Notes du cours “Introduction aux raisonnements mathématiques”, Groupe BMW, Université Paris VIII

Chen Huayi

Chapitre 1

Une essquisse de l'histoire de la logique

Le mot **logique** provient du mot grec $\lambda\acute{o}\gamma o\varsigma$ (logos). Depuis l'antiquité la logique fut un domaine important de la philosophie, notamment la métaphysique. Cependant, ce ne fut qu'au XIX^{e} siècle que les problèmes de la logique commencèrent à intéresser les mathématiciens.

La logique au sens général repose sur l'examen critique de la méthodologie et de l'épistémologie. Poutant, la logique au sens formel cherche à trouver de règles générales des raisonnements en s'appuyant sur leur forme plutôt que sur leur contenu.

1.1 Logique aristotélicienne

L'étude systématique de la logique formelle fut commencée par Aristote (IV$^{\text{ème}}$ siècle avant notre ère). Sa théorie (logique des termes) fut exposée dans un traité intitulé *Organon* (instrument) par Andronicus de Rhodes. Selon Aristote, la logique était un instrument du savoir, mais pas le savoir lui-même. Elle devrait donner des principes pour déterminer si un raisonnement est vrai ou faux. Il est évident que l'analyse des raisonnements nécessite l'emploi de mots, mais Aristote aperçus que la considération des mots (ou des symboles) n'était importante que au niveau d'application. Cette observation le conduisit à l'étude des propositions dites *catégoriques*.

Propositions catégoriques

Toute proposition catégorique est la combinaison de termes de la forme :

(**Quantificateur**) **Sujet** **Copule** **Prédicat**.

On considère l'exemple suivant :

Certains hommes ne sont pas mortels.

Il s'agit d'une proposition catégorique. Ici la quantificateur (certains) exprime la quantité de la proposition. Le sujet (hommes) est ce à quoi l'on attribue le prédicat. La copule (ne sont pas) exprime la qualité de pa proposition (affirmative ou négative). Et le prédicat (mortels) est ce que l'on attribue au sujet. Il faut noter que Aristote ne considéra que les énoncés déclaratifs qui sont susceptibles d'être vrais ou faux. Ainsi, les phases du type "*Est-ce que tous les hommes sont mortels ?*" ne sont pas considérée par la théorie d'Aristote.

Aristote adopta un point de vue **extensionnel** sur les termes. Pour lui, un terme porte une **compréhension** (les propriétés qui définissent le terme) et une **extension** (l'ensemble des objets que le terme désigne). Par exemple, le terme *nombre paire* admet pour comphérension le caractère *être entier et divisible par* 2 et pour extension $\{0,\ \pm 2,\ \pm 4,\ \cdots\}$. Ainsi, une proposition **universelle** considère toute l'extension du terme ; et une proposition **particulière** considère seulement un de ses sous-ensembles. On obtient, en combinant la qualité et la quantité, quatre types de proposition catégorique dans le tableau 1.1.

	Type	Exemple
A	**universelle affirmative**	*Tous les hommes sont mortels*
E	**universelle négative**	*Aucun homme n'est mortel*
I	**particulière affirmative**	*Certains hommes sont mortels*
O	**particulière négative**	*Certains hommes ne sont pas mortels*

TAB. 1.1 – Types de proposition

On remarque que les abbrégés A, E, I, O proviennent des mots latins AffIrmo et nEgO. On dit que l'**extension du sujet** est universelle (resp. particulière) si la proposition est universelle (resp. particulière). On dit que l'**extension du prédicat** est universelle (resp. particulière) si la proposition est négative (resp. affirmative).

Ce n'est pas vrai que tout énoncé est concluant. Par conséquent, souvent il faut rendre les énoncés catégoriques. Par exemple, au lieu de dire "*Tous les hommes mange du pomme*", il faut plutôt dire "*Tous les hommes sont pomme-mangeants*".

Inférence immédiate

Étant donnée une proposition catégorique (**prémisse**), jugée vraie ou fausse, en utilisant la théorie de l'**inférence immédiate**, on obtient la valeur de vérité de ses inférences plus compliquées. Attention : un raisonnement peut être valide même si certaines des propositions dedans sont fausses. On résume au-dessous les principes de l'inférence immédiate :

- La relation de **contradiction** oppose deux propositions de quantité et de qualité différents. Les contradictoires prennent toujours une valeur de vérité opposée.
- La relation de **contrariété** oppose deux proposition de quantité universelle et de qualité différente. Les contraires ne peuvent être vraies en même temps.
- La relation de **subcontrariété** oppose deux proposition de quantité particulière et de qualité différente. Les subcontraires ne peuvent être fausses en même temps.
- La relation de **subalternation** oppose deux proposition de même qualité mais de quantité différente. La vérité de la subalterne inférieure suit de la vérité de la supérieure.

Dans le tableau 1.2, on présente les valeurs de vérité des inférences.

	A	E	I	O
AV	V	F	V	F
EV	F	V	F	V
IV		F	V	
OV	F			V
AF	F			V
EF		F	V	
IF	F	V	F	V
OF	V	F	V	F

TAB. 1.2 – Valeurs de vérité des inférences

La **conversion** est une autre méthode de passer d'une proposition à une autre en conservant la valeur de vérité. Elle consiste à échanger le sujet et le prédicat.

Les prémisses du type E ou I autorisent des conversions dites **simples**, i.e., le type de la proposition reste inchangé. Par exemple, la proposition "*Aucun homme est mortel*" donne par conversion simple "*Aucune chose mortelle*

n'est homme" ; la proposition "*Certains hommes sont mortels*" devient "*Certaines choses mortelles sont des hommes*". La composition de deux conversions simples donne la proposition initiale.

Un autre type de conversion dit **par accident** passe A à I, en diminuant la quantité de la proposition. Par exemple, la proposition "*Tous les hommes sont mortels*" peut être convertie en "*Certaines choses mortelles sont des hommes*".

L'**obvertion** consiste à changer la qualité de la prémisse en niant le prédicat. Une obvertion est valable pour tous les propositions. On trouve dans le tableau 1.3 des exemples :

Prémisse (type)	Obvertion (type)
Tous les hommes sont mortels (A)	*Aucun homme n'est immortel* (E)
Aucun homme n'est mortel (E)	*Tous les hommes sont immortels* (A)
Certains hommes sont mortels (I)	*Certains hommes n'est pas immortels* (O)
Certains hommes ne sont pas mortels (O)	*Certains hommes sont immortels* (I)

TAB. 1.3 – Exemples des obversions

La **contraposition simple** échange le sujet et le prédicat et les nier ensuite, tout en respectant la quantité, la qualité et la valeur de vérité (et donc le type de la proposition ne change pas). Elle est valable seulement pour les proposition du type A ou O. Par exemple, la proposition "*Tous les hommes sont mortels*" devient "*Toutes les choses immortelles sont des non hommes*" ; la proposition "*Certains hommes ne sont pas mortels*" devient "*Certains choses immortelles sont des hommes*". A partir d'une proposition du type E, il faut appliquer la **contraposition par limitation** (i.e., limiter la quantité). Par exemple "*Aucun homme n'est mortel*" donne "*Certaines choses immortelles ne sont pas des non hommes*".

Théorie du syllogisme

Un syllogisme est le procédé d'associer à deux propositions (appelées également prémisses) une autre (appelée **conclusion**). Cette théorie fut d'abord développée par Aristote. Les deux prémisses sont appelées respectivement la **majeure** et la **mineure**.

Un exemple typique est présenté dans le tableau 1.4 : La validité de ce raisonnement résulte simplement de sa structure formelle.

Un syllogisme est formé par trois termes. Le prédicat de la conclusion est appelé le **terme majeur**. Le sujet de la conclusion est appellé le **terme mineur**. Le troisième est appelé le **terme moyen**. Il faut que le terme majeur

Majeure	Tous les hommes sont mortels	Tous les b sont a
Mineure	Tous les Grecs sont des hommes	Tous les c sont b
Conculsion	Tous les Grecs sont mortels	Tous les c sont a

TAB. 1.4 – Syllogisme

(resp. terme mineur) apparaisse une fois et une seule dans la prémisse majeure (resp. mineure). On appelle **mode** syllogistique toute combinaison possible de types de propositions dans un syllogisme. Les syllogismes sont alors classés, selon la position du terme moyen, dans les quatre **figures** suivantes (tableau 1.5) :

Figure	Description	Exemple
Figure 1	Le moyen terme est le sujet de la majeure et le prédicat de la mineure	Tout Mo est Ma Tout Mi est Mo Tout Mi est Ma
Figure 2	Le moyen terme est le prédicat des prémisses	Tout Mo est Ma Aucun Mi n'est Mo Aucun Mi n'est Mo
Figure 3	Le moyen terme est le sujet des prémisses	Tout Mo est Ma Tout Mo est Mi Quelque Mi est Mo
Figure 4	Le moyen terme est le prédicat de la majeure et le sujet de la mineur	Tout Ma est Mo Tout Mo est Mi Quelque Mi est Ma

TAB. 1.5 – Exemples des figures

Exercice 1.1 Dans chaque figure combien y a-t-il de modes possibles ? Combien y a-t-il de modes possibles en tout ?

Tous les syllogismes ne sont pas concluants. Il faut examiner les règles suivants :

- l'extension des termes de la conclusion ne peut être plus importante que dans les prémisses ;
- les deux prémisses ne peuvent pas être simultanément particulières ;
- les deux prémisses ne peuvent pas être simultanément négatives ;
- le moyen terme doit être universel au moins une fois dans les prémisses ;
- la conclusion négative ne peut pas être tirée de deux prémisses affirmatives ;
- si l'une des prémisse est particulière, alors la conclusion ne peut pas être universelle.

Il y a en gros 19 modes valables plus 5 modes qui proviennent de certains modes parmi les 19 en limitant la quantité de la conclusion. Depuis le Moyen Âge, ces modes sont désignées par des noms où les trois voyelles donnent le type des 3 propositions engagées dans le syllogisme. Dans la première figure, il y a 4 mode concluants :

B**A**rb**A**r**A**	Tout Mo est Ma Tout Mi est Mo Tout Mi est Ma	C**E**l**A**r**E**nt	Aucun Mo n'est Ma Tout Mi est Mo Aucun Mi n'est Ma
D**A**r**II**	Tout Mo est Ma Quelque Mi est Mo Quelque Mi est Ma	F**E**r**IO**	Aucun Mo n'est Ma Quelque Mi est Mo Quelque Mi n'est pas Ma

Les modes concluants dans les autres figures peuvent être déduite à l'aide de transformation des 4 modes ci-dessus. Pour cette raison, Aristote appelait les syllogismes de ces 4 types les syllogismes parfaits.

Exercice 1.2 Essayer de trouver les 15 modes concluants dans les figures 2,3,4. Préciser, pour chaque mode concluant, la mode dans la première figure qui la correspond ; préciser également les transformations dans le procédé de réduction.

1.2 L'école mégarique et l'école stoïcienne

L'école de Mégarique fut fondée par Euclid de Mégare (450-380 avant notre ère). Les Mégariques furent les premiers qui eurent la consience de l'importance de **paradoxes** logiques. Par exemple, le paradoxe du **menteur** proposé par Euboulide de Milet demande de fixer la valeur de vérité de

l'énoncé "*Ce que je dis est faux*". S'il est vrai que je mens, alors la valeur de vérité de cet énoncé est faux, donc il n'est pas vrai que je mens. Par contre, s'il est faux que je mens, alors la valeur de vérité est vrai, et donc je dis la vérité. Il faut attendre jusqu'à Bertrand Russell (1872-1970) que ce genre de paradoxes était résolu.

L'école stoïcienne fut une école philosophique fondée par Zénon de Kition (335-262/261 avant notre ère). La logique stoïcienne est une logique des propositions qui analyse les raisonnement sans entrer dans la structure des propositions. La logique stoïcienne fut présentée sous une forme axiomatique. On trouve une similitude entre la logique stoïcienne et le calcul de proposition moderne.

1.3 Médieval et Renaissance

Logique médievale

La logique médieval (ou scholastique) est une continuation de la logique Aristotélicienne, développeé en Europe médievale. Pendant cette période, la logique médieval s'inspira des philosophie islamique.

Période classique

Leibniz (1646-1716) proposa un projet révolutionnel pour symboliser la logique. Ce projet consiste à chercher une "caractérisation universelle et artificielle" des raisonnement en les symbolisant, et à établir des méthodes automatisables de combiner ces symobles. Cependant, la révolution scientifique pendant cette période demanda une profonde réforme de pensée sur le rôle de la logique car la logique formelle devenait insuffisant comme un outil de source de savoir.

Pendant le XVII^{e} siècle apparaît le **calcul infinitésimal** qui permet d'établir le calcul différentiel et le calcul intégral. Le calcul infinitésimal demande la notion de la limite qui ne pouvait être définie que par une approche intuitive à l'époque. Or les résultats obtenus par cette approche étaient si puissants et importants que les mathématiques ont quitté la logique formelle pour utiliser des outils intuitifs que la logique refuse.

1.4 Logique morderne (mathématique)

C'est le debut du XIX^{e} siècle que les mathématiciens commençaient à étudier systématiquement la logique. L'apparition des paradoxes demandait

de résoudre les probème de fondation des mathématiques.

De Morgan (1806-1976) et Boole (1815-1864) ont découvert l'existence de structures algébriques permettant de définir un "calcul de vérité". Mais cette théorie ne prend pas compte la notion de variable.

Frege publiait en 1879 le livre **Begriffsschrift** qui "*librérait la logique d'une connexion artificielle avec les mathématiques, tandis qu'en même temps il préparait une interrelation plus profonde entre ces deux sciences*" (J. Van Heijenoort).

En 1900, David Hilbert a proposé dans sa liste de 23 problèmes non résolus des mathématiques la cohérence de l'arithmétique comme le deuxième problème. Il a demandé si la non-contradiction des axiomes de l'arithmétique peut être démontrer par des **moyens finitistes**. Motivé par ce programme, nombreux résultats en logique sont obtenus pendant le début du XX^{e} siècle parmi lequels on voudrais sousligner :

1) les axiomes de Peano pour l'arithmétique,
2) les axiomes de Zermelo complétés par Skolem et Frænkel pour la théorie des ensemble,
3) théorie des modèles, théorème de Löwenheim-Skolem,
4) formalisation des mathématiques proposée par Whitehead et Russell,
5) théorème de complétude du calcul des prédicats démontré par Gödel.

Malheuresement les deux théorèmes d'incomplétude de Gödel montrait l'impossibilité de réaliser le programme de Hilbert.

Pendant les année 30 du XX^{e} siècle, l'approche algorithmique de la logique a été dévéloppé par Turing, von Neumann, Church... etc. Du côté de la théorie de démonstration, Gentzen a démontré la cohérence de l'arithmétique de Peano en utilisant une induction jusqu'à l'ordinal dénombrable.

Concernant la théorie des ensemble, Paul Cohen a démontré l'indépendance de l'hypothèse du continu en utilisant la méthode de **forcing** qui l'a permis de gagner un médaille de Fields (considéré comme le prix de Nobel pour les mathématiciens).

On a aussi découvert le lien entre l'information et la logique par l'intermédiaire du *lambda-calcul* (la correspondance de Curry-Howard).

Aujourd'hui, la logique mathématique est un domain très actif, qui trouve de plus en plus d'applications en informatique, en ingénierie, en linguistique et bien sur, en philosophie.

Dans les chapitres suivants, on introduit systématiquement les notions élémentaires de la logique mathématique, notamment le calcul propostionnel et le calcul des prédicats.

Chapitre 2

Syntaxe des propositions

2.1 Formules propositionnelles

Il s'avère que les langues habituelles ont des ambiguïtés qui conduisent aux multiples inconvénients. Par exmple, un philosophe chinois, Gongsun Long (325-250 avant notre ère) proposa le paradoxe suivant :

Un cheval blanche n'est pas un cheval.

Son arguement fut que, si un cheval blanc était un cheval, pour la même raison, un cheval jaune devrait être aussi un cheval ; par conséquent, un cheval blanc est un cheval jaune. Ceci est absurde. Ici dans son arguement, l'ambiguïté provient du mot "*être*". Dans la phrase "*un cheval blanc est un cheval*", le verbe "*être*" remplace "appartenir dans l'ensemble des". En revanche, dans la seconde phrase "*un cheval blanc est un cheval jaune*", le verbe "être" représente "équivaloir à". Pour enlever ces genres d'ambiguïté, il faut proposer un nouveau language qui adapte bien à l'étude du raisonnement.

Soit $\mathscr{P}$ un ensemble non-vide dont les éléments sont appelés **variables propositionnelles**. Soient en outre cinq symboles

$$\neg \quad \vee \quad \wedge \quad \Rightarrow \quad \Leftrightarrow$$

appelés les **symboles de connecteur propositionnel**, ou respectivement le symbole de **négation**, le symbole de **disjonction**, le symbole de **conjonction**, le symbole d'**implication** et le symbole d'**équivalence**. Ces symboles sont lits respectivement "**non**", "**ou**", "**et**", "**implique**" et "**equivaut à**".

Attention : On suppose par convention que les cinq symboles de connecteur propositionnel n'appartiennent pas à l'ensemble $\mathscr{P}$.

On dit que le symbole $\neg$ est **uniaire** et les autre symboles de connecteur propositionnel sont **binaire** (on verra plus tard pourquoi).

On considère également deux symbols

$$) \qquad ($$

appelés respectivement **parenthèse fermante** et **parenthèse ouvrante**. On suppose qu'ils sont distincts des variables propositionnelles et des symboles de connecteur propositionnel.

Soient $\mathscr{A}$ l'union

$$\mathscr{A} = \mathscr{P} \cup \{ \neg, \vee, \wedge, \Rightarrow, \Leftrightarrow \} \cup \{), (\}.$$

et $\mathscr{M}(\mathscr{A})$ l'ensemble des **mots** sur l'alphabet $\mathscr{A}$. Plus précisément, un élément F dans $\mathscr{M}(\mathscr{A})$ est de la forme $a_0 a_1 \cdots a_{n-1}$, où $a_i \in \mathscr{A}$ pour tout entier $0 \leq i \leq n-1$. L'entier n est appelé la *longueur* de F, noté $\lg[F]$. Bien entendu, dans $\mathscr{M}(\mathscr{A})$ il y a le **mot vide**, sa longueur est 0. Tout élément de $\mathscr{A}$ peut être considéré comme un mot de longueur 1 sur l'alphabet $\mathscr{A}$. Ainsi on peut identifier $\mathscr{A}$ au sous-ensemble de $\mathscr{M}(\mathscr{A})$ des mots de longueur 1.

On construit par récurrence une suite de mots dans $\mathscr{M}(\mathscr{A})$. On pose

- $\mathscr{F}_0 = \mathscr{P}$,
- pour chaque entier $n \geq 0$,

$$\mathscr{F}_{n+1} = \mathscr{F}_n \cup \{\neg F \mid F \in \mathscr{F}_n\} \cup \{(F \alpha G) \mid F, G \in \mathscr{F}_n,\ \alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}.\}$$

Soit $\mathscr{F}$ l'union $\bigcup_{n \geq 1} \mathscr{F}_n$. Les éléments dans $\mathscr{F}$ sont appelés des **formules propositionnelles**.

Exercice 2.1 Supposons que A, B et C sont des variables propositionnelles dans $\mathscr{P}$. Les mots suivants sont-ils des formules propositionnelles ? Pourquoi ?

a)	$\neg\neg\neg A$	b)	AB	c)	$A \Rightarrow B$
d)	$\neg(A \Rightarrow B)$	e)	$((A) \Rightarrow (B))$	f)	$(A \vee B \vee C)$

Exercice 2.2 Déterminer la longueur de chaque formule propositionnelle au-dessous :

$$A \qquad (A \Rightarrow (B \Leftrightarrow A)) \qquad \neg(A \Rightarrow A)$$

Théorème 2.1 *L'ensemble $\mathscr{F}$ est le plus petit sous-ensemble de $\mathscr{M}(\mathscr{A})$ vérifiant les conditions suivantes :*

1) $\mathscr{P} \subset \mathscr{F}$;

2) pour chaque mot $F \in \mathscr{F}$, on a $\neg F \in \mathscr{F}$;

3) si F et G sont deux éléments de $\mathscr{F}$, alors les mots $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$ et $(F \Leftrightarrow G)$ sont tous dans $\mathscr{F}$.

Démonstration On vérifie d'abord que $\mathscr{F}$ vérifie les conditions 1)—3). D'abord on a $\mathscr{P} = \mathscr{F}_0 \subset \mathscr{F}$, donc la condition 1) est vérifiée pour $\mathscr{F}$. Si $F \in \mathscr{F}_n$, alors $\neg F \in \mathscr{F}_{n+1} \subset \mathscr{F}$, donc la condition 2) est aussi vérifiée pour $\mathscr{F}$. Enfin, si $F \in \mathscr{F}_n$, $G \in \mathscr{F}_m$, alors F et G sont toutes dans $\mathscr{F}_{\max(m,n)}$. Par conséquent, pour tout symbole $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, $(F \alpha G) \in \mathscr{F}_{\max(m,n)+1} \subset \mathscr{F}$, donc la condition 3) est vérifiée pour $\mathscr{F}$.

Si $\mathscr{G}$ est un sous-ensemble de $\mathscr{M}(\mathscr{A})$ vérifiant les conditions 1)—3), alors $\mathscr{G} \supset \mathscr{F}$. En effet, la condition 1) montre que $\mathscr{F}_0 \subset \mathscr{G}$. Ensuite, si $\mathscr{F}_n \subset \mathscr{G}$, alors les conditions 2) et 3) impliquent que $\mathscr{F}_{n+1} \subset \mathscr{G}$. Par récurrence on déduit que $\mathscr{F}_n \subset \mathscr{G}$ pour tout $n \in \mathbb{N}$. Donc on a $\mathscr{F} \subset \mathscr{G}$.

□

Définition 2.2 On appelle **hauteur** d'une formule $F \in \mathscr{F}$ le plus petit entier n tel que $F \in \mathscr{F}_n$, notée $h[F]$.

Exercice 2.3 Montere les propriétés suivantes concernant la hauteur :

1) pour toute formule $F \in \mathscr{F}$, $h[\neg F] \leq h[F] + 1$;
2) pour toutes formules $F, G \in \mathscr{F}$ on a $h[(F \alpha G)] \leq \sup(h[F], h[G]) + 1$ quelque soit le symbole de connecteur propositionnel α.

2.2 Modélisation de la language habituelle

On peut modéliser la language habituelle par des formules propositionnelles (on ignore la validité du raisonnement). Considérons par exemple la phrase suivante :

> *Soit elle n'est pas chez elle, soit elle ne répond pas au téléphone. Mais si elle n'est pas chez elle, alors, elle a été kidnappée. Et si elle ne répond pas au téléphone, c'est qu'elle court un autre danger. Donc soit elle a été kidnappée, soit elle est en danger.*

Si on désigne

- "elle est chez elle" par P,
- "elle répond au téléphone" par Q,
- "elle a été kidnappée" par R,
- "elle court un autre danger" par S,

alors l'énoncé ci-dessus peut être modélisé par

$$(((\neg P \vee \neg Q) \wedge (\neg P \Rightarrow R) \wedge (\neg Q \Rightarrow S)) \Rightarrow (R \vee S))$$

Exercice 2.4 Que pensez-vous sur l'expression "*Si tu as faim, il y a de la viande dans le frigo*" ? Si on désigne "tu as faim" par A et "il y a de la viande dans le frigo" par B, est-ce que cette phrase peut être modélisée par la formule $(A \Rightarrow B)$?

Exercice 2.5 On désigne par A l'énoncé "Pierre aime Marie" et par B l'énoncé "Marie aime Pierre". Modéliser les énoncés suivantes par des formules propositionnelles :

1) Pierre aime Marie mais ce n'est pas réciproque ;

2) Pierre et Marie ne s'aiment pas ;

3) Il est faux que Pierre et Marie s'aiment l'un l'autre.

2.3 Prinicipe de récurrence

Supposons que l'on veut vérifier une propriété $\mathbb{P}$ pour toute formule $F \in \mathscr{F}$, on peut éventuellement le faire par récurrence.

Le principe est le suivant : le premier étape est de montrer que la propriété $\mathbb{P}$ est vérifiée pour toute formule dans $\mathscr{P}$; l'étape d'induction consiste à prouver, d'une part, si une formule F satisfait à la propriété $\mathbb{P}$, il en est de même de $\neg F$, d'autre part, si deux formules F et G satisfont à $\mathbb{P}$, il en est de même des formules $(F \vee G)$, $(F \wedge G)$, $(F \Rightarrow G)$ et $(F \Leftrightarrow G)$.

Exercice 2.6 Justifier le principe de récurrence au-dessus par un procédé de récurrence habituel sur la hauteur.

Exercice 2.7 En utilisant le principe de récurrence au-dessus, montrer que la hauteur d'une formule est toujours strictement plus petite que sa longueur.

2.4 Théorème de lecture unique

Définition 2.3 Pour chaque mot $M \in \mathscr{M}(\mathscr{A})$, on désigne par $\mathrm{o}[M]$ le nombre de parenthèse ouvrant dans M, et par $\mathrm{f}[M]$ le nombre de parenthèse fermant dans M.

Exercice 2.8 Montrer que pour toute formule $F \in \mathscr{F}$, on a $\mathrm{o}[F] = \mathrm{f}[F]$.

Proposition 2.4 *Supposons que F soit une formule dans $\mathscr{F}$. Pour tout segment initial M de F, on a toujours* $\mathrm{o}[M] \geq \mathrm{f}[M]$.

Démonstration La proposition est vraie pour les formules dans $\mathscr{F}$ car pour tout segment initial M de $F \in \mathscr{P}$, on a $\mathrm{o}[M] = \mathrm{f}[M] = 0$.

Supposons que $F \in \mathscr{F}$ est une formulle telle que, pour tout segment initial M de F, on ait $\mathrm{o}[M] \geq \mathrm{f}[F]$. Soit N un segment initial de $\neg F$. Si N est vide, alors $\mathrm{o}[N] = \mathrm{f}[N] = 0$; sinon N s'écrit sous la forme $N = \neg M$, où M est un segment initial de F ; d'après l'hypothèse de récurrence, on a

$$\mathrm{o}[N] = \mathrm{o}[M] \geq \mathrm{f}[M] = \mathrm{f}[N].$$

Soient F et G deux formules vérifiant la conlusion de la proposition, et α un symbole de connecteur propositionnel binaire. Soient $H = (F\alpha G)$ et N un segment initial de H. Alors l'un des quatre cas suivants se présente :

1) N est vide, et donc $\mathrm{o}[N] = \mathrm{f}[N] = 0$;
2) N s'écrit sous la forme (M, où M est un segment initial de F, et alors $\mathrm{o}[N] = \mathrm{o}[M] + 1 \geq \mathrm{f}[M] + 1 = \mathrm{f}[N] + 1$;
3) N est de la forme ($F\alpha M$, où M est un segment initial de G, et alors $\mathrm{o}[N] = \mathrm{o}[F] + \mathrm{o}[M] + 1 \geq \mathrm{f}[F] + \mathrm{f}[M] + 1 = \mathrm{f}[N] + 1$;
4) $N = (F\alpha G)$, et donc $\mathrm{o}[N] = \mathrm{f}[N]$.

□

Proposition 2.5 *Supposons que F soit une formule dans $\mathscr{F}$ commençant par une parenthèse ouvrante. Pour tout segment initial non-vide et propre M de F, on a toujours l'inégalité stricte* $\mathrm{o}[M] > \mathrm{f}[M]$.

Démonstration Comme le prmier symbole de F est (, elle est de la forme $(G\alpha H)$, où G et H sont deux formules dans $\mathscr{F}$ et α est un symbole de connecteur propositionnel binaire. Soit M un segment initial non-vide et propre de F, alors M se trouve dans l'une des deux situations suivantes :

1) $M = ($, où N est un segment initial de G, dans ce cas-là, on a

$$\mathrm{o}[M] = 1 + \mathrm{o}[N] \geq 1 + \mathrm{f}[N] = 1 + \mathrm{f}[M];$$

2) $M = (G\alpha K$, où K est un segment initial de H, dans ce cas-là, on a

$$\mathrm{o}[M] = 1 + \mathrm{o}[G] + \mathrm{o}[K] \geq 1 + \mathrm{f}[G] + \mathrm{f}[K] = 1 + \mathrm{f}[M].$$

Par conséquent, on a toujours $\mathrm{o}[M] \geq 1 + \mathrm{f}[M] > \mathrm{f}[M]$.

□

Proposition 2.6 *Soit F une formule quelconque dans $\mathcal{F}$. Tout segment initial non-vide et propre de F n'est pas une formule.*

Démonstration On raisonne par récurrence. D'abord pour toute formule A dans $\mathscr{P}$, il n'y a pas de segment initial non-vide et prore.

Supposons que F est une formule vérifiant la conlusion de la proposition. Soit M un segment initial non-vide et propre de F. Alors l'un des deux cas suivants se produit.

1) $M = \neg$, qui n'est pas une formule.
2) $M = \neg N$, où N est un segment initial non-vide et propre de F. D'après l'hypothèse de récurrence, on obtient que N n'est pas une formule, et donc $M = \neg N$ n'est pas une formule non-plus (Exercice : Justifier cette assertion).

Enfin, si F et G sont deux formules, α est un symbole de connecteur propositionnel binaire, et M est un segment initial non-vide et propre de $(F\alpha G)$, alors on a $\mathrm{o}[M] > \mathrm{f}[M]$ (proposition 2.5). Par conséquent, M n'est pas une formule (Exercice 2.8).

□

Théorème 2.7 (Lecture unique) *Soit F une formule quelconque. Alors un et un seul des trois cas suivante se présente :*

1) $F \in \mathscr{P}$;
2) il existe une unique formule $G \in \mathscr{F}$ telle que $F = \neg G$;
3) il existe un unique couple de formules $(G, H) \in \mathscr{F}^2$ et un unique symbole de connecteur propositionnel binaire α tels que $F = (G\alpha H)$.

Démonstration Il est évident que les trois cas sont exclus. D'autre part, soit $F \in \mathscr{P}$, soit il existe $G \in \mathscr{F}$ tel que $F = \neg G$, et soit encore il existe $G, H \in \mathscr{F}$ et $\alpha \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$ tels que $F = (G\alpha H)$. Par conséquent, il reste à vérifier l'unicité dans les cas 2) et 3). Pour le cas 2), ceci est évident car $\neg G = \neg H$ entraîne $G = H$.

Supposons que $F = (G\alpha H) = (K\beta L)$, où G, H, K et L sont des formules et α et β sont des symboles de connecteur propositionnel binaires. On a alors $G\alpha H = K\beta L$. Si la longueur de G est strictement inférieure à celle de K, alors G est un segment initial non-vide et propre de K, cela est absurde car G est une formule. Par conséquent, on a $\lg[G] \geq \lg[K]$. Par la symétrie on obtient $\lg[K] \geq \lg[G]$. Par conséquent, on a $G = K$ et donc $\alpha = \beta$ et $H = L$.

□

Corollaire 2.8 *1) Pour toute formule $F \in \mathscr{F}$ on a $h[\neg F] = h[F] + 1$.*

2) Pour tout couple de formules $F, G \in \mathscr{F}$ et tout symbole de connecteur propositionnel binaire α, on a $h[(F\alpha G)] = \max(h[F], h[G]) + 1$.

Exercice 2.9 En utilisant le théorème de lecture unique, démontrer le corollaire au-dessus.

2.5 Construction par induction

On s'intéresse à la construction de fonctions sur $\mathscr{F}$. Le théorème de lecture unique nous permet de construire des fonctions par récurrence.

Proposition 2.9 *Soit E un ensemble. Supposons donnés*

i) une application $\varphi : \mathscr{P} \to E$,

ii) un endomorphisme $a : E \to E$,

iii) une application $\Psi : \{\wedge, \vee, \Rightarrow, \Leftrightarrow\} \times E^2 \to E$.

Alors il existe une unique application $f : \mathscr{F} \to E$ telle que

1) la restriction de f en $\mathscr{P}$ identifie à φ ;

2) pour toute formule $F \in \mathscr{F}$, $f[\neg F] = a[f[F]]$;

3) pour tout couple de formules $F, G \in \mathscr{F}$ et tout symbole de connecteur propositionnel binaire α, on a $f[(F\alpha G)] = \Psi[\alpha, f[F], f[G]]$.

Démonstration On construit par récurrence une unique fonction $f_n : \mathscr{F}_n \to E$ qui prolonge φ et qui vérifie les conditions 2) et 3).

On pose $f_0 = \varphi : \mathscr{P} \to E$. Supposons que l'on a construit la fonction $f_n : \mathscr{F}_n \to E$. D'après le théorème de lecture unique, une formule $H \in \mathscr{F}_{n+1} \setminus \mathscr{F}_n$ s'écrit de façon unique sous la forme $\neg F$ ou $(F\alpha G)$, où F et G sont des formules dans $\mathscr{F}_n$. Si $H = \neg F$, on pose $f_{n+1}[H] = a[f_n[F]]$; si $H = (F\alpha G)$, on pose $f_{n+1}[H] = \Phi[\alpha, F, G]$. On a ainsi étendu l'application f_n sur $\mathscr{F}_{n+1}$. Cette construction est unique grâce aux conditions 2) et 3).

□

Soit **Arb** l'ensemble des arbres binaires (c'est-à-dire qu'un nœude possède au plus deux branches) où les nœudes sont marqués par des fomules propositionnelles. Soit $\varphi : \mathscr{P} \to$ **Arb** l'application qui associe à chaque variable propositionnelle $A \in \mathscr{P}$ l'arbre à un seul nœude marqué par A. Si **A** est une arbre dans **Arb** dont la racine est marquée par la formule F, on désigne par

$a[\mathbf{A}]$ l'arbre dont la racine est marquée par $\neg F$ et telle que la seule branche de la racine est l'arbre $\mathbf{A}$. Ainsi on a défini un endomorphisme $a : E \to E$. Enfin, si $\mathbf{A}$ et $\mathbf{B}$ sont deux arbres dans **Arb** dont les racines sont respectivement marquées par F et G, et si α est un symbole de connecteur propositionnel binaire, on désigne par $\Psi[\alpha, \mathbf{A}, \mathbf{B}]$ l'abre dont la racine est marquée par $(F\alpha G)$ et dont la brache à gauche (resp. à droite) est $\mathbf{A}$ (resp. $\mathbf{B}$). Ainsi on a défini une application Ψ de $\{\wedge, \vee, \Rightarrow, \Leftrightarrow\} \times \mathbf{Arb}^2$ vers **Arb**. La proposition 2.9 montre que ces donnés déterminent une unique application ar : $\mathscr{F} \to \mathbf{Arb}$ qui prolonge φ. Si F est une formule propositionnelle, ar$[F]$ est appelé l'**arbre de décomposition** de la formule F.

Exercice 2.10 Déssigner l'arbre de décomposition de la formule suivante :

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

Exercice 2.11 Montrer que pour tout formule propositionnelle F, la hauteur de F est égale à la profondeur de son arbre de décomposition.

Exercice 2.12 En utilisant le résultat de l'exercice précédent, déterminer la hauteur de la formule suivante :

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

On associe à chaque formule $F \in \mathscr{F}$ un sous-ensemble sf$[F]$ de $\mathscr{F}$ qui est l'ensemble des formules figurant dans l'arbre de décomposition de la formule F.

À une formule, on peut aussi associer une **arbre de décomposition** sous forme simplifiée. D'abord, on associe à chaque variable propositionnelle A l'arbre $\widetilde{\text{ar}}[A]$ à un seul nœud marqué par A. Si F est une formule telle que $\widetilde{\text{ar}}[F]$ a été défini, l'arbre $\widetilde{\text{ar}}[\neg F]$ est par définition l'arbre dont la racine est marquée par le symbole $\neg$ et que la seule branche de la racine est l'arbre $\widetilde{\text{ar}}[F]$. Enfin, si F et G sont deux formules telles que $\widetilde{\text{ar}}[F]$ et $\widetilde{\text{ar}}[G]$ ont été définis, et si α est un symbole de connecteur binaire, alors $\widetilde{\text{ar}}[(F\alpha G)]$ est l'arbre dont la racine est marquée par le symbole α et telle que les branches de la racine sont respectivement $\widetilde{\text{ar}}[F]$ et $\widetilde{\text{ar}}[G]$.

Remarque 2.10 Soit F une formule propositionnelle. Dans l'arbre $\widetilde{\text{ar}}[F]$, les feuilles sont marquées par des variables propositionnelles tandis que les autres nœuds sont marqués par des symboles de connecteurs. Un nœud marqué $\neg$ admet une seule branche et un nœud marqué par $\wedge$, $\vee$, $\Rightarrow$ ou $\Leftrightarrow$ admettent deux branches.

2.6 Substitutions dans une formule

Soit F une formule propositionnelle. Si $(A_i)_{1\leq i\leq n}$ est une famille de variables propositionnelles dans $\mathscr{P}$ et si $(G_i)_{1\leq i\leq n}$ est une famille de formules propositionnelles, on désigne par $F_{G_1/A_1,\cdots,G_n/A_n}$ le mot obtenu de F en substituant systématiquement les variables A_i apparues dans F par G_i.

Par exemple, si $F = (A \Rightarrow (\neg B \vee A))$ et si $G = (\neg A \Leftrightarrow B)$, alors

$$F_{G/A} = ((\neg A \Leftrightarrow B) \Rightarrow (\neg B \vee (\neg A \Leftrightarrow B)))$$

Il faut remarquer que les substitutions sont faites simultanément. Considérons l'exemple suivant : Soient

$$F = (A_1 \wedge A_2) \qquad G_1 = (A_1 \vee A_2) \quad \text{et} \quad G_2 = (A_1 \Rightarrow A_2).$$

On a

$$F_{G_1/A_1,G_2/A_2} = ((A_1 \vee A_2) \wedge (A_1 \Rightarrow A_2))$$

Pourtant

$$[F_{G_1/A_1}]_{G_2/A_2} = [((A_1 \vee A_2) \wedge A_2)]_{G_2/A_2} = ((A_1 \vee (A_1 \Rightarrow A_2)) \wedge (A_1 \Rightarrow A_2))$$

$$[F_{G_2/A_2}]_{G_1/A_1} = [(A_1 \wedge (A_1 \Rightarrow A_2))]_{G_1/A_1} = ((A_1 \vee A_2) \wedge ((A_1 \vee A_2) \Rightarrow A_2))$$

Exercice 2.13 Soient $F = (A \Rightarrow B)$, $G = (A \vee C)$ et $H = (C \wedge D)$, où A, B, C et D sont des variables propositionnelles. Déterminer les mots suivants :

$$F_{G/A,H/B} \qquad \text{et} \qquad F_{H/A,G/C}$$

Il s'avère que les mots obtenus par substitions dans une formule est encore une formule, mais il mérite d'une démonstration.

Proposition 2.11 *Soient F une formule propositionnelle, $(A_i)_{1\leq i\leq n}$ une famille de variables propositionnelles et $(G_i)_{1\leq i\leq n}$ une famille de formules propositionnelles. Alors le mot $F_{G_1/A_1,\cdots,G_n/A_n}$ est une formule propositionnelle.*

Exercice 2.14 Démontrer la proposition 2.11.

Soient F une formule propositionnelle, $(A_i)_{1\leq i\leq n}$ une famille de variables propositionnelles et $(G_i)_{1\leq i\leq n}$ une famille de formules propositionnelles. Si $H = F_{G_1/A_1,\cdots,G_n/A_n}$, alors $\widetilde{\text{ar}}[H]$ s'obtient par substituer simultanément les feuilles marquée par A_i par l'arbre $\widetilde{\text{ar}}[G_i]$.

Chapitre 3

Sémantique des propositions

3.1 Corps à deux éléments

Soit E un ensemble. On appelle *loi de composition* sur E toute application de $E \times E$ dans E. Si $*$ est une loi de composition sur E et si x et y sont deux éléments dans E, on désigne par $x * y$ l'image canonique de (x, y) dans E par la loi de composition $*$. On dit qu'une loi de composition $*$ sur E est **associative** si pour tout triplet (x, y, z) dans E^3, on a $(x*y)*z = x*(y*z)$. On dit que $*$ est **commutative** si pour tout couple (x, y) dans E^2 on a $x * y = y * x$. On dit que E adment un **élément unité** pour la loi de composition $*$ (ou $(E, *)$ est unitaire) s'il existe un élément $e \in E$ (appelé l'**élément unité**) tel que $e * x = x * e = x$ pour tout élément $x \in E$.

Exercice 3.1 Montrer que si E admet un élément unité pour la loi de composition $*$, alors cet élément unité est unique.

On dit que $(E, *)$ est un **semi-groupe** si $*$ est associative ; si de plus $(E, *)$ est unitaire e, on dit que $(E, *, e)$ est un **monoïde**. On dit que $(E, *, e)$ est un **groupe** si $(E, *, e)$ est un monoïde d'élément unité e et si tout élément dans E est *inversible*, i.e., pour tout élément $x \in E$, il existe un élément $y \in E$ tel que $x * y = y * x = e$. L'élément x^{-1} est unique (Exercice : Justifier cette énoncé), appelé l'*inverse* de x. Si $(E, *)$ (resp. $(E, *, e)$) est un semi-groupe (resp. monoïde, groupe) et si $*$ est une loi de composition commutative, on dit alors que $(E, *)$ (resp. $(E, *, e)$) est un **semi-groupe commutatif** (resp. **monoïde commutatif**, **groupe commutatif**).

Supposons que E est un ensemble muni de deux lois de composition $+$ et $*$, et que 0 et 1 sont deux éléments distincts de E. On dit que $(E, +, *, 0, 1)$ est un **anneau** (unitaire) si les conditions suivantes sont vérifiées :

1) $(E, +, 0)$ est un groupe commutatif ;

2) $(E, *, 1)$ est un monoïde ;

3) $*$ est distributif par rapport à $+$, c'est-à-dire que pour tous les éléments x, y et z dans E, on a

$$(x + y) * z = x * z + y * z, \qquad z * (x + y) = z * x + z * y.$$

Si $(E, +, *, 0, 1)$ est un anneau, pour tout élément $x \in E$, on désigne par $-x$ l'élément inverse à x dans le groupe commutatif $(E, +, 0)$, et l'expression $y + (-x)$ se simplifie en $y - x$. Parfois, on utilise l'expression xy pour signifier $x * y$. Enfin, l'élément 1 est appelé l'**élément unité** de $(E, +, *, 0, 1)$.

Exercice 3.2 Montrer que si $(E, +, *)$ est un anneau, alors pour tout élément $x \in E$, on a $x * 0 = 0 * x = 0$.

Par exemple, l'ensemble des entier $\mathbb{Z}$, muni de l'addition et la multiplication naturelles, est un anneau.

Soit $(E, +, *, 0, 1)$ un anneau. Pour tout élément $x \in E$, s'il existe $y \in E$ tel que $xy = yx = 1$, on dit que x est inversible dans l'anneau E. L'élément y est unique, on le notera x^{-1}. On dit que $(E, +, *, 0, 1)$ est un **corps** si chaque élément non-nul de E est inversible pour la loi de composition $*$. Dans ce cas-là, $E^\times := E \setminus \{0\}$ est un groupe pour la loi de composition $*$ et l'élément unité 1. L'ensemble $\mathbb{Q}$ des nombres rationnels et l'ensemble $\mathbb{R}$ des nombres réels sont des corps.

On dit qu'un anneau ou un corps $(E, +, *, 0, 1)$ est **commutatif** si $*$ est une loi de composition commutative.

Lorsqu'il n'y a aucune ambiguïté sur les lois de composition et les éléments distingués, on utilisera le symbole décrivant l'ensemble sous-jacent à un semi-groupe (resp. monoïde, groupe, anneau, corps, etc.) pour déssigner le semi-groupe (resp. monoïde, groupe, anneau, corps, etc.) lui-même. Par exemple, au lieu de dire "$(\mathbb{Z}, +, \times, 0, 1)$" est un anneau, on dit simplement $\mathbb{Z}$ est un anneau.

Soit $\mathbb{F}_2$ l'ensemble à deux éléments 0 et 1. On définit deux opérateur $+$ et $\cdot$ sur $\mathbb{F}_2$ tels que

$$0 + 0 = 0, \qquad 0 + 1 = 1 + 0 = 1, \qquad 1 + 1 = 0,$$
$$1 \cdot 0 = 0 \cdot 1 = 0 \cdot 0 = 0, \qquad 1 \cdot 1 = 1.$$

Exercice 3.3 Vérifier que $(\mathbb{F}_2, +, \cdot)$ est un corps commutatif.

3.2 Distributions de valeurs de vérité

Définition 3.1 On appelle **distribution de valeurs de vérité** toute application de $\mathscr{P}$ dans $\mathbb{F}_2$.

Théorème 3.2 *Pour toute distribution de valeurs de vérité $\delta : \mathscr{P} \to \mathbb{F}_2$, il existe une unique application $\overline{\delta} : \mathscr{F} \to \mathbb{F}_2$ qui prolonge δ et telle que*

1) $\overline{\delta}[\neg F] = 1 + \overline{\delta}[F]$;

2) $\overline{\delta}[(F \wedge G)] = \overline{\delta}[F] \cdot \overline{\delta}[G]$;

3) $\overline{\delta}[(F \vee G)] = \overline{\delta}[F] + \overline{\delta}[G] + \overline{\delta}[F] \cdot \overline{\delta}[G]$;

4) $\overline{\delta}[(F \Rightarrow G)] = 1 + \overline{\delta}[F] + \overline{\delta}[F] \cdot \overline{\delta}[G]$;

5) $\overline{\delta}[(F \Leftrightarrow G)] = 1 + \overline{\delta}[F] + \overline{\delta}[G]$.

Exercice 3.4 Démontrer le théorème au-dessus en utilisant la proposition 2.9. Préciser l'endomorphisme a et l'application Ψ.

Pour toute formule F, $\overline{\delta}[F]$ est appelé la **valeur de vérité** de F par rapport à la distribution de valeurs de vérité δ. On convient que la valeur 1 signifie "vrai" tandi que la valeur 0 signifie "faux". Si $\overline{\delta}[F] = 1$, on dit que la formule F est **satisfaisante** par la distribution de valeur de vérité δ.

Ci-dessous sont quelques tables de valeurs de vérité. On voit que si F est vraie, alors $\neg F$ est fause ; si F est fause, alors $\neg F$ est vraie. Si F et G sont deux formules, alors $(F \vee G)$ est vraie lorsque l'une des F et G est vraie ; par contre, $(F \wedge G)$ est vraie uniquement lorsque tous les deux formules F et G sont toutes vraies. La valeur de vérité de la formule $(F \Leftrightarrow G)$ examine s'il y a une égalité entre les valeurs de vérités de F et de G. Lorsque F et G admettent la même valeur de vérité, alors $(F \Leftrightarrow G)$ prend la valeur de vérité 1, c'est-à-dire vraie, sinon $(F \Leftrightarrow G)$ est fause. Enfin, le table de valeurs de vérité pour $(F \Rightarrow G)$ est un peu difficile à comprendre. Tout particulièrement la partie "faux implique faux" et "faux implique vrai". Mais c'est tout-à-fait naturel. Considérons par exemple l'énoncé "si un entier est divisible par 6, alors il est pair" qui est sans doute vrai comme un raisonnement mathématique. Mais si on accepte ces genres d'énoncés, il est inévidable d'inclure les énoncés du type "si 1 est divisible par 6, alors 1 est paire" (faux implique faux) et du type "si 2 est divisible par 6, alors 2 est pair" (faux implique vrai).

Une autre difficulté de comprendre l'implication est que, dans un raisonnement habituel, l'implication est considérée comme la causalité, or ce n'est pas du tout le cas dans le calcul propositionnel. Par exemple, si F et G sont deux énoncés vrais, alors le calcul propositionnel impose la valeur de vérité vrai pour l'énoncé "F implique G". Maintenant, considérons l'énoncé, "si 1 est impaire, alors un pomme est un fruit". On refuse en général ces genres de raisonnemments, parce que, en acceptant cet énoncé, on attend une démonstration effective du résultat "un pomme est un fruit" à partir de l'énoncé "1 est impaire".

F	$\neg F$
0	1
1	0

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

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

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

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

Définition 3.3 On dit qu'une formule F est une **tautologie** si pour toute distribution de valeur de vérité δ on a $\overline{\delta}[F] = 1$. Si F est une tautologie, on note $\vdash^* F$. Si F et G sont deux formules, on dit que F est **logiquement équivalente** à G et on note $F \sim G$ si l'on a $\vdash^* (F \Leftrightarrow G)$.

Définition 3.4 Soit E un ensemble. On appelle **relation** sur E tout sous-ensemble de $E \times E$. Si $R \subset E \times E$ est une relation sur E et si (x, y) est un élément dans R, on note xRy. On dit que R est une **relation d'équivalence** si les conditions suivantes sont vérifiées :

1) le diagonale est contenu dans R, c'est-à-dire que xRx pour tout élément $x \in E$;
2) l'ensemble R est symétrique, c'est-à-dire que si xRy, alors yRx ;
3) la relation R est transitive, c'est-à-dire que si xRy et yRz, alors on a xRz.

Si E est un ensemble et si R est une relation d'équivalence sur E. Pour tout élément $x \in E$, on désigne par E_x le sous-ensemble de E des éléments $z \in E$ tels que xRz. L'ensemble $E_{R,x}$ est appelé la **classe d'équivalence** de x pour la relation d'équivalence R.

Exercice 3.5 Soit x et y deux éléments dans E. Montrer que $E_{R,x}$ et $E_{R,y}$ sont soit identiques soit disjoints.

On désigne par E/R l'ensemble des classes d'équivalence dans E, appelé le **quotient** de E modulo la relation d'équivalence R.

Exercice 3.6 Montrer que la relation $\sim$ est en fait une relation d'équivalence sur $\mathscr{F}$.

Théorème 3.5 *Soient δ une distribution de valeurs de vérité, F une formule, $(A_i)_{1\leq i\leq n}$ une famille finie de variables propositionnelles distinctes dans $\mathscr{P}$ et $(G_i)_{1\leq i\leq n}$ une famille de formules. Si on désigne par λ la distribution de valeurs de vérité telle que*

$$\lambda(B) = \begin{cases} \overline{\delta}[G_i], & B = A_i, \\ \delta[B], & B \notin \{A_1, \cdots, A_n\}. \end{cases} \tag{3.1}$$

Alors $\overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[F]$.

Démonstration On raisonne par récurrence sur F. Lorsque F est une variable propositionnelle, soit $F \notin \{A_1, \cdots, A_n\}$, soit F est l'une des A_i et donc $F_{G_1/A_1,\cdots,G_n/A_n} = G_i$. L'égalité $\overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[F]$ provient donc de la définition (3.1).

Si F est une formule et $H = \neg F$, alors on a $H_{G_1/A_1,\cdots,G_n/A_n} = \neg F_{G_1/A_1,\cdots,G_n/A_n}$. Par conséquent, $\overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[F]$ implique que

$$\overline{\delta}[H_{G_1/A_1,\cdots,G_n/A_n}] = 1 + \overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = 1 + \overline{\lambda}[F] = \overline{\lambda}[H].$$

Si F et G sont deux formules, α est un symbole de connecteur propositionnel binaire et $H = (F\alpha G)$. On a

$$H_{G_1/A_1,\cdots,G_n/A_n} = (F_{G_1/A_1,\cdots,G_n/A_n}\alpha G_{G_1/A_1,\cdots,G_n/A_n}).$$

Par conséquent, si $\overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[F]$ et $\overline{\delta}[G_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[G]$, alors

$$\begin{aligned} &\overline{\delta}[H_{G_1/A_1,\cdots,G_n/A_n}] = \Psi[\alpha, \overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}], \overline{\delta}[G_{G_1/A_1,\cdots,G_n/A_n}]] \\ &= \Psi[\alpha, \overline{\lambda}[F], \overline{\lambda}[G]] = \overline{\lambda}[H], \end{aligned}$$

où Ψ est la fonction précisée dans l'exercice 3.4. Par conséquent, pour toute formule F, on a $\overline{\delta}[F_{G_1/A_1,\cdots,G_n/A_n}] = \overline{\lambda}[F]$.

□

Corollaire 3.6 *Si F est une tautologie, alors il en est de même de $F_{G_1/A_1,\cdots,G_n/A_n}$.*

Soit F une formule. Il est aussi possible de substituer une sous-formule G dans F par une autre formule H. Si G est logiquement équivalente à H, alors la formule F', obtenue par la substitution la formule H à la sous-formule G, est logiquement équivalente à F.

Soient A, B et C trois variables propositionnelles. On désigne par $\top$ une tautologie quelconque et par $\bot$ une formule quelconque qui prend toujours la valeur 0 quelque soit la distribution de valeurs de vérité.

Exercice 3.7 Montrer que les formules suivantes sont des tautologies.

$1)((A \wedge A) \Leftrightarrow A)$	$2)((A \vee A) \Leftrightarrow A)$
$3)((A \wedge B) \Leftrightarrow (B \wedge A))$	$4)((A \vee B) \Leftrightarrow (B \vee A))$
$5)(((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C)))$	$6)(((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C)))$
$7)((A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C)))$	$8)((A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)))$
$9)((A \wedge (A \vee B)) \Leftrightarrow A)$	$10)((A \vee (A \wedge B)) \Leftrightarrow A)$
$11)(\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B))$	$12)(\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B))$
$13)((A \wedge \top) \Leftrightarrow A)$	$14)((A \vee \bot) \Leftrightarrow A)$
$15)((A \vee \top) \Leftrightarrow \top)$	$16)((A \wedge \bot) \Leftrightarrow \bot)$
$17)((A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A))$	

Les deux premières tautologies représentent l'idempotence de la conjonction et de la disjonction ; Les 3) et 4) sont leur commutativité ; les 5) et 6) sont leur associativité ; les 7) and 8) sont la distributivité de l'une par rapport à l'autre ; les 9) et 10) sont des lois d'absorption ; les 11) et 12) sont des lois de de Morgan. La 13) montre que la classe des tautologies est l'élément unité pour la conjonction et la 14) montre que la classe des antilogies pour la disjonction. La 15) montre que la classe des tautologies est absorbante pour la conjonction et la 16) montre que la classe des antilogies est absorbante pour la la disjonction. Enfin, la 17) montre que que toute formule sous forme d'implication est logiquement équivalente à sa contraposée.

Il faut être consient que le calcul propositionnel ne peut pas modéliser tout les raisonnement dans la vie courante. Par exemple, considérons la phrase "s'il pleut, alors je porte mon paraplui". Sa contraposée est "si je ne porte pas mon parapluie, alors il ne pleut pas". Mais cette dernière, dans la langue courante, présente "je ne porte pas mon parapluie, donc il ne pleut pas". Par conséquent, on doit considérer le calcul propositionnel comme un calcul entre 0 et 1, qui est trops simplifié pour être appliqué dans la vie réelle.

Exercice 3.8 Montrer que les formules suivantes sont des tautologies :

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

Exercice 3.9 Montrer que les formules suivantes sont des tautologies :

$((A \Rightarrow B) \Leftrightarrow (\neg A \vee B))$ $\qquad$ $((A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A)))$
$((A \Leftrightarrow B) \Leftrightarrow ((A \vee B) \Rightarrow (A \wedge B)))$

3.3 Formes normales

Si ε est un élément dans $\mathbb{F}_2$ et si F est une formule, on désigne par εF la formule suivante :

$$\varepsilon F = \begin{cases} F, & \varepsilon = 1; \\ \neg F, & \varepsilon = 0. \end{cases}$$

La conjonction et la disjonction sont commutatives et associatives modulo la relation d'équivalence logique. Par exemple, dans l'expression $A \vee B \vee C$, quelle que soit la façon de permuter les variables A, B, C et de mettre des parenthèse pour que le mot devienne une formule, la formule obtenue est toujours dans la même classe d'équivalence. Cette observation nous autorise d'utiliser l'écriture $\bigvee_{i\in I} F_i$ et $\bigwedge_{i\in I} F_i$, où I est un ensemble fini et $(F_i)_{i\in I}$ est une famille de formules paramétrée par I.

On a vu dans les exerecices 3.8 et 3.9 que la formule $(A \Rightarrow B)$ est logiquement équivalente à $(\neg A \vee B)$ et que la formule $(A \Leftrightarrow B)$ est logiquement équivalente à $((A \Rightarrow B) \wedge (B \Rightarrow A))$ et donc à $((\neg A \vee B) \wedge (\neg B \vee A))$. Il est alors naturel d'espérer que toute formule est équivalente à une formule qui ne contient que des symboles de connecteur propositionnels de la forme $\neg$, $\wedge$ ou $\vee$.

En effet, on a le théorème suivant :

Théorème 3.7 *Soient F une formule dans $\mathscr{P}$ et $(A_i)_{1\leq i\leq n}$ l'ensemble des varaibles propositionnelles apparues dans F.*

1) Si la formule F n'est pas une antilogie, alors il existe un unique sous-ensemble E de $\mathbb{F}_2^n$ tel que F soit logiquement équivalente à la formule

$$\bigvee_{(\varepsilon_i)_{1\leq i\leq n}\in E} \bigwedge_{1\leq i\leq n} \varepsilon_i A_i. \tag{3.2}$$

2) Si la formule F n'est pas une tautologie, alors il existe un unique sous-ensemble E' de $\mathbb{F}_2^n$ tel que F soit logiquement équivalente à la formule

$$\bigwedge_{(\varepsilon_i)_{1\leq i\leq n}\in E'} \bigvee_{1\leq i\leq n} \varepsilon_i A_i. \tag{3.3}$$

Démonstration 1) Pour tout élément $(\varepsilon_i)_{1\leq i\leq n} \in \mathbb{F}_2^n$ et toute distribution de valeur de vérité, la formule $\bigwedge_{1\leq i\leq n} \varepsilon_i A$ est satisfaisante par δ si et seulement si δ prend valeur ε_i en A_i pour tout $1 \leq i \leq n$. En effet, $\bigwedge_{1\leq i\leq n} \varepsilon_i A_i$ est satisfaisante par δ si et seulement si tous les $\varepsilon_i A_i$ sont satisfaisante par δ, i.e., $\delta[A_i] = \varepsilon_i$. Il est anodin de supposer que l'ensemble $\mathscr{P}$ des variables propositionnelles est juste $(A_i)_{1\leq i\leq n}$. Pour tout élément $(\varepsilon_1, \cdots, \varepsilon_n) \in \mathbb{F}_2^n$ on désigne par $\delta_{\varepsilon_1,\cdots,\varepsilon_n}$ la distribution de valeur de vérité qui prend valeur ε_i en A_i. On remarque que toute distribution de valeur de vérité s'écrit sous la forme $\delta_{\varepsilon_1,\cdots,\varepsilon_n}$ avec certain $(\varepsilon_1, \cdots, \varepsilon_n) \in \mathbb{F}_2^n$. Soit E l'ensemble des éléments $(\varepsilon_i)_{1\leq i\leq n} \in \mathbb{F}_2^n$ tel que $\overline{\delta}_{\varepsilon_1,\cdots,\varepsilon_n}[F] = 1$. Comme F n'est par une antilogie, l'enemble E est non-vide. Si Δ est un sous-ensemble de $\mathbb{F}_2^n$, on désigne par G_Δ la formule

$$\bigvee_{(\varepsilon_1,\cdots,\varepsilon_n)\in\Delta} \bigwedge_{1\leq i\leq n} \varepsilon_i A_i.$$

On a

$$\overline{\delta}_{\varepsilon_1,\cdots,\varepsilon_n}[G_\Delta] = \begin{cases} 1, & (\varepsilon_1, \cdots, \varepsilon_n) \in \Delta, \\ 0, & (\varepsilon_1, \cdots, \varepsilon_n) \notin \Delta. \end{cases}$$

Par conséquent, F est logiquement équivalente à G_E. D'autre part, si U et U' ne sont pas identiques, alors G_U et $G_{U'}$ ne sont pas logiquement équivalentes puisque un élément $(\varepsilon_1, \cdots, \varepsilon_n)$ est dans $U \setminus U'$ ou dans $U' \setminus U$ implique que $\overline{\delta}_{\varepsilon_1,\cdots,\varepsilon_n}[G_U] \neq \overline{\delta}_{\varepsilon_1,\cdots,\varepsilon_n}[G_{U'}]$.

2) Si on applique le résultat de 1) à $\neg F$, on obtient qu'il existe un sous-ensemble U de $\mathbb{F}_2^n$ tel que $\neg F$ soit logiquement équivalente à

$$\bigvee_{(\varepsilon_1,\cdots,\varepsilon_n)\in U} \bigwedge_{1\leq i\leq n} \varepsilon_i A_i.$$

Par conséquent, F (qui est logiquement équivalente à $\neg\neg F$) est logiquement équivalente à

$$\neg \bigvee_{(\varepsilon_1,\cdots,\varepsilon_n)\in U} \bigwedge_{1\leq i\leq n} \varepsilon_i A_i \sim \bigwedge_{(\varepsilon_1,\cdots,\varepsilon_n)\in U} \bigvee_{1\leq i\leq n} \neg\varepsilon_i A_i.$$

Soit E' l'ensemble des $(\eta_1, \cdots, \eta_n) \in \mathbb{F}_2^n$ tel que $(1+\eta_1, \cdots, 1+\eta_n) \in U$. On obtient alors que F est logiquement équivalente à

$$\bigwedge_{(\eta_1,\cdots,\eta_n)\in E'} \bigvee_{1\leq i\leq n} \eta_i A_i.$$

Enfin, l'unicité de E' provient du résultat d'unicité dans 1). En effet, on a la relation $E' = \mathbb{F}_2^n \setminus E$.

□

Les formules de la forme (3.2) sont appelées des formules sous forme **normale disjonctive canonique** (FDNC) ; les formules de la forme (3.2) sont appelées des formules sous forme **normale conjonctive canonique** (FDCC).

Exercice 3.10 Transformer les formules suivantes sous forme FDNC et sous forme FDCC.

$$A \Leftrightarrow B \qquad ((\neg A \Leftrightarrow B) \Rightarrow (\neg B \vee (\neg A \Leftrightarrow B))) \tag{3.4}$$

Chapitre 4

Algèbre de Boole

4.1 Préliminaires

Soit $\mathcal{A}$ et $\mathcal{B}$ deux anneaux. On appelle **homomorphisme** de $\mathcal{A}$ dans $\mathcal{B}$ toute application φ qui préserve l'addition, la multiplication et l'élément unité. D'autre terme, si x et y sont deux éléments dans $\mathcal{A}$, on a

$$\varphi(x+y) = \varphi(x) + \varphi(y), \qquad \varphi(xy) = \varphi(x)\varphi(y) \quad \text{et} \quad \varphi(1) = 1.$$

Soit $\mathcal{A}$ un anneau commutatif. On appelle **algèbre** sur $\mathcal{A}$ (ou $\mathcal{A}$-algèbre) tout anneau $\mathcal{B}$ muni d'un homomorphisme $\varphi : \mathcal{A} \to \mathcal{B}$. Si a est un élément de $\mathcal{A}$ et si b est un élément de $\mathcal{B}$, on désigne par ab l'élément $\varphi(a)b$ dans $\mathcal{B}$. On dit qu'une $\mathcal{A}$-algèbre est **commutative** si l'anneau $\mathcal{B}$ est commutatif.

On considère un exemple simple. Soit $\varphi : \mathbb{Z} \to \mathbb{Q}$ l'application d'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$. Ainsi $\mathbb{Q}$ devient une algèbre sur $\mathbb{Z}$.

Exercice 4.1 1) Montrer que l'application $\varphi : \mathbb{Z} \to \mathbb{F}_2$ qui envoie n en 0 si n est paire et en 1 si n est impaire est un homomorphisme d'anneaux ;

2) Montrer que tout anneau est canoniquement muni d'une structure d'algèbre sur $\mathbb{Z}$.

Définition 4.1 On appelle **anneau de Boole** (ou **algèbre de Boole**) tout anneau $\mathcal{A}$ dont tout élément est idempotent (c'est-à dire $x^2 = x$ pour tout $x \in \mathcal{A}$).

Exercice 4.2 Vérifier que le corps à deux éléments $\mathbb{F}_2$ est un anneau de Boole.

Pourquoi un anneau de Boole s'appelle aussi une algèbre de Boole ? En effet, on a la proposition suivante :

Proposition 4.2 *Soit $\mathcal{A}$ un anneau de Boole. Pour tout élément $a \in A$, on $a\ a + a = 0$.*

Démonstration En effet, on a $(a+1)(a+1) = a^2 + a + a + 1$. Or $a+1$ et a sont idempotents, on obtien donc $a + 1 = a + a + a + 1$. On en déduit donc $a + a = 0$.

□

La proposition 4.2 montre en particulier que l'application $\varphi : \mathbb{F}_2 \to \mathcal{A}$ qui envoie 0 en 0 et 1 en 1 est en fait un homomorphisme d'anneaux. Ainsi $\mathcal{A}$ est canoniquement muni d'une structure d'algèbre sur $\mathbb{F}_2$. Par conséquent, tout anneau de Boole est une algèbre sur $\mathbb{F}_2$.

Proposition 4.3 *Si $\mathcal{A}$ est une algèbre de Boole, alors elle est commutative.*

Démonstration Soient x et y deux éléments dans $\mathcal{A}$. Comme $x + y$ est idempotent, on a

$$x + y = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + y + xy + yx,$$

d'où $xy + yx = 0$. Comme $xy + xy = 0$, on a donc $xy = yx$.

□

Définition 4.4 Soit E un ensemble et $\leq$ une relation sur E. On dit que $\leq$ est une relation d'ordre si les conditions suivantes sont vérifiés :

1) pour tout élément $x \in E$, on a $x \leq x$;

2) si $x \leq y$ et si $y \leq x$, alors $x = y$;

3) si $x \leq y$ et si $y \leq z$, alors $x \leq z$.

Le couple $(E, \leq)$ est appelé un ensemble ordoné.

Par exemple, on considère la relation $\leq$ sur $\mathbb{Z}$ tel que $x \leq y$ si et seulement si $y - x \in \mathbb{N}$. Alors $\leq$ est une relation d'ordre sur $\mathbb{Z}$. En effet, on a $x - x = 0 \in \mathbb{N}$, donc $x \leq x$. D'autre part, si $x \leq y$ et si $y \leq x$, alors $y - x$ et $x - y$ sont tous dans $\mathbb{N}$, donc $x = y$. Enfin, si $x \leq y \leq z$, c'est-à-dire $y - x$ et $z - y$ sont tous dans $\mathbb{N}$, alors $z - x = (z - y) + (y - x)$ est aussi dans $\mathbb{N}$, donc on a $x \leq z$.

Soient E un ensemble et $\leq$ une relation d'ordre sur E. On dit qu'un élément m est **minimal** pour la relation $\leq$ si pour tout élément $x \in E$ on a $m \leq x$; on dit qu'un élément M est **maximal** pour la relation $\leq$ si pour tout élément $x \in E$ on a $x \leq M$. En fait, si E adment un élément minimal (resp. maximal), alors cet élément minimal (resp. maximal) est unique. Ce n'est pas vrai que dans un ensemble ordonné il existe toujour un élément

minimal. L'énoncé similaire pour l'élément maximal n'est pas vrai non plus. Par exemple, dans l'ensemble ordonné $\mathbb{Z}$, il n'existe ni élément minimal ni élément maximal. En effet, si n est un entier, alors $n-1 \leq n \leq n+1$ mais $n-1 \neq n \neq n+1$. Par conséquent, n ne peut être ni maximal ni minimal.

Soit $\mathcal{A}$ une algèbre de Boole. Sur $\mathcal{A}$ on définit une relation $\leq$ telle que $x \leq y$ si et seulement si $xy = x$.

Proposition 4.5 *La relation $\leq$ est une relation d'ordre sur $\mathcal{A}$.*

Démonstration Comme $\mathcal{A}$ est une algèbre de Boole, on a $x^2 = x$, donc $x \leq x$. Si $x \leq y$ et $y \leq x$, alors $x = xy = yx = y$ car $\mathcal{A}$ est commutative. Enfin si $x \leq y$ et $y \leq z$, alors $xz = xyz = xy = x$.

□

Il s'avère que 0 est toujours l'élément minimal et 1 est l'élément maximal. En effet, on a $x \cdot 0 = 0$ et $1 \cdot x$ pour tout $x \in \mathcal{A}$.

Proposition 4.6 *Pour tout couple d'éléments $(x, y) \in \mathcal{A}^2$, $x \frown y = xy$ est la borne inférieure des éléments x et y.*

Démonstration On montre d'abord que xy est un minorant commun de x et de y. En effet, $xyx = x^2y = xy$ et $xyy = xy^2 = xy$. D'autre part, si z est un minorant commun de x de y, i.e., $xz = yz = z$. Alors $xyz = xz = z$. Donc on a $xy \leq z$.

□

Proposition 4.7 *Pour tout couple d'éléments $(x, y) \in \mathcal{A}^2$, $x \smile y = x + y + xy$ est la borne supérieure de x et y.*

Démonstration D'abord on montre que $x \smile y$ est un majorant de x et de y. En effet, on a $x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x$ et $y(x + y + xy) = xy + y^2 + xy^2 = xy + y + xy = y$. Si de plus z est un majorant commun de x et de y, alors on a $zy = y$ et $zx = x$. D'où $z(x + y + xy) = zx + zy + zxy = x + y + xy$, i.e., $x + y + xy \leq z$.

□

Exercice 4.3 Monter les énoncés suivants :

1) les opérateurs $\smile$ et $\frown$ sont commutatifs et associatifs ;

2) pour tout élément $x \in \mathcal{A}$, on a les égalités

$$x \smile 0 = x, \quad x \frown 0 = 0, \quad x \smile 1 = 1, \quad x \frown 1 = x.$$

3) les opérateurs $\smile$ et $\frown$ sont distributive l'un à l'autre.

Proposition 4.8 *Pour tout élément $x \in \mathcal{A}$, il existe un unique élément $x^c \in \mathcal{A}$ tel que $x \smile x^c = 1$ et que $x \frown x^c = 0$.*

Démonstration En effet, si un tel élément x^c existe, alors $xx^c = 0$ et $x+x^c+xx^c = 1$. D'où $x^c = 1+x$. Donc x^c est existe. D'autre part, $x(1+x) = x + x^2 = x + x = 0$, $x + (1 + x) + x(1 + x) = x + 1 + x = 1$. Donc $x^c = 1 + x$ exite et est unique.

□

L'élément x^c est appelé le **complémentaire** de x. Il est claire que $x^{cc} = 1 + 1 + x = x$, donc $x \mapsto x^c$ est une involution sur $\mathcal{A}$.

Exercice 4.4 Montre que l'involution $x \mapsto x^c$ renverse l'ordre, c'est-à-dire que si $x \leq y$, alors $y^c \leq x^c$. En déduire la loi de de Morgan :

$$(x \smile y)^c = x^c \frown y^c, \qquad (x \frown y)^c = x^c \smile y^c.$$

Proposition 4.9 *Soient x et y deux éléments dans $\mathcal{A}$. Alors $x \leq y^c$ si et seulement si $xy = 0$.*

Démonstration On a $x(1+y) = x+xy$. Donc $x(1+y) = x$ si et seulement si $xy = 0$.

□

Soient Ω un ensemble non-vide et $\mathcal{P}(\Omega)$ l'ensemble des parties de Ω. Si U et V sont deux sous-ensemble de Ω, on désigne par $U \cup V$ l'union de U et V et par $U \cap V$ l'intersection de U et V. Si U est un sous-ensemble de Ω, on désigne par U^c le complémentaire de U dans U. Il est claire que l'on a les proprétés suivantes :

1) on a $U \cup \emptyset = U \cap \Omega = U$, $U \cap \emptyset = \emptyset$ et $U \cup \Omega = \Omega$;

2) les opérateurs $\cap$ et $\cup$ sont commutatifs et associatifs ;

3) les opérateurs $\cap$ et $\cup$ sont distributive l'un par rapport à l'autre ;

4) $U \mapsto U^c$ est une involution de l'ensemble $\mathcal{P}(\Omega)$;

5) $(U \cap V)^c = U^c \cup V^c$ et $(U \cup V)^c = U^c \cap V^c$.

D'autre part, l'inclusion d'ensembles définit une relation d'ordre sur $\mathcal{P}(\Omega)$.

Exercice 4.5 Soient U et V deux sous-ensemble de Ω. Vérifier que $U \subset V^c$ si et seulement si $U \cap V = \emptyset$.

On voit donc une resemblance des opérateurs $\cap$ et $\cup$ sur $\mathcal{P}(\Omega)$ et les opérateurs $\frown$ et $\smile$ sur une algèbre de Boole. En effet, si pour tout couple de parties (U, V) de Ω, on désigne par $U\Delta V$ la différence symétrique de U et de V, c'est-à-dire $U\Delta V = (U \cap V^c) \cup (V \cap U^c)$.

Proposition 4.10 *Le triplet $(\mathcal{P}(\Omega), \Delta, \cap)$ est une algèbre de Boole. De plus, l'opérateur $\smile$ associé à cette algèbre de Boole coïncide avec $\cup$.*

Démonstration Par définition Δ est un opérateur commutatif. Si U, V et W sont trois sous-ensemble de Ω, on a

$$\begin{aligned}
&(U\Delta V)\Delta W = ((U\Delta V) \cap W^c) \cup (W \cap (U\Delta V)^c) \\
&= (((U \cap V^c) \cup (V \cap U^c)) \cap W^c) \cup (W \cap ((U \cap V^c) \cup (V \cap U^c))^c) \\
&= (U \cap V^c \cap W^c) \cup (V \cap U^c \cap W^c) \cup (W \cap ((U \cap V^c)^c \cap (V \cap U^c)^c)) \\
&= (U \cap V^c \cap W^c) \cup (V \cap U^c \cap W^c) \cup (W \cap ((U^c \cup V) \cap (V^c \cup U))) \\
&= (U \cap V^c \cap W^c) \cup (V \cap U^c \cap W^c) \cup (W \cap ((U^c \cap V^c) \cup (V \cap U))) \\
&= (U \cap V^c \cap W^c) \cup (V \cap U^c \cap W^c) \cup (W \cap U^c \cap V^c) \cup (U \cap V \cap W).
\end{aligned}$$

Par la commutativité de l'opérateur Δ et par la symétrie, on voit que

$$\begin{aligned}
&U\Delta(V\Delta W) = (V\Delta W)\Delta U \\
&= (U \cap V^c \cap W^c) \cup (V \cap U^c \cap W^c) \cup (W \cap U^c \cap V^c) \cup (U \cap V \cap W) \\
&= (U\Delta V)\Delta W.
\end{aligned}$$

D'autre part, on a $\emptyset\Delta U = (U \cap \emptyset^c) \cup (\emptyset \cap U^c) = U$. Donc $(\mathcal{P}(\Omega), \Delta)$ est un anneau commutatif d'élément neutre $\emptyset$.

L'opérateur $\cap$ est commutatif et associatif sur $\mathcal{P}(\Omega)$. En outre, $U \cap \Omega = U$ pour tout sous-ensemble U de Ω. Comme Ω est non-vide (pourquoi il faut que Ω soit non-vide ?) $(\mathcal{P}(\Omega) \setminus \{\emptyset\}, \cap)$ est un monoïde commutatif avec l'élément identié Ω. De plus, on a

$$\begin{aligned}
&(U\Delta V) \cap W = ((U \cap V^c) \cup (V \cap U^c)) \cap W \\
&= (U \cap V^c \cap W) \cup (V \cap U^c \cap W)
\end{aligned}$$

et

$$\begin{aligned}
&(U \cap W)\Delta(V \cap W) \\
&= ((U \cap W) \cap (V \cap W)^c) \cup ((V \cap W) \cap (U \cap W)^c) \\
&= ((U \cap W) \cap (V^c \cup W^c)) \cup ((V \cap W) \cap (U^c \cup W^c)).
\end{aligned}$$

On obtient donc que l'opérateur $\cap$ est distributive par rapport à Δ. Ainsi $(\mathcal{P}(\Omega), \Delta, \cap)$ est un anneau commutatif. Evidemment pour tout sous-ensemble U de Ω on a $U \cap U$. Donc $(\mathcal{P}(\Omega), \Delta, \cap)$ est en fait une algèbre de Boole.

Enfin, on vérifie que l'opérateur $\smile$ sur $\mathcal{P}(\Omega)$ coïncide avec $\cup$. En effet, pour tout couple (U, V) de sous-ensemble de Ω, on a

$$\begin{aligned} & U \smile V = U\Delta V\Delta(U \cap V) \\ &= U\Delta((V \cap (U \cap V)^c) \cup (V^c \cap (U \cap V))) = U\Delta(V \cap (U^c \cup V^c)) \\ &= U\Delta(V \cap U^c) = (U \cap (V^c \cup U)) \cup (V \cap U^c \cap U^c) \\ &= (U \cap V^c) \cup U \cup (V \cap U^c) = U \cup (V \cap U^c) = U \cup V. \end{aligned}$$

□

Exercice 4.6 Redémontrer la proposition 4.10 en utilisant le graphe de Veen ?

4.2 Atoms dans une algèbre de Boole

Chapitre 5

Syntaxe des prédicats

5.1 Langages du premier ordre, termes

Nous avons vu dans les chapitres précédents des enembles munis de certains structures (opérateurs, éléments unités, relations). Dans notre démonstrations, il paraîsait des quantificateurs (pour tout, il existe). Tous ces objets ne peuvent pas être modélisés par le calcul propositionnel. Par conséquent, il faut des outils plus compliqués pour les modéliser. Par exemple, pour modéliser les monoïdes, il faut un symbole de constante pour désigner l'élément neutre et un symbole d'opérateur binaire pour représenter la multiplication. Les langage du premier ordre et le calcul des prédicat sont pour but de modéliser ces genres d'objets et raisonnements.

Un **langage du premier ordre** est un ensemble $\mathscr{L}$ de symboles qui se décompose en deux sous-ensembles qui n'ont pas de partie commune non-vide :

1) le prémier sous-ensemble, qui est commun à tous les langages, est la réunion disjonte des parties suivantes :
   i) un ensemble infini dénombrable $\mathscr{V} = \{v_0, v_1, \cdots, v_n, v_{n+1}, \cdots\}$ dont les éléments sont appelés **symboles de variables**,
   ii) un ensemble consistituant de neuf symboles
      - les parenthèse) et (,
      - les symobles de connecteurs $\neg$, $\wedge$, $\vee$, $\Rightarrow$ et $\Leftrightarrow$, comme dans le calcul propositionnel,
      - $\forall$, appelé **quantificateur universel** et que l'on lit "**pour tout**",
      - $\exists$, appelé **quantificateur existentiel**et que l'on lit "**il existe**"
2) La deuxième sous-ensemble, qui varie selon les langages, est la réunion disjonte de

i) un ensemble $\mathscr{C}$ dont les éléments osnt appelés **symboles de constante**,

ii) pour chaque entier $n \geq 1$, un ensemble $\mathscr{F}_n$ dont les éléments sont appelés **symboles de fonction** à n places (ou n-aires),

iii) pour chaque entier $n \geq 1$, un ensemble $\mathscr{R}_n$ dont les éléments sont appelés **symboles de relation** à n places (ou n-aires).

Pour déterminer un langage du premier ordre, il suffit de préciser les constantes, les fonctions et les relations.

Définition 5.1 On désigne par $\mathscr{T}(\mathscr{L})$ le plus petit sous-ensemble de $\mathscr{M}(\mathscr{L})$ qui continent $\mathscr{V} \cup \mathscr{C}$ et qui est stable pour tous les applications de la forme $(m_1, \cdots, m_n) \mapsto f m_1 \cdots m_n$, où f est un élément dans $\mathscr{F}_n$.

On peut aussi construire "par récurrence" les termes du langage $\mathscr{L}$. On pose $\mathscr{T}_0(\mathscr{L}) = \mathscr{V} \cup \mathscr{C}$. Une fois construits les $\mathscr{T}_0(\mathscr{L}), \cdots, \mathscr{T}_k(\mathscr{L})$, on définit

$$\mathscr{T}_{k+1}(\mathscr{L}) = \mathscr{T}_k(\mathscr{L}) \cup \bigcup_{n \geq 1} \{f t_1 t_2 \cdots t_n \mid f \in \mathscr{F}_n,\ t_1 \in \mathscr{T}_k(\mathscr{L}), \cdots, t_n \in \mathscr{T}_k(\mathscr{L})\}.$$

Exercice 5.1 (à la maison) Montrer que cette nouvelle définition "par récurrence" est en fait équivalente à la définition 5.1.

Soit $t \in \mathscr{T}(\mathscr{L})$ un terme. On appelle **hauteur** de t le plut petit entier $k \geq 0$ tel que t soit dans $\mathscr{T}_k(\mathscr{L})$.

Exercice 5.2 Considérons un langage $\mathscr{L}$ qui comporte un symbole de constante c, un symbole unaire f et un symbole binaire g. Déterminer si les mots suivants sont des termes :

$$f v_1 \qquad g f c c \qquad g f c g c f c \qquad c g f c$$

si oui, déterminer la hauteur de chaque terme.

Comme dans le calcul propositionnel, on souhaite une méthode automatique pour vérifier si un mot est un terme. On voit que dans le calcul propositonnel, on se dispose de deux quantités o[M] et f[M] pour un mot M, en comparant la différence de ces deux quantités pour les préfixes d'un mot M, on obtient si le mot M et bien une formule. Dans le cas du langage du premier ordre, on introduira une fonction p[$\cdot$] appelée **poids** pour les mots dans $\mathscr{M}(\mathscr{L})$ qui est similaire à la différence de o[$\cdot$] et f[$\cdot$]. En examinant cette fonction en tous les préfixe d'un mot M, on déduit si le mot M est un terme.

Définition 5.2 Pour tout symbole de fonction f dans $\mathscr{F}_n$, le **poids** de f est par définition l'entier positif $n - 1$. Le poids d'un symbole de variable ou

d'un symbole de constante est par définition -1. On appelle **poids** d'un mot $M \in \mathscr{M}(\mathscr{L})$ la somme des poids de tous les symboles constituant le mot M, noté $\mathrm{p}[\mathscr{M}]$. Enfin le **poid** du mot vide est par convention 0.

Exercice 5.3 Calculer les poids des préfixes des mots dans l'exercice 5.2. Que pouvez-vous dire sur votre résultats ?

Théorème 5.3 *Un mot $M \in \mathscr{M}(\mathscr{L})$ est un terme si et seulement si les conditions suivantes sont vérifiées :*

1) $\mathrm{p}[M] = -1$,

2) pour tout préfix propre N de M, $\mathrm{p}[N] \geq 0$.

Avant de démontrer le théorème 5.2, on introduit le principe d'induction suivant. Supposons que l'on veut vérifier une condition $\mathbb{P}$ pour tous les termes dans $\mathscr{T}(\mathscr{L})$. Il suffit de la démontrer en deux étapes. Premièrement on vérifie que la condition $\mathbb{P}$ est vérifiée pour des symboles de constante ou de variable, c'est-à-dire des symboles dans $\mathscr{T}_0(\mathscr{L})$; ensuit, pour tout entier $n \geq 1$ et tout symbole de fonction f à n places, en supposons que la propiété $\mathbb{P}$ soit vérifiée pour les termes $t_1, \cdots, t_n$, on montre que elle est également vraie pour $ft_1 \cdots t_n$. Ce principe d'induction peut être justifié par la récurrence sur la hauteur des termes, comme ce que l'on a fait dans le chapitre 2.

Démonstration du théorème 5.3

"Nécessité" : Si t est un mot dans $\mathscr{T}_0(\mathscr{L})$, alors par définition on a $\mathrm{p}[t] = -1$. Le seule préfixe propre de t est le mot vide et donc de poids 0. On a alors montré que les conditions 1) et 2) sont vérifé pour le mot t.

Considérons maintenant un symbole de fonction f de n places ($n \geq 1$) et une famille $(t_i)_{1 \leq i \leq n}$ de termes. On suppose que les terme t_i satisfont les conditions 1) et 2). Considérons le temer $M = ft_1 \cdots t_n$. On a évidement

$$\mathrm{p}[M] = \mathrm{p}[f] + \sum_{i=1}^{n} \mathrm{p}[t_i] = n - 1 + (-1) \times n = n - 1 - n = -1.$$

Un préfixe propre N de M s'écrit sous l'une des formes suivantes :

i) N est vide ;

ii) il existe un entier $0 \leq j < n$ et un préfixe u_j de t_j tels que $N = ft_1 \cdots t_{j-1} u_j$;

iii) il existe un préfixe propre u_n de t_n tel que $N = ft_1 \cdots t_{n-1} u_n$.

Dans le premier cas, on a $\mathrm{p}[N] = 0$ par convention ; dans le deuxième, on a

$$\mathrm{p}[N] = \mathrm{p}[f] + \sum_{i=1}^{j-1} \mathrm{p}[t_i] + \mathrm{p}[u_j] \geq n - 1 - j \geq 0;$$

enfin, dans le troisième, on a

$$\mathrm{p}[N] = \mathrm{p}[f] + \sum_{i=1}^{n-1} \mathrm{p}[t_i] + \mathrm{p}[u_n] \geq n - 1 + (-1) * (n-1) = 0.$$

On a donc démontré que M satisfait les deux conditions.
"Suffisance" : Supposons que M est un mot dans $\mathscr{M}(\mathscr{L})$ vérifiant les conditions 1) et 2). Si la longueur de M est égale à 1, donc M est dans $\mathscr{T}_0(\mathscr{L})$ puisque $\mathrm{p}[M] = -1$. Donc M est un terme. Dans la suite, on suppose que la longueur de M est supérieure ou égale à 2 et que la suffisance soit vérifiée pour les mots de longueur strictement inférieure à celle de M. Dans ce cas-là, le premier symbole f du mot M est un symbole de fonction puisque la condition 2) implique que $m = \mathrm{p}[f] \geq 0$. Soit M_1 le sous-mot de M tel que $M = fM_1$. On va décomposer M_1 en l'union disjointe de sous-mots vérifiant les deux conditons 1) et 2). Soit t_1 le plus court préfixe tel que $\mathrm{p}[t_1] = -1$. Comme le premier symbole de t_1 est de poids ≥ -1 et comme $\mathrm{p}[M_1] = -1 - m \leq -1$, on obtient que le mot t_1 existe et vérifie les conditions 1) et 2). Par l'hypothèse de récurrence, le mot t_1 est bien un terme.

Si $t_1 \neq M_1$ on désigne par M_2 le sous-mot tel que $M_1 = t_1 M_2$. On a $\mathrm{p}[M_2] = -m$. En itérant le précédé ci-dessus on obtient des sous-mots $t_1, \cdots, t_m$ qui vérifie les conditions 1) et 2). On suppose $M_1 = t_1 \cdots t_m M_m$. Alors M_m doit être vide puisque $\mathrm{p}[ft_1 \cdots t_m] = -1 < 0$ et que M satisfait à la condition 2). Par conséquent, $M = ft_1 \cdots t_m$ est un terme.

Corollaire 5.4 *Si M est un terme, alors tout préfixe propre n'est pas un terme.*

Théorème 5.5 (Lecture unique) *Soit $t \in \mathscr{T}(\mathscr{L})$ un terme quelconque. Alors un et un seul des deux cas suivant se présente :*

1) $t \in \mathscr{V} \cup \mathscr{C}$;

2) il existe un unique entier $n \geq 1$, un unique symbole de fonction à n places f, et un unique élément $(t_1, \cdots, t_n) \in \mathscr{T}(\mathscr{L})^n$ tels que $t = ft_1 \cdots t_n$.

Démonstration En effet, il est claire que les deux cas sont exclus l'un l'autre et que un terme quelconque est tombé dans l'un des deux cas. Il suffit donc de vérifier l'unicité dans le deuxième cas. Supposons qu'il existe deux

entiers $n, m \geq 1$, un symbole f à n places, un symbole g à m places et des éléments $t_1, \cdots, t_n, u_1, \cdots, u_m$ dans $\mathscr{T}(\mathscr{L})$ tels que

$$t = ft_1 \cdots t_n = gu_1 \cdots u_m.$$

On obtient $f = g$ et donc $n = m$. S'il existe un indice j tel que $t_j \neq u_j$, on désigne par i le plus petit indice tel que $t_i \neq u_i$. De l'égalité $t_i \cdots t_n = u_i \cdots u_n$ on obtient que, ou bien t_i est un préfixe propre de u_i ou bien u_i est un préfixe propre de t_i. Par conséquent, l'un des mots u_i et t_i n'est pas un terme, cela est absurde. Donc pour tout entier $1 \leq i \leq n$, on a $u_i = t_i$.

□

Soient t un terme, $(u_i)_{1 \leq i \leq k}$ une famile de symboles de variables **distincts** et $(t_i)_{1 \leq i \leq k}$ des termes. On désigne par $t_{t_1/u_1, \cdots, t_k/u_k}$ le mot obtenu par substituer systématiquement les u_i qui apparaissement dans t par t_i.

Par exemeple, si $t = u_i$, alors $t_{t_1/u_1, \cdots, t_k/u_k} = t_i$; si $t = c$ est un symbole de constant, alors $t_{t_1/u_1, \cdots, t_k/u_k} = c$; si $t = fs_1 \cdots s_n$, alors

$$t_{t_1/u_1, \cdots, t_k} = fs_{1\, t_1/u_1, \cdots, t_k/u_k} \cdots s_{n\, t_1/u_1, \cdots, t_k/u_k}.$$

Proposition 5.6 *Le mot $t_{t_1/u_1, \cdots, t_k/u_k}$ obtenu ci-dessus par substitution est en fait un terme.*

Exercice 5.4 Un exercice de substitution, a compléter.

5.2 Formules d'un langage du premier ordre

On introduit d'abord un symbole "$\simeq$". Un langage $\mathscr{L}$ du premier order peut contenir ce symbole, ou ne pas le contenir. Mais si c'est le cas, alors "$\simeq$" est un symbole de relation à 2 places, et on l'appelle le **symbole d'égalité**. Si $\mathscr{L}$ contient $\simeq$, on dit que $\mathscr{L}$ est un **langage égalitaire**.

Définition 5.7 Soit $M \in \mathscr{M}(\mathscr{L})$ un mot. On dit que M est une **formule atomique** s'il existe un entier $n \geq 1$, un symbole de relation à n places R et n termes $t_1, \cdots, t_n$ du langage $\mathscr{L}$ tels que $M = Rt_1 \cdots t_n$. L'ensemble des formules atomique de $\mathscr{L}$ est noté $\mathbf{At}(\mathscr{L})$.

Si $\mathscr{L}$ est un langage égalitaire, pour tous les termes t_1 et t_2 dans $\mathscr{T}(\mathscr{L})$, on convient que la formule atomique $\simeq t_1 t_2$ s'écrit autrement comme $t_1 \simeq t_2$.

Définition 5.8 On désigne par $\mathscr{F}(\mathscr{L})$ le plus petit sous-ensemble de $\mathscr{M}(\mathscr{L})$ qui contient toutes les formules atomiques et qui satisfait aux conditions suivantes :

1) si M et N sont dans $\mathscr{F}(\mathscr{L})$, alors les mots

$$\neg M,\ (M \wedge N),\ (M \vee N),\ (M \Rightarrow N),\ (M \Leftrightarrow N)$$

sont tous dans $\mathscr{F}(\mathscr{L})$,

2) si M est un mot dans $\mathscr{F}(\mathscr{L})$, alors pour tout entier $n \geq 1$, les mots $\forall v_n M$ et $\exists v_n M$ sont aussi dans $\mathscr{F}(\mathscr{L})$.

Un élément dans $\mathscr{F}(\mathscr{L})$ est appelé une **formule** du langage $\mathscr{L}$. Comme dans le calcul propositionnel, si M et N sont deux formules dans $\mathscr{F}(\mathscr{L})$, alors $\neg M$ est appelée la **négation** de la formule M, $(M \wedge N)$ et $(M \vee N)$ sont appelées respectivement la **conjonction** et la **disjonction** des formules M et N.

On peut également construire par récurrence les formules du langage $\mathscr{L}$. On pose d'abord $\mathscr{F}_0(\mathscr{L}) = \mathbf{At}(\mathscr{L})$. Si $n \geq 0$ est un entier, on définit

$$\begin{aligned}\mathscr{F}_{n+1}(\mathscr{L}) = \mathscr{F}_n(\mathscr{L}) &\cup \{\neg F \mid ; F \in \mathscr{F}_n(\mathscr{L})\} \\ &\cup \{(F \alpha G) \mid F,\ G \in \mathscr{F}_n(\mathscr{L}),\ \alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}\} \\ &\cup \{\forall v_k F \mid F \in \mathscr{F}_n(\mathscr{L}),\ k \geq 1\} \cup \{\exists v_k F \mid F \in \mathscr{F}_n(\mathscr{L}),\ k \geq 1\}.\end{aligned}$$

Exercice 5.5 Montrer que $\mathscr{F}(\mathscr{L}) = \bigcup_{n \geq 1} \mathscr{F}_n(\mathscr{L})$.

Proposition 5.9 *Toute formule $F \in \mathscr{F}(\mathscr{L})$ est dans un et un seul des cinq cas suivant :*

1) F est une formule atomique,

2) il existe une unique formule G telle que $F = \neg G$,

3) il existe un unique symbole de connecteur binaire $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ et un unique couple $(G, H) \in \mathscr{F}(\mathscr{L})^2$ tels que $F = (G \alpha H)$,

4) il existe un unique entier k et une unique formule $G \in \mathscr{F}(\mathscr{L})$ tels que $F = \forall v_k G$,

5) il existe un unique entier k et une unique formule $G \in \mathscr{F}(\mathscr{L})$ tels que $F = \exists v_k G$.

5.3 Variablese libres et variables liées

Soient F une formule dans $\mathscr{F}(\mathscr{L})$ et $k \geq 1$ est un entier. Les occurrences du symbole v_k dans F sont classifiés en deux catégories, les occurences libres et les occurences liées :

1) si F est atomique alors tous les v_k apparus dans F sont libres ;

2) si $F = \neg G$ avec $G \in \mathscr{F}(\mathscr{L})$, alors les occurences libres dans G sont par définition les occurence libres dans G ;
3) si $F = (G\alpha H)$ avec $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ et $G, H \in \mathscr{F}(\mathscr{L})$, alors les occurences libres de v_k dans F sont les occurences libres de v_k dans G et les occurences libres de v_k dans H ;
4) si $F = \forall v_k G$ ou si $F = \exists v_k G$ avec $G \in \mathscr{F}(\mathscr{L})$, alors aucune occurence de v_k dans F n'est libre ;
5) si $F = \forall v_m G$ ou si $F = \exists v_m G$ avec $m \neq k$, alors les occurences libres de v_k dans F sont les occurences libres de v_k dans G.

Les **occurences liées** de v_k dans F sont par définition les occurences de v_k dans F qui ne sont pas libres.

On appelle **variable libre** dans F tout symoble de variables qui a au moinds une occurence libre dans F. Si F n'a aucune variable libre, on dit que F est une **formule close**.

Supposons qu'une formule F n'est pas close et que $(v_{i_j})_{1\leq j\leq k}$ est l'enemble des variables libres dans F, où $i_1 < \cdots < i_k$. Alors la formule $\forall v_{i_1} \cdots \forall v_{i_k} F$ est close, appelée la **clôture universelle** de la formule F.

Soient F une formule, $(w_i)_{1\leq i\leq k}$ une famille de symobles de variables distincts et $(t_i)_{1\leq i\leq k}$ une famille de termes. On désigne par $F_{t_1/w_1,\cdots,t_k/w_k}$ le mot obtenu par substituer toutes les occurences libres de w_i dans F par t_i. Dans la suite, on donne quelques égalités concernant les substitutions :

1) si F est de la forme $F = Ru_1 \cdots u_n$, alors
$$F_{t_1/w_1,\cdots,t_k/w_k} = Ru_{1\,t_1/w_1,\cdots,t_k/w_k} \cdots u_{n\,t_1/w_1,\cdots,t_k/w_k};$$
2) si $F = \neg G$ avec $G \in \mathscr{F}(\mathscr{L})$, alors
$$F_{t_1/w_1,\cdots,t_k/w_k} = \neg G_{t_1/w_1,\cdots,t_k/w_k};$$
3) si $F = (G\alpha H)$, où $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, et $G, H \in \mathscr{F}(\mathscr{L})$,
$$F_{t_1/w_1,\cdots,t_k/w_k} = (G_{t_1/w_1,\cdots,t_k/w_k} \alpha H_{t_1/w_1,\cdots,t_k/w_k});$$
4) si F est de la forme $\forall v_j G$ avec $v_j \notin \{w_1, \cdots, w_k\}$ et $G \in \mathscr{F}(\mathscr{L})$, alors
$$F_{t_1/w_1,\cdots,t_k/w_k} = \forall v_j G_{t_1/w_1,\cdots,t_k/w_k},$$
il y a aussi une égalité similaire pour le cas où $F = \exists v_j G$;
5) si $F = \forall w_i G$ avec $G \in \mathscr{F}(\mathscr{L})$, alors
$$F_{t_1/w_1,\cdots,t_k/w_k} = \forall w_i G_{t_1/w_1,\cdots,t_{i-1}/w_{i-1},t_{i+1}/w_{i+1},\cdots,t_k/w_k},$$
il y a une égalité similaire pour le cas où $F = \exists w_i G$.

Exercice 5.6 Montrer que pour toute formule $F \in \mathscr{F}(\mathscr{L})$, $F_{t_1/w_1,\cdots,t_k/w_k}$ est aussi une formule.

Chapitre 6

Sémantique des prédicats

6.1 Modélisation des structures mathématiques

On appelle **structure mathématique** tout ensemble muni de certain nombre de relations et opérateurs. Par exemple, l'anneau ordonné des entiers peut être exprimé par la structure $\langle \mathbb{Z}, \leq, +, \times, 0, 1\rangle$, où $\mathbb{Z}$ est l'ensembles des entier, $+$ et $\times$ sont deux opérateurs (c'est-à-dire fonctions à deux places, ou encore fonctions de $\mathbb{Z}^2$ dans $\mathbb{Z}$) ; 0 est l'élément neutre et 1 est l'élément unité, qui sont des constantes ; et $\leq$ est la relation d'ordre habituel sur $\mathbb{Z}$. On voit que la structure $\langle \mathbb{Z}, \leq, +, \times, 0, 1\rangle >$ de l'anneau ordonné des nombres réels est très similaire à celle des entiers. Dans la suite, en utlisant les langage du premier order, on va formaliser cette observation.

Soit $\mathscr{L}$ un langage du premier ordre. On appelle **réalisation** du langage $\mathscr{L}$, ou $\mathscr{L}$-**structure** toute structure $\mathfrak{M}$ qui consiste :

1) d'un ensemble non-vide M, appelé **ensemble sous-jacent** à la réalisation $\mathfrak{M}$,
2) pour chaque symbole de constante c, d'un élément $\overline{c}^{\mathfrak{M}}$ (noté aussi $\overline{c}$ s'il n'y a pas d'ambiguïté) de M, appelé l'**interprétation** du symbole de constante c dans la réalisation $\mathfrak{M}$,
3) pour chaque entier $k \geq 1$ et chaque symbole de fonction à k places de $\mathscr{L}$, d'une application $\overline{f}^{\mathfrak{M}}$ (noté aussi $\overline{f}$ s'il n'y a pas d'ambiguïté) de M^k dans M, appelé l'**interprétation** du symbole de fonction f dans la réalisation $\mathfrak{M}$,
4) pour chaque entier $k \geq 1$ et chaque symbole de relations à k places, d'un sous-ensemble $\overline{R}$ (noté aussi $\overline{R}$ s'il n'y a pas d'ambiguïté) de M^k, appelé l'**interprétation** du symbole de relation R dans la réalisatin $\mathfrak{M}$.

Si $\mathscr{L}$ est un langage égalitaire et si l'interprétation de $\simeq$ dans $\mathfrak{M}$ est la relation d'égalité sur M. D'autre terme, $\overline{\simeq}^{\mathfrak{M}}$ est le diagonale dans M^2.

Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathscr{L}$-structures dont les ensembles sous-jacents sont respectivement M et N. On dit que $\mathfrak{N}$ est une **sous-structure** de $\mathfrak{M}$ (ou que $\mathfrak{M}$ est une **extension** de $\mathfrak{N}$ si les conditions suivantes sont vérifiées :

1) N est un sous-ensemble de M,
2) pour tout symbole de constante c de $\mathscr{L}$, $\overline{c}^{\mathfrak{N}} = \overline{c}^{\mathfrak{M}}$,
3) pour tout symbole de fonction f à k places, $\overline{f}^{\mathfrak{N}}$ est la restriction de $\overline{f}^{\mathfrak{M}}$ à N^k,
4) pour tout symbole de relation à k places, $\overline{R}^{\mathfrak{N}} = \overline{R}^{\mathfrak{M}} \cap N^k$.

Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathscr{L}$-structures dont les ensembles sous-jacents sont respectivement M et N. On appelle **homomorphisme de $\mathscr{L}$-structures** de $\mathfrak{M}$ dans $\mathfrak{N}$ tout application $\varphi : M \to N$ qui vérifie les conditions suivantes :

1) pour tout symbole de constante c de $\mathscr{L}$, on a $\varphi(\overline{c}^{\mathfrak{M}}) = \overline{c}^{\mathfrak{N}}$,
2) pour tout symbole de fonction f à k places et tous les éléments $x_1, \cdots, x_k$ dans M, on a

$$\varphi(\overline{f}^{\mathfrak{M}}(x_1, \cdots, x_k))\overline{f}^{\mathfrak{N}}(\varphi(x_1), \cdots, \varphi(x_k)),$$

3) pour tout symbole de relation R à k places, $(x_1, \cdots, x_k) \in \overline{R}^{\mathfrak{M}}$ implique $(\varphi(x_1), \cdots, \varphi(x_k)) \in \overline{R}^{\mathfrak{N}}$.

Exercice 6.1 Soient $\mathfrak{M}$ une $\mathscr{L}$-structure et $\mathfrak{N}$ une sous-structure de $\mathfrak{M}$. On suppose que l'ensemble sous-jacent à $\mathfrak{M}$ (resp. $\mathfrak{N}$) est respectivement M (resp. N). Alors l'application d'inclusion $i : N \to M$ est un homomorphisme de $\mathscr{L}$-structure.

Définition 6.1 On dit qu'un homomorphisme de $\mathscr{L}$-structures $\varphi : \mathfrak{M} \to \mathfrak{N}$ est un **monomorphisme** si φ vérifie les conditions suivantes :

1) l'application φ est injective,
2) pour tout symbole de relation R à k-places et tous les éléments $a_1, \cdots, a_k \in M$, $(a_1, \cdots, a_k) \in \overline{R}^{\mathfrak{M}}$ si et seulement si $(\varphi(a_1), \cdots, \varphi(a_k)) \in \overline{R}^{\mathfrak{N}}$.

Exercice 6.2 Supposons que $\mathscr{L}$ est un langage égalitaire et que $\mathfrak{M}$ et $\mathfrak{N}$ sont des réalisation égalitaires. Alors la condition 1) dans définition 6.1 est une conséquence de 2).

On dit qu'un homomorphisme de $\mathscr{L}$-structures $\varphi : \mathfrak{M} \to \mathfrak{N}$ est un **isomorphisme** s'il est un monomorphisme et est surjectif.

Exercice 6.3 Montrer que si φ est un isomorphisme, alors il en est de même de φ^{-1}.

6.2 Interprétation des termes dans une structure

Dans ce paragraphe, on fixe un langage du premier ordre $\mathscr{L}$.

Soien $(w_i)_{1\leq i\leq k}$ une famille de variables distinctes, t un terme du langage $\mathscr{L}$ et $\mathfrak{M}$ une $\mathscr{L}$-structure dont l'ensemble associé est M. Si $(x_i)_{1\leq i\leq k}$ est une famille d'éléments dans M, on désigne par $\overline{t}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k}$ l'**interprétation** du terme t où les occurences de w_i dans t sont interprétées par x_i. Plus précisément, on a

1) si $t = c$ est un symbole de constante, alors $\overline{t}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k} = \overline{c}^{\mathfrak{M}}$;
2) si $t = w_i$ $(1 \leq i \leq k)$, alors
$$\overline{t}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k} = x_i;$$
3) si $t = ft_1\cdots t_n$, où f est un symbole de fonction à n places, et $t_1,\cdots,t_n$ sont des termes, alors
$$\overline{t}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k} = \overline{f}^{\mathfrak{M}}(\overline{t}^{\mathfrak{M}}_{1\ w_1\mapsto x_1,\cdots,w_k\mapsto x_k},\cdots,\overline{t}^{\mathfrak{M}}_{n\ w_1\mapsto x_1,\cdots,w_k\mapsto x_k})$$

Soient $\mathfrak{M}$ une $\mathscr{L}$-structure dont l'ensemble associé est M, $(w_i)_{1\leq i\leq k}$ une famille de symboles de variable distincts et $(x_i)_{1\leq i\leq k}$ une famille d'éléments dans M. On définira une condition pour les formules où les occurences libres sont tous parmi $(w_i)_{1\leq i\leq k}$. Si une formule F satisfait à cette condition, on dit que la formule F est **satisfaite** dans la structure $\mathfrak{M}$ lorsque les symboles de variable $w_1,\cdots w_k$ sont respectivement interprétés par les éléments $x_1,\cdots,x_k$, et on note
$$\langle\mathfrak{M}; w_1\mapsto x_1,\cdots,w_k\mapsto x_k\rangle \vDash F.$$
Si cette condition n'est pas vérifiée, on note
$$\langle\mathfrak{M}; w_1\mapsto x_1,\cdots,w_k\mapsto x_k\rangle \nvDash F.$$

Cette condition sera définie par récurrence comme la suite.

1) Si F est une formule atomique, c'est-à-dire $F = Rt_1\cdots t_n$, où R est un symbole de relation à n places et $t_1,\cdots,t_n$ sont des termes, on a $\langle\mathfrak{M}; w_1\mapsto x_1,\cdots,w_k\mapsto x_k\rangle \vDash F$ si et seulement si
$$(\overline{t}^{\mathfrak{M}}_{1\ w_1\mapsto x_1,\cdots,w_k\mapsto x_k},\cdots,\overline{t}^{\mathfrak{M}}_{n\ w_1\mapsto x_1,\cdots,w_k\mapsto x_k}) \in \overline{R}^{\mathfrak{M}}.$$
En particulier, si s et t sont deux termes, alors
$$\langle\mathfrak{M}; w_1\mapsto x_1,\cdots,w_k\mapsto x_k\rangle \vDash s\simeq t$$
si et seulement si $\overline{s}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k} = \overline{t}^{\mathfrak{M}}_{w_1\mapsto x_1,\cdots,w_k\mapsto x_k}$.

2) Si $F = \neg G$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash$ si et seulement si $\langle M; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \nvDash G$.
3) Si $F = (G \wedge H)$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement si $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash G$ et $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ sont simultanément satisfaites.
4) Si $F = (G \vee H)$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement si l'une des conditions $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash G$ et $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ est satisfaite ;
5) Si $F = (G \Rightarrow H)$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ si et seulement si l'une des conditions $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \nvDash G$ et $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ est satisfaite.
6) Si $F = (G \Leftrightarrow H)$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ si et seulement si les conditions $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash G$ et $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash H$ sont simultanément satisfaites ou simultanément refusées (?).
7) Si $F = \forall v G$ avec $v \notin \{w_1, \cdots, w_k\}$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement si pour tout élément $x \in M$,

$$\langle \mathfrak{M}; v \mapsto x, w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash G.$$

8) Si $F = \exists v G$ avec $v \notin \{w_1, \cdots, w_k\}$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement s'il existe au moins un élément $x \in M$ tel que

$$\langle \mathfrak{M}; v \mapsto x, w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash G.$$

9) Si $F = \forall w_i G$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement si, pour tout élément $x \in M$,

$$\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_{i-1} \mapsto x_{i-1}, w_i \mapsto x, w_{i+1} \mapsto x_{i+1}, \cdots, w_k \mapsto x_k \rangle \vDash G$$

10) Si $F = \exists w_i G$, $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$ si et seulement s'il exists au moins un élément $x \in M$ tel que

$$\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_{i-1} \mapsto x_{i-1}, w_i \mapsto x, w_{i+1} \mapsto x_{i+1}, \cdots w_k \mapsto x_k \rangle \vDash G$$

En particulier, si F est une formule close et si la condition $\mathfrak{M} \vDash F$ est satisfaite, on dit que la condition F est **vraie** dans $\mathfrak{M}$, ou $\mathfrak{M}$ est un **modèle** de F.

Exercice 6.4 Soient $(w_i)_{1 \leq i \leq k+l}$ une famille de symboles de variable distincts et $(x_i)_{1 \leq i \leq k+l}$ une famille d'éléments dans M. Si F est une formule où les occurences libres sont tous parmi $(w_i)_{1 \leq i \leq k+l}$, alors $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_{k+l} \mapsto x_{k+l} \rangle \vDash F$ si et seulement si $\langle \mathfrak{M}; w_1 \mapsto x_1, \cdots, w_k \mapsto x_k \rangle \vDash F$.

6.3 Équivalence universelle

Soit $\mathscr{L}$ un langage du premier ordre. On dit qu'une formule close de $\mathscr{L}$ est **universellement valide** si elle est satisfaite dans toutes les $\mathscr{L}$-structures. Si F est universellement valide, on note $\vdash^* F$, sinon on note $\nvdash^*$. On dit qu'une fomule close F est **contradictoire** si $\neg F$ est universellement valide. On dit qu'une formule générale est **universellement valide** si sa clôture universelle est universellement valide. On dit qu'une formule G est **universellement équivalente** à une autre formule H si la formule $(F \Leftrightarrow G)$ est universellement valide. Si F est universellement équivalente, on note $F \sim G$.

On appelle **théorie** de $\mathscr{L}$ tout ensemble de formules closes de $\mathscr{L}$. Soit T une théorie de $\mathscr{L}$. Si $\mathfrak{M}$ est une $\mathscr{L}$-structure, on dit que $\mathfrak{M}$ est un **modèle** de T si toute formule dans T est vraie dans $\mathfrak{M}$. Si $\mathfrak{M}$ est un modèle de T, on note $\mathfrak{M} \vDash T$, sinon on note $\mathfrak{M} \nvDash T$.

On appelle **théorie consistante** toute théorie qui admet au moins un modèle. Si une théorie T n'admet aucun modèle, on dit que T est **inconsistante**. On dit qu'une théorie T est **finiement consistante** si toute partie finie de T est consistante.

Soient T une théorie et F une formule close du langage L. On dit que F est une **conséquence sémantique** de T si tout modèle de T est aussi un modèle de F. Si F est une conséquence sémantique de T, on note $T \vdash^* F$, sinon on note $T \nvdash^* F$.

Soient T une théorie et F une formule quelconque. On dit que F est une **conséquence sématique** de T si la clôture suniverselle de F est une conséquence sémantique de T.

Soient S et T deux théories. On dit que S et T sont **équivalentes** si chaque formule dans S est une conséquence de T et si chaque formule dans T est une conséquence de S.

Exercice 6.5 Soit T une théorie. Montrer les assertions suivantes.

1) Une formule F est une conséquence de T si et seulement si $T \cup \{\neg F\}$ est inconsistante.
2) Si T est consistante, alors toute partie de T est consistante.
3) Si une formule F est une conséquence d'une partie de T, alors elle est aussi une conséquence de T.
4) Pous toutes les formules F et G, $T \cup \{F\} \vdash^* G$ si et seulement si $T \vdash^* (F \Rightarrow G)$.
5) Pour toutes les formules F et G, $T \vdash^* (G \wedge H)$ si et seulement si $T \vdash^* G$ et $T \vdash^* H$.

6) Soit $(F_i)_{1\leq i\leq n}$ une théorie finie. Alors $\{F_1, \cdots, F_n\} \vdash^* G$ si et seulement si $\vdash^* (\wedge_{i=1}^n F_i \Rightarrow G)$.

Exercice 6.6 Soient v un symobole de varaible et F et G deux formules. Montrer les équivalences universelles suivantes :

1) $\forall v(F \wedge G) \sim (\forall vF \wedge \forall vG)$,

2) $\exists v(F \vee G) \sim (\exists vF \vee \exists vG)$,

3) $\exists v(F \Rightarrow G) \sim (\forall vF \Rightarrow \exists vG)$,

4) $\neg\forall vF \sim \exists v\neg F$.

Exercice 6.7 Soit v un symbole de variable et G une formule où toutes les occurences de v sont liées. Démontrer les assertions suivantes :

1) $\forall vG \sim G \sim \exists vG$;

2) pour toute formule F,

$$\begin{array}{ll} \forall v(F \wedge G) \sim (\forall vF \wedge G), & \forall v(F \vee G) \sim (\forall vF \wedge G), \\ \forall v(F \Rightarrow G) \sim (\exists vF \Rightarrow G), & \forall v(G \Rightarrow F) \sim (G \Rightarrow \forall vF); \end{array}$$

3) pour toute formule F,

$$\begin{array}{ll} \exists v(F \wedge G) \sim (\exists F \wedge G), & \exists v(F \vee G) \sim (\exists vF \vee G), \\ \exists v(F \Rightarrow G) \sim (\forall vF \Rightarrow G), & \exists v(G \Rightarrow F) \sim (G \Rightarrow \exists vF). \end{array}$$

Exercice 6.8 Soient v et w deux symbole de variables et F une formule. Montrer les équivalence universelle suivantes :

1) $\forall v\forall wF \sim \forall w\forall vF$,

2) $\exists v\exists wF \sim \exists w\exists vF$.

Théorème 6.2 *La condition $\sim$ est une condition d'équivalence sur l'ensemble des formules du langage $\mathscr{L}$.*

Démonstration 1) Soit F une formule. Soient $(v_{i_j})_{1\leq j\leq k}$ les variables libres dans F, où $i_1 < \cdots < i_k$. La clôture universelle de F est donc $\forall v_{i_1} \cdots \forall v_{i_k} F$. Pour toute $\mathscr{L}$-structure $\mathfrak{M}$ où l'ensemble sous-jacent est M et tout famille $(x_j)_{1\leq j\leq k}$ d'éléments dans M, on a toujours

$$\langle \mathfrak{M}, v_{i_1} \mapsto x_1, \cdots, v_{i_k} \mapsto x_k \rangle \vDash (F \Leftrightarrow F).$$

Par conséquent, on a

$$\mathfrak{M} \vDash \forall v_{i_1} \cdots \forall v_{i_k} (F \Leftrightarrow F),$$

et donc $F \sim F$.

2) Soient F et G deux formules telles que $F \sim G$. Soit $(v_{i_j})_{1\leq j\leq k}$ la famille des variables libres de $(F \Leftrightarrow G)$, où $i_1 < \cdots < i_k$. C'est aussi la famille des variables libres de $(G \Leftrightarrow F)$. Pour toute $\mathscr{L}$-structure $\mathfrak{M}$ où l'ensemble sous-jacent est M et toute famille $(x_j)_{1\leq j\leq k}$ d'éléments dans M, $\langle \mathfrak{M}, v_{i_1} \mapsto x_1, \cdots, v_{i_k} \mapsto x_k\rangle \vDash (F \Leftrightarrow G)$ si et seulement si $\langle \mathfrak{M}, v_{i_1} \mapsto x_1, \cdots, v_{i_k} \mapsto x_k\rangle \vDash (G \Leftrightarrow F)$. Donc on a $G \sim F$.

3) La démonstration de la transtitivité, qui est toujours dans le même esprit que 1) et 2), est reservé aux lecteurs.

□

Exercice 6.9 Montrer que la relation "être équivalente à" est en fait une relation d'équivalence sur l'ensemble des théories.

6.4 Formes prénexes

On dit qu'une formule F est **prénexe** s'il existe des symboles de variable $w_1, \cdots, w_k$ et des symboles de quantificateur $Q_1, \cdots, Q_k$ et une formule sans quantificateur G tels que $F = Q_1 w_1 \cdots Q_k w_k G$. Le mot $Q_1 w_1 \cdots Q_k w_k$ est appelé le **préfixe** de la formule prénexe F. Si $k = 0$, c'est-à-dire $F = G$, on dit que F est une formule **sans quantificateur**. On dit qu'une formule prénexe est **polie** si les variables dans son préfixe sont distinctes.

Exercice 6.10 La formule $\forall v_1(\exists v_2 R v_1 \Rightarrow R v_2)$ est-elle une formule prénexe.

Théorème 6.3 *Toute formule du langage $\mathscr{L}$ est universellement équivalente à au moins une formule prénexe polie.*

Démonstration On raisonne par récurrence. Si F est atomique, alors F est déjà une formule prénexe polie.

1) Si Q est un symbole de quantificateur, on note

$$\overline{Q} = \begin{cases} \forall, & Q = \exists, \\ \exists, & Q = \forall. \end{cases}$$

2) Si F est de la forme $\neg G$ et si G est universellement équivalente à $Q_1 w_1 \cdots Q_k w_k G'$, où G' est sans quantificateur et où $w_1, \cdots, w_k$ sont distincts, alors F est universellement équivalente à $\overline{Q}_1 w_1 \cdots \overline{Q}_k w_k \neg G'$.

3) Supposons $F = (G \vee H)$, où G est universellement équivalente à $P_1 u_1 \cdots P_n u_n G'$ et où H est universellement équivalente à $Q_1 w_1 \cdots Q_m w_m H'$, G' et H' étant sans quantificateur, $u_1, \cdots u_n$ étant distincts et $w_1, \cdots, w_m$

étant dinstincts. On choisit des symbole de variable distincts $x_1, \cdots x_{n+m}$. Soient

$$G'' = G'_{x_1/u_1,\cdots,x_n/u_n}, \quad H'' = H'_{x_{n+1}/w_1,\cdots,x_{n+m}/w_{n+m}}$$

alors $P_1x_1 \cdots P_mx_nG''$ est universellement équivalente à G et $Q_1x_{n+1} \cdots Q_mx_{n+m}H''$ est universellement équivalente à H. Comme $x_1, \cdots, x_{n+m}$ sont distincts, on obtient que la formule

$$P_1x_1 \cdots P_nx_nQ_{n+1}x_{n+1} \cdots Q_{n+m}x_{n+m}(G'' \wedge H'')$$

est universellement équivalente à F. Cette nouvelle formule est clairement prénexe polie. La démonstration pour le cas où $F = (G \vee H)$, $F = (G \Rightarrow H)$ et $F = (G \Leftrightarrow H)$ est analogue.

4) Supposons que $F = \exists vG$ et que G est universellement équivalente à $P_1u_1 \cdots P_ku_kG'$, où $u_1, \cdots, u_k$ sont distinct, et G' n'a pas de quantificateur. Lorsque $v \notin \{u_1, \cdots, u_k\}$,

$$\exists vGP_1u_1 \cdots P_Ku_kG',$$

qui est universellement équivalente à F, est prénexe polie. Lorsque v est dans $\{u_1, \cdots, u_k\}$, la variable v n'est pas libre dans G. Par conséquent, F est universellement équivalente à G, et donc est universellement équivalente à $P_1u_1 \cdots P_ku_kG'$. La démonstration pour le cas où $F = \forall vG$ est similaire.

□

6.5 Équivalence élémentaire

Définition 6.4 Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathscr{L}$-structures. On dit que $\mathfrak{M}$ est **élémentairement équivalente** à $\mathfrak{N}$ si toute formule close de $\mathscr{L}$ qui est satisfaite dans $\mathfrak{M}$ est aussi satisfaite dans $\mathfrak{N}$. Si $\mathfrak{M}$ est élémentairement équivalente à $\mathfrak{N}$, on note $\mathfrak{M} \equiv \mathfrak{N}$; sinon on note $\mathfrak{M} \not\equiv \mathfrak{N}$. Si deux $\mathfrak{L}$-structures sont isomorphes, elles sont élémentairement équivalentes.

Soit $\mathbb{P}$ une propriété pour les $\mathscr{L}$-structures. On dit que la propriété $\mathbb{P}$ est **axiomatisable** s'il existe une théorie T de $\mathscr{L}$ telle que, pour toute $\mathscr{L}$-strucutre $\mathfrak{M}$, $\mathbb{P}(\mathfrak{M})$ est équivalente à $\mathfrak{M} \vDash T$. On dit que $\mathbb{P}$ est **finiement axiomatisable** s'il existe une théorie finie T telle que, pour toute $\mathscr{L}$-structure $\mathfrak{M}$, $\mathbb{P}(\mathfrak{M})$ est équivalente à $\mathfrak{M} \vDash T$. On dit que $\mathbb{P}$ est **pseudo-axiomatisable** s'il existe un langage $\mathscr{L}'$ plus riche que $\mathscr{L}$ et une théorie T de $\mathscr{L}'$ tels que, $\mathbb{P}(\mathfrak{M})$ si et seulement si $\mathfrak{M}$ est la restriction d'une $\mathscr{L}'$-structure qui est un modèle de T.

Théorème 6.5 *Sous l'axiome du choix, une théorie dans un langage du premier ordre est consistante si et seulement si elle est finiement consistante.*

On dit qu'une théorie T dans un langage $\mathscr{L}$ est **complète** si T est consistante et si tous les modèles de T sont élémentairement équivalents.

Soit $\mathfrak{M}$ une $\mathscr{L}$-structure. On appelle **théorie** de $\mathfrak{M}$ et on note $\mathrm{Th}(\mathfrak{M})$ l'ensemble des formules closes de $\mathscr{L}$ satisfaisantes dans $\mathfrak{M}$.

Théorème 6.6 *Pour toute $\mathscr{L}$-structure $\mathfrak{M}$, $\mathrm{Th}(\mathfrak{M})$ est une théorie complète.*

Chapitre 7

Modélisation des preuves

7.1 Modélisation des axiomes

En mathématiques, la démonstration d'un théorème est le procédé de déduire des énoncés *a priori* appelés des **axiomes**, par plusieurs étape de raisonnemments "faciles", le résultat annoncé dans le théorème. Dans ce chapitre, on va formaliser les démonstrations.

D'abord on modélise les axiomes. Les axiomes logiques sont classées en deux types.

1) Les **tautologies**, c'est-à-dire les formules universellement valides obtenues par substitution dans des tautologies dans le calcul des propositions.
2) Les **axiomes des quantificateurs** de l'une des formes suivantes :
   a) $\exists v F \Leftrightarrow \neg \forall v \neg F$,
   b) $(\forall v(F \Rightarrow G) \Rightarrow (F \Rightarrow \forall v G))$, où v n'a pas d'occurence libre dans F,
   c) $\forall v F \Rightarrow F_{t/v}$, où F est une formule, t est un terme et aucune occurence libre de v dans F ne se trouve dans le champs d'un quantificateur liant une variable de t.

Ensuit on modélise les règles de déduction. Ces règles perment de déduire une formule d'une formule ou de plusieures formules.

1. À partir de deux formules F et $(F \Rightarrow G)$ on déduit G. Ce procédé est appelé le **modus ponens**
2. Si F est une formule et v est une variable, on déduit $\forall v F$ de F. Cette règle est appelée la **règle de généralisation**.

Définition 7.1 Soient T une théorie et F une formule de $\mathscr{L}$. On appelle **démonstration formelle** de F dans T toute suite finie de formules $(F_0, \cdots, F_n)$ de $\mathscr{L}$ telle que $F_n = F$, et que pour tout $0 \leq i < n$, l'une des conditions suivantes soit vérifiée :

1) $F_i \in T$,
2) F_i est un axiome logique,
3) F_i se déduit de F_{i-1} par la règle de généralisation ou de F_{i-1} et F_{i-2} par le modus ponens.

S'il existe une démonstration de F dans T, on dit que F est **démontrable** dans T, ou que F est un **théorème** de T et on note $T \vdash F$. Si T est la théorie vide, on dit que F est **démontrable** et on note $\vdash F$.

Définition 7.2 On dit qu'une théorie T est **cohérente** s'il n'existe pas de formule F telle que $T \vdash F$ et $T \vdash \neg F$ soient simultanément satisfaites.

7.2 Théorème de finitude

Théorème 7.3 *Pour toute théorie T et toute formule F telles que $T \vdash F$, il existe une partie finie T' de T telle que $T' \vdash F$.*

On déduit du théorème 7.3 que, si T est une théorie telle que toute partie finie de T soit cohérente, alors T est aussi cohérente.

Proposition 7.4 *Soient T une théorie et F une formule. Alors $T \cup \{F\} \vdash G$ implique que $T \vdash (F \Rightarrow G)$.*

Théorème 7.5 *Soient T une théorie, F une formule et G la clôture universelle de F. Alors $T \vdash F$ implique $T \vdash^* F$.*

7.3 Théorème de compétude

Soit T une théorie. On dit que T est **syntaxiquement complète** si T est cohérente et si pour toute formule close F de $\mathscr{L}$, on a $T \vdash F$ ou $T \vdash \neg F$. On dit que T admet des **témoins de Henkin** dans $\mathscr{L}$ si pour toute formule F qui a une seule variable libre v, il existe un symbole de constante dans $\mathscr{L}$ tel que $(\exists v F \Rightarrow F_{c/v}) \in T$.

Proposition 7.6 *Si une théorie T est syntaxiquement complète et admet des témons de Henkin dans $\mathscr{L}$, alors T admet un modèle.*

Proposition 7.7 *Si T est une théorie cohérente, alors il existe un langage $\mathscr{L}'$ plus riche que $\mathscr{L}$ et une théorie T' de $\mathscr{L}'$ contenant T qui est syntaxiquement complète et qui admet des thémoins de Henkin dans $\mathscr{L}'$.*

Théorème 7.8 (Gödel) *Toute théorie cohérente admet un modèle.*

Théorème 7.9 *Si T est une théorie dont toute partie finie a un modèle, alors T admet aussi un modèle.*