tout sur sa dernière colonne.

- Deux formules logiquement équivalentes ont les même tables de vérité.

2) \sim définit sur \mathcal{F} une relation d'équivalence l'ensemble quotient

$\frac{\mathcal{F}}{\sim} = \{[F], F \in \mathcal{F}\}, [F] = \{G \in \mathcal{F} / F \sim G\}$ = les classes d'équivalence de F . Quant on compare deux formules "à équivalence logique" cela veut dire qu'on compare les classe correspondantes dans $\frac{\mathcal{F}}{\sim}$.

$$\left. \begin{array}{l} F \text{ tautologie} \iff \forall v, \bar{v}(F) = 1 \\ G \text{ tautologie} \iff \forall v, \bar{v}(G) = 1 \end{array} \right\} \iff F \sim G$$

donc : toutes les tautologie sont logiquement équivalentes est froments la classe 1.

De même toutes les anti-tautologies sont logiquement équivalentes et forment la classe 0.

3) $F = G \Rightarrow F \sim G$.

$$F \sim G \not\Rightarrow F = G.$$

$$F \sim G \Rightarrow [F] = [G].$$

Exemple. Voici quelque tautologie sous-forme d'équivalence :

1) Idempotente de la conjonction et de la disjonction

$$((p \wedge p) \iff p)$$

$$((p \vee p) \iff p)$$

2) Commutativité de la conjonction, disjonction et équivalence :

$$((p \wedge q) \iff (q \wedge p)), ((p \vee q) \iff (q \vee p)), ((p \iff q) \iff (q \iff p))$$

3) Associativité de la conjonction, disjonction, équivalence :

$$(((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))), \quad (((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))),$$

$$(((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r)))$$

4) Distributivité de la disjonction/conjonction et réciproquement :

$$(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r)), \quad (p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$$

5) Absorption :

$$((p \wedge (p \vee q)) \Leftrightarrow p), \quad ((p \vee (p \wedge q)) \Leftrightarrow p)$$

6) Lois de Demorgan :

$$(\neg (p \vee q)) \Leftrightarrow (\neg p \wedge \neg q), \quad (\neg (p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$$

7) Contra posé e :

$$((p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p))$$

8) $(\neg \neg p \Leftrightarrow p)$, $((p \Rightarrow q) \Leftrightarrow (\neg p \vee q))$

Voici des formules non équivalente :

$$(p \wedge p) \text{ et } (q \wedge q) \quad (\text{prendre } v(p) = 1 - v(q))$$

$$(p \Rightarrow p) \text{ et } p \quad (\text{prendre } v(p) = 0)$$

$$(p \Leftrightarrow q) \text{ et } (p \Rightarrow q) \quad (\text{prendre } v(p) = 0, v(q) = 1)$$

$$(p \Rightarrow (p \Rightarrow p)) \text{ et } ((p \Rightarrow p) \Rightarrow p) \quad (\text{prendre } v(p) = 0)$$

Remarque. Grâce à l'associativité de \wedge et \vee on peut adapter les notations suivantes :

La formule $((F \wedge G) \wedge H)$ sera notée $(F \wedge G \wedge H)$.

La formule $((F \vee G) \vee H)$ sera notée $(F \vee G \vee H)$. plus généralement, pour tout

entier naturel non k si F_1, F_2, \dots, F_k sont des formules on représentera par :

$$\underbrace{(F_1 \wedge F_2 \wedge \dots \wedge F_k)}_{\bigwedge_{i=1}^k F_i} \stackrel{def}{=} F_1 \wedge (F_2 \wedge (\dots \wedge F_k \dots))$$

$$\underbrace{(F_1 \vee F_2 \vee \dots \vee F_k)}_{\bigvee_{i=1}^k F_i} \stackrel{def}{=} F_1 \vee (F_2 \vee (\dots \vee F_k \dots))$$

dans la liste ci-dessous, les formule qui se trouvent sur une même ligne sont deux à deux logique équivalentes :

1) $(A \Rightarrow B), (\neg A \vee B), ((A \wedge B) \Leftrightarrow A), ((A \vee B) \Leftrightarrow B)$.

- 2) $\neg(A \Rightarrow B), (A \wedge \neg B)$.
- 3) $(A \Leftrightarrow B), ((A \wedge B) \vee (\neg A \wedge \neg B)), ((\neg A \cup B) \wedge (\neg B \cup A))$.
- 4) $(A \Leftrightarrow B), ((A \Rightarrow B) \wedge (B \Rightarrow A)), (\neg A \Leftrightarrow \neg B), (B \Leftrightarrow A)$.
- 5) $(A \Leftrightarrow B), ((A \cup B) \Rightarrow (A \wedge B))$.
- 6) $\neg(A \Leftrightarrow B), (A \Leftrightarrow \neg B), (\neg A \Leftrightarrow B)$.
- 7) $A, (A \wedge T), (A \vee T), (A \Leftrightarrow T), (T \Rightarrow A)$.
- 8) $\neg A, (A \Rightarrow \neg A), ((A \Rightarrow B) \wedge (A \Rightarrow \neg B))$.
- 9) $\neg A, (A \Rightarrow \perp), (A \Leftrightarrow \perp)$
- 10) $\perp, (A \wedge \perp), (A \Leftrightarrow \neg A)$.
- 11) $T, (A \vee T), (A \Rightarrow T), (\perp \Rightarrow A)$.
- 12) $(A \Rightarrow (B \wedge C)), ((A \Rightarrow B) \wedge (A \Rightarrow C))$.
- 13) $(A \Rightarrow (B \vee C)), ((A \Rightarrow B) \vee (A \Rightarrow C))$.
- 14) $((A \wedge B) \Rightarrow C), ((A \Rightarrow C) \vee (B \Rightarrow C))$.
- 15) $((A \vee B) \Rightarrow C), ((A \Rightarrow C) \wedge (B \Rightarrow C))$.

On retiendra des lignes de 12) à 15) qu'il n'y a pas distributivité de l'implication par rapport à la conjonction ou à la disjonction. On voit qu'il y a cependant distributivité à gauche 12) et 13), c'est à dire lorsque le " \wedge " ou le " \vee " se situent à droite du \Rightarrow . Dans le cas 14) et 15) on remarque qu'il y a une sorte de fausse distributivité le " \wedge " (resp : le \vee) étant transformé en " \vee " (resp : en \wedge).

Théorème 2.4 (substitutions et valuation) Soient v une valuation, F, G_1, G_2, \dots, G_n des formules et p_1, p_2, \dots, p_n des propositions élémentaires.

Soit v' la valuation défini par :

$$v' = \begin{cases} v(p) & \text{si } p \neq p_1, p_2, \dots, p_n. \\ \bar{v}(G_i) & \text{si } p = p_i \ (1 \leq i \leq n) \end{cases}$$

Alors : $\bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(F)$.

Preuve. On raisonne par indication sur les formules :

$$* F = p$$

$$- \text{ Si } p \neq p_i \text{ alors } F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}} = F \text{ et } \bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}(F) = v(F) = v'(F) = \bar{v}'.$$

$$- \text{ Si } p = p_i \text{ alors } F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}} = G_i \text{ et } \bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}(G_i) = v'(p_i) = v'(F) = \bar{v}'(F)$$

$$* F = \lceil G \text{ et } \bar{v}(G_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(G)$$

$$\bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}(\lceil G_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = 1 + \bar{v}(G_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = 1 + \bar{v}'(G) = \bar{v}'(\lceil G) = \bar{v}'(F).$$

$$* F = (G \wedge H) \text{ et } \bar{v}(G_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(G) \text{ et } \bar{v}(H_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(H)$$

$$\bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}((G_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}} \wedge (H_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}))) = \bar{v}(G) \cdot \bar{v}(H) = \bar{v}'(G) \cdot \bar{v}'(H) = \bar{v}'(G \wedge H) = \bar{v}'(F).$$

Même chose pour les autres cas.

Corolaire. Si F est une tautologie alors la forme $F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}$ est aussi une tautologie.

Preuve : Pour toute valuation v on a : $\bar{v}(F_{\frac{G_1}{p_1} \dots \frac{G_n}{p_n}}) = \bar{v}'(F) = 1.$

2.6.1 Formes normales

2.7 Systèmes complets se connecteurs

Définition 2.12.

1) Pour tout n-uple $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \{0, 1\}^n$, on note $V_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}$ la valuation définie par $V_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}^{(p_i = \varepsilon_i)}$ pour tout $i \in \{1, 2, \dots, n\}$

2) Pour chaque variable propositionnel p est pour chaque élément $\varepsilon \in \{0, 1\}$, nous notons ε_p la formule :

$$\varepsilon_p = \begin{cases} p \text{ si } \varepsilon = 1 \\ \lceil p \text{ si } \varepsilon = 0 \end{cases}$$

3) Pour toute formule F on note par $\Delta(F) = \{v \in \{0, 1\}^P, \bar{v}(F) = 1\}$ toute formule F définit une application :

$$\Delta_F : \{0, 1\}^n \longrightarrow \{0, 1\}$$

$$(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \longmapsto \bar{v}_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}(F)$$

\varnothing_F est compatible avec la relation d'équivalence logique. Autrement dit

$$F \sim G \Leftrightarrow \varnothing_F = \varnothing_G.$$

\varnothing_F définit donc par passage au quotient une application

$$\begin{aligned} \varnothing : \frac{\mathcal{F}}{\sim} &\longrightarrow \{0, 1\}^{(0,1)^n} \\ [F] &\longmapsto \varnothing_F \end{aligned}$$

$[F]$ la classe d'équivalence de la formule F pour la relation \sim

Théorème 2.5 \varnothing est une bijection.

Preuve.

1) \varnothing injective : soient $[F], [G]$ deux classes de formules

$$\varnothing([F]) = \varnothing([G]) \Rightarrow \varnothing_F = \varnothing_G \Leftrightarrow F \sim G \Leftrightarrow [F] = [G].$$

Donc : \varnothing est injective.

2) \varnothing surjective : Soit $\varnothing : \{0, 1\}^n \longrightarrow \{0, 1\}, \exists F \in \mathcal{F} / \varnothing =$

varnothinging_F?

* Si \varnothing ne prend que la valeur 0, alors toute anti-tautologie F vérifie $\varnothing = \varnothing_F$, par exemple $F = (p_1 \wedge \neg p_1)$

* Si non, l'ensemble $x = \varnothing^{-1}(\{1\}) = \{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \{0, 1\}^n / \varnothing(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) = 1\}$ est non vide.

Soit $F_x = \bigvee_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in X} (\bigwedge_{1 \leq i \leq n} \varepsilon_i p_i)$, alors $\Delta(F_x) = \{ \bigvee_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n} , (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in X \}$* i.e : $\bar{v}_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}(F_x) = 1 \Leftrightarrow \varnothing(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) = 1$, donc : $\varnothing = \varnothing_{F_x}$

pour, $\forall (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n), \Delta(\bigwedge_k \varepsilon_k p_k) = \bigvee_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}$,

$$\begin{aligned} \Delta(\bigvee_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in x} (\bigwedge_i \varepsilon_i p_i)) &= \{v_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}, (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in x\}, \bar{v}(\bigwedge_k \varepsilon_k p_k) = 1 \Leftrightarrow \\ \bar{v}(\bigwedge_k \varepsilon_k p_k) = 1 &\Leftrightarrow v(p_k) = v_{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n}(p_k). \end{aligned}$$

Corolaire. Si $\#p = n$ alors il ya exactement 2^{2^n} classes de formules correspondant chacune à une application $\varnothing : \{0, 1\}^n \longrightarrow \{0, 1\}$

Définition 2.12. Une application $\varnothing : \{0, 1\}^n \longrightarrow \{0, 1\}$ est appelé connecteur propositionnel à n places.

Exemple. On a déjà vu le connecteur

1) Selon la définition précédente il correspond aux connecteurs à 2, places.

$$\begin{aligned} \emptyset : \{0, 1\}^2 &\longrightarrow \{0, 1\} \\ (0, 0) &\longmapsto 0 \\ (0, 1) &\longmapsto 0 \\ (1, 0) &\longmapsto 0 \\ (1, 1) &\longmapsto 1 \end{aligned}$$

Ou de façon équivalente à la classe de la formule $p_1 \wedge p_2$.

2) Un exemple de connecteur à une place est :

$$\begin{aligned} \emptyset : \{0, 1\} &\longrightarrow \{0, 1\} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 0 \end{aligned}$$

Correspondant à la classe de $\neg p_1$ est donc au connecteur usuelle \neg .

3) Le connecteur à deux places suivant est appelé la barre de chefferie “ou“.

$$\begin{aligned} \emptyset : \{0, 1\}^2 &\longrightarrow \{0, 1\} \\ (0, 0) &\longmapsto 1 \\ (0, 1) &\longmapsto 0 \\ (1, 0) &\longmapsto 0 \\ (1, 1) &\longmapsto 0 \end{aligned}$$

de formule $\neg(p_1 \vee p_2)$.

2.7.1 Formes normales

Définition 2.13. Une formule F est dit sous-forme normale disjonction canonique (FNDC)

s'il existe un sous-ensemble non vide x de $\{0, 1\}^n / F = \bigvee_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in X} (\bigwedge_{1 \leq i \leq n} \varepsilon_i p_i)$ elle est dite sous-forme normale disjonctive (FND) s'il existe :

- * Un entier $m \geq 1$
- * Des entiers $k_1, \dots, k_m \geq 1$

2.7. Systèmes complets se connecteurs

* Pour $1 \leq i \leq m$, k_i variable $p_{i_1}, p_{i_2}, \dots, p_{i_{k_i}}$ et k_i éléments $\varepsilon_{i_1}, \dots, \varepsilon_{i_{k_i}}$ de $\{0, 1\}$ tel que :

$$F = \bigvee_{1 \leq i \leq m} (\varepsilon_{i_1} p_{i_1} \wedge \varepsilon_{i_2} p_{i_2} \wedge \dots \wedge \varepsilon_{i_{k_i}} p_{i_{k_i}})$$

On définit de même les formes normales conjonctives (FNC) et conjonctives canonique (FNCC)(en échangeant les symboles de disjonction et de conjonction)

Remarque. Une FNDC est une FND. De même une (FNCC) est une (FNC)

$$(n = k_i, \forall i, p_{ij} = p_j)$$

Théorème2.6 Toute formule F est logiquement équivalente à une FNC et une FND. la barre de chiffre : “ou“ $\neg (p_1 \vee p_2) = (p_1 \vee p_2) \vee$:barre de chiffre “ou“.

p_1	p_2	F
1	1	0
1	0	0
0	1	0
0	0	1

$$\varnothing_F : \{0, 1\}^2 \longrightarrow \{0, 1\}$$

$$\{0, 1\}^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

$$(0, 0) \longmapsto 1, (0, 1) \longmapsto 0$$

$$F = \neg (p_1 \wedge p_2) \stackrel{def}{=} (p_1 \vee p_2)$$

\wedge : barre de chiffre “et“

$$\varnothing = \varnothing_F : \{0, 1\}^2 \longrightarrow \{0, 1\}$$

$$(0, 0) \longmapsto 1$$

$$(0, 1) \longmapsto 1$$

Un connecteur à n places est une application $\varnothing \{0, 1\}^n \longrightarrow \{0, 1\}$

Exemple. $F = ((p_1 \wedge p_2) \Rightarrow p_3)$

$$\varnothing \{0, 1\}^3 \longrightarrow \{0, 1\}$$

p_1	p_2	$\neg(p_1 \wedge p_2)$
1	1	0
1	0	1
0	1	1
0	0	1

$$(0, 0, 0) \mapsto 1$$

$$(0, 0, 1) \mapsto 1$$

$$(1, 1, 0) \mapsto 0$$

\emptyset connecteur à 3 places.

Théorème 2.7 (de forme normale) Toute formule F est logiquement équivalente à (FND) au moins une formule sous-forme normale disjonctive et à au moins une formule sous-forme normale conjonctive (FNC).

Preuve. * Si F est une tautologie, elle est logiquement équivalente à $p_1 \wedge \neg p_1$ qui est une FND et une FNC. * Si F ni une tautologie, ni une anti-tautologie alors par le théorème précédente, il existe $x \neq \emptyset / \emptyset_F = \emptyset_{F_x}$, x de $\{0, 1\}^n$ i.e : $F \sim F_x$ qui est une FNDC donc aussi FND pour $\neg F$, il existe aussi $x' / \neg F \sim F_{x'}$, donc :

$$F = \neg \neg F \sim \neg(\vee(\wedge)) = \wedge(\vee) \sim FNCC \text{ (d'après le loi de demorgan)}$$

Exemple. $G = (A \Rightarrow (((B \wedge \neg A) \vee (\neg c \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B))))$ posons $H = (B \wedge \neg A)$, $I = (\neg c \wedge A)$, $j = (A \Rightarrow \neg B)$, $k = (H \vee I)$, $L = (A \vee j)$ et $M = (k \Leftrightarrow L)$. On a alors $G = (A \Rightarrow M)$ la table de vérité de G :

2.7. Systèmes complets de connecteurs

A	B	C	$\neg A$	$\neg B$	$\neg C$	H	I	J	K	L	M	G
1	1	1	0	0	0	0	0	0	0	1	0	0
1	1	0	0	0	1	0	1	0	1	1	1	1
1	0	1	0	1	0	0	0	1	0	1	0	0
1	0	0	0	1	1	0	1	1	1	1	1	1
0	1	1	1	0	0	1	0	1	1	1	1	1
0	1	0	1	0	1	1	0	1	1	1	1	1
0	0	1	1	1	0	0	0	1	0	1	0	1
0	0	0	1	1	1	0	0	1	0	1	0	1

d'après la table de vérité G est satisfaite par les valuation $(0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 1)$, $(1, 0, 0)$, $(1, 1, 0)$ tendit que $\neg G$ est satisfaite par $(1, 0, 1)$ et $(1, 1, 1)$ on enduit la FNDC de G :

$$(\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$$

puis la FNDC de $\neg G (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C)$ et enfin la FNCC de G : $(\neg A \wedge B \wedge \neg C) \wedge (\neg A \wedge \neg B \wedge \neg C)$

Exemple. $F = \neg((\neg p \Rightarrow q) \Rightarrow \neg(q \Leftrightarrow p))$ on utilise l'équivalences :

$$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$$

$$(p \Leftrightarrow q) \Leftrightarrow ((\neg p \vee q) \wedge (\neg q \vee p))$$

$$F \sim \neg(\neg(\neg p \Rightarrow q) \vee \neg(q \Leftrightarrow p))$$

$$\sim \neg(\neg(\neg p \vee q) \vee \neg((\neg q \vee p) \wedge (\neg p \vee q)))$$

$$\sim \neg(\neg(p \vee q) \vee \neg((\neg q \vee p) \wedge (\neg p \vee q)))$$

on utilise ensuite les lois de Demorgan :

$$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$$

$$\neg(\neg p \vee \neg q) \Leftrightarrow (p \wedge q)$$

donc :

$$F \sim \neg(\neg(p \vee q) \wedge \neg((\neg q \vee p) \wedge (\neg p \vee q)))$$

$$\sim (p \vee q) \wedge (\neg q \vee p) \wedge (\neg p \vee q)$$

$$\sim (p \vee q) \wedge (\neg q \vee p) \wedge (\neg p \vee q)$$

2.8 Système complets de connecteur

Définition 2.14.

- 1) Soit $\alpha_1, \alpha_2, \dots, \alpha_k$ un ensemble de connecteur d'arité quelconques, $\alpha_1, \alpha_2, \dots, \alpha_k$ est système complet ssi : pour toute formule $F \in \mathcal{F}$, il existe une formule G basée sur l'alphabet $P \cup \{\alpha_1, \dots, \alpha_k\} \cup \{(,)\} / F \sim G$
- 2) $\alpha_1, \alpha_2, \dots, \alpha_k$ est un système complet minimal si aucun sous-ensemble $A \subsetneq \{\alpha_1, \dots, \alpha_k\}$ n'est un système complet.

Exemple : $\{\neg, \vee, \wedge\}$ est système complet de connecteurs.

Proposition :

- 1) Le système $\{\neg, \vee, \wedge\}$ n'est pas minimal.
- 2) Le système $\{\neg, \vee\}$ est complet minimal.
- 3) Le système $\{\neg, \wedge\}$ est complet minimal.

Preuve.

- 1) $(p \wedge q) \sim \neg(\neg p \vee \neg q)$ donc \wedge s'exprime en terme de \neg et \vee .
- 2) Supposons que \vee s'exprime en terme de \neg toute formule est donc $\sim \neg \dots \neg p$ et donc à p ou $\neg p$ ce qui n'est pas le cas de $(p \wedge q)$

2.8.1 Les théories

Définition 2.15 Une théorie \mathcal{Z} du calcule propositionnel est un ensemble de formules $T \subseteq \mathcal{F}$.

Soit \mathcal{M} un modèle défini par la valuation v on dit que :

- 1) T est satisfaite dans \mathcal{M} si $\mathcal{M} \models F, \forall F \in T$ on écrit $\mathcal{M} \models T$.
- 2) T est consistant ou non contradictoire ou satis faible, s'il existe un modèle $\mathcal{M} \models T$.
- 3) T est finement satis faible si et seulement si chaque sous-théorie finie $T' \subseteq T$ est satis faible (cette définition d'intérêt que pour les parties T infinies).
- 4) T est contradictoire ssi s'il n'est pas satis faible, i.e : n'a pas de modèle.

- 5) La formule F est une conséquence de T ssi tout modèle de T est un modèle de F , $\mathcal{M} \models T \Rightarrow \mathcal{M} \models F$, on note $T \models F$ ou $(T \stackrel{*}{\vdash} F)$.
- 6) T et T' sont deux théories équivalentes ssi elle ont exactement les même modèles ou (toute formule de T conséquence de T' et toute formule de T' et conséquence de T).

Exemples. considérons des variables propositionnelles deux à deux distinctes $p, q, p_1, p_2, \dots, p_m \dots$: l'ensemble $\{p, q, (\neg p \vee q)\}$ est satis faible; $\{p, \neg q\}$ contradictoire; l'ensemble vide est satis fait par l'importe quelle valuation.

$\{p, q\} \models (p \wedge q)$, $\{p, (p \Rightarrow q)\} \models q$, l'ensemble $\{p, q\}$ et $\{(p \wedge q)\}$ sont équivalentes de même que $\{p_1, p_2, \dots, p_m, \dots\}$ et $\{p_1 \wedge p_2 \wedge \dots p_m \wedge \dots\}$.

Lemme. quelque soient les théories T et T' les entiers et $p \geq 1$ et les formules $G, H, F_1, F_2, \dots, F_m$ et G_1, G_2, \dots, G_p les propriétés suivants sont vérifiées :

- * $T \models G$ ssi $T \cup \{\neg G\}$ est contradictoire.
- * Si T est satis faible et si $T' \subseteq T$ alors T' est satisfait.
- * Si T est satis faible, alors T est finiment satis faible.
- * Si T est contradictoire et si $T \subseteq T'$ alors T' est contradictoire.
- * Si $T \models G$ et si $T \subseteq T'$ alors $T' \models G$.
- * $T \cup \{G\} \models H$ si et seulement si $T \models (G \Rightarrow H)$.
- * $T \models (G \wedge H)$ ssi $T \models G$ et $T \models H$.
- * $\{F_1, F_2, \dots, F_m\} \models G$ ssi $\models ((F_1 \wedge F_2 \wedge \dots \wedge F_m) \Rightarrow G)$.
- * G est une tautologie ssi G est conséquence de l'élément.
- * G est une tautologie ssi G est conséquence de l'importe quel ensemble de formules.
- * G est contradictoire ssi $T \models (G \wedge \neg G)$.
- * G est contradictoire ssi toute anti-tautologie est conséquence.

Calcul des prédicats

Définition 3.1 Une “prédicat“ est une affirmation qui porte sur des objets d’une théorie mathématique et qui peut vraie ou fausse selon ses objets.

Exemple.

- 1) “être un nombre paire“ est vraie p ou 2 mais fausse pour
- 2) “être plus petit que“ est vraie pour (2,3) mais fausse pour (3,)

Les calculs des prédicats permet de construire des énoncé complexe à partir des prédicats en utilisant des symboles spéciaux pour représenter les variables, les fonctions sur ces variables et les relations entre elle. Certaine variable ne changent jamais : ce sont les constantes.

En se sens le calcul des prédicats est plus riche que le calcul des propositions.

3.1 Syntaxe du calcul des prédicats

3.1.1 Alphabet des premier ordre

Soit $v = \{x_0, x_1, x_2, \dots\}$ un ensemble dont les éléments sont appelé variables.

* $\mathcal{C} = \{c_0, c_1, c_2, \dots\}$ un ensemble dont les éléments sont les constantes.

* $\mathcal{F} = \bigcup_{n>0} \mathcal{F}_n$ sont les fonctions d’arité n.

* $\mathcal{R} = \bigcup_{n>0} \mathcal{R}_n$ une rennion d’ensemble \mathcal{R}_n dont les éléments sont des relations d’arité n.

(On admet que \mathcal{R}_2 contient un élément particulier l'égalité)

* Les symboles \forall et \exists (quelque soit, il existe).

Définition 3.2 Un alphabet du premier ordre est un alphabet A de la forme :

$$A = \cup \cup \{ (,), \lceil, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists \} \cup \mathcal{C} \cup \mathcal{F} \cup \mathcal{R}.$$

- La partie $\cup \cup \{ (,), \lceil, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists \}$ est la partie logique de l'alphabet ou du langage.

- La partie $\sum = \mathcal{C} \cup \mathcal{R} \cup \mathcal{F}$. est appelée la signature du langage.

- La partie logique est commune à tous les langage ce qui caractérise un langage est donc sa partie ne logique ou signature.

Exemple. Signature de l'arithmétique élémentaire

$$\sum = \{ +, ., <, 0, 1 \}$$

$$\mathcal{C} = \{ 0, 1 \}$$

$$\mathcal{F} = \{ +, . \} = \mathcal{F}_2$$

$$\mathcal{R} = \{ <, = \} = \mathcal{R}_2$$

3.1.2 Termes

Soit A^* l'ensemble des mots de l'alphabet A .

Définition 3.3 l'ensemble des termes T construits à partir de A est la plus petite de A^*

$$1) \cup \cup \mathcal{C} \subseteq T.$$

$$2) t_1, t_2, \dots, t_n \in T \Rightarrow f t_1, \dots, t_n \in T, \forall f \in \mathcal{F}_n \forall n \geq 1.$$

Exemple. dans la théorie des nombres réels, les constants sont \mathbb{R} , les variables x, y, \dots , les fonctions = fcts de vraie, réelle : $\cos, \sin, +, ., \dots$

* $\sin x$ est un terme.

* $.xx$ est un terme représenté habituelle par x^2 .

* $+xy$ est un terme représenté habituelle par $x + y$.

* L'expression $\sin(x + \sin(y^2 + x))$ est représentée par le terme : $\sin + x \sin + x.yy$

Remarque. En tant que mot, chaque terme à une écriture unique.

3.1. Syntaxe du calcule des prédicats

3.1.2.1 Le hauteur d'un terme

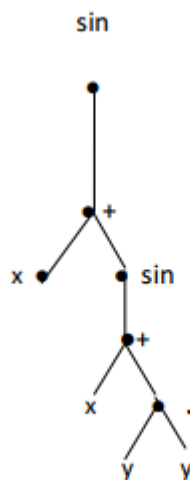
$$T = \bigcup_{n \geq 0} T_n \text{ avec } T_0 = v \cup \mathcal{C} \text{ et } T_{n+1} = T_n \cup \{ft_1, \dots, t_k, f \in \mathcal{F}_k \text{ et } t_1, \dots, t_k \in T_n\}$$

$$h(t) = \min\{n/t \in T_n\}$$

* On peut aussi parler de l'arbre de décomposition d'un terme. Le hauteur d'un terme est la hauteur de son arbre de décomposition :

Exemple. Le terme : $\sin + x \sin + x.yy$

$$h = 5$$



3.1.3 Formule

Une formule atomique est mot de A^* qui sont $Rt_1...t_n$ avec R une relation d'arité n ($R \in \mathcal{R}$) et $t_1...t_n$ des termes (on écrit $= t_1t_2$ pour $t_1 = t_2$).

Définition 3.4 L'ensemble des formules du 1^{er} ordre est la plus petite partie \mathcal{F} de A^*

- *1) Toute formule atomique $\in \mathcal{F}$.
- *2) $F, G, \in \mathcal{F} \Rightarrow \neg F, (F \wedge G), (F \vee G), (F \Rightarrow G), (F \Leftrightarrow G) \in \mathcal{F}$.
- *3) $F, \in \mathcal{F} \Rightarrow \forall v_n F$ et $\exists v_n F \in \mathcal{F}, \forall n$.

Remarque.

- 1) On a $\mathcal{F} = \bigcup_{n \geq 0} \mathcal{F}_n, \mathcal{F}_0 = \text{formule et ou,}$
 $\mathcal{F}_{n+1} = \mathcal{F} \cup \{\neg F, F \in \mathcal{F}\} \cup \{(F * G), F, G \in \mathcal{F}_n, * = \} \cup \{\forall v_k F, F \in \mathcal{F}_n, k \in \mathcal{N}\} \cup \{\exists v_k F, F \in \mathcal{F} \text{ et } h(F) = \min\{n/F \in \mathcal{F}_n\}$.

- 2) En tant que mot, toute formule a une écriture unique.
- 3) Une formule a aussi son arbre de décomposition de ses terminaisons sont les formules atomiques.

Exemple. Soit la signature $\Sigma = \{p, Q, R, f, g, T\}$

- * $\forall x (Rxy \Rightarrow Qxfy)$.
- * $\neg \exists x (Rxy \vee Qxgyx)$.
- * $\forall x (px \wedge \exists y (Tyx \Rightarrow sxy))$ sont des formules.

Les sous-formules de F se définissent de la façon suivante : * Si F est atomique alors $sf(F) = \{F\}$.

- * $F = \neg G, sf(F) = \{F\} \cup sf\{G\}$.
- * Si $F = (G_1 * G_2), sf(F) = \{F\} \cup sf\{G_1\} \cup sf\{G_2\}$.
- * Si $F = \forall x_k G, sf(F) = \{F\} \cup sf(G)$.
- * $F = \exists x_k G$.

3.2 Variable libre et liée

Une variable v_n peut apparaître plusieurs fois dans une formule F . On dit qu'elle a plusieurs occurrences. Ces apparitions sont de deux sortes : libre et liées.

Définition 3.5 On définit par induction les occurrences libres de v_n :

- * Si F est atomique, toutes les occurrences de v_n dans F sont libres.
- * Si $F = \neg G$, les occurrences libres de v_n dans F sont celles de v_n dans G .
- * Si $F = (G \alpha H)$, les occurrences libres de v_n sont celles de v_n dans G et celles de v_n dans H .
- * Si $F = \forall v_k G$ ou $F = \exists v_k G$ avec $k \neq n$, les occurrences libres de v_n dans F sont celles de v_n dans G .
- * Si on dit alors que x_n est quantifiée dans $F = \forall v_n G$ ou $F = \exists v_n G$ aucune occurrence de v_n dans F n'est libre.

Exemple. $\Sigma = \{R, c, f\}$

R : Relation, c : constante, f : fonction

$$F = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow] x_0 \simeq x_3) \wedge \forall x_2(\exists x_2(Rx_1x_2 \vee fx_0 \simeq c) \wedge x_2 \simeq x_2)$$

Toute les occurrences de x_0 et de x_2 sont liées les deux premier occurrences de x_1 sont liées le troisième est libre. x_3 est libre.

Définition 3.6 Une variable dans F est libre si elle a au moins une occurrence libre. Une formule close est une formule sans variables libre dans l'exemple précédent F n'est pas close ($(x_1$ et $x_3)$ sont libres). Une clôture une variable de F est une formule de la forme $\forall v_{i_1}, v_{i_2}, \dots, v_{i_n} F$ ou v_{i_1}, \dots, v_{i_n} sont les variables libre de F une clôture inversible est close.

3.2.1 Portée d'un quantificateur

Posons $\ominus = \exists$ ou \forall . Dans toute formule F contenant Ox , le mot Ox , est suit d'une sous-formule unique G dans laquelle sous le Ox , le variable x soit libre.

Définition 3.7 G le portée du quantificateur O les occurrences de x sont qui sont dans le champ de O sont les occurrences libres de x dans G .

Exemple : $F = \exists x((px \vee Qy \wedge gy = z) \Rightarrow (\exists x \forall^{21} y Rxy \wedge fzx =) y$ libre 8 et 12, liée en 22 et 25 quantifiée en 22 et 25 quantifiée en 22 et 25 dans le champ du 21.

3.2.2 Substitution dans les termes

3.2.2.1 Notation

$t = t[x_{i_1}, x_{i_2}, \dots, x_{i_n}]$ signifie que les variables ayant au moins une occurrence dans le terme t sont permit x_{i_1}, \dots, x_{i_n} . Si $m = \max_j x_j$ on peut aussi écrit $t = t[x_0, x_1, \dots, x_m]$.

Définition 3.8 Soient y_1, \dots, y_k des variables et t, u_1, \dots, u_k des termes. Le mot $t_{\frac{u_1}{x_1}, \dots, \frac{u_k}{x_k}}$ est le mot obtenu par substitution des termes u_1, u_2, \dots, u_k aux variables y_1, \dots, y_k dans toute les occurrences des y_i dans t . plus exactement :

$$\star t = \text{constante ou variable} \neq y_i \text{ alors } t_{\frac{u_1}{y_1}, \dots, \frac{u_k}{y_k}} = t.$$

$$\star t = y_i (1 \leq i \leq k) t_{\frac{u_1}{y_1}, \dots, \frac{u_k}{y_k}} = u_i.$$

$$\star t = ft_1 t_2 \dots t_n t_{\frac{u_1}{y_1}, \dots, \frac{u_k}{y_k}} = ft_1 \frac{u_1}{y_1}, \dots, \frac{u_k}{y_k} \dots t_n \frac{u_1}{y_1}, \dots, \frac{u_k}{y_k}$$

3.2. Variable libre et liéé

Proposition 3.1 $t_{\frac{u_1}{y_1}, \dots, \frac{u_k}{y_k}}$ est un terme.

Preuve. Par induction sur le terme t .

3.2.3 Substitution dans les formules

3.2.3.1 Notation

$F = F[x_{i_1}, \dots, x_{i_n}]$ veut dire que les variable libres dans F se trouvent parmi les x_{i_1} . On va substituer des termes à des variables libres dans une formules.

Définition 3.9 Soient F une formule, y_1, \dots, y_k des termes. Le mot $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}}$ obtenu par substitution des termes u_1, \dots, u_k aux variable y_1, \dots, y_k est défini comme suit :

- ★ Si $F = Rt_1 \dots t_n$ est atonique alors $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} = Rt_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} \dots t_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}}$.
- ★ Si $F = \lceil G$ alors $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} = \lceil G_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}}$.
- ★ Si $F = (G \alpha H)$, $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} = (G_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} \alpha H_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}})$.
- ★ Si $F = OxG(x \neq y_i)$, $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} = OxG_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}}$, $O = \exists$ ou \forall .
- ★ Si $F = OyiG(i = 1, 2, \dots, k)$, $F_{\frac{u_1}{y_1} \dots \frac{u_k}{y_k}} = OyiG_{\frac{u_1}{y_1} \dots \frac{u_{i-1}}{y_{i-1}}, \frac{u_{i+1}}{y_{i+1}} \dots \frac{u_k}{y_k}}$

Exemple. $F = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow \lceil x_0 = x_3) \wedge \forall x_2(\exists x_2(Rx_1x_2 \vee fx_0 = c) \wedge v_2 = v_2))$

$$t = ffc$$

$$F_{\frac{t}{x_1}} = \forall x_0(\exists x_1 \forall x_0(Rx_1x_0 \Rightarrow \lceil x_0 = x_3) \wedge \forall x_2(\exists x_2(Rffcx_0 \vee fx_0 = c) \wedge x_2 = x_0))$$

3.3 Sémantique du calcules des prédicats

Nous volons donner des valeurs de vérité aux formules du calcules des prédicats pour cela il faut spécifier un domaine dans lequel les variables prennent des valeurs et ou les symboles de relation et de fonction aient un sens .

Exemple 1. Soit la formule $\exists y \forall x Ryx$ pour donner une valeur de vérité à cette formule il

faut donner des valeurs aux variables x, y et préciser la définition de la “ralation“ R .

Cela dépend donc de la l'ensemble dans lequel les variables x, y prennent leurs valeur et de la définition de R dans cet ensemble.

- ★ Si $R = \leq$ sur \mathbb{N} , alors la formule est vraie.
- ★ Si $R = <$ sur \mathbb{N} , la formule est fausse.
- ★ Si $R = \leq$ ou $<$ sur \mathbb{Z} , la formule est fausse.

On a donc besoin de spécifier un ensemble dans lequel les variables prennent des valeurs et dans lequel les symboles de relations et de fonctions deviennent des vraies relations et fonctions. Cet ensemble sera une structure (ou une réalisation du langage ou alphabet A du calcule des prédicats considère)

Exemple2. Rcx

- ★ Vraie pour \mathbb{N} , $c = 0$, $x = 1$, $R = \leq$.
- ★ fausse pour \mathbb{N} , $c = 0$, $x = -1$, $R = \leq$.

3.3.1 Définition d'une structure

Soit A une alphabet du 1^{er} ordre.

Définition3.10 Une A structure est la donnée d'un ensemble S tel que :

- ★ Toute constant c de A est associée à un élément \bar{c} de S .
- ★ Chaque symbole de fonction f d'arité n est associée une application $\bar{f} : S^n \rightarrow S$.
- ★ Chaque symbole de relation R d'arité n est associée une relation \bar{R} d'arité n sur S ($\bar{R} \subseteq S^n$) (la relation d'égalité correspondant à l'égalité dans S).

Exemple. Soit la langage de signature $\Sigma = \{R, f, c_0, c_1\}$ une structure possible est $S = \mathbb{N}$, $\bar{R} = \leq$, $\bar{f} = +$, $\bar{c}_0 = 0$, $\bar{c}_1 = 1$. Une autre structure possible est $S = \mathbb{R}$, $\bar{R} = <$, $\bar{f} = x$, $\bar{c}_0 = e$, $\bar{c}_1 = T$

Remarque. Quand on considère plusieurs structures associées au même langage et pour tout entier s on peut écrire \bar{c}_s , \bar{f}_s et \bar{R}_s .

Définition3.11 Soient S et S' deux structures du même langage (alphabet). On dit que S est une sous-structure de S' si :

- ★ $S \subseteq S'$.
- ★ $\bar{c}_s = \bar{c}'_s$ pour toute constante c .
- ★ $\bar{f}_s = \bar{f}'_s$ pour toute f d'arité n .

3.3. Sémantique du calcul des prédicats

$\star \bar{R}_s = \bar{R}_{s'} \cap S^n$ pour toute relation R d'arité n .

Exemple. $\Sigma = \{R, f, g, c_0, c_1\}$

$\star S' = \mathbb{Z}, \bar{R}_{s'} = \leq, \bar{f}_{s'} = +, \bar{g}_{s'} = +, c_{0_{s'}} = 0, c_{1_{s'}} = 1$

$\star S = \mathbb{N}, \bar{R}_s = \leq, \bar{f}_s = +, \bar{g}_s = +, c_{0_s} = 0, c_{1_s}$

Soient toujours S et S' deux structures du même alphabet. Un morphisme de structure entre S et S' est une application $\varnothing : S \rightarrow S'$.

$\star \varnothing(\bar{c}_s) = \bar{c}_{s'}, \forall c$

$\star \varnothing(\bar{f}_{a_1, \dots, a_n}) = \bar{f}_{s'}(\varnothing(a_1), \dots, \varnothing(a_n))$

pour toute f d'arité $n, \forall a_i \in S \star (a_1, \dots, a_n) \in \bar{R}_s^n \Rightarrow (\varnothing(a_1), \dots, \varnothing(a_n)) \in \bar{R}_{s'}^n$

$\forall a_1, \dots, a_n \in S, \forall R$ d'arité n

Exemple. $\Sigma = \{f, c\}$

$S = \langle \mathbb{R}_+, 1, x \rangle; S' = \langle \mathbb{R}, 0, + \rangle$

$$\varnothing : \mathbb{R}_+^* \rightarrow \mathbb{R}$$

$$x \mapsto \log x$$

Définition 3.12 Un morphisme de structures $\varnothing : S \rightarrow S'$ est un monomorphisme . Si pour toute relation R d'arité n , si $a_1, \dots, a_n \in S$ alors $(a_1, a_2, \dots, a_n) \in \bar{R}_s \Leftrightarrow (\varnothing(a_1), \dots, \varnothing(a_n)) \in \bar{R}_{s'}$

Exemple. Toute sous-structure définit un monomorphisme (toute injection $S \hookrightarrow S'$) l'inverse est aussi vraie

Proposition 3.2 Toute monomorphisme est injectif.

Preuve. Parmi les symboles la relation, on a la relation d'égalité $=$, elle définit sur S et S' la relation d'égalité des ensembles : " $=_S$ " = " $=_{S'}$ ", " $=_S$ " = " $=_{S'}$ ", donc soient $a_1, a_2 \in S / \varnothing(a_1) = \varnothing(a_2), \varnothing$ est un monomorphisme on a : $\varnothing(a_1) = \varnothing(a_2) \Leftrightarrow a_1 = a_2$, donc \varnothing est injective.

Définition 3.13 Une isomorphisme de structure $\varnothing : S \rightarrow S'$ est un monomorphisme surjectif en particulier \varnothing doit être une bijection l'ensemble un automorphisme est un isomorphisme $\varnothing : S \rightarrow S'$

3.3. Sémantique du calcul des prédicats

Exemple. $S = \langle \mathbb{R}_+^*, 1, \rangle$ et $S' = \langle \mathbb{R}, 0, + \rangle$.

$\varnothing : \mathbb{R}_+^* \rightarrow \mathbb{R}, x \mapsto \log x$ est une automorphisme.

L'étape suivante est l'interprétation des termes.

Définition 3.14 Soient $t = t[x_0, \dots, x_{n-1}]$ un terme et S une structure du logique du premier ordre. Soient a_0, \dots, a_{n-1} un élément de S .

L'interprétation \bar{t}_s de t dans S quant $x_i = a_i, 0 \leq i \leq n$ est défini de façon suivante :

★ Si $t = x_i$ alors $\bar{t}_s = a_i$.

★ $t = c$ alors $\bar{t}_s = \bar{c}_s$.

★ $t = ft_1t_2\dots t_k$ alors $\bar{t}_s = \bar{f}_s(\bar{t}_{1_s}, \dots, \bar{t}_{k_s})$.

Exemple. $\Sigma = \{f, g, c_0, c_1\}$.

$S = \mathbb{N}, \bar{f} = +, \bar{g} = \cdot, \bar{c}_0 = 0, \bar{c}_1 = 1$.

$t = gyfxc_1 = t[x, y]$

$$\begin{pmatrix} x = x_0 \\ y = x_1 \end{pmatrix}$$

On prend $a_0 = 2, a_1 = 3$.

$\bar{t}_s = \bar{g}(3, \bar{f}(2, 1)) = 3 \cdot (2 + 1) = 3 \cdot 3 = 9$

Proposition 3.3 Soient $t = t[x_0, \dots, x_{n-1}]$ et $t' = t'[y, x_0, \dots, x_{n-1}]$ deux termes et a_0, \dots, a_{n-1} des éléments de la structure S . Alors on a $\bar{u}_s = \bar{t}_s$, avec $u = \bar{t}'_{\frac{t}{y}}$ et $y \rightsquigarrow \bar{t}_s = b \in S$

Preuve. Par indication sur le terme t'

$$\star t' = c, u = t' = c$$

$$\bar{u}_s = \bar{c}_s = \bar{t}'_s$$

$$\star t' = x_i, u = t' = x_i$$

$$\bar{u}_s = a_i = \bar{t}'_s$$

$$\star t' = y, u = t$$

$$\bar{u}_s = \bar{t}_s = \bar{t}'_s$$

$$\star t' = ft_1\dots t_k \text{ alors } u = fu_1\dots u_k \text{ avec } u_i = \bar{t}'_{\frac{t}{y}}$$

Par l'hypothèse $\bar{u}_{i_s} = \bar{t}_{i_s}$

Donc : $\bar{u}_s = \bar{f}(u_{1_s}, \dots, u_{k_s}) = f(\bar{t}_{1_s}, \dots, \bar{t}_{k_s}) = \bar{u}'_s$

3.3. Sémantique du calcul des prédicats

3.3.2 Satisfaction d'une formule dans un structure

Soit A un alphabet du 1^{er} ordre et S une A structure. Soit $F = F[x_0, \dots, x_{n-1}]$ une formule (cette notation veut dire que les variables libres de F sont parmi les x_i).

On a défini la satisfaction d'une formule F dans S quand les variables x_i sont interprété par les éléments a_0, a_1, \dots, a_n de S .

Ce qu'on écrira :

$$S \models F[a_0, a_1, \dots, a_{n-1}]$$

Définition 3.15 \star Si F est la formule atomique $Rt_1t_2\dots t_k$ avec $t_i = t_i[x_0, \dots, x_{n-1}]$ alors

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow (t_{1s}, \dots, t_{ks}) \in \bar{R}_s$$

$$\star \text{ Si } F = \neg G$$

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow S \not\models G[a_0, \dots, a_{n-1}]$$

$$\star \text{ Si } F = (G \wedge H) \text{ alors}$$

$$S \models F \Leftrightarrow S \models G \text{ et } S \models H$$

$$\star \text{ Si } F = (G \Rightarrow H) \text{ alors}$$

$$S \models F \Leftrightarrow S \not\models G \text{ ou } S \models H$$

$$\star \text{ Si } F = (G \vee H) \text{ alors}$$

$$S \models F \Leftrightarrow S \models G \text{ ou } S \models H$$

$$\star \text{ Si } F = (G \Leftrightarrow H) \text{ alors}$$

$$S \models F \Leftrightarrow (S \models G \text{ et } S \models H) \text{ ou } (S \not\models G \text{ et } S \not\models H)$$

$$\star \text{ Si } F = \forall x G(x \neq x_i)$$

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow S \models G[a, a_0, \dots, a_{n-1}] \forall a \text{ avec } x \text{ interprété par } a$$

$$\star \text{ Si } F = \exists x G(x \neq x_i)$$

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow \text{si } \exists a \in S /$$

$$S \models G[a, a_0, \dots, a_{n-1}], \text{ avec } x \rightsquigarrow a$$

$$\star \text{ Si } F = \forall x_i G$$

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow S \models G[a_0, \dots, a_{i-1}, x_i \rightarrow a, a_{i+1}, a_{n-1}] \forall a \in S$$

$$\star \text{ Si } F = \exists x_i G$$

$$S \models F[a_0, \dots, a_{n-1}] \Leftrightarrow \exists a \in S/$$

$$S \models G[a_0, \dots, a_{i-1}, a, a_{i+1}, \dots, a_{n-1}]$$

Remarque. Si F est close (sans variable libres) on écrit $S \models F$, F est soit satisfaite dans S

Exemple. $\Sigma = \{R, f, c\}$ est le structure $S = \mathbb{R}$, $\bar{R}_s = \leq$, $\bar{f}_s = \cos$, $\bar{c}_s = \pi$

$$\star F = Rcx (= Rt_1t_2)$$

$$S \models F[a] \Leftrightarrow t_{1s}, t_{2s} \in \bar{R}_s$$

$$\Leftrightarrow t_{1s} \leq t_{2s}$$

$$\Leftrightarrow \pi \leq a$$

$$\text{donc : } S \models F[a] \Leftrightarrow a \in [\pi, +\infty[$$

$$\star F = "fx_0 = c" = cfx_0$$

$$S \models F[a] \Leftrightarrow \bar{c}_s = fx_{0s} \Leftrightarrow \pi = \cos a$$

$$\text{donc : } \forall a \in \mathbb{R}, S \not\models F[a]$$

$$\exists x_1 \underbrace{fx_1}_G = x_0, \text{ variable libre } x_0.$$

$$S \models F[a_0] \Leftrightarrow S \models G[a_0, a_1] \text{ pour un certaine } a_1$$

$$\Leftrightarrow \exists a_1 / \cos a_1 = a_0$$

$$\Leftrightarrow a_0 \in [-1, 1]$$

$$\star \forall x_1 \underbrace{Rx_0fx_1}_G, \text{ variable libre } x_0$$

$$S \models F[a_0] \Leftrightarrow S \models G[a_0, a_1] / \forall a_1$$

$$\Leftrightarrow \forall a_1 / a_0 \leq \cos a_1$$

$$\Leftrightarrow a_0 \in]\infty, -1]$$

$$\star \forall x_1 \underbrace{\exists x_2 (Rx_1x_2 \wedge fx_2 = x_0)}_G, \text{ variable libre } x_0$$

$$S \models F[a_0] \Leftrightarrow \forall a_1 \exists a_2 / S \models G[a_0, a_1, a_2]$$

$$\Leftrightarrow \forall a_1 / \exists a_2 / a_1 \leq a_2 \text{ et } a_0 = \cos a_2$$

$$\Leftrightarrow a_0 \in [-1, 1]$$

$$\begin{aligned} & \star x_0 \exists x_1 \underbrace{f x_1 = x_0}_G \text{ formule close} \\ & \forall a_0, \exists a_1 / \cos a_1 = a_0 \quad S \models F \\ & \star \exists x_1 \forall x_2 \underbrace{R f x_2 x_1}_G \text{ formule close} \\ & \exists a_1 / \forall a_2, \cos a_2 \leq a_1 \quad S \models F \end{aligned}$$

Proposition 3.4 Soit $t = t[x_0, \dots, x_{n-1}]$ un terme et $F = F[z, x_0, \dots, x_{n-1}, y_0, \dots, y_{m-1}]$ une formule telle que aucune occurrence de z ne se trouve dans le champ de $\forall x_i$ ou $\exists x_i$. Alors pour toute structure S et $\forall a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1} \in S$ on a :

$$S \models F_{\frac{t}{z}}[a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}] \Leftrightarrow S \models F[\bar{t}_s, a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}]$$

Preuve. Par récurrence sur la formule F

$$\star F = R t_1 t_2 \dots t_k \quad t_i = t_i[z, x_0, \dots, x_{n-1}, y_0, \dots, y_{m-1}]$$

$$F_{\frac{t}{z}} = R t_{1\frac{t}{z}} \dots t_{k\frac{t}{z}} = R r_1 \dots r_k$$

$$S \models F_{\frac{t}{z}} \Leftrightarrow (r_{1s}^-, \dots, r_{ks}^-) \in \bar{R}_s$$

$$\text{Posons : } c_i = \bar{t}_{i_s}[t, a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}]$$

$$\text{On } r_{i_s}^- = c_i \text{ donc } S \models F_{\frac{t}{z}} \Leftrightarrow (t_{i_s}^-[t_s, a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}]) \in \bar{R}_s, i = 1, \dots, k \Leftrightarrow S \models F[\bar{t}_s, a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}]$$

3.3.2.1 Conséquence et équivalence universelle

Soit A un alphabet du 1^{er} ordre :

★ Une formule F close est universellement valide si $S \models F$ pour toute A structure S .

On note $\models F$

★ Une formule close F est contradictoire ssi $\neg F$ est universellement valide.

★ Une formule F comportant des variables libres est universellement valide si sa clotûre universelle l'est.

★ F est universellement équivalente à G ($F \sim G$) ssi ($F \Leftrightarrow G$) est universellement valide.

★ Une théorie T de A est un ensemble de formule close.

★ Le structure S est un module de la théorie T si et seulement si $S \models F, \forall F \in T$ (on dit aussi que S et T) on note $S \models T$

★ Une théorie T est consistante si elle admet au moins un modèle sinon elle est contradictoire

3.3. Sémantique du calcul des prédicats

laquelle toute partie finie est consistante.

★ F close est conséquence de T si tout modèle de T satisfait F on note $T \models F$

(Si F est non close, considère le clôture universelle)

★ T_1 est équivalente à T_2 ssi toute modèle de T_1 est un modèle de T_2 et uni-versement.

Proposition 3.5

1) Si $F \sim F'$ et $G \sim G'$ alors $\neg F \sim \neg F'$ ($F \alpha G \sim (F' \alpha G')$ $\alpha = \wedge, \vee, \Rightarrow, \Leftrightarrow$)

$$\forall x F \sim \forall x F'$$

$$\exists x F \sim \exists x F'$$

2) Soit F une formule, G une sous-formule de F et $G' \sim G$, alors $F' = F_{\frac{G'}{G}} \sim F$.

Preuve.

1) Traitons la close \forall il faut montrer que la clôture de $(\forall x F \Leftrightarrow \forall x F')$ est satisfait dans toute structure S écrivons

$$F = F[x_0, \dots, x_{n-1}, x]$$

$$F' = F'[x_0, \dots, x_{n-1}, x]$$

$$x \longrightarrow a$$

$$\begin{aligned} S \models \forall x F[a_0, \dots, a_{n-1}] &\Leftrightarrow \forall a S \models F[a_0, \dots, a_{n-1}, a] \\ &\Leftrightarrow \forall a S \models F'[a_0, \dots, a_{n-1}, a] \\ &\Leftrightarrow S \models \forall x F'[a_0, \dots, a_{n-1}] \\ &\Leftrightarrow S \models (\forall x F \Leftrightarrow \forall x F') \end{aligned}$$

2) Par induction sur la formule F .

Exemple.

$$\left. \begin{array}{l}
 \neg \forall x F \sim \exists x \neg F \\
 \forall x(F \wedge G) \sim (\forall x F \wedge \forall x G) \\
 \exists x(F \vee G) \sim (\exists x F \vee \exists x G) \\
 \exists x(F \Rightarrow G) \sim (\forall x F \Rightarrow \exists x G) \\
 \forall x \forall y F \sim \forall y \forall x F \\
 \exists x \exists y F \sim \exists y \exists x F
 \end{array} \right\} \text{Formule é'quivalents}$$

$$\left. \begin{array}{l}
 \exists x(F \wedge G) \Rightarrow (\exists x F \wedge \exists x G) \\
 (\forall x F \vee \forall x G) \Rightarrow \forall x(F \vee G) \\
 \exists x \forall y F \Rightarrow \forall y \exists x F
 \end{array} \right\} \text{Formule universelle valide}$$

Si x n'est pas libre dans F , on a : $\forall x F \sim \exists x F \sim F$

Corolaire. Toute formule du 1^{er} ordre est équivalente à une formule un comportant que \neg, \wedge, \vee

Preuve. $\{\neg, \vee\}$ est complet pour les connecteurs logique et \exists s'exprime en-terme de \neg et \forall .

Axiomatique de ZF et AC

4.1 Paradoxes, théorie naïve des ensembles

L'idée de base de la théorie naïve est un concept très puissant, celui d'ensemble. Un ensemble est une collection d'objets, qui peuvent être eux des ensembles. Ces objets sont dits éléments de l'ensemble. (on peut distinguer un élément d'un autre par ses propriétés, qui sont des assertions qui seront vraies pour certains éléments et fausses pour d'autres. Deux ensembles "naïfs" sont très intuitifs : l'ensemble vide et l'ensemble Oméga de tous les ensembles. Malheureusement, le concept naïf d'ensemble s'avère être trop puissant. Il peut conduire à des paradoxes. Le plus important de ces paradoxes est basé sur un théorème démontré par Georg Cantor en 1891, qui stipule que l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E est toujours plus gros que E lui-même ; cela signifie que les éléments de $\mathcal{P}(E)$ ne peuvent être mis en correspondance biunivoque avec ceux de l'ensemble E .

Par exemple si $E = \{1, 2, 3\}$, ensemble qui contient trois éléments,

$$\mathcal{P}(E) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

possède huit éléments et on a $8 > 3$. De même pour un ensemble E fini, $\mathcal{P}(E)$ est plus gros que E car on ne peut établir de correspondance biunivoque entre les éléments de E et ceux de $\mathcal{P}(E)$. On dit que E et $\mathcal{P}(E)$ n'ont pas la même puissance. Le paradoxe survient lorsqu'on considère l'ensemble oméga de tous les ensembles : le théorème de Cantor nous dit que $\mathcal{P}(\omega)$ est un ensemble plus gros qu' ω , qui est pourtant censé contenir tous les ensembles ! Voici

maintenant quelques autres paradoxes (ou antinomies) classiques :

4.1.1 Paradoxe de Russel

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

4.1.1.1 Énoncé du paradoxe

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

Réécrit plus formellement, si l'on pose : $y = \{x \mid x \notin x\}$ on a immédiatement que $y \in y \Leftrightarrow y \notin y$, donc chacune des deux possibilités, $y \in y$ et $y \notin y$, mène à une contradiction.

4.1.1.2 Solutions du paradoxe

Les principales solutions apportées pour éluder ce paradoxe furent :

1. Restriction du principe de compréhension, due à Zermelo (1908) :

Un prédicat ne définit pas un ensemble mais ce que l'on appelle une classe et son intersection avec un ensemble donne un sous-ensemble de celui-ci. Il est possible d'écrire le prédicat " $x \notin x$ ", mais celui-ci ne définit plus un ensemble. Il peut définir un sous-ensemble d'un ensemble donné, mais cela ne conduit pas à une contradiction, pour développer les mathématiques à un paradoxe. Il est nécessaire de modifier les mathématiques, d'introduire un certain nombre d'autres instances du principe de compréhension générale comme axiomes particuliers

(paire, réunion, enemble des parties, ...). Plus tard Abraham Fraenkel et Thoralf Skolem introduisirent. (incompréhensible) le schéma d'axiomes de remplacement, qui est toujours une restriction du principe de compréhension général, mais étend encore le schéma d'axiomes de compréhension introduit par Zermelo. Ils précisèrent également la notion de prédicat, et, en particulier Skolem, le contexte logique (le calcul des prédicats du premier ordre).

2. Théorie des types de Russell :

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

4.1.2 Paradoxe du coiffeur (barbier)

Le paradoxe du barbier est une illustration à but didactique du paradoxe de Russell, attribuée à Bertrand Russell lui-même. Il ne faut donc pas donner une importance excessive à ce "paradoxe" que le logicien E. W. Beth qualifie "d'antinomie prétendue" ou de "pseudoantinomie".

4.1.2.1 Énoncé du paradoxe

On peut énoncer le paradoxe ainsi :

Le conseil municipal d'un village a émis une ordonnance qui enjoint à son barbier (masculin)

4.1. Paradoxes, théorie naïve des ensembles

de raser tous les habitants masculins du village qui ne se rasent pas eux-mêmes et soulèvent ceux-ci.

Le barbier, qui est bien un habitant du village, n'a pas pu respecter cette règle car :

- S'il se rase lui-même, il enfreint la règle, car le barbier ne peut raser que les hommes qui ne se rasent pas eux-mêmes.
- S'il ne se rase pas lui-même - qu'il se fasse raser ou qu'il conserve la barbe - il est en tort également, car il a la charge de raser les hommes qui ne se rasent pas eux-mêmes.

Cette règle est donc inapplicable. S'agit-il pour autant d'un paradoxe ? Il n'y a aucune raison de penser qu'un conseil de village ou toute autre instance ne puisse rendre une ordonnance absurde. De fait, loin d'être une antinomie logique, ce "paradoxe" montre simplement qu'un barbier respectant cette règle ne peut exister. Il s'agit d'une illustration de ce que, si R est une relation binaire quelconque (en l'occurrence " ...rase..."), l'énoncé suivant, écrit en langage formel : $\neg\exists y\forall x(yRx \Leftrightarrow \neg xRx)$, est une formule universellement valide du calcul des prédicats du premier ordre. On se reportera à l'article sur le paradoxe de Russell pour voir pourquoi cela peut conduire, dans le cas de la relation d'appartenance dans une théorie des ensembles trop naïve, à une véritable antinomie, c'est-à-dire à une contradiction démontrée dans la théorie.

4.1.3 Paradoxe du menteur

Le paradoxe du menteur est un paradoxe dérivé du paradoxe du Crétois (ou paradoxe d'Épiménide). Ce paradoxe aurait été inventé par Euclide, un adversaire d'Aristote. Sous sa forme la plus concise, il s'énonce ainsi : "un homme déclare : Je mens. Si c'est vrai, c'est faux. Si c'est faux, c'est vrai". On peut y voir deux interprétations :

- En tant qu'énoncé, cette phrase dit : "Cette phrase est fautive";
- En tant que propos, il faut comprendre : "Je mens maintenant".

4.1.3.1 Énoncé du paradoxe

On attribue le paradoxe du menteur à Épiménide le Crétois (VIIe siècle av. J.-C.), bien qu'il semblerait que cette première formulation du paradoxe du menteur ne soit apparue paradoxale

que bien plus tard ; lorsqu'au IV^e siècle av. J.-C., Euclide de Milet énonça : "Un homme disait qu'il était en train de mentir. Ce que l'homme disait est-il vrai ou faux ?".

On pourrait allonger ce paradoxe par cet énoncé : "La phrase suivante est fausse. La phrase précédente est vraie".

Attribuons à Épiménide le propos : "Tous les Crétois sont des menteurs " Ceci était considéré par les philosophes antiques comme un paradoxe puisqu'il échappait au principe de non-contradiction, En effet, soit Épiménide dit vrai, alors il ment (puisque c'est un Crétois), donc son affirmation est fausse (puisque tous les Crétois mentent). soit ,au contraire, Epiménide ment en disant cela , alors il existe au moins un Crétois qui dit la vérité, et donc son affirmation est fausse. Dans tous les cas, Son affirmation est fausse, ce qui n' est pas contradictoire ; c'est la solution du paradoxe.

4.1.3.2 Solution du paradoxe

Aristote semble faire allusion à ce paradoxe dans "les Réfutations sophistiques" et donne cette solution : on peut mentir en général, tout en disant la vérité sur un point particulier. La contradiction disparaît dès lors qu'on comprend la proposition ainsi : "je dis vrai en disant que je mens" : la vérité en question n'est plus alors absolue, mais relative à un contenu déterminé. Une ambiguïté naît donc de la confusion entre le langage et le métalangage (celui qui parle du langage dans lequel il parle au moment où il parle).

Les interprètes modernes ont résolu ce paradoxe en l'étalant dans l'espace. En effet, tout ce qu'on peut déduire de la citation d'Épiménide, c'est qu'elle est fausse ; en particulier tous les Crétois ne sont pas des menteurs, mais Epiménide, lui, en est un. On résout ainsi le paradoxe en létalant dans l'espace. Néanmoins la phrase, au présent, nécessiterait une analyse au même temps, avec toute l'instantanéité nécessaire à la résolution de l'assertion d'Epiménide.

En fait, la négation de "Tous les Crétois sont des menteurs" n'est pas : "Tous les Crétois disent la vérité", mais : "l existe au moins un Crétois qui dit la vérité" (et il faudrait même dire, dans le sens où menteur est utilisé jusqu'ici, "Il existe au moins un Crétois qui dit parfois la vérité"). Donc, il peut exister un ou plusieurs menteurs crétois, mais il est vrai que celui-ci peut être Epiménide.

De manière analogue, le paradoxe "Je mens toujours" cesse de l'être lorsqu'on l'étale dans le temps : au moment où je dis "Je mens toujours" , je mens nécessairement (sinon, on a le même problème qu'avec Épiménide), ce qui implique que je ne mens pas toujours. il n'y pas de contradiction logique :il m'arrive de mentir, mais pas toujours !

Le paradoxe du menteur devient plus intéressant lorsqu'on en considère la version suivante : "Je mens en ce moment même". Si alors elle devient vraie !

Cela indique que quand une phrase peut se prendre elle-meme pour énoncé, cela peut conduire à une situation instable.

Cette phrase réalise une action du fait de son énonciation, c'est une contradiction performative. Autre exemple : "je suis mort" (si je parle c'est que je suis encore vivant).

4.1.4 Paradoxe de Cantor

Le paradoxe de Cantor, ou paradoxe du plus grand cardinal, est un paradoxe de la théorie des ensembles dont l'argument a été découvert par Georg Cantor dans les années 1890 (on le trouve dans une lettre à David Hilbert datée de 1897). Il est appelé ainsi par Bertrand Russell dans ses "Principles of Mathematics" de 1903. Le paradoxe énonce que l'existence d'un plus grand cardinal conduit à une contradiction. Dans une théorie des ensembles trop naive, qui considèrerait que toute propriété définit un ensemble, ce paradoxe est bel et bien une antinomie, une contradiction déduite de la théorie, puisque le cardinal de la classe de tous les ensembles serait alors le plus grand cardinal Mais ce n'en est pas une pour Cantor, qui n'a d'ailleurs jamais parlé de paradoxe. Pour lui, cela montre que le plus grand cardinal, s'il peut d'une certaine façon se définir, n'est pas un ensemble : reformulé en termes modernes et dans une théorie des ensembles axiomatique que ne connaissait pas Cantor, la classe des cardinaux n'est pas un ensemble.

4.1.4.1 Énoncé du paradoxe

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

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

4.1.4.2 Paradoxe de Cantor et paradoxe de Russell

Pour Cantor peut éliminer tout appel à la notion de cardinal, et donc à l'axiome *du* choix dans le second raisonnement. Soit la classe de tous les ensembles (dont le cardinal serait naturellement le plus grand cardinal).

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

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

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

l'axiome de l'ensemble des parties).

4.1.5 Paradoxe de Richard

Le paradoxe de Richard apparait dans une théorie des ensembles qui n'est pas suffisamment formalisée. Il a joué un rôle important dans les recherches sur les fondements des mathématiques, en particulier au début du XXe siècle, et a suscité depuis sa publication en 1905 de nombreux commentaires. Son auteur, le mathématicien français Jules Richard, professeur au lycée de Dijon, le décrit dans une lettre au directeur de la Revue générale des Sciences Pures et Appliquées. Ce dernier décida de la publier, sous forme d'un court article, dans le numéro du 30 juin 1905 de cette revue.

4.1.5.1 Énoncé du paradoxe

Si l'on numérote tous les nombres réels définissables en un nombre fini de mots, alors on peut construire, en utilisant l'argument de la diagonale de Cantor un nombre réel hors de cette liste. Pourtant ce nombre a été défini en un nombre fini de mots.

Voici quelques détails sur la construction :

1. Les nombres réels définissables avec un nombre fini de mots forment, de ce fait même, un ensemble dénombrable, soit E .
2. On peut construire un réel N qui n'est pas dans E par le procédé de diagonalisation suivant : on numérote les éléments de E , puis, on choisit chaque chiffre de N de sorte que le n -ième chiffre de N soit différent du n -ième chiffre du n -ième élément, et que ce ne soit pas 9 (pour éviter la double écriture des décimaux). Ainsi, pour chaque n , l'élément numéro n diffère de N pour au moins un chiffre, donc n diffère bien de N (tous les réels, en dehors des décimaux, ont une écriture décimale unique).
3. Cependant, en décrivant ce procédé de construction, on a défini N en un nombre fini de mots : c'est une contradiction.

Ce paradoxe, qui se formule très simplement, comme le paradoxe de Russell, pose cependant un problème de nature différente, qui est celui du langage licite pour les énoncés mathématiques,

4.1. Paradoxes, théorie naïve des ensembles

comme le remarque Giuseppe Peano dès 1906. Comme le paradoxe de Russell, il joue un rôle important dans la crise des fondements des mathématiques au début du XXe siècle, crise que voulut résoudre d'une façon définitive le programme de Hilbert. Il est mentionné par Kurt Gödel dans l'introduction de son article de 1931 sur les théorèmes d'incomplétude : quand il résume l'argument permettant de construire une proposition indécidable, il déclare que "L'analogie qui existe entre ce raisonnement et l'antinomie de Richard saute aux yeux". Il s'agit de la construction de l'énoncé indécidable, qui utilise bien un raisonnement diagonal et l'énumération des formules du langage, énumération qui doit cependant être effective dans la preuve du théorème de Gödel. L'énoncé que Gödel construit est inspiré lui du paradoxe du menteur, sous une forme - une proposition qui énonce d'elle-même qu'elle n'est pas démontrable (ou qu'elle est fausse, pour que ce soit vraiment le paradoxe du menteur) - qui pose le même genre de questions que le paradoxe de Richard

Le paradoxe de Richard eut également de nombreuses reformulations, notamment le paradoxe de Berry sur le plus petit entier non définissable en moins de 10^{10} ou n'importe quel nombre supérieur au non ω , il est interdit d'utiliser pour définir cet entier), appelé d'ailleurs parfois également paradoxe de Richard.

4.1.5.2 Solution du paradoxe

Le plus souvent, on résout ce paradoxe en distinguant deux niveaux de langage, celui de la théorie que l'on décrit, appelé parfois langage objet, et le langage, le plus souvent non formalisé, que l'on utilise pour décrire cette théorie, le métalangage. Quand on définit l'ensemble dénombrable des réels définissables en un nombre fini de mots, ce ne peut être que dans un langage particulier. La description du réel N se fait en un nombre fini de mots dans le métalangage. Sa construction montre simplement qu'il ne peut se décrire en un nombre fini de mots dans le langage du départ. Pour pouvoir refléter le paradoxe dans le langage objet, il faudrait coder le métalangage dans le langage objet, comme le fait Gödel pour le paradoxe du menteur. Alors il n'y a plus de paradoxe.

Cette solution (distinguer deux niveaux de langage) n'était pas vraiment celle proposée par Richard dans son article. Pour lui, le paradoxe vient de la définition même de N qui invoque

l'ensemble E , alors que celui-ci n'est pas encore complètement défini. Pour Richard, quand on construit l'énumération, au moment où l'énoncé définissant N (et où donc la lettre E apparaît), est énuméré, il n'a pas encore de sens. C'est ce que Henri Poincaré, qui s'est beaucoup intéressé au paradoxe de Richard, a systématisé sous le nom de définitions "non prédicatives". Il voyait dans le refus de ces définitions la "vraie solution" aux paradoxes. On a depuis mis en évidence des théories non prédicatives cohérentes (non paradoxales), mais néanmoins la prédicativité reste un bon principe d'élaboration de théories cohérentes. Aussi la prédicativité est un principe souhaité par certains, comme Quine qui y voit une manière d'éviter un "engagement ontologique" qui n'a pas de sens sauf à soutenir la position philosophique qu'est le platonisme mathématique.

4.1.6 Paradoxe de Grelling

Le paradoxe de Grelling-Nelson est un paradoxe sémantique formulé en 1908 par Kurt Grelling et Leonard Nelson, et parfois attribué par erreur au philosophe et mathématicien allemand Hermann Weyl. Il est alors appelé paradoxe de Weyl, mais aussi paradoxe de Grelling.

4.1.6.1 Énoncé du paradoxe

Le paradoxe de Grelling peut être énoncé de la manière suivante : certains adjectifs décrivent des propriétés qui s'appliquent à eux-mêmes, tels que «polysyllabique», «français». De tels adjectifs peuvent être qualifiés d'autologiques. D'autres adjectifs, à l'inverse, décrivent des propriétés qui ne s'appliquent pas à eux-mêmes. Par exemple, «long», «monosyllabique». On peut qualifier de tels mots d'hétérologiques. Ceci conduit à classer les mots en deux catégories :

- (a) autologiques ;
- (b) hétérologiques.

Une telle distinction conduit toutefois à un paradoxe. Compte tenu des définitions précédentes, le paradoxe apparaît en effet lorsqu'on s'interroge sur le statut du prédicat hétérologique lui-même. Ainsi, «hétérologique» est-il autologique ou bien hétérologique ? Car si «hétérologique» est hétérologique, alors par définition, «hétérologique» est autologique. Et inversement, si «hétérologique» est autologique, il en résulte qu'il est hétérologique. La conclusion est paradoxale,

car il s'ensuit qu'«hétérologique» est hétérologique si et seulement s'il est autologique.

Le paradoxe provient de ce que si le mot hétérologique ne s'applique pas à lui-même, alors il est ainsi hétérologique tout en ne l'étant pas, et s'il s'applique à lui, il n'est alors pas hétérologique tout en l'étant. Les raisonnements qui conduisent au paradoxe de Grelling peuvent être présentées de façon plus détaillée de la manière suivante : On constate alors que la proposition $P(X) = \ll \text{le mot } X \text{ est hétérologique} \gg$ est une proposition pour laquelle la valeur de A -vérité est indéfinie si X est le mot hétérologique. Mais on voit également que le mot hétérologique n'est pas non plus autologique. La proposition $P(X)$ admet donc trois plages de valeurs, dont l'une est indéfinie, quand X parcourt l'ensemble des mots de la langue.

4.1.6.2 Solution du paradoxe

Parmi les solutions qui ont été proposées pour résoudre le paradoxe de Grelling, l'une d'entre elles conduit à observer que la structure du paradoxe est très similaire à celle du paradoxe de Russell. Ainsi, les deux paradoxes présenteraient une structure commune et condition conduit, de même de même nature.

a rejeter les définitions de tous les prédicats qui présentent structure auto-référentielle. Pourtant, une telle solution ne s'avère pas non plus satisfaisante. En effet, elle apparaît beaucoup trop restrictive, car il s'avère que l'on parvient tout à fait valablement à déterminer le statut de nombreux prédicats auto-référentiels tels que par exemple polysyllabique. Proscrire purement et simplement tous les prédicats dont la structure est auto-référentielle serait payer un prix beaucoup trop fort pour la seule élimination du paradoxe.

4.2 Axiomes de Zermelo-Fraenkel (ZF)

Nous allons parler de l'axiome du choix, spécifiquement en logique mathématique dans l'axiomatisation usuelle des ensembles appelée ZF (pour la théorie de Zermelo-Fraenkel). Nous allons donc dans un premier temps présenter cette axiomatisation et faire tous les rappels nécessaires à un énoncé précis de l'axiome du choix.

La théorie axiomatique de Zermelo-Fraenkel est une théorie fondée sur la logique du premier

4.2. Axiomes de Zermelo-Fraenkel (ZF)

ordre avec identité, et un seul symbole non logique. Il s'agit d'une théorie axiomatique du premier ordre, construite sur le langage $\{2, =\}$. Les objets dont parle cette théorie, c'est-à-dire les éléments d'un modèle de ZF sont des ensembles : toute variable représente un ensemble et il n'existe pas d'autres types d'objets.

Voici les axiomes de la théorie ZF :

4.2.1 Axiome d'extentionnalité

Deux ensembles sont identiques s'ils ont les mêmes éléments.

$$\forall A \forall B [(\forall x (x \in A \Leftrightarrow x \in B)) \Rightarrow A = B]$$

Il stipule que si A et B sont deux ensembles ayant exactement les mêmes éléments, alors ils sont égaux ; ainsi pour définir un ensemble A il suffira de définir ses éléments

4.2.2 Axiomes de construction

4.2.2.1 Axiome de la paire

$$\forall x \forall y \exists A \forall z ((z \in A) \Leftrightarrow (z = x \vee z = y)).$$

Il signifie qu'étant donnée deux ensembles x et y , il existe un ensemble A qui n'a pour éléments que x et y ; cet ensemble est unique par l'axiome d'extensionnalité et on le notera $\{x, y\}$. Par l'axiome d'extensionnalité, cet ensemble est unique et l'on peut définir la paire $\{a, b\}$ par l'unique c tel que $\forall z ((z \in c) \Leftrightarrow (z = a \vee z = b))$. On peut également définir le singleton $\{a\}$ comme l'ensemble $\{a, a\}$. Comme $\{a, b\} = \{b, a\}$; on définit également la paire ordonnée (a, b) par $(a, b) = \{\{a\}, \{a, b\}\}$.

4.2.2.2 Axiome de la réunion

$$\forall E \exists A (\forall z (z \in A) \Leftrightarrow (\exists y \in E, z \in y)).$$

4.2. Axiomes de Zermelo-Fraenkel (ZF)

Cela veut dire que les éléments de A sont exactement les éléments des éléments de E . Encore une fois, un tel ensemble est unique. On le notera $\cup E$ (lire union de E). Cela correspond informellement à une union indexée par l'ensemble d'indices E , les ensembles que l'on réunit étant précisément les éléments de E . Par exemple, si l'on sait que $\{\{1, 2\}, \{3, 4, 5\}\}$ est un ensemble (à deux éléments), on en déduit l'existence de l'ensemble $\{1, 2, 3, 4, 5\}$.

Cet axiome nous permet ainsi de définir l'union de deux ensembles arbitraires par $x \cup y = \cup\{x, y\}$. Cette définition illustre bien l'union ensembliste "naïve" car il est possible de démontrer $\forall x \forall y \forall z ((z \in x \cup y) \Leftrightarrow (z \in x \vee z \in y))$ à partir des axiomes établis jusqu'ici.

4.2.2.3 Axiome des parties

Si x est un ensemble, il existe un ensemble y dont les éléments sont les sous-ensembles de x .

$$\forall x \exists y \forall t ((t \in y) \Leftrightarrow (\forall v (v \in t) \Rightarrow (v \in x)))$$

Soient a et b deux ensembles. L'énoncé $\forall x (x \in a) \Rightarrow (x \in b)$ exprime l'inclusion des ensembles. On abrègera les énoncés en remplaçant cette formule par $a \subset b$. L'axiome des parties peut alors se reccrire de manière abrégée :

$$\forall x \exists y \forall t ((t \in y) \Leftrightarrow (t \subset x))$$

Cet axiome énonce donc que si x est un ensemble, il existe un ensemble, que l'on notera $\mathcal{P}(x)$, l'ensemble des parties de x , dont les éléments sont exactement les sous-ensembles de x .

4.2.2.4 Schéma d'axiomes de compréhension

Si $\mathfrak{P}(x)$ est une propriété et E un ensemble, alors le regroupement des objets x de E qui vérifient la propriété $\mathfrak{P}(x)$ est encore un ensemble. Notons que cet axiome permet de définir un ensemble à partir d'une propriété, mais seulement si les éléments appartiennent déjà à un autre ensemble : cela évite la définition d'ensembles trop gros et évite les deux paradoxes de Russell et de Cantor. Donc l'ensemble naïf de tous les ensembles n'est pas un ensemble de la théorie ZF!

4.2. Axiomes de Zermelo-Fraenkel (ZF)

On peut énoncer formellement le schéma de compréhension ainsi :

$$\forall a_1 \dots \forall a_n \forall A \exists B \forall x [x \in B \Leftrightarrow ((x \in A) \wedge P(x, a_1, \dots, a_n))]$$

pour toute formule P ne contenant pas d'autres variables libres que x, a_1, \dots, a_n (en particulier B ne peut apparaître dans P). Les a_1, \dots, a_n sont des paramètres de la formule P .

Ce schéma implique en particulier l'existence d'un ensemble n'ayant aucun élément. En effet, l'ensemble Y défini par :

$$\forall x(x \in Y) \Leftrightarrow ((x \in X) \wedge (x \neq x))$$

existe justement par l'axiome de compréhension et est vide. Un tel ensemble est unique par extensionnalité, on le notera \emptyset par la suite.

Ce schéma permet aussi de définir l'intersection de deux ensembles, disons A et B . Il s'agit simplement de l'ensemble X défini par :

$$\forall z(z \in X) \Leftrightarrow ((z \in A) \wedge (z \in B))$$

(en le considérant ici comme un sous-ensemble de A). Une fois encore, l'extensionnalité prouve l'unicité d'un tel ensemble, on le notera $A \cap B$.

4.2.2.5 Axiome de remplacement

Les axiomes précédents ne permettent en fait pas de parler de tous les ensembles dont on aurait envie. Il faut encore ajouter la chose suivante :

On dit que $F(x, y, a_1, \dots, a_n)$ une formule à $(n + 2)$ variables libres est une relation fonctionnelle (ou classe fonctionnelle) en x et y si elle vérifie la condition suivante :

$$\forall x \forall y \forall y' \forall a_1, \dots, \forall a_n$$

$$((F(x, y, a_1, \dots, a_n) \wedge F(x, y', a_1, \dots, a_n)) \Rightarrow (y = y')).$$

Cela veut exactement dire qu'étant donnés x, a_1, \dots, a_n , il y a au plus un y qui vérifie $F(x, y, a_1, \dots, a_n)$; c'est l'image de x par la fonctionnelle F .

Le schéma de remplacement dit que pour toute fonctionnelle F , si A est un ensemble, il en est de même de $F(A)$. On aimerait donc indexer les axiomes par des fonctionnelles. Seulement,

4.2. Axiomes de Zermelo-Fraenkel (ZF)

cela n'est pas possible, car la propriété d'être une fonctionnelle dépend fortement de l'univers considéré et on aimerait que les axiomes n'en dépendent pas quand même. On indexe en fait les axiomes par toutes les formules et on procède ainsi :

$$\begin{aligned}
 & F(x, y, a_1, \dots, a_n) \text{ fonctionnelle} \Rightarrow \\
 & \forall a_1 \dots \forall a_n \forall A \exists B \forall y \\
 & ((y \in B) \Leftrightarrow (\exists x \in A \wedge F(x, y, a_1, \dots, a_n))).
 \end{aligned}$$

L'ensemble B sera noté $F(A)$.

Une variante du schéma de remplacement tel qu'énoncé ci-dessus, est de supposer qu'en plus d'être fonctionnelle, la relation définie par F (avec les notations ci-dessus) est partout définie sur l'univers, on ajoute donc l'hypothèse :

$$\forall a_1 \dots \forall a_n \forall x \exists y F(x, y, a_1, \dots, a_n)$$

Dans ce cas on peut utiliser la notation $y = \phi(x)$ pour la fonctionnelle $F(x, y, a_1, \dots, a_n)$. Si A est un ensemble, alors l'ensemble obtenu par remplacement, à partir de la relation fonctionnelle F se note alors $\{\phi(x) \mid x \in A\}$.

Quand f est une fonction (au sens ensemble de couples) définie sur A , on note également

$$\{f(x) \mid x \in A\} = \{y \mid \exists x \in A \text{ tel que } y = f(x)\}$$

l'ensemble dont l'existence se justifie par le schéma de compréhension.

4.2.2.6 Axiome de l'infini

Il existe un ensemble infini, c'est à dire par définition un ensemble qui comporte un sous ensemble différent de lui-même et aussi gros que lui-même. Il y a moult façons de le formuler, par exemple :

$$\exists X((\exists x \in X) \wedge (\forall x \in X, x \cup \{x\} \in X))$$

où $\{x\}$ est l'ensemble contenant uniquement x , il existe en vertu de l'axiome de la paire.

4.2. Axiomes de Zermelo-Fraenkel (ZF)

4.2.2.7 Axiome de fondation

Il n'existe pas de chainnes infinies descendantes d'ensembles (x_n) tel que x_{n+1} appartient à x_n appartient à... x_1 , appartient à x_0 . En particulier cet axiome évite l'existence d'un ensemble x qui appartienne à x . Plus précisément, l'axiome de fondation précise que tout ensemble non vide contient un autre ensemble dont l'intersection avec le premier ensemble est vide. La façon la plus simple d'écrire cela sous forme d'un axiome est sans doute la suivante :

$$\forall x(x \neq \emptyset) \Rightarrow (\exists y \in x, (x \cap y) = \emptyset).$$

4.2.3 Théorie de Zermelo

La théorie de Zermelo est une présentation moderne de la théorie publiée par ce dernier en 1908, présentée explicitement ou implicitement dans le cadre de la logique du premier ordre avec égalité. Elle comporte les axiomes suivants :

- Axiome d'extensionnalité;
- Axiomes de construction :
 - Axiome de la paire;
 - Axiome de la réunion;
 - Axiome de l'ensemble des parties;
 - Axiome de l'infini;
 - Schéma d'axiomes de compréhension.

Remarque. L'axiome de l'ensemble vide, parfois introduit séparément, se déduit du schéma d'axiomes de compréhension (en logique du premier ordre)

4.2.4 Théorie de Zermelo-Fraenkel

Elle comporte en plus :

- Schéma d'axiomes de remplacement;
- Axiome de fondation.

4.2. Axiomes de Zermelo-Fraenkel (ZF)

Le schéma d'axiomes de remplacement permet en particulier le développement de la théorie des ordinaux.

- Le schéma d'axiomes de compréhension se déduit du schéma d'axiomes de remplacement (et donc en particulier l'existence de l'ensemble vide, étant admis que tout univers ensembliste possède au moins un élément).
- L'axiome de la paire se déduit de l'axiome des parties et du schéma de remplacement.

4.3 Axiome du choix (AC)

On note ZFC le système axiomatique obtenu en ajoutant au système de Zermelo-Fraenkel (ZF) l'axiome du choix (AC).

4.3.1 Axiome du choix

Soit E un ensemble non vide, il existe une fonction f de $P(E) \setminus \{\emptyset\}$ dans E qui à toute partie non vide A de E associe un élément de cette partie. De façon plus formelle, cela s'écrit :

$$\forall E \exists f (f \text{ fonction de } P(E) \setminus \{\emptyset\} \text{ dans } E)$$

et

$$[\forall A \in P(E) \setminus \{\emptyset\} (A, a) \in f \Rightarrow a \in A]$$

Une fonction f qui vérifie cette propriété s'appelle une fonction de choix sur E . L'axiome du choix dit exactement que tout ensemble admet une fonction de choix.

Par exemple si $E = \{\{1, 2, 3\}, \{a, b\}, \{x, y\}\}$ alors on peut constituer l'ensemble $f = \{(\{1, 2, 3\}, 1), (\{a, b\}, b), (\{x, y\}, x)\}$.

4.3.2 Quelques formes équivalentes

L'axiome du choix est équivalent à de nombreux autres énoncés :

1. Produit cartésien d'ensembles : de façon équivalente et plus compacte, il dit qu'un produit non vide (i.e. indexé par un ensemble non vide) d'ensembles non vides est non vide.

4.3. Axiome du choix (AC)

2. Théorème de Zermelo : Tout ensemble possède un bon ordre.
3. Lemme de Zorn : Tout ensemble ordonné dans lequel toute partie non vide, totalement ordonnée, est majorée, possède au moins un élément maximal
4. Principe de maximalité de Hausdorff : Tout ensemble ordonné possède une partie totalement ordonnée maximale.
5. Toute surjection est inversible à droite : soient X et Y deux ensembles et $f : X \rightarrow Y$ une application surjective, alors il existe une application $g : Y \rightarrow X$ telle que $g \circ f = Id_Y$.

4.3.3 Lemme de Zorn

Définition 4.1 Soit E un ensemble muni d'une relation binaire que l'on note \leq . On dit que cette relation est un ordre si elle vérifie les trois propriétés suivantes :

- (réflexivité) : $\forall x \in E, x \leq x$
- (transitivité) : $\forall x \in E \forall y \in E \forall z \in E ((x \leq y \wedge y \leq z) \Rightarrow (x \leq z))$
- (antisymétrie) : $\forall x \in E \forall y \in E ((x \leq y \wedge y \leq x) \Rightarrow (x = y))$.

Une relation sur E qui vérifie juste les deux premières conditions est ce que l'on appelle un préordre.

Définition 4.2 On dit que l'ordre est total, ou encore que E est totalement ordonné, si la relation \leq vérifie en outre la condition :

$$\forall x \in E \forall y \in E (x \leq y \vee y \leq x)$$

Remarque. On dira souvent de E qu'il est un ensemble partiellement ordonné s'il est juste muni d'une relation d'ordre. Le mot "partiellement" ne sous-entend aucunement que la relation d'ordre n'est pas totale, il est juste là pour préciser qu'elle ne l'est pas forcément.

Définition 4.3 Soit E un ensemble partiellement ordonné. Ce que l'on appelle un plus grand élément de E , c'est un élément x de E plus grand que tous les autres, c'est-à-dire vérifiant $y \leq x$ pour tout y dans E .

Remarque.

4.3. Axiome du choix (AC)

- La propriété d'antisymétrie prouve directement que s'il existe un plus grand élément, alors celui-ci est unique.
- Il est important de ne pas confondre cette notion avec la notion d'élément maximal. Un élément maximal de E , c'est un élément x de E tel qu'il n'existe pas de y strictement supérieur (i.e. supérieur et différent) à x .

Exemple. Pour illustrer la distinction, il est intéressant de remarquer que si E est un ensemble muni de la relation "égalité" (i.e. $x \leq y$ si et seulement si $x = y$) qui est une relation d'ordre, alors tout élément de E est un élément maximal mais E n'admet pas de plus grand élément dès qu'il est de cardinal plus grand que 2. Il est intéressant aussi de remarquer que cet exemple prouve qu'un élément maximal n'est pas du tout forcément unique.

Remarque. Il est cependant vrai que si E est totalement ordonné, alors un élément maximal est forcément unique et que les notions d'élément maximal et de plus grand élément coïncident. Il est également vrai que si E est un ensemble partiellement ordonné admettant un plus grand élément x , alors il admet un unique élément maximal qui est précisément x .

Définition 4.4 Reprenons maintenant E un ensemble partiellement ordonné. Soit A est une partie de E , la relation d'ordre, \leq disons, se restreint à A (formellement il s'agit de faire l'intersection de l'ensemble \leq avec l'ensemble AA).

- On dit que A est majoré dans E s'il existe un élément x de E plus grand que tous les éléments de A , c'est-à-dire tel que $y \leq x$ pour tout y dans A .
- On dit que A est une chaîne si l'ordre induit sur A est total.
- On dit que E est inductif si toute chaîne de E est majorée.
- Finalement, on dit que E est bien ordonné si toute partie A non vide admet un plus petit élément.

Principe de maximalité de Hausdorff (PM) : Tout ensemble partiellement ordonné admet une chaîne maximale.

Une autre formulation plus courante de cet énoncé est le lemme de Kuratowski-Zorn, sans doute plus connu sous le nom de lemme de Zorn.

Lemme de Zorn : Tout ensemble préordonné inductif a un élément maximal.

Equivalence de ces deux énoncés : Supposons dans un premier temps le principe de maximalité de Hausdorff et prenons E un ensemble partiellement ordonné inductif. Il s'agit de prouver que E admet un élément maximal. On considère pour cela, un sous-ensemble A de E qui est une chaîne maximale. Elle est majorée par hypothèse. Notons x un majorant. S'il existait dans E un élément y strictement supérieur à x , alors l'ensemble $A \cup \{y\}$ serait une chaîne de E contenant strictement A , ce qui est exclu. Cela prouve bien que x est un élément maximal de E ,

Réciproquement, supposons le lemme de Zorn. Soit E un ensemble partiellement ordonné. On considère X le sous-ensemble de $P(E)$ formé des chaînes de E que l'on ordonne par inclusion. On affirme que cet ensemble est inductif. En effet, étant donné une partie X^n de X , il est immédiat de constater que la réunion de X^* (qui est une partie de E) majore X' . Le lemme de Zorn appliqué à X fournit précisément ce que l'on cherche.

4.3.4 Applications de l'axiome du choix

L'axiome du choix est un outil central dans les mathématiques appliquées. Une des toutes premières mentions explicites de cet axiome est due à Peano, en 1890, dans sa preuve de l'existence d'une solution pour un système d'équations différentielles. Parmi les preuves classiques de mathématiques qui utilisent l'axiome du choix, on peut mentionner :

- En topologie générale : Le théorème de Tychonoff .

Théorème 4.1 Tout produit d'espaces topologiques compacts est compact.

- En algèbre : L'axiome du choix est utilisé souvent en algèbre sous une forme différente : le lemme de Zorn.

Théorème 4.2 Tout espace vectoriel possède une base.

Théorème 4.3 Tout idéal propre d'un anneau est inclus dans un idéal propre maximal.

Théorème 4.4 Tout corps possède une unique clôture algébrique.

- En analyse fonctionnelle : Le théorème de Hahn-Banach (forme géométrique).

4.3. Axiome du choix (AC)

Théorème 4.5 Soient E un espace vectoriel topologique, A et B deux ensembles convexes non vides, disjoints, dont l'un est ouvert. Alors il existe un hyperplan H qui sépare A et B .

- **En théorie des jeux :** L'axiome du choix a pour conséquence qu'il existe un ensemble A de suites d'entiers tel qu'aucun des deux joueurs ne possède une stratégie gagnante dans le jeu suivant : ils choisissent tour à tour un entier, et le premier joueur gagne si et seulement si la suite ainsi formée appartient à A .
- **En théorie de la mesure :** L'axiome du choix permet d'affirmer l'existence de parties de \mathbb{R} non mesurables au sens de Lebesgue.

L'axiome du choix est donc très utile en mathématiques. C'est pourquoi il est accepté par les mathématiciens malgré le fait qu'il ait aussi des conséquences paradoxales, comme par exemple le célèbre paradoxe de Banach-Tarski. Celui-ci énonce qu'on peut découper une boule de rayon r de manière à obtenir des morceaux permettant de recomposer deux boules de rayon r .

4.3.5 Indépendance de l'axiome du choix

Deux résultats de logique indiquent que l'axiome du choix est indépendant des autres axiomes de la théorie des ensembles.

Théorème 4.6 (Gödel, 1938) ZFC est consistant si ZF l'est.

Ici consistant signifie qu'aucune contradiction ne pourra être trouvée à partir de ces axiomes. On sait que s'il est consistant, le système ZF ne réfute pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de la négation de AC à partir des axiomes du système ZF .

Théorème 4.7 (Cohen, 1963) $ZF + \neg AC$ est consistant si ZF l'est.

S'il est consistant, le système ZF ne démontre pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de AC à partir des axiomes du système ZF .

La preuve utilise la technique du forcing, laquelle est difficile. Une autre approche, basée sur les algèbres booléennes, est censée être plus simple. Pour plus de détails,

4.4 Exercices

Exercice 1. Montrer que si $(a, b) = (c, d)$, alors $a = c$ et $b = d$.

Exercice 2. Soit $y = \{\{a, b, c\}, \{\{a, b\}\}, \{a\}, \{\{d\}\}\}$, quels sont les éléments de y ?

Exercice 3. Montrer que si a, b, c sont des ensembles, on peut définir un ensemble d dont les éléments sont exactement a, b et c . On notera $d = \{a, b, c\}$

Exercice 4. Soient a, b deux ensembles. Montrer que ab est un ensemble.

Exercice 5. Montrer que l'axiome de la paire est une conséquence du schéma de substitution et de l'axiome des parties.

Exercice 6. Montrer que le schéma de séparation est une conséquence du schéma de remplacement.

Exercice 7. Soit A et B deux classes. On définit la classe $A\Delta B$, la différence symétrique de A et B par :

$$A\Delta B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

- Montrer que si a et b sont des ensembles, la classe $a \Delta b$ est un ensemble.

Exercice 8. On appelle axiome de fondation la formule suivante :

$$\forall x(x \neq \emptyset \Rightarrow \exists y[(y \in x) \wedge (y \cap x = \emptyset)]).$$

- Montrer que l'axiome de fondation implique :
 1. qu'un ensemble x ne peut se contenir, c'est-à-dire que pour tout ensemble $x, x \notin x$;
 2. que pour tous ensembles x_1, \dots, x_n tels que pour tout $i \geq 1$ et $i \leq n - 1$, on ait $x_i \in x_{i+1}$, on a nécessairement $x_n \notin x_1$;
 3. (avec l'axiome de l'infini) qu'il n'existe pas de suite x_1, \dots, x_n, \dots , d'ensembles tels que pour tout $i \geq 1, x_{i+1} \in x_i$.

Exercice 9. Montrer que l'axiome de la paire est une conséquence du schéma de substitution et de l'axiome des parties.

Exercice 10. On considère la théorie ZFC_{fin} qui est la théorie ZF (schéma de remplacement, axiome des parties, axiome de la réunion, axiome d'extensionnalité) avec l'axiome du choix et l'axiome de fondation. Le but de l'exercice est de donner un modèle de ZFC_{fin} qui ne satisfait pas l'axiome de l'infini. Pour tout entier q , on définit $[q]$ comme l'unique ensemble d'entiers $\{p_1, \dots, p_n\}$ tel que $q = \sum_{i=1}^n 2^{p_i}$ (penser à l'écriture de q en base 2).

On définit la relation binaire E sur \mathbb{N} par : $pEq \iff p \in [q]$; montrer que :

1. La structure (N, E) satisfait l'axiome d'extensionnalité ;
2. Pour tout entier q , l'ensemble $[q]$ des E -éléments de q est fini ;
3. Pour tout ensemble fini d'entiers $\{p_1, \dots, p_n\}$, il existe un unique entier q tel que $[q] = \{p_1, \dots, p_n\}$;
4. La structure (N, E) est un modèle de ZFC_{fin} , et que l'axiome de l'infini n'est pas satisfait dans cette structure.

Bon ordre et preuve par récurrence

5.1 Preuve par récurrence

5.1.1 Preuve par récurrence simple

Théorème 5.1 Soit $\mathcal{P}(n)$ un prédicat dépendant d'un élément n de \mathbb{N} .

On suppose que $\mathcal{P}(0)$ est vraie. (Initialisation)

On suppose également que pour tout entier n l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n + 1)$ est vraie.

(Hérédité)

0. Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier n .

Preuve. On raisonne par l'absurde.

Soit $E = \{n \in \mathbb{N}, \mathcal{P}(n) \text{ est faux} \}$.

En tant que partie non vide de \mathbb{N} , l'ensemble E a un plus petit élément n_0 .

n_0 est différent de 0 car on a supposé $\mathcal{P}(0)$ vraie comme $0 < n_0$ on sait que $n_0 - 1 \in \mathbb{N}$.

$\mathcal{P}(n_0 - 1)$ est vraie car $n_0 - 1 \notin E$.

Par hypothèse $\mathcal{P}(n) \Rightarrow \mathcal{P}(n + 1)$ d'où $\mathcal{P}(n_0)$ est vraie ce qui contredit le fait que $n_0 \in E$.

Cette méthode de démonstration utilise le principe dit : "principe du bon ordre".

Exemple. Soit la suite définie par la relation de récurrence :

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}$$

On va montrer par récurrence que $(u_n)_{n \in \mathbb{N}}$ est majorée par 1.

Pour $n = 0$ on a $u_0 = \frac{1}{2} \leq 1$.

On suppose ensuite que la proposition est vraie pour n et on la démontre pour $n + 1$.

On remarquera que les termes de la suite sont positifs.

$$0 \leq u_n \leq 1 \Rightarrow u_n^2 \leq 1 \Rightarrow u_n^2 + 1 \leq 1 + 1 \Rightarrow \frac{1 + u_n^2}{2} \leq \frac{2}{2} = 1$$

5.1.2 Schéma de preuve par le principe du bon ordre

1. Définir l'ensemble $E = \{n \in \mathbb{N} : P(n) \text{ est faux} \}$
2. Supposer que E est non vide comme base pour une preuve par contradiction.
3. Comme \mathbb{N} est bien ordonné, il y a un plus petit élément n_0 dans E .
4. Le plus petit élément ne peut pas être celui de la proposition de départ. Utiliser l'hérédité pour arriver à la contradiction.

Exemple.

Soit la suite définie par la relation de récurrence :

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}$$

On va montrer par le principe du bon ordre que $(u_n)_{n \in \mathbb{N}}$ est majorée par 1. On raisonne par l'absurde.

Soit $E = \{n \in \mathbb{N}, u_n > 1\}$

En tant que partie non vide de \mathbb{N} l'ensemble E a un plus petit élément n_0 . On a n_0 différent de 0 car on a $u_0 = \frac{1}{2} \leq 1$.

Comme $0 < n_0$ on sait que $n_0 - 1 \in \mathbb{N}$ et $n_0 - 1 \notin E$.

$0 \leq u_{n_0-1} \leq 1 \Rightarrow u_{n_0-1}^2 \leq 1 \Rightarrow u_{n_0-1}^2 + 1 \leq 1 + 1 \Rightarrow \frac{1+u_{n_0-1}^2}{2} \leq \frac{2}{2} = 1 \Rightarrow u_{n_0} \leq 1 \Rightarrow u_{n_0} \notin E$.

Ce qui contredit le fait que $n_0 \in E$.

Exemple. (Importance de l'initialisation)

Est ce que $3^{2n+4} - 2^n$ est un multiple de 7 ?

Supposons que $3^{2n+4} - 2^n$ est un multiple de 7 .

On va montrer que $3^{2(n+1)+4} - 2^{n+1}$ est un multiple de 7 .

On a

$$\begin{aligned} 3^{2n+6} - 2^{n+1} &= 93^{2n+4} - 22^n = (7 + 2)3^{2n+4} - 22^n \\ &= 73^{2n+4} + 23^{2n+4} - 22^n \end{aligned}$$

On a par conséquent la somme de deux multiples de 7 qui est donc un multiple de 7.

Ici l'initialiation est impossible pour $n = 0$ on a $3^4 - 2^0 = 80$ qui n'est pas divisible par 7.

On peut démontrer en utilisant le calcul par congruences que $3^{2n+4} - 2^n$ n'est pas un multiple de 7.

En effet on a :

$$3^2 \equiv 2[7] \Rightarrow 3^{2n} \equiv 2^n[7] \text{ de plus on } a3^4 \equiv 4[7] \text{ d'où } 3^{2n+4} \equiv 4 \cdot 2^n[7]$$

$$\text{On a également } 2^n \equiv 2^n[7] \text{ d'où } 3^{2n+4} - 2^n \equiv 3 \cdot 2^n[7]$$

Comme 7 ne divise pas 3 ni 2 alors 7 ne divise pas $3^{2n+4} - 2^n$.

Remarque. Pour montrer qu'une proposition $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$, on remplace l'hypothèse d'initialisation par $\mathcal{P}(n_0)$ est vraie.

Exemple. Preuve par récurrence simple (avec un pas supérieur à 1)

La suite de Fibonacci est donnée par

$$\begin{cases} F_0 = 0. \\ F_1 = 1. \\ \forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n. \end{cases}$$

Soient $\varphi = \frac{1+\sqrt{5}}{2}$ et $\varphi' = \frac{1-\sqrt{5}}{2}$ (φ est appelé le nombre d'or). On a φ et φ' sont solution de l'équation $x^2 - x - 1 = 0$.

Question : Montrer que pour tout $n \geq 1$ nous avons $F_n \leq \varphi^{n-1}$.

Réponse : Pour $n = 1$ on a $F_1 = 1 \leq 1 = \varphi^0$.

$$\text{Pour } n = 2 \text{ on a } F_2 = F_1 + F_0 = 1 \leq \frac{1+\sqrt{5}}{2} = \varphi^1.$$

On doit ensuite démontrer que :

$$\forall n \geq 1 : P(n) \wedge P(n+1) \Rightarrow P(n+2)$$

On a par définition

$$\forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^n + \varphi^{n-1} \text{ (Par hypothèses de récurrence)}$$

$$\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi + 1) \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi^2) \quad (\text{Car } \varphi^2 - \varphi - 1 = 0)$$

$$\text{Donc } \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n+1}$$

5.1.3 Preuve par récurrence généralisée

Théorème 5.2 Soit $\mathcal{P}(n)$ une proposition dépendant d'un élément n de \mathbb{N} .

On suppose que $\mathcal{P}(0)$ est vraie. (Initialisation)

On suppose également que pour tout entier n que l'implication $(\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)) \Rightarrow \mathcal{P}(n+1)$ est vraie. (Hérédité)

Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier n .

Preuve. Soit la proposition $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n) = Q(n)$.

On va montrer que $Q(n)$ est vraie pour toute valeur de \mathbb{N} si et seulement si $\mathcal{P}(n)$ est vraie pour toute valeur de \mathbb{N} .

Ici il s'agit de montrer une équivalence, on doit donc montrer deux implications.

Implication n°1

On va montrer que si $Q(n)$ est vraie pour toute valeur de \mathbb{N} alors $\mathcal{P}(n)$ est vraie pour toute valeur de \mathbb{N} .

On a $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)$ Vrai, par conséquent $\mathcal{P}(0)$ Vrai et $\mathcal{P}(1)$ Vrai ...et $\mathcal{P}(n)$ Vrai donc $\mathcal{P}(n)$ est vrai.

Implication n°2

On va montrer que si $\mathcal{P}(n)$ est vrai pour toute valeur de \mathbb{N} , alors $Q(n)$ est vrai pour toute valeur de \mathbb{N} .

Comme $\mathcal{P}(n)$ est vraie pour toute valeur de \mathbb{N} par conséquent $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)$ est également vrai et donc $Q(n)$ est vrai pour toute valeur de \mathbb{N} .

Exemple. Démontrer que tout entier n entier supérieur ou égal à 2 peut se décomposer de façon unique en produit de facteurs premiers.

Démonstration.

Notons $P(n)$ la propriété : tout entier k de $\{2; 3; 4 \dots; n - 1; n\}$ peut se décomposer en produit de facteurs premiers.

i) On a $P(2)$ est vraie car $2 = 2$.

ii) Supposons que $P(k)$ est vraie pour tout entier naturel $2 \leq k \leq n$. Il faut prouver que $P(n + 1)$ est vraie.

- Si $n + 1$ est premier on peut écrire $n + 1 = n + 1$.

- Si $n + 1$ n'est pas premier il admet donc un diviseur premier p et on a $n + 1 = q.p$

On a nécessairement $q \leq n$ et donc selon (ii) q se décompose en produit de facteurs premiers.

Par conséquent, $P(n + 1)$ est vraie.

5.1.4 Preuve par récurrence forte

Théorème 5.3 Soit \mathcal{P} une proposition dépendant d'un élément n de \mathbb{N} .

Si pour tout n on a : $\forall k < n : \mathcal{P}(k) \Rightarrow \mathcal{P}(n)$

Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier n .

Preuve. On effectue la preuve par récurrence généralisée sur n .

On a pour $n = 0$.

$\forall k < 0 : \mathcal{P}(k)$ Cette proposition est vraie car k appartient à l'ensemble vide.

On suppose que la proposition $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)$ est vraie et on démontre que $\mathcal{P}(n + 1)$.

Comme $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge \dots \wedge \mathcal{P}(n)$ est vraie alors $\forall k < n + 1 : \mathcal{P}(k)$ est vraie.

D'où on obtient $\mathcal{P}(n + 1)$ est vraie.

5.1.5 Cas particulier de preuve par récurrence (récurrence de Cauchy)

Proposition 5.1 Soit $P(n)$ un prédicat qui vérifie :

$$\left\{ \begin{array}{l} (i) : P(1) \text{ est vraie.} \\ (ii) : \forall n \in \mathbb{N} : P(n) \Rightarrow P(2n) \\ (iii) : \forall n \in \mathbb{N} : P(n+1) \Rightarrow P(n) \end{array} \right.$$

Alors $P(n)$ est vraie pour toute valeur de n .

5.1.6 Preuve de l'inégalité de Cauchy Schwartz par récurrence.

Théorème 5.4 Moyenne harmonique, géométrique et arithmétique.

Soient a_1, a_2, \dots, a_n des nombres réels positifs, alors :

$$\frac{n}{\frac{1}{a_1} + \dots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$$

L'égalité ayant lieu si et seulement si tous les a_i sont égaux.

Preuve. Pour $n = 2$, il faut établir que $a_1 a_2 \leq \left(\frac{a_1 + a_2}{2}\right)^2$ c'est à dire $(a_1 - a_2)^2 \geq 0$ ce qui est vrai.

On va montrer $P(n) \Rightarrow P(n-1)$ Posons $A = \sum_{k=1}^{n-1} \frac{a_k}{n-1}$ alors :

$$\left(\prod_{k=1}^{n-1} a_k\right) A \stackrel{P(n)}{\leq} \left(\sum_{k=1}^{n-1} \frac{a_k + A}{n}\right)^n = \left(\frac{(n-1)A + A}{n}\right)^n = A^n$$

5.2 Ordre bien fondé

5.2.1 Ordre et ordre strict

Définition 5.1 Soit \mathcal{R} une relation binaire sur E .

- On dit que \mathcal{R} est réflexive quand : $\forall x \in E, x\mathcal{R}x$.
- On dit que \mathcal{R} est symétrique quand : $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

- On dit que \mathcal{R} est anti-symétrique quand : $\forall(x, y) \in E^2, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$.
- On dit que \mathcal{R} est transitive quand : $\forall(x, y, z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Définition 5.2 Une relation binaire est une relation d'ordre si elle est réflexive, antisymétrique et transitive.

Exemple. L'ensemble \mathbb{R} muni de la relation d'ordre usuel (\leq).

$$\text{Donc } \prod_{k=1}^{n-1} a_k \leq A^{n-1} = \left(\sum_{k=1}^{n-1} \frac{a_k}{n-1}\right)^{n-1}$$

On démontre à présent que $P(n) \Rightarrow P(2n)$

$$\begin{aligned} \prod_{k=1}^{2n} a_k &= \left(\prod_{k=1}^n a_k\right) \left(\prod_{k=n+1}^{2n} a_k\right) \stackrel{P(n)}{\leq} \left(\sum_{k=1}^n \frac{a_k}{n}\right)^n \left(\sum_{k=n+1}^{2n} \frac{a_k}{n}\right)^n \\ &\stackrel{P(2)}{\leq} \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} = \left(\frac{\sum_{k=1}^{2n} a_k}{2n}\right)^{2n} \end{aligned}$$

L'inégalité de gauche se déduit de la précédente en considérant $\frac{1}{a_1}, \dots, \frac{1}{a_n}$

Exemple. Sur l'ensemble des parties d'un ensemble, la relation \subset est une relation d'ordre.

Définition 5.3 Une relation binaire est une relation d'ordre strict si elle est transitive et anti réflexive.

$$\mathcal{R} \text{ anti réflexive : } \forall x \in E : x/\mathcal{R}x$$

Exemple. L'ensemble \mathbb{R} muni de la relation $<$.

Proposition 5.2 Une relation d'ordre strict est antisymétrique.

Preuve. \mathcal{R} est par définition transitive et anti réflexive.

Une relation est antisymétrique si elle vérifie

$$\forall(x, y) \in E^2, (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$$

On va montrer que dans une relation d'ordre strict la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est toujours fausse.

On raisonne par l'absurde.

On suppose qu'il existe $(x, y) \in E^2$ tel que la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est vraie. Alors par transitivité on obtient $x\mathcal{R}x$ vraie ce qui contredit le fait que \mathcal{R} est anti réflexive.

Par conséquent, la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est toujours fausse et donc l'implication logique $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$ est toujours vraie.

5.2. Ordre bien fondé

Définition 5.4 Soit (E, \mathcal{R}) un ensemble ordonné. Deux éléments x et y sont dits comparables si on a $x\mathcal{R}y$ ou $y\mathcal{R}x$. Dans le cas contraire on dit que x et y sont incomparables.

Exemple. Soit l'ensemble $\mathcal{P}(\{a, b, c\})$ -l'ensemble des parties de $\{a, b, c\}$ - muni de la relation d'ordre \subset .

Les éléments $\{a, b\}, \{b, c\}$ sont incomparables.

Définition 5.5 Un ordre \mathcal{R} sur E est dit total si deux éléments sont toujours comparables $\forall (x, y) \in E, x\mathcal{R}y$ ou $y\mathcal{R}x$.

Un ordre qui n'est pas total est dit partiel.

Définition 5.6 Un ordre strict est dit strict total si deux éléments distincts sont toujours comparables

$$\forall (x, y) \in E, x \neq y \Rightarrow x\mathcal{R}y \text{ ou } y\mathcal{R}x$$

Remarque. Dans ce qui suit nous noterons une relation d'ordre par \preceq une relation d'ordre stricte par \prec .

5.2.2 Minorants, majorants, minimaux et maximaux

Définition 5.7 Soit (E, \preceq) un ensemble ordonné et F une partie non vide de E .

On dit que $x \in E$ est un minorant de F si on a :

$$\forall y \in F, x \preceq y$$

Si le minorant de F est un élément de F on dit que c'est le plus petit élément ou le minimum de F .

On dit que $x \in E$ est un majorant de F si on a :

$$\forall y \in F, y \preceq x$$

Si le majorant de F est un élément de F on dit que c'est le plus grand élément ou le maximum de F .

Définition 5.8 Soit (E, \preceq) un ensemble ordonné et F une partie non vide de E .

- Un élément x est un élément minimal de F quand aucun élément de F n'est strictement

plus petit que x :

$$\forall y \in F, y \preceq x \Rightarrow x = y$$

- Un élément x est un élément maximal dans de F quand aucun élément de F n'est strictement plus grand que x :

$$\forall y \in F, x \preceq y \Rightarrow x = y$$

Remarque. Si la relation est d'ordre total alors les notions d'élément minimal et de minimum coïncident. (Même remarque pour la notion d'élément maximal et de maximum).

Exemple. 0 est un élément minimal de (\mathbb{N}, \leq) c'est également son minimum.

Exemple. Soit l'ensemble $\mathcal{P}(\{a, b, c\}) \setminus \{\emptyset\}$ muni de la relation d'ordre partiel \subset . Les éléments $\{a\}, \{b\}, \{c\}$ sont des éléments minimaux mais il n'y a pas de minimum.

Bibliographie

- [1] P. Franceschi. Introduction la philosophie analytique paradoxes, aryuments et problèmes contemporains. Paul Franceschi, 2015.
- [2] S. Fratani and al. Cours Logique et Calculabilite, L3 Informatique, 2015.https://page-perso.lislab.fr/luigi.santocanale/teaching/1415teaching/LC/DOCS/old/cours_2303-2015.pdf.
- [3] C. Huayi. Notes du cours : Introduction aux raisonnements mathématiques, 2008.http://www-fourier.ujfgrenoble.fr/huayi/Enseignements/ParisVIII/2007_2008/logique.pdf.
- [4] T. Seiller. Théorie des Ensembles, 2010.<http://www.pps.univ-paris-diderot.fr/seiller/documents/thens.pdf>.
- [5] O. Simon. Nombres réels, 2005.<http://capes-math.univrennes1.fr/cours-pdf/reels.pdf>.
- [6] F. Sturm. Cours de mathématiques - ASINSA-1 : Introduction la logique mathématique, 2013.http://maths.insalyon.fr/fsturm/TELECHARGEMENT/COURSASINSA1/che_cours_ASINSA1_logique.pdf.
- [7] A. Torres. Introduction la logique, 2003. <http://www.adelino-torres.com/metodologia/INTRODU%C3%87%C3%83O%20%C3%80%20%C3%93GICA.pdf>.
- [8] J. Vélú. Méthodes mathématiques pour Informatiques. Dunod, 2003.
- [9] Wikipedia. https://fr.wikipedia.org/wiki/Logique_intuitionniste.
- [10] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_de_Russell.
- [11] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_du_barbier.
- [12] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_du_menteur.
- [13] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_de_Cantor.
- [14] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_de_Richard.
- [15] Wikipedia. https://fr.wikipedia.org/wiki/Paradoxe_de_GrellingNelson.